MIMIR365
ProperCore

Vindkraft · BESS · NIS2 Bilaga I · Ei-tillsyn

NIS2-compliance för vindkraft, BESS och elproducenter

Från OT-inventering i vindparken till IEC 61850-säkerhet i BESS — den kompletta guiden för energibolag som möter Ei:s tillsyn 2025.

INNEHÅLL

72h	Bilaga I	IEC 61850	10 MEUR
Ei-incidentrapport	Väsentlig entitet	Protokollstöd	Max sanktion

Mimir365 AB · mimir365.se · Utgiven maj 2026 · 24 sidor

NIS2 Bilaga I och energisektorn — vad gäller?

Energisektorn listas explicit i NIS2 Bilaga I (Annex I) som "väsentlig sektor". Det innebär den strängaste tillsynsregimen — proaktiva revisioner av Energimarknadsinspektionen (Ei), personligt ledningsansvar och sanktioner upp till 10 MEUR.

Tre operatörstyper under NIS2 Bilaga I — energi

Operatörstyp	NIS2-bilaga	Tillsynsmyndighet	Sanktionsnivå
Elproducenter (vindkraft, BESS, vattenkraft, sol)	Bilaga I — Väsentlig	Ei (Energimarknadsinspektionen)	10 MEUR / 2 % omsättning
DSO — Distributionsnätsoperatörer	Bilaga I — Väsentlig	Ei	10 MEUR / 2 % omsättning
TSO — Transmissionsnätsoperatörer (SvK)	Bilaga I — Kritisk	Ei + MSB	Strängaste regimen

Storleksgränser för elproducenter

Elproducenter med "e50 anställda eller "e10 MEUR omsättning är väsentliga entiteter. Många vindparksoperatörer och BESS-bolag är mindre — men DSO-koppling, kritisk infrastrukturklassning eller SvK-kontraktsåtaganden kan ändå leda till NIS2-skyldighet. Ei bedömer detta individuellt.

NIS2 Artikel 21 — tio obligatoriska åtgärdsdomäner för energi

- !’ Riskhantering: täcker ALLA system — IT och OT (SCADA, BMS, PCS, RTU, turbinstyrenheter)
- !’ Incidenthantering: definierade roller, 72h-process mot Ei, SvK-störningsprotokoll
- !’ Kontinuitetsplanering: inkluderar OT-haveri (SCADA-fel, BMS-bortfall, kommunikationsavbrott till SvK)
- !’ Leverantörskedjans säkerhet: Vestas/SG Digital/Fluence fjärråtkomst — avtalad och loggad
- !’ Nätverkssäkerhet: OT-segmentering — SCADA/BMS/PCS separerat från IT-nät
- !’ MFA för all privilegierad åtkomst inklusive OT-management-system och vendor-VPN
- !’ Sårbarhantering: firmware-CVE:er i turbinstyrenheter, BMS och RTU kartlagda
- !’ Kryptografipolicy: IEC 62351 för IEC 61850-kommunikation mot SvK
- !’ HR-säkerhet: tillträde till OT-system och leverantörskontrakt med cybersäkerhetsklausuler
- !’ Styrelseansvar: ledningen personligen ansvarig och genomgår regelbunden utbildning i cybersäkerhet

&¡ Ei startar proaktiv tillsyn 2025

Energimarknadsinspektionen inleder proaktiva NIS2-revisioner av elproducenter och DSO under 2025. Tillsynen fokuserar på OT-inventering, leverantörsåtkomst, incidentrapporteringsförmåga och styrelseansvar. Utan dokumenterad riskhanteringsprocess och OT-logg är er anläggning exponerad.

OT-inventering i vindparken — turbinstyrning och SCADA

En 150 MW vindpark har typiskt 40+ turbinstyrenheter, ett SCADA-system, RTU mot SvK, meteorologisk IoT och 3–5 leverantörers permanenta VPN-anslutningar. Ingen av dessa är inventerad, loggad eller skyddad hos en typisk operatör.

Vindparkens OT-systemkarta — sju systemkategorier

System	Protokoll / Leverantör	Cybersäkerhetsrisk	Mimir365-åtgärd
SCADA (Park Pilot)	Vestas VPP, SG Digital SCADA — VPN utan MFA/logg	Full parkstyrning via phishade leverantörscredentials	VPN-loggning, MFA-krav, session-monitoring
Turbinstyrenheter (WTG)	IEC 61400-25 Modbus TCP — ingen autentisering	Modbus Write !' nödstopp alla turbiner	Nätverkssegmentering, anomalidetektion
Stationsautomation (RTU)	IEC 61850 mot SvK — IEC 62351 ej implementerat	Falsk produktionsdata !' elnätsstörning	IEC 62351, RTU-loggning
SCADA Historian (PI)	OSIsoft PI — IT/OT-brygga, kända CVE:er	Lateral rörelse IT!'OT, data-exfiltration	CVE-scan, segmentering, loggning
Meteorologisk IoT	MQTT mot leverantörsmolnet × 3	Manipulerade vindprognoser !' elmarknadsfraud	MQTT-segmentering, cloudflödes-loggning
Skyddsreläer / elstation	ABB REF/REX — ABB Ability portal, default-creds	Transformatorstyring utan autentisering	Default-creds-scan, Ability-loggning
Kommunikationsinfrastruktur	Cisco IE-serien — SNMP v2c, Telnet aktivt	4G-fallback okrypterad, OT-nåbart från internet	Konfigurationsrevision, SNMP v3

O&M-avtalet är vindkraftens strukturella cybersäkerhetsproblem

Vindparksleverantörerna (Vestas, Siemens Gamesa, Nordex) levererar SCADA och turbinstyrning med krav på permanent VPN-åtkomst som villkor för O&M-avtalet och turbingarantin. Nätverkssegmentering kan bryta leverantörsgarantin. Firmware-uppdateringar kräver leverantörsgodkännande och servicebesök.

Ø=Ý Lösningsansats: separera loggning från styrning

Mimir365 implementerar passiv OT-nätverksloggning som varken stör Vestas VPP-kommunikation eller bryter O&M-avtalets krav på leverantörsåtkomst. Vestas VPN-sessioner loggas och tidsstämplas utan att tunneln påverkas. Det ger NIS2-krav på loggning utan att störa driften.

BESS cybersäkerhet — BMS, PCS och balansmarknaden

Batterilager (BESS) kombinerar fyra kritiska cybersäkerhetsrisker i ett system: termisk säkerhetsrisk (BMS-manipulation), elmarknadsrisk (SvK API-missbruk), leverantörsmolnexponering (Fluence/Tesla) och IEC 61850-exponering mot SvK.

BESS OT-systemkarta — åtta systemkategorier

System	Protokoll / Leverantör	Cybersäkerhetsrisk	Mimir365-åtgärd
BMS (Battery Management System)	Fluence Mosaic / Tesla — REST API, Modbus TCP	BMS-konfiguration via molnet !' termisk runaway	BMS API-loggning, cloud-trafikanalys
PCS (Power Conversion System)	SMA Sunny Central — Modbus TCP, webserver	Default-creds !' skyddsparametrar ändrade	Default-creds-scan, Modbus-anomalidetektion
BESS SCADA (Ignition)	Ignition 8.x — OPC-UA, port 8088	SCADA-åtkomst !' SvK API-nyckel stals	Segmentering, MFA, API-nyckel-vault
SvK Balansmarknads-API	aFRR/FCR via eSett — API-nyckel i klartext	Falska FCR-bud !' elnätsstörning	API-nyckel-hantering, budloggning
Brandskydd (HI-FOG)	BACnet/IP — ingen BACnet/SC	Suppression inaktiverad !' termisk incident utan skydd	BACnet/SC, kommandologgning
Miljöbevakning (gas/ temp)	MQTT !' sensorcloud — ingen auth	Manipulerade sensorvärden maskar brandförlopp	MQTT-auth, sensoranomali-detektion
Leverantörsmolnet	Fluence/Tesla permanent VPN — ej loggat	Kompromitterat moln !' firmware-manipulation	VPN-loggning, cloud-session-monitoring
RTU / nätanslutning	ABB REX640 — IEC 61850, SNMP v2c	Falska produktionsvärden !' frekvensavvikelse	IEC 62351, RTU-loggning, SNMP v3

Balansmarknads-API — en direkt elnätsattackvektor

BESS-anläggningar deltar i FCR-N, FCR-D och aFRR-marknaderna via SvK:s eSett API. En angripare med åtkomst till BESS SCADA kan läsa API-nyckeln (ofta lagrad i klartext), lämna falska kapacitetsbud och programmera PCS att inte svara vid aktivering.

Ø=Ý Termisk runaway och cybersäkerhet

BMS-manipulation som ändrar temperaturlarmtrösklar och SOC-skyddsgränser skapar direkt personrisk. En BESS-cybersäkerhetsincident kan klassas som säkerhetskritisk incident och involvera MSB och räddningstjänst utöver Ei och NIS2-processen.

IEC 61850 och GOOSE — protokollsäkerhet i elproduktion

IEC 61850 är standardprotokollet för kommunikation i elproduktionsmiljöer — RTU mot SvK, skyddsreläer, stationsautomation och BESS-nätanslutning. GOOSE-meddelanden är realtidskommandon utan inbyggd autentisering.

IEC 61850 i energimiljö — tre kritiska exponeringar

- GOOSE (Generic Object Oriented Substation Events): realtidskommandon för skyddsutlösning och ö-drift. Inga inbyggda autentiseringsmekanismer. Manipulerade GOOSE-paket kan trigga felaktigt skyddsutlösning på millisekunder.
- REPORT: periodisk rapportering av mätvärden och statusinformation till SvK. Komprometterad RTU kan injicera falska produktionsvärden i rapporteringsdataset — SvK planerar elnätet baserat på fel data.
- MMS (Manufacturing Message Specification): konfigurationsprotokoll för RTU och stationsautomation. Komprometterat MMS ger angriparen möjlighet att ändra skyddsinställningar, kalibreringsdata och kommunikationsparametrar.

IEC 62351 — kryptering och autentisering för IEC 61850

IEC 62351-del	Skyddar	Implementeringsstatus i Sverige
62351-3 (TLS)	MMS och REPORT — krypterad TCP-kommunikation	Sällan implementerat hos vindparkoperatörer och BESS
62351-4 (MMS auth)	Autentisering på MMS-protokollnivå	Nästan aldrig implementerat — kräver leverantörsstöd
62351-6 (GOOSE/SV)	GOOSE-meddelandeautentisering via digital signatur	Implementerat i nya anläggningar — inte retroaktivt
62351-8 (RBAC)	Rollbaserad åtkomstkontroll för IEC 61850-system	Sällsynt — kräver komplett stationsautomationsuppdatering

Mimir365 och IEC 61850 — vad övervakas

- Passiv IEC 61850 GOOSE-analys: flaggar GOOSE-kommandon som avviker från normalflöde
- REPORT-integritetsövervakning: avvikelse i rapporterade produktionsvärden mot historisk baseline
- MMS-sessionsloggning: alla konfigurationsändringar och fjärranslutningar loggas med tidsstämpel
- IEC 62351-statusrapportering: identifierar vilka kommunikationsvägar som saknar kryptering

Ø=Üá GOOSE och frekvensreglering

En angripare med åtkomst till IEC 61850-nätverkssegmentet kan injicera falska GOOSE-skyddskommandon som triggar felaktig ö-drift eller felaktig skyddsutlösning. I en BESS-anläggning ansluten till SvK:s stamnät kan detta orsaka spänningsinstabilitet i det lokala elnätssegmentet inom millisekunder.

Ei-tillsyn 2025 — vad granskas och hur förbereder ni er

Energimarknadsinspektionen har signalerat proaktiva NIS2-revisioner av elproducenter och DSO från och med 2025. Tillsynen baseras på NIS2-direktivet och den svenska genomförandelagen. Ei fokuserar på sex granskningsområden.

Sex granskningsområden i Ei:s NIS2-tillsyn

Granskningsområde	Ei fokuserar på	Vanlig brist
OT-inventering	Komplett förteckning av alla OT-system inkl. leverantörsutrustning	SCADA/BMS/PCS saknas — ingen OT-inventering genomförd
Riskhantering	Dokumenterad riskbedömning som inkluderar OT och leverantörsrisker	IT-risk dokumenterat, OT-risk saknas helt
Leverantörsåtkomst	Kontrakt med cybersäkerhetsklausuler, loggade VPN-sessioner	Vestas/Fluence permanent VPN utan logg eller kontrakt
Incidenthantering	72h-process mot Ei, testad och dokumenterad med OT-logg	Process på papper — ingen OT-logg att rapporten baseras på
Nätverkssegmentering	OT isolerat från IT — verifierat med nätverksdokumentation	Platt nät — SCADA/BMS direkt åtkomligt från kontorsnät
Styrelseansvar	Styrelsebeslut om NIS2-policy, utbildning i cybersäkerhet	NIS2 aldrig diskuterat på styrelsenivå

72h-incidentrapport till Ei — tre krav

- !’ Tidig varning (24h): Ei informeras om händelse som kan vara en NIS2-incident
- !’ Fullständig anmälan (72h): rekonstruerad händelsekedja med OT-tidslinje, påverkade system och initialt identifierad orsak
- !’ Slutrapport (30 dagar): fullständig forensisk analys, vidtagna åtgärder och förebyggande åtgärder

Ø=ÜË OT-logg är förutsättningen för alla tre

Utan OT-nätverkslogg kan ni inte rekonstruera händelsekedjan som Ei kräver. En ofullständig 72h-rapport kan i sig trigga en fördjupad tillsyn. Bristen på logg är ett självständigt NIS2-brott — separat från incidenten.

Checklista: NIS2-beredskap för energiproducenter

Denna checklista täcker de mest kritiska NIS2-kraven för vindparksoperatörer, BESS-förvaltare och elproducenter inför Ei:s tillsyn. Bocka av, identifiera gap och prioritera åtgärder.

OT-inventering och riskhantering

Checklista

- [ ] Komplett OT-inventering genomförd — alla turbinstyrenheter, BMS, PCS, RTU och SCADA dokumenterade
- [ ] Firmware-versioner kartlagda för alla OT-enheter — CVE:er kontrollerade mot NVD
- [ ] Riskbedömning dokumenterad som inkluderar OT-risker och leverantörsrisker
- [ ] Leverantörers fjärråtkomst (Vestas/Fluence/SG Digital) inventerad och dokumenterad
- [ ] Nätverkstopologi dokumenterad med segmentering verifierad

Leverantörskedjans säkerhet (NIS2 art. 21.2d)

Checklista

- [ ] Vestas/SG Digital/Nordex O&M-avtal innehåller NIS2-cybersäkerhetsklausul
- [ ] Fluence/Tesla BESS-driftsavtal innehåller krav på incidentnotifiering och loggning
- [ ] Leverantörs-VPN-sessioner loggas tekniskt (tidsstämpel, käll-IP, duration)
- [ ] Leverantörers molnanslutningar (Fluence Cloud, ABB Ability) identifierade och loggade
- [ ] MFA krävs av leverantörer för fjärranslutning till OT-systemen

Incidenthantering och Ei-rapportering

Checklista

- [ ] OT-nätverksloggning aktiv med minimum 12 månaders retention
- [ ] 72h-incidentprocess mot Ei dokumenterad, roller tilldelade och testövning genomförd
- [ ] SvK-störningsprotokoll integrerat med NIS2 incidentprocess
- [ ] Kontaktlista till Ei etablerad och verifierad
- [ ] Styrelsebeslutat NIS2-policy med personligt ledningsansvar dokumenterat

Protokollsäkerhet och nätverksskydd

Checklista

- [ ] IEC 61850 GOOSE-kommunikation övervakad och loggad
- [ ] IEC 62351 implementeringsstatus dokumenterad — plan för kryptografi mot SvK
- [ ] Modbus TCP-kommunikation till turbinstyrenheter och BMS/PCS övervakad
- [ ] BACnet/IP brandskydds-kommunikation loggad och skyddad
- [ ] API-nycklar för SvK balansmarknads-API lagrade i secrets vault — ej i klartext

Redo att ta nästa steg?

Boka ett kostnadsfritt strategisamtal med en av våra specialister.

mimir365.se/kontakt

security@mimir365.se · privacy@mimir365.se · legal@mimir365.se