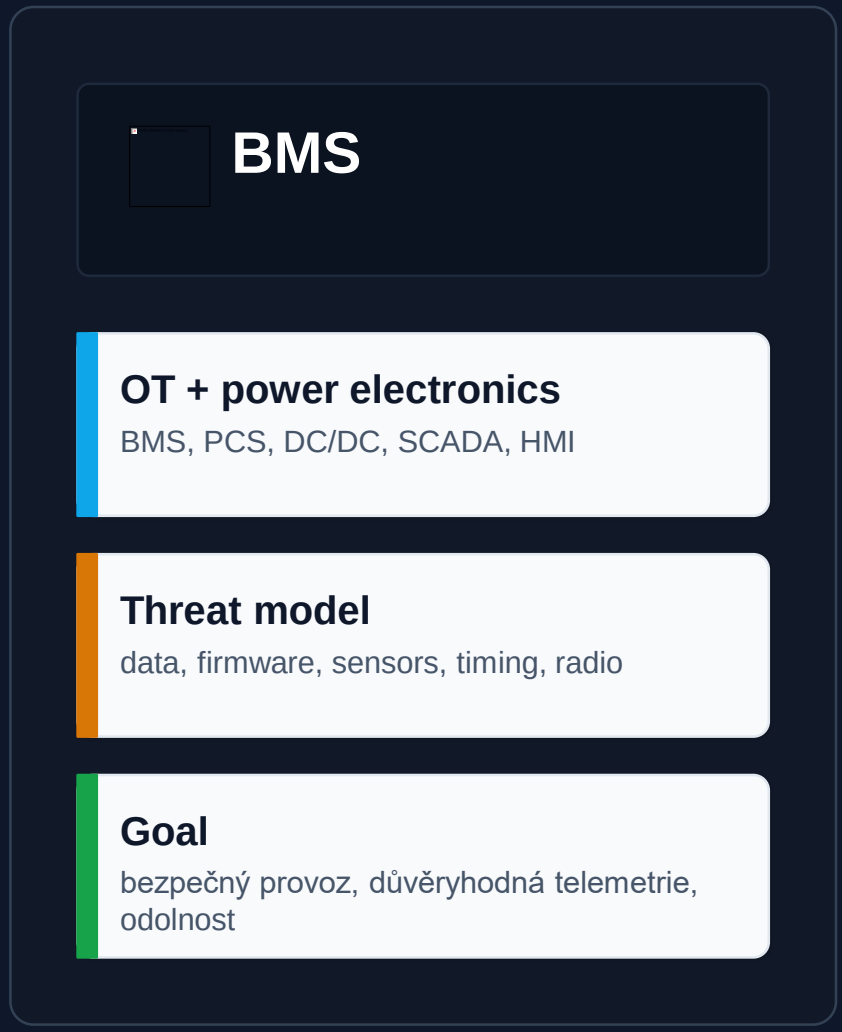
Kyberbezpečnost a bateriové zdroje v digitální energetice

BESS, BMS a physics-based monitoring

Tomáš Pitner
Konference Digitální energetika 2026 · 8. 4. 2026



Proč je kyberbezpečnost BESS kritická

- BMS je „mozek“ bateriového systému: sleduje napětí, proud, teplotu, SOC a SOH a spouští ochranné reakce.
- Útok na BMS nebo navazující řídicí vrstvu může zhoršit výkon, zkrátit životnost a v krajním případě přispět k thermal runaway.
- U stacionárního BESS nejde jen o baterii samotnou, ale i o dostupnost služby, plnění dispečerských požadavků a stabilitu provozu.

Safety

přehřátí, chybné charging/discharging, havarijní odstavení

Availability

loss of view, ztráta řízení, nedostupnost flexibility

Business impact

smluvní dopady, audit, reputace, vyšší compliance náklady

Digitální attack surface bateriového zdroje

- Útočník obvykle nejde přímo na článek baterie, ale na rozhraní: identita, perimetr, servis, data a řídicí příkazy.

Co přesně BMS v BESS dělá

SOC a SOH

Průběžný odhad stavu nabití a kondice článků pro bezpečný a ekonomický provoz.

Thermal management

Hlídání teplot a ochranné zásahy proti přehřátí a degradaci.

Cell balancing

Vyrovnávání článků, prevence přebití a hlubokého vybití.

Komunikace

Napojení na nadřazené řízení, diagnostiku a infrastrukturu.

- Čím je BMS chytřejší a propojenější, tím širší je attack surface.
- V BESS navíc jeho chyby dopadají na řiditelnost výkonu a vazbu na síť.

Tři základní kategorie útoků

Communication-based

Zneužití komunikačních protokolů, setpointů, telemetrie nebo bezdrátové vrstvy.

Physical-based

EMI, přímý fyzický zásah, kompromitace senzoru, tampering hardwaru.

Software & data-based

Malware, firmware abuse, falešná data, timestamp manipulace.

- Hranice mezi nimi se stírají: jeden incident často kombinuje více vrstev najednou.

Malware a firmware tampering

- Malware může přijít přes update proces, fyzický servisní přístup nebo slabě chráněné komunikační kanály.
- Dopadem může být změna algoritmů řízení, falešná senzorická data nebo chybné charging/discharging rozhodnutí.
- Praktická obrana: secure boot, digitálně podepsané aktualizace, MFA/RBAC, ochrana debug rozhraní, pravidelné testování.

Entry points
OTA/update chain · maintenance port · remote access

Main effect
manipulace dat a řídicí logiky

Primary controls
secure firmware + strong auth + anomaly detection

Manipulace senzorů a teploty

- Teplotní čidla a odhady teploty jsou kritické pro prevenci thermal runaway.
- Útok může posunout čtení senzoru, změnit kalibraci nebo zkreslit vstupy pro tepelný model.
- Silnější varianta je adversarial útok: současná manipulace proudu a napětí tak, aby model vypočítal věrohodnou, ale chybnou teplotu.

Riziko

pozdní detekce přehřátí, špatné ochranné zásahy

Detekce

redundance senzorů + křížová verifikace s modelem

Opatření

tamper-resistant sensors, encrypted comms, secured calibration

EMI a fyzické narušení elektroniky

- EMI fault injection zavádí do elektroniky řízené elektromagnetické rušení a může vyvolat chybné čtení nebo chování BMS.
- Zasažené mohou být senzory, napájecí větve, komunikační cesty i integrované obvody.
- Obrana stojí na stínění, uzemnění, filtrech, návrhu PCB, oddělení napájecích domén a fail-safe mechanismech.

Injection points

wiring harness · sensor lines · IC I/O · power supply

Symptoms

erroneous readings · shutdowns · damaged components

Design goal

EMI resilience by design, not only by monitoring

wBMS a jamming

- Wireless BMS snižuje kabeláž a zvyšuje flexibilitu, ale otevírá novou rádiovou attack surface.
- Jamming může způsobit ztrátu dat, zkreslení přenosu a chybné charging/discharging reakce.
- Dopad je bezpečnostní i provozní: špatný balancing, rychlejší degradace, ztráta kontroly nad packem.

Controls

FHSS / DSSS · encrypted comms · redundant channels

Monitoring

signal anomalies, packet loss, failover events

Lesson

wireless convenience musí mít security budget

Timestamp a integrita dat

- Timestamp attack nemění nutně samotná data, ale jejich pořadí a časový kontext.
- U BMS to může zkreslit SOC trend, diagnostiku, predictive maintenance i digitální dvojče.
- Obrana: kryptografické timestamping mechanismy, bezpečná synchronizace času, end-to-end integrita a vícezdrojová verifikace.

Attack pattern
packet interception · replay · clock desync

Operational effect
nesprávná interpretace událostí a historie

Technical answer
HMAC / signatures · authenticated NTP/PTP

Jaké dopady útoků uvidí provozovatel BESS

Telemetrie vypadá věrohodně
ale fyzikálně si veličiny přestávají odpovídat

Setpointy a realita se rozcházejí
výkon nebo SOC trend nesedí s měřením

Zásahy přicházejí pozdě nebo špatně
fault response a ochrany pracují na chybných datech

- Incident nemusí mít podobu „zašifrovaných serverů“; často se projeví jako nepřesná telemetrie, chybné alarmy nebo nespolehlivé chování.
- Právě proto je u BESS důležitá kombinace OT monitoringu a fyzikální konzistence dat.

BESS-Set: co přesně dataset modeluje

- Dataset zachycuje elektrické a řídicí veličiny při normálním provozu i při kybernetických útocích.
- Je cenný tím, že nepracuje jen se síťovým provozem, ale i s fyzikálními měřeními BESS.

Jaké útoky BESS-Set obsahuje

Bad Data Injection

Manipulace setpointů aktivního nebo jalového výkonu; např. překročení limitů či oscilace.

False Data Injection

Změna měření posílaných do SCADA, např. active power nebo SOC tampering.

Firmware Modification

Změna vnitřního chování výkonové elektroniky, např. THD nebo V battery tampering.

- Většina scénářů vede k fyzikálně nemožné nebo velmi nepravděpodobné kombinaci měřených veličin.
- To je důvod, proč lze stavět physics-based detekci i bez detailní znalosti konkrétního malware.

Jaká data má smysl historizovat a hlídat

Power path
P/Q setpoint vs. measured P/Q

Battery state
SOC trend · SOH · battery voltage

Electrical quality
DC-link · currents · THD

Thermal
temperatures · gradients · anomalies

Ops
alarms · config changes

- Samotné logy přístupů nestačí. Klíčové je spojit identitu a změny konfigurace s fyzickým dopadem v čase.
- Dobré minimum: kdo změnil setpoint/konfiguraci, jak se změnil výkon, a zda tomu odpovídaly napětí, proud, SOC a teplota.

Physics-based anomaly detection: proč dává smysl

- Neptá se jen „přišel podezřelý packet?“, ale i „odpovídá tomu fyzika systému?“
- Odhalí útok, i když telemetrie vypadá formálně korektně, ale výkon, napětí, proud a SOC už spolu nesedí.
- Pro BESS je to silné právě tam, kde klasický IT monitoring nevidí chybu v samotném procesu.

Input
telemetry + operating context

Model
physical laws / learned process relations

Output
anomaly score + operational explanation

Obranné vrstvy BESS projektu

Governance
odpovědnosti, servisní pravidla, audit trail

Identity
MFA, PAM, oddělené identity dodavatelů

Segmentation
IT / OT / cloud, jump host, controlled access

Hardening
secure boot, signed firmware, protected interfaces

Monitoring
IDS + physics-based anomaly detection

Prepared operations
degraded mode, recovery, zálohy konfigurací, krizové kontakty a nacvičené role

- Bezpečnost BESS není jedna krabice. Je to architektura, provozní disciplína a schopnost incident zvládnout i během krize.

Compliance a návrhové minimum

- Kyberbezpečnost má být v návrhu od začátku, ne až jako dodatečný audit před spuštěním.
- Relevantní referenční rámce: ISO/SAE 21434, ISO 26262 a IEC 62443.
- Praktické minimum pro investora: bezpečné aktualizace, řízený vzdálený servis, segmentace, historizace dat a testovaný recovery postup.

ISO/SAE 21434
řízení kyberrizik v životním cyklu

ISO 26262
funkční bezpečnost a fault response

IEC 62443
bezpečnost průmyslových a OT systémů

Tři hlavní závěry

BESS je cyber-physical systém

Proto incident nemusí vypadat jako klasický IT problém.

Bez fyzikální konzistence dat část útoků neuvidíme

Physics-based monitoring dává BESS provozu praktickou výhodu.

Bezpečnost musí být navržena jako vícevrstvá obrana

Architektura, identity, firmware, monitoring i recovery.

Děkuji za pozornost

Tomáš Pitner · **MENDELU** a **CyberSecurity Hub, z.ú.**

Zdroje: IEEE Access 2025; IEEE OAJPE 2024