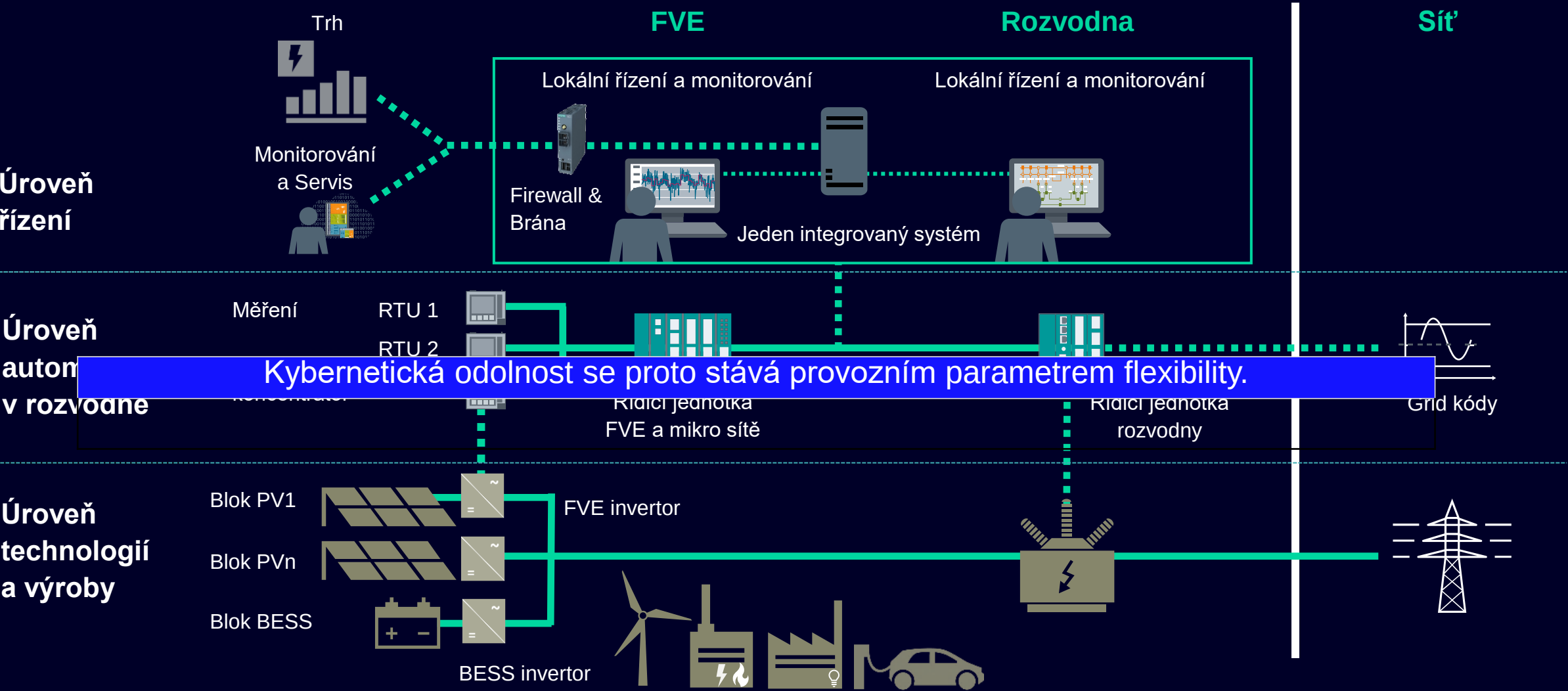


Kybernetická odolnost součást systémové přiměřenosti

[illegible]

Flexibilita, digitalizace, důvěryhodnost



Kybernetická bezpečnost

Jsem v regulaci?

odvětví podle § 4 zákona č. 264/2025 Sb.

1. Veřejná správa
2. Energetika
3. Výrobní průmysl
4. Potravinářský průmysl
5. Chemický průmysl
6. Vodní hospodářství
7. Odpadové hospodářství
8. Doprava
9. Digitální infrastruktura a digitální služby
10. Finanční trh
11. Zdravotnictví
12. Věda, výzkum a vzdělávání
13. Poštovní a kurýrní služby
14. Obranný průmysl
15. Vesmírný průmysl

Ve vyhlášce 408/2025 Sb. jsou mezi regulovanými službami zejména:

1. výroba elektřiny,
2. přenos elektřiny,
3. distribuce elektřiny,
4. agregace,
5. poskytování služeb výkonové rovnováhy,
6. provozování významných energetických zařízení,
7. provozování soustav a sítí.

Významnost podniku

1. Mikropodnik
2. Střední podnik
3. Velký podnik.

Kybernetická bezpečnost

Motivace

Zákon č.264/2025 Sb. – Zákon o kybernetické bezpečnosti

- definuje kontrolu plnění povinností souvisejících s kybernetickou bezpečností
- definuje odpovědnosti managementu, možnost pozastavení činnosti min. na 6 měsíců
- definuje přestupky a pokuty (projednává úřad, tedy NÚKIB)
- plán kontinuity provozu a obnovy po havárii
- ochrana významných partnerů

Obchodní motivace

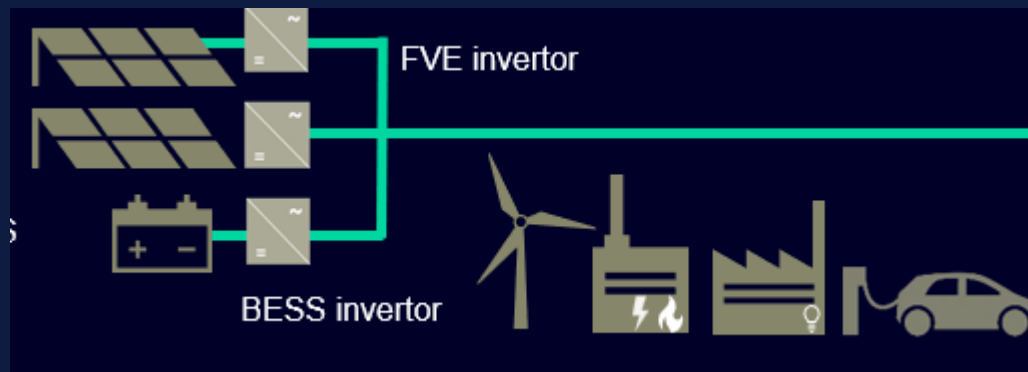
- jméno společnosti
- obchodní model – kontinuita
- spolehlivost – dodavatel významných partnerů

Stanovení rozsahu řízení kybernetické bezpečnosti

Určení všech primárních aktiv v organizace v takovém detailu, aby bylo možné kvalifikovaně rozhodnout, zda aktivum souvisí s regulovanou službou či nikoliv, režim vyšších / nižších povinností

Posouzení primárních aktiv - rozhodnutí, zda primární aktivum souvisí s poskytováním regulované služby,

Určení podpůrných aktiv - součástí je evidence vazeb podpůrných aktiv na primární aktiva související s poskytováním regulované služby.



<https://portal.nukib.gov.cz/pruvodce-novym-zaknem-o-kyberneticke-bezpecnosti>

Kybernetická bezpečnost v energetické síti



Klíčové standardy



- IEC 62443 (System Security)
- IEC 62351 (Communication Security)



- ISO/IEC 27001 (Security Mgmt.)

Bezpečnost vyžaduje holistický přístup

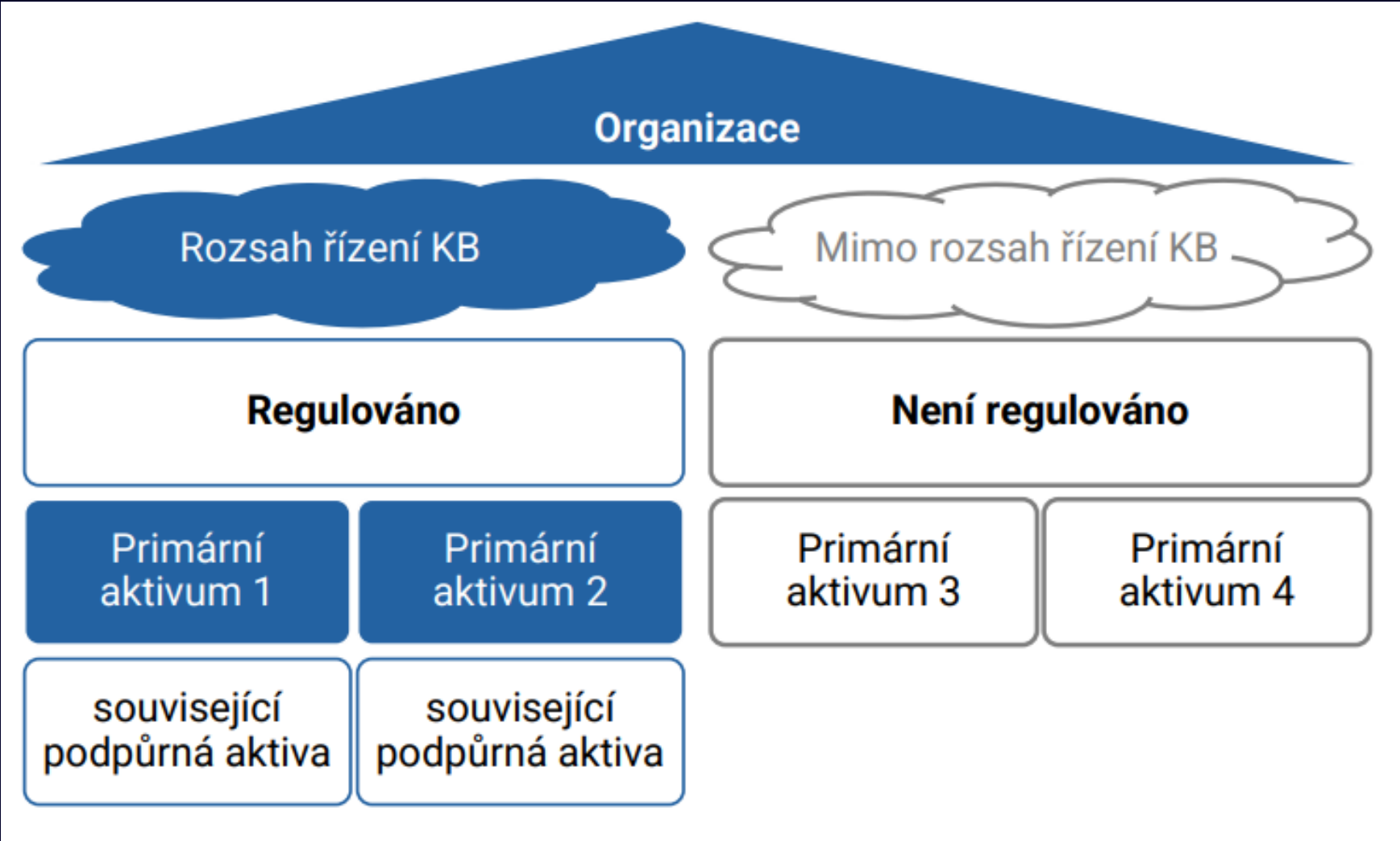
Lidé

- Povědomí a porozumění kybernetické bezpečnosti

Procesy

- Pokrývá celý životní cyklus výrobku
- Podpora požadavků na řešení a provoz
- **(Produkty)Technologie**
- Podpora cílů ochrany (Důvěrnost, Integrita, Dostupnost)
- Soulad s mezinárodními standardy

Stanovení rozsahu řízení kybernetické bezpečnosti



Stanovení rozsahu řízení kybernetické bezpečnosti v režimu nižších povinností

Vyhláška č.410/2025 (ze 14.10. 2025, platnost od 1.11.2025) – vyhláška o bezpečnostních opatřeních poskytovatele služby v režimu nižších povinností

- provádět řízení rizik
- mít stanovené odpovědnosti managementu
- školit zaměstnance
- mít plán reakce na incidenty
- hlásit významné incidenty NÚKIB
- řídit přístupy a identity
- zajistit zálohování a kontinuitu provozu
- vést dokumentaci o zavedených opatřeních

Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

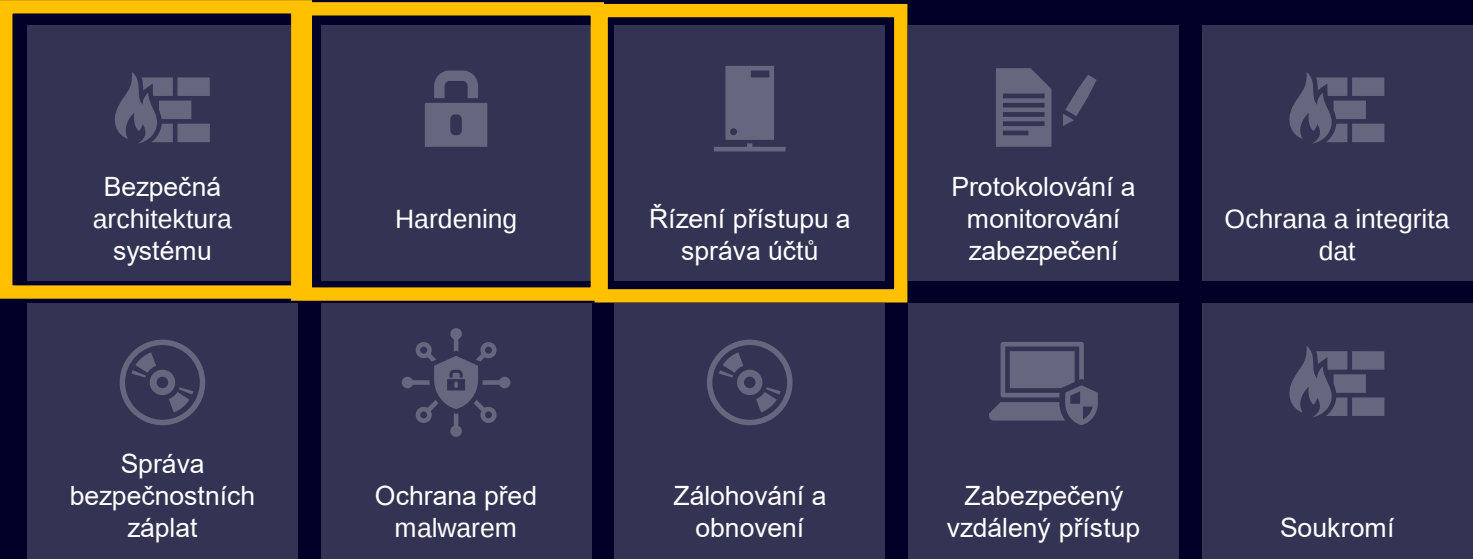
Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



Technologie

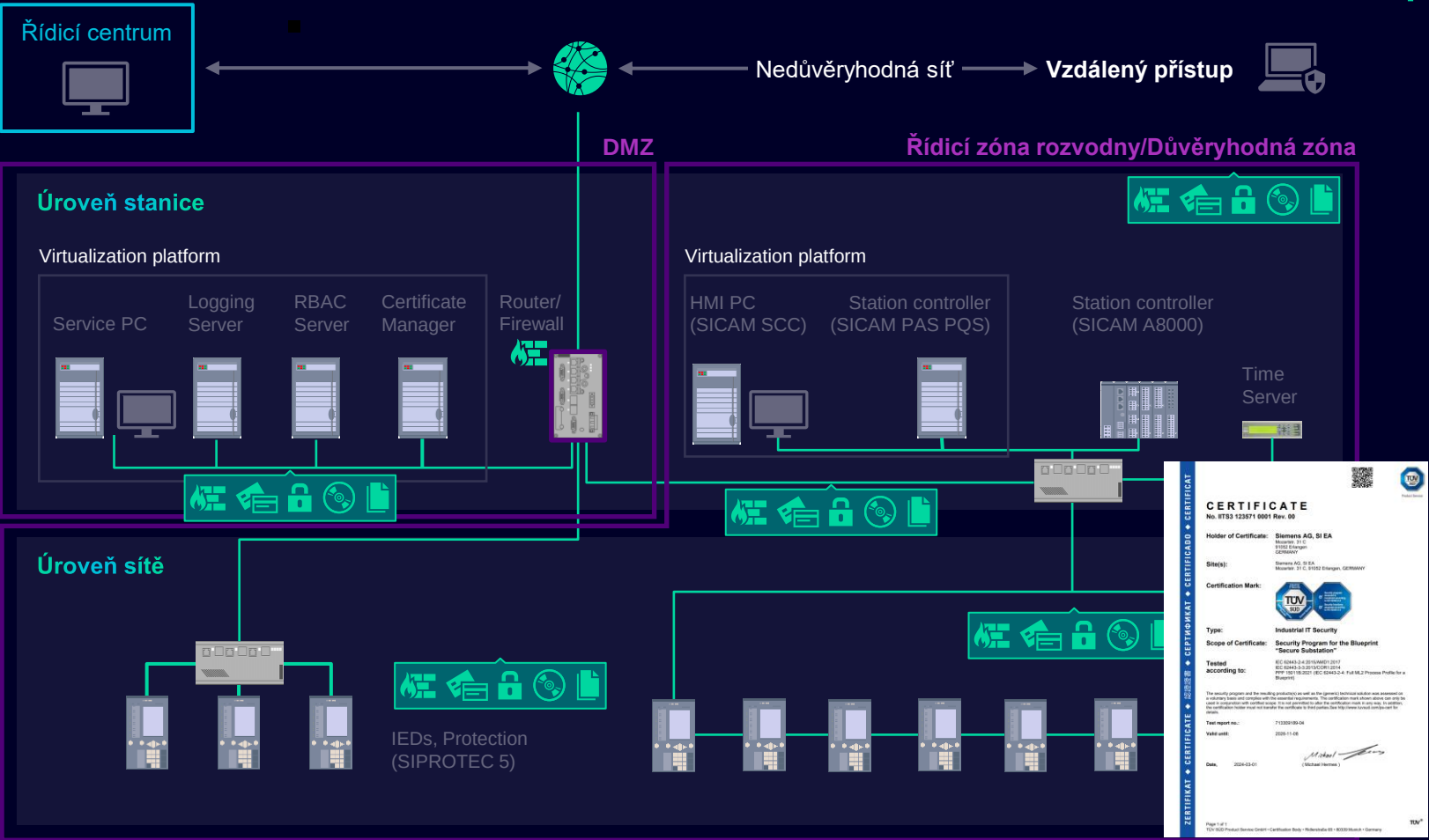
Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře



Přístupová kontrola

Segmentace, autentifikace, role, hardening

Úroveň řízení sítě



Plán zabezpečené rozvodny na základě

- Siemens SICAM Automation komponent
- Siemens SIPROTEC 5 ochran
- Siemens RuggedCom firewallů
- Siemens RuggedCom síťových komponent
- Microsoft Windows operačního systému
- Fortinet Firewalls
- Serveru času třetí strany
- PC hardware třetí strany



IEC 62443
certifikované řešení

- **Certifikace TUV SÜD**
- IEC 62443-2-4 – procesy integrace
- IEC 62443-3-3 – Technické funkce



• Řízení přístupu



• Ochrana před malwarem



• Správa oprav



• Hardening



• Protokolování zabezpečení



• Ochrana dat, bezpečná architektura

Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



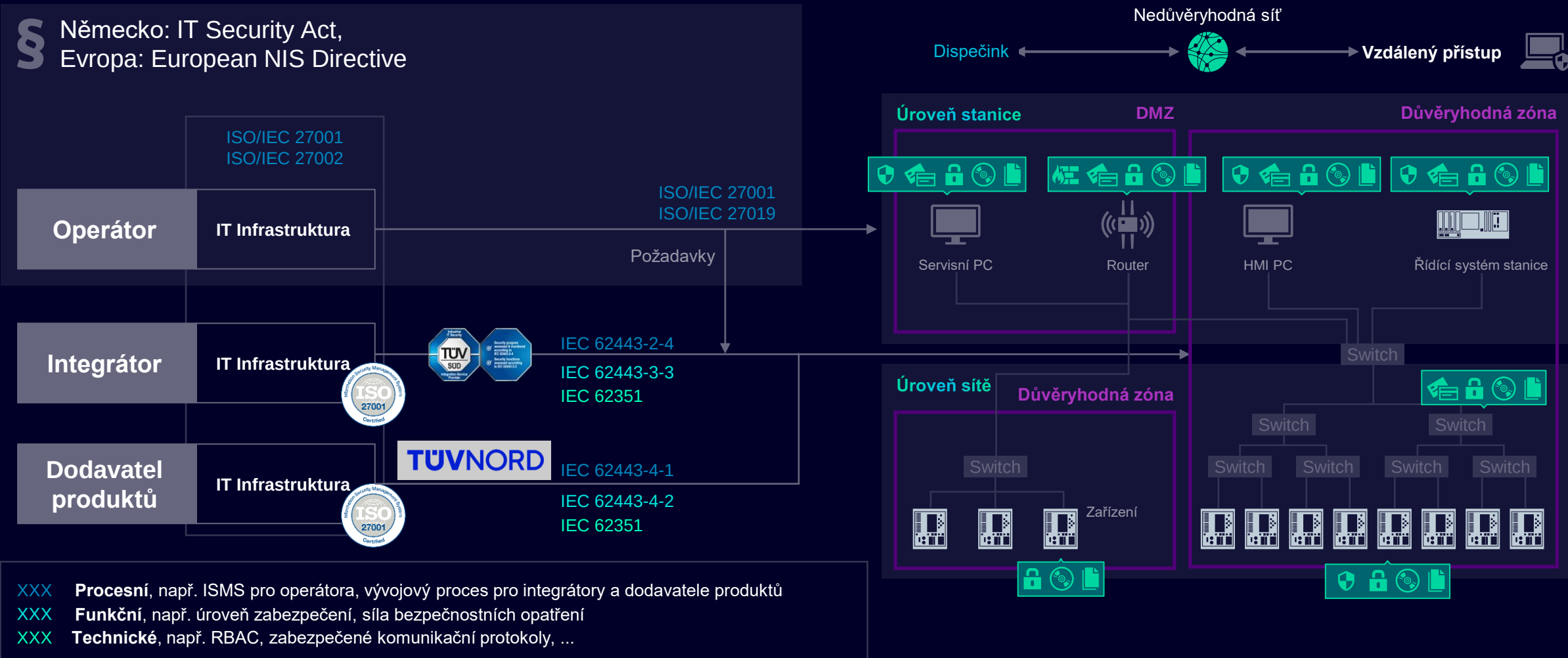
Technologie

Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře

 Bezpečná architektura systému	 Hardening	 Řízení přístupu a správa účtů	 Protokolování a monitorování zabezpečení	 Ochrana a integrita dat
 Správa bezpečnostních záplat	 Ochrana před malwarem	 Zálohování a obnovení	 Zabezpečený vzdálený přístup	 Soukromí

Přístupová kontrola

Vzdálená připojení



Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



Technologie

Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře

Bezpečná architektura systému

Hardening

Řízení přístupu a správa účtů

Protokolování a monitorování zabezpečení

Ochrana a integrita dat

Správa bezpečnostních záplat

Ochrana před malwarem

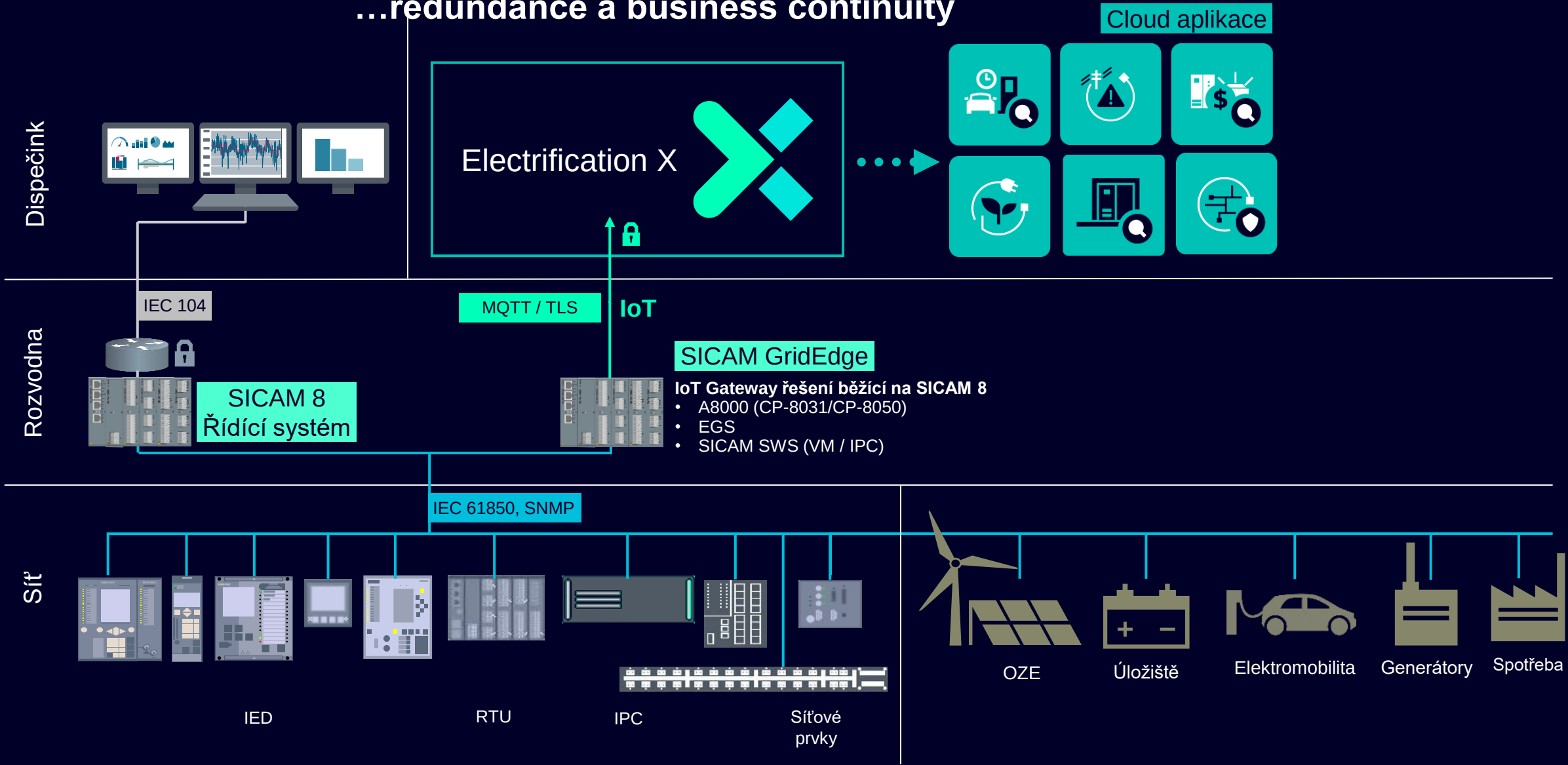
Zálohování a obnovení

Zabezpečený vzdálený přístup

Soukromí

Monitorování, detekce a reakce na incidenty... ...redundance a business continuity

Kybernetická bezpečnost



Security Information & Event Management (SIEM)

Sběr logů ze zařízení v síti pro systémy analýzy a detekce kybernetických útoků SIEM.

[siemens.com/ot-siem](https://www.siemens.com/ot-siem)



Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



Technologie

Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře

 Bezpečná architektura systému	 Hardening	 Řízení přístupu a správa účtů	 Protokolování a monitorování zabezpečení	 Ochrana a integrita dat
 Správa bezpečnostních záplat	 Ochrana před malwarem	 Zálohování a obnovení	 Zabezpečený vzdálený přístup	 Soukromí

Kybernetická bezpečnost v energetické síti

Řešení zranitelností a incidentů pro produkty a systémy



Siemens ProductCERT a SiemensCERT

Centrální týmy odborníků pro okamžitou reakci na bezpečnostní hrozby a problémy ovlivňující produkty, řešení, služby nebo infrastrukturu Siemens.

Oznámení a doporučení

- Siemens:
<https://www.siemens.com/cert/advisories>
- ICS-CERT
<https://ics-cert.us-cert.gov/advisories>

ID	CVSS Score	Dokumenttitel	Info	Version	Aktualisiert	Download
SSA-158227	5.9	Denial-of-Service Vulnerability in Automation License Manager		V1.0	2021-08-10	PDF TXT
SSA-309571	7.5	IPU 2021.1 Vulnerabilities in Siemens Industrial Products using Intel CPUs (June 2021)		V1.0	2021-08-10	PDF TXT
SSA-365387	7.0	Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.2.0.1		V1.0	2021-08-10	PDF TXT
SSA-553445	9.0	DNS "NameBleed" Vulnerabilities in Multiple Siemens Energy AGT and SGT solutions		V1.0	2021-08-10	PDF TXT
SSA-479335	8.8	Multiple Vulnerabilities in Embedded FTP Server of SIMATIC NET CP Modules		V1.0	2021-08-10	PDF TXT
SSA-756744	7.2	OS Command Injection Vulnerability in SINEC NMS		V1.0	2021-08-10	PDF TXT
SSA-818603	7.0	Multiple Vulnerabilities in Solid Edge before SE2021MP7		V1.0	2021-08-10	PDF TXT
SSA-830194	8.1	Missing Authentication Vulnerability in S7-1200 Devices		V1.0	2021-08-10	PDF TXT
SSA-885527	5.3	Incorrect Authentication Vulnerability in Industrial Products		V1.0	2021-08-10	PDF TXT
SSA-930830	7.0	SQL and REX File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.2.0.2		V1.0	2021-08-10	PDF TXT
SSA-206030	9.0	Multiple Vulnerabilities in SINAMICS Medium Voltage Products		V1.1	2021-08-10	PDF TXT
SSA-524955	7.4	SAD DNS Attack in Linux Based Products		V1.0	2021-08-10	PDF TXT
SSA-439005	n/a	Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1515SP-4		V3.6	2021-08-10	PDF TXT
SSA-492020	5.9	Denial-of-Service Vulnerability in SIMATIC S7-500 CPUs and SINUMERIK Controller		V1.1	2021-08-10	PDF TXT
SSA-541018	6.5	Embedded TCP/IP Stack Vulnerabilities (SINEMA33) in SENTRON PAC / IMA Devices (Part 2)		V1.2	2021-08-10	PDF TXT

Informace o opravách

Zprávy o kompatibilitě bezpečnostních záplat

[SIOS Portal](#)

www.siemens.com/gridsecurity

Industry Online Support International | Language | Contact | Help | Support Request

Home > Product Support

Entry type: Download Entry ID: 109808612, Entry date: 04/30/2024

★★★★★ (2) > Rate

Security Patch Management

Entry Associated product(s)

Security Patch Management for Microsoft Windows based SIPROTEC and SICAM Products

Security Patch Compatibility Report for DIGSI 4
📄 DIGSI4_Security_patches.xlsx (48,2 KB)

Security Patch Compatibility Report for DIGSI 5
📄 DIGSI5_Security_patches.xlsx (48,0 KB)

Security Patch Compatibility Report for SICAM PAS PQ S, PQ Analyzer, SICAM SCC
📄 SICAM_PAS_Security_patches.xlsx (54,5 KB)

Security Patch Compatibility Report for SICAM Device Manager, SICAM TOOLBOX II
📄 SICAM_DM_TOOLBOXII_Security_patches.xlsx (55,4 KB)

Tested anti-virus pattern version: Windows Defender security intelligence update; 1.409.454.0
📄 Pattern_files.zip (133.7 MB) (SHA-256)

Security information

In order to protect technical infrastructures, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art IT security concept. Siemens' products and solutions constitute one element of such a concept. For more information about cyber security, please visit <https://www.siemens.com/cybersecurity#Ouraspiration>.

Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



Technologie

Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře

 Bezpečná architektura systému	 Hardening	 Řízení přístupu a správa účtů	 Protokolování a monitorování zabezpečení	 Ochrana a integrita dat
 Správa bezpečnostních záplat	 Ochrana před malwarem	 Zálohování a obnovení	 Zabezpečený vzdálený přístup	 Soukromí

Kybernetická bezpečnost v energetické síti

Lidé, Procesy, Technologie



Procesy

Organizační bezpečnost a procesy
Lidé, zásady, procesy, správa

Organizační připravenost

Bezpečný vývoj

Bezpečná integrace a servis

Zranitelnosti a řešení incidentů



Technologie

Technologie kybernetické bezpečnosti přispívající k celkové bezpečnostní architektuře



Bezpečná architektura systému



Hardening



Řízení přístupu a správa účtů



Protokolování a monitorování zabezpečení



Ochrana a integrita dat



Správa bezpečnostních záplat



Ochrana před malwarem



Zálohování a obnovení



Zabezpečený vzdálený přístup



Soukromí

Kybernetická bezpečnost v energetické síti



Klíčové standardy



- IEC 62443 (System Security)
- IEC 62351 (Communication Security)



- ISO/IEC 27001 (Security Mgmt.)

Bezpečnost vyžaduje holistický přístup

Lidé

- Povědomí a porozumění kybernetické bezpečnosti

Procesy

- Pokrývá celý životní cyklus výrobku
- Podpora požadavků na řešení a provoz
- **(Produkty)Technologie**
- Podpora cílů ochrany (Důvěrnost, Integrita, Dostupnost)
- Soulad s mezinárodními standardy

Požadavky dle ISO/IEC 27001 pro průmyslové řídicí systémy (ICS)

Bezpečnost v technologiích

Podepsaný software/firmware

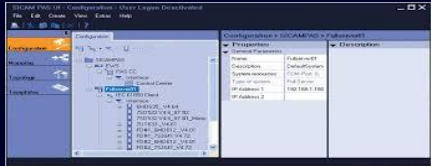
Ochrana proti manipulaci s firmwarem/softwarem

Firewall & VLAN

Oddělení ethernetového provozu přes integrovaný firewall a VLAN

Protokolování zabezpečení / Syslog

Energeticky nezávislá perzistence záznamu bezpečnostního auditu a přenosu přes Syslog



RBAC s centrální správou uživatelů

Centrálně spravujte uživatele a přiřazujte role pro autorizaci (na základě IEC 62351-8)

Bezpečný vývoj v souladu s IEC 62443-4-1

Správa certifikátů

Snadná správa certifikátů pomocí SICAM GridPass

Funkce brány v SICAM 8

- Zabezpečení VPN a TLS
- Zabezpečení IEC 80670-5-104, IEC 61850, DNP3i
- Hardwarový firewall aplikační vrstvy v SICAM8



Produkty vyhovující IEC 62443-4-2

Kybernetická bezpečnost v energetické síti

Procesem k bezpečné MW



Poradenství – Assessment & Compliance 	Technické posouzení a penetrační testy 	Poradenství a implementace ISMS (ISO/IEC 27001) 	Školení o kybernetické bezpečnosti 
Bezpečné produkty 	Migrace digitálních rozvoden/hardening  1010101 010101 IEC 62443 Certifikace	Zabezpečený vzdálený přístup 	Pevný základ a volitelné pokročilé funkce zabezpečení 
Školení kybernetické bezpečnosti 	Správa bezpečnostních záplat  Patching	Bezpečnostní monitoring SIEM jako služba 	Správa aktiv OT 

Kybernetická bezpečnost v energetické síti

Procesem k bezpečné MW

Identifikace rozsahu řízení KB – fyzické zajištění, hlavní technologie, kamerové systémy...stanovení priorit

Osoby, zařízení, subdodavatelé – řízení rizik

Školení – zaměstnanců, správců, partnerů

Technologické zajištění systému – implementace IT opatření v OT

Monitorování technologie a incidentů – sledování provozních parametrů, sledování přístupů, autentifikace

Scénáře pro řešení incidentů – připravený scénář, kam budu volat, koho informovat...

Obnova ze záloh – zálohovat nastavení, dokumentaci, fotky zařízení, papírová forma - vyzkoušené zálohy

Kontakt

Zbyněk Bělina

Head of BU Electrification & Automation

Siemens, s.r.o.

Siemensova 1

155 00 Praha 13-Stodůlky

Czechia

Mobile: +420 737 206 699

zbynek.belina@siemens.com