



ARCHITEKTÚRNE A TECHNOLOGICKÉ ŠTANDARDY ICS

VERZIA 15.01.2024



1. KOMPATIBILITA PRODUKTOV

1.1 HARDVÉROVÁ PLATFORMA

Procesorová architektúra: x86 a x64 CPU, ARM, AMD64

Komunikačné technológie: komunikácia je povolená len prostredníctvom metallickej/ optickej linky prípadne rádiom, ak to nie je možné zabezpečiť linkou, ostatné komunikačné technológie ako napr. WiFi, Bluetooth, IR, NFC sú zakázané, periférne zariadenia ako napr. klávesnica a myš musia byť pripojené káblom.

Manažovateľné aktívne sieťové / bezpečnostné prvky: Cisco, Fortinet, Moxa, Flowmon, Claroty, HP

Zdroje nepretržitého napájania UPS: štandard IEC 60320, IEC 62040, certifikácia NQA-1

NAS server: RAID 5 prevedenie hot-swap + spare disk

1.2 SOFTVÉROVÁ PLATFORMA

Virtualizačná platforma: VMware

Operačné systémy: Microsoft Windows, GNU/Linux

Databázové platformy: Microsoft SQL, PostgreSQL, MariaDB, Oracle DB, MySQL

PLC Protokoly: IEC 60870-5-104, MODBUS, OPC UA, PROFIBUS, PROFINET

Sieťové komunikačné protokoly pre správu zariadení: SSH, HTTPS, SFTP, LDAPS, IPSEC, TLS min. 1.2

Monitoring: SNMP min. ver. 3, NetFlow min. v9, ICMP

Antivírusová ochrana: preferované riešenie ESET, Windows Defender

Zálohovanie a obnova údajov: preferované riešenie Acronis

Aplikačná architektúra: 3 vrstvomá architektúra, webová aplikácia s tenkým klientom, HTML 5 štandard (nepožívať Adobe flash, silverlight, shockwave a pod.). Obsah tretích strán (fonty, obrázky, skripty a pod.) musí byť lokálne integrovaný.

2. RIADENIE PRÍSTUPOV

Používať technológiu, ktorá umožňuje centralizované vytváranie jedinečných používateľských účtov, vrátane privilegovaných účtov, založenej na AAA technológii (napr. Active Directory, LDAP, TACACS+, RADIUS).

Autentizačné informácie nesmú byť v systémoch ukladané v čitateľnej forme (napr. v hash a nesmú byť súčasťou skriptov).

3. BEZPEČNOSŤ PRI PREVÁDZKE SYSTÉMOV A SIETÍ

Pri hardeningu systémov a služieb požadujeme zohľadniť odporúčania [CIS Benchmark](https://www.cisecurity.org/cis-benchmarks/) (<https://www.cisecurity.org/cis-benchmarks/>), ktoré sú voľne dostupné a uznané NIST, PCI DSS, HIPAA, DoD Cloud Computing SRG, FedRAMP.



Pozn.: Podľa odporúčaní sú nakonfigurované [CIS Hardened Images \(https://www.cisecurity.org/cis-hardened-images\)](https://www.cisecurity.org/cis-hardened-images).

4. HODNOTENIE ZRANITEĽNOSTÍ A BEZPEČNOSTNÝCH AKTUALIZÁCIÍ

Pre potreby automatizovaného sledovania zraniteľností komponentov ICS požadujeme od dodávateľov v rámci inventárneho zoznamu dodať zoznam použitých HW a SW produktov vo formáte „cpe:2.3:h:abb:pm590-eth:2.0:*:*:*:*:*“ ako ich uvádza stránka [NIST \(https://nvd.nist.gov/products/cpe/search\)](https://nvd.nist.gov/products/cpe/search).

5. OCHRANA PROTI ŠKODLIVÉMU KÓDU

Ochrana pred škodlivým kódom je povinná na servisných a operátorských staniciach a na zariadeniach s prístupom do internetu a/alebo s požiadavkou na vzdialený prístup, a na všetkých staniciach využívajúcich externé (prenosné) médiá.

6. SIEŤOVÁ A KOMUNIKAČNÁ BEZPEČNOSŤ

Riešenie musí zohľadňovať referenčnú sieťovú architektúru uvedenú v prílohe A tohto dokumentu a byť kompatibilné s existujúcou infraštruktúrou, všetky aktívne prvky musia byť manažovateľné (prostredníctvom samostatného portu) a musia podporovať:

- nastavenie statickej lokálnej IP adresy, adresný rozsah určí SE,
- protokol SNMP min. ver.2 (konfigurácia read-only),
- protokoly HTTPS/SSL, SSH, TACACS+, RADIUS,
- presmerovanie logov do centrálneho úložiska (syslog),
- monitorovanie sieťovej prevádzky formou multi-port mirroringu, alebo tzv. SPAN port (nesmie sa jednať len o single port mirroring), dimenzovať počet portov, vrátane portu pre účel zrkadlenia, rovnako zohľadniť dostatočný výkon pre zrkadlenie dátového toku.

6.1 SEGMENTÁCIA SIETÍ

Segmentácia sietí musí byť v súlade s [Referenčná sieťová architektúra](#), pričom:

- servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch (DMZ),
- v rovnakom segmente môžu byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
- koncové zariadenia, vrátane serverov, nesmú mať priame pripojenie do viacerých sietí (zón).

6.2 KOMUNIKÁCIA MEDZI ZÓNAMI

Komunikácia medzi zónami musí byť smerovaná cez hardvérový aplikačný firewall podľa zásady všetko zakázané („default deny all“), povoliť len autorizované („allow list“), na princípe zásady najnižších privilégií.



Prevádzkové a bezpečnostné záznamy firewallu, vrátane kópie komunikácie, musia byť presmerované prostredníctvom jednosmerných dátových diód do systému monitorovania kybernetickej bezpečnosti.

6.3 IDENTIFIKÁCIA ŠKODLIVEJ SIEŤOVEJ PREVÁDZKY

Na identifikáciu škodlivej sieťovej prevádzky v prostredí SaIS kat. II a III s väzbou na základnú službu musí byť v zóne riadenia výroby zahrnuté aj hardvérové riešenie (sonda) schopné zaznamenávať a vyhodnocovať sieťové pakety s presmerovaním detegovaných anomálií do systému monitorovania kybernetickej bezpečnosti (napr. Flowmon ADS, Claroty).

7. ZAZNAMENÁVANIE UDALOSTÍ A MONITOROVANIE

Vytvárané prevádzkové a bezpečnostné záznamy musia byť z miesta vzniku záznamu presmerované prostredníctvom jednosmerných dátových diód do systému monitorovania kybernetickej bezpečnosti.

Zaznamenáva sa najmenej:

- a) prihlásenie a odhlásenie používateľa, ako aj neúspešné pokusy o prístup,
- b) zmenu konfigurácie aktívneho sieťového prvku (napr. pravidiel firewallu),
- c) automatické varovné alebo chybové systémové hlásenia,
- d) pripojenia a odpojenia periférií na koncovom zariadení (napr. USB klávesnice).

Pozn.: Pre SaIS kat. III s väzbou na základnú službu požadujeme minimálne lokálne zaznamenávať aj aktivity používateľov na aplikačnej úrovni.

Minimálny interval lokálneho uchovávanía prevádzkových a bezpečnostných záznamov, vrátane aktivít používateľov na aplikačnej úrovni, sú 3 mesiace, alebo do naplnenia úložiska zariadenia. Po naplnení úložiska musí pokračovať ukladanie záznamov prepisovaním najstarších záznamov.

Riešenie musí zabezpečovať synchronizáciu času na prevádzkovaných systémoch podľa informácií od presného časového zdroja SE.

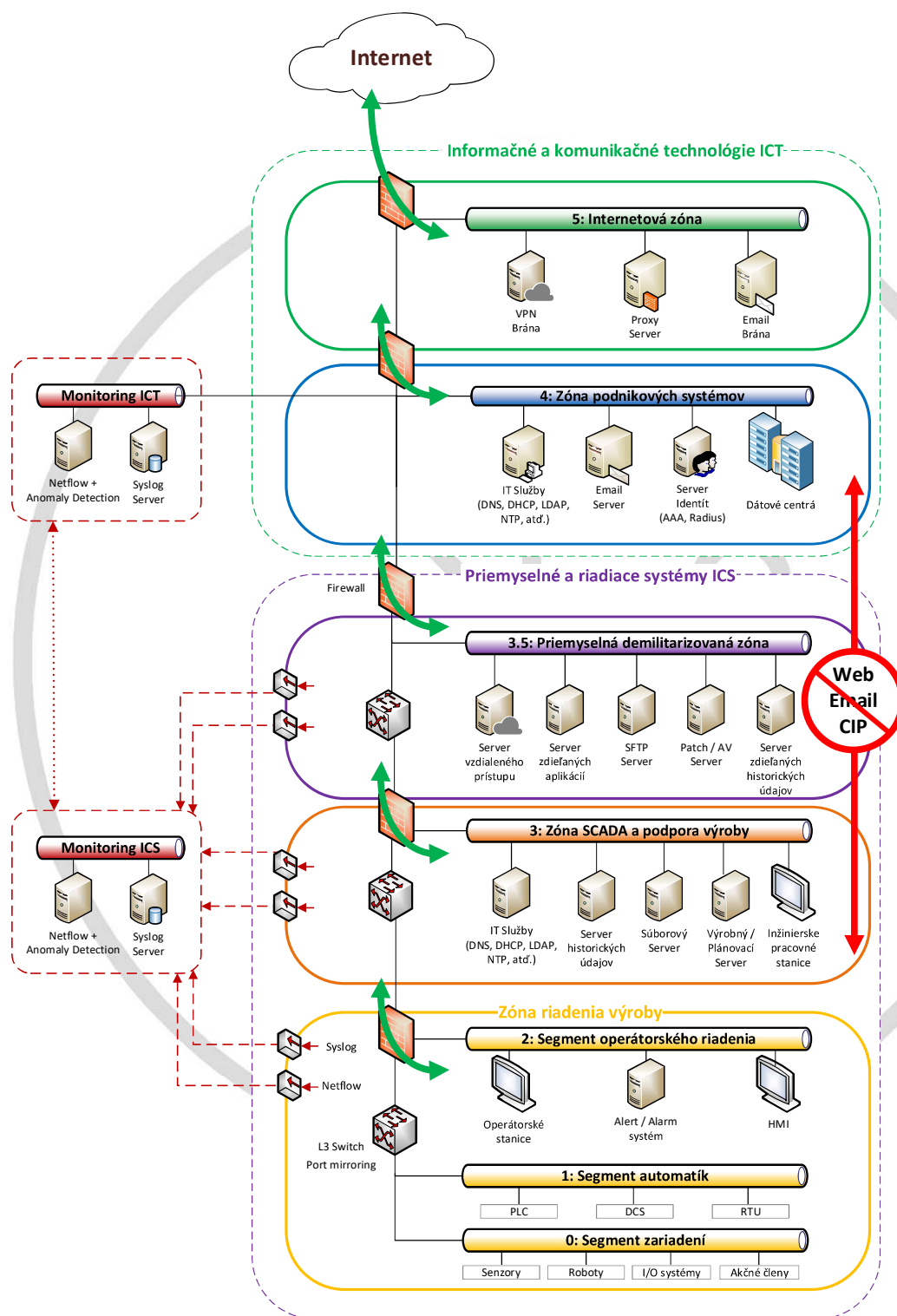
8. KRYPTOGRAFICKÉ OPATRENIA

Používanie kryptografických opatrení v prostredí ICS, predstavuje najmä používanie:

- zabezpečených protokolov pri správe a konfigurácii zariadení (napr. https namiesto http, ssh namiesto telnet),
- virtuálne privátne siete (VPN) pre komunikáciu point-to-point,
- podpisovanie softvérového kódu,
- certifikátov vydaných off-line internou CA (pozn.: vydávanie zabezpečujú SE, a.s.).



9. REFERENČNÁ SIEŤOVÁ ARCHITEKTÚRA





Legenda

5: Internetová zóna

Internetová zóna sprístupňuje verejne publikované služby web, e-mail, VPN.

4: Zóna podnikových systémov

Infraštruktúra podnikových informačných a komunikačných technológií, poskytujúca služby na podporu procesov spoločnosti.

3.5: Priemyselná demilitarizovaná zóna

Označovaná ako IDMZ oddeľuje prostredie priemyselných riadiacich systémov od zóny podnikových systémov.

3: Zóna SCADA a podpora riadenia výroby

Zóna pozostáva z infraštruktúry na riadenie nižších úrovní a zabezpečenia dohľadu a riadenia výroby (bloková dozorňa, dispečerské pracovisko).

Zóna má zakázané priamo komunikovať s vyššími zónami prostredníctvom priemyselných protokolov a službami WEB a e-mail.

2: Segment operátorského riadenia

Tento segment zahŕňa ovládanie cez HMI a inžinierske pracovné stanice, ktoré riadia segment 1.

1: Segment automatík

Tento segment zahŕňa RTU, PLC, DCS.

0: Segment zariadení

Táto úroveň zahŕňa akčné členy, armatúry, motory, senzory, a pod.

Pozn.: Každá zóna môže obsahovať viac VLAN.