Všeobecné pravidlá pre partnerské firmy dodávajúce OT infraštruktúru a softvér

1. Účel

Tento dokument ustanovuje pravidlá pre partnerské firmy dodávajúce IT/OT infraštruktúru a softvér pre MH Teplárenský Holding, a.s. Dokument je určený vedeniu partnerských spoločností, ich zamestnancom a subdodávateľom a slúži ako technický štandard MHTH.

1.1 Všeobecné ustanovenia

Pravidlá uvedené v tomto dokumente, v prípade, že ich možno aplikovať na rozsah dodávky, sú povinné. Ich neplnenie je možné len v prípade, že Zadanie na dodávku má iné požiadavky. V takom prípade je Zadanie nadradené tomuto dokumentu. Akýkoľvek dokument vyžadovaný v rámci realizačnej dokumentácie je automaticky vyžadovaný aj v rámci dokumentácie skutkového stavu vo svojej finálnej podobe, kde zachytáva aktuálny stav.
Okrem tohto dokumentu sa dodávateľ musí riadiť aj relevantnými štandardami a opatreniami vyplývajúcimi najmä, avšak nielen z IEC 62443, IEC 61508, IEC 61511, IEC 63303 a platnými zákonmi a vyhláškami vzťahujúcimi sa na MHTH a rozsah diela.

1.2 Výnimky

Výnimka na neplnenie niektorej z požiadaviek uvedených v tomto dokumente je prípustná výlučne vtedy, ak dodávateľ preukáže a hodnoverne zdokumentuje, že na relevantnom trhu nie je v aktuálnom čase dostupné žiadne technické riešenie (hardvér, softvér, služby alebo postupy), ktoré by spĺňalo stanovenú požiadavku.
Pre zdôvodnenie výnimky musia existovať objektívne okolnosti spôsobujúce všeobecnú nedostupnosť riešenia na trhu (stav techniky). Subjektívna nemožnosť dodávateľa získať, zazmluvniť alebo dodať požadovaný produkt (napríklad z dôvodu chýbajúcich partnerských vzťahov s výrobcami, interných logistických limitov dodávateľa, či jeho obchodných dohôd) nie je dôvodom na výnimky a považuje sa za nesplnenie technických požiadaviek Zadania. Dodávateľ je povinný preukázať nedostupnosť riešenia faktickými dôkazmi. Samotné čestné prehlásenie dodávateľa sa považuje za nepostačujúce.
Dodávateľ musí k zdôvodneniu výnimky, zapísanej v prílohe č.1 predložiť minimálne:

- Oficiálne vyjadrenie výrobcov: Písomné stanovisko aspoň dvoch relevantných globálnych výrobcov v danej oblasti potvrdzujúce, že požiadavka je technicky nerealizovateľná alebo že daný typ produktu nevyrábajú.
- Trhovú analýzu: Dokumentovaný prieskum trhu preukazujúci absenciu produktov s požadovanými parametrami u alternatívnych dodávateľov alebo
- Technické zdôvodnenie: Odbornú analýzu vysvetľujúcu, prečo súčasný stav techniky neumožňuje splnenie požiadavky v plnom rozsahu.
- Vydokladovanie výnimky vrátane všetkých dôkazov musí byť predložené ako povinná súčasť ponuky. Dodatočné uplatňovanie výnimiek v procese realizácie nebude akceptované.
- K ponuke musí byť súčasne priložený návrh náhradného riešenia, ktoré sa v maximálnej možnej miere približuje pôvodným požiadavkám.
- Súčasťou návrhu musí byť aj popis kompenzačných opatrení (mitigácia rizík), ktoré dodávateľ implementuje na elimináciu negatívnych dopadov vyplývajúcich z udelenej výnimky.

2. Definície pojmov a skratky

2.1 Pojmy

Dodávateľ - partnerská firma dodávajúca IT/OT infraštruktúru a softvér pre MH Teplárenský Holding, a.s.
Marshalling kabinet – samostatný rozvádzač na prepoj medzi poľovou technikou a riadiacim systémom
Zadanie – funkčná a nefunkčná špecifikácia požiadaviek na dodávku. V závislosti od rozsahu môže mať rôzne formy (Opis diela, Opis predmetu zákazky a pod.)
Realizačná dokumentácia – dokumentácia potrebná ku realizácii diela(DRS, DFŠ, DNR, pracovný postup, postup na inštaláciu, vykonávací projekt a pod.), na základe zadaných požiadaviek
Dokumentácia skutkového stavu – finálna dokumentácia zachytávajúca aktuálny stav diela pri jeho odovzdávaní(DSRS a pod.) dokumentujúca splnenie všetkých zmluvných požiadaviek
ZoBOaNP - Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatváraná ako príloha hlavnej zmluvy

2.2 Použité skratky

AD	Active directory
APN	Acces point network – prístupový bod
CFAT	Cybersecurity Factory Acceptance Test
CSAT	Cybersecurity Site Acceptance Test
DFŠ	Detailná funkčná špecifikácia
DMZ	Demilitarizovaná zóna
DNR	Detailný návrh riešenia
DRP	Disaster recovery plan – plán obnovy z havárie
DRS	Dokumentácia realizácie stavby
DSV	Dokumentácia skutkového vyhotovenia/stavu
EWS	Inžinierska stanica
FAT	Factory acceptance test, testovanie pred dodaním u dodávateľa
FSM	Functional Safety Management – Manažment funkčnej bezpečnosti
FW	Firewall
HAZOP	Hazard and Operability Study – Analýza bezpečnosti a prevádzkovateľnosti
HBOM	Hardware Bill of Materials
HMI	Human Machine Interface
HW	Hardware
IS	Informačný systém
IT	Information Technology
Logic solver	Procesorová jednotka PLC
MaR	Meracia a regulačná technika
MHTH	MH Teplárenský Holding, a.s.
NDA	Non-disclosure agreement, Zmluva o mlčanlivosti.
NIDS	Network Intrusion Detection System
NRS	Nadradený riadiaci systém
NVR	Network Video Recorder
OS	Operating system
OT	Operational Technology
PLC	Programable logic controler – programovateľný automat(kontrolér)
POE	Power Over Ethernet
RD	Realizačná dokumentácia
RIS	Riadiaci a informačný systém
RS	Riadiaci systém
Safety PLC	Bezpečnostné PLC, certifikované podľa STN EN 61508
SAT	Site acceptance test, testovanie počas inštalácie u objednávateľa
SBOM	Software Bill of Materials

SIF	Safety Instrumented Function – Bezpečnostná funkcia(obvod)
SIL	Safety Integrity Level – Bezpečnostný level
SIS	Safety Instrumented System – bezpečnostný systém
SPoF	Single Point of Failure
SW	Software

3. Sieťová infraštruktúra

Nová sieťová infraštruktúra sa pripája na existujúcu sieťovú infraštruktúru MHTH len v miestach na to určených a podľa definovaných pravidiel. Pripojenie do sieťovej infraštruktúry MHTH je možné len po podpise ZoBOaNP. Vytváranie izolovaných ostrovných riešení je zakázané.
Navrhovaná sieťová infraštruktúra pre systémy zabezpečujúce výrobné procesy a ich napojenie na distribučné siete musí byť navrhnutá s dôrazom na vysokú dostupnosť a prevádzkovú kontinuitu. Architektúra siete musí minimalizovať výskyt jednotlivých bodov zlyhania (SPoF).
Požaduje sa redundancia kľúčových komponentov infraštruktúry, najmä aktívnych sieťových prvkov (napr. prepínače, smerovače alebo ich funkčné ekvivalenty), napájacích zdrojov zariadení a prenosových trás v chrbticovej a agregačnej vrstve siete, minimálne na úrovni uplink/downlink. Každý napájací zdroj aktívneho sieťového zariadenia musí byť pripojený na samostatný a nezávislý napájací okruh, tak aby zlyhanie jedného napájacieho okruhu nespôsobilo výpadok prevádzky zariadenia. Navrhnuté riešenie musí umožňovať zachovanie prevádzky siete aj pri zlyhaní jedného redundantného prvku bez prerušenia poskytovaných služieb.

3.1 Switche

V rámci dodávky je možné dodať len manažovateľné L2/L3 switche s nasledujúcimi vlastnosťami:

- Rozhranie pre manažment cez SSH.
- Podpora SNMP V3 pre pripojenie na centrálny monitoring (viď Kapitola 17.2).
- Podpora RSTP a MSTP.
- Podpora štandardu 802.1x.
- Podpora syslogu a napojenia na centrálne sledovanie logovacích hlásení (viď Kapitola 17.1).
- Podpora externého manažmentu užívateľov (RADIUS, TACACS+, alebo Active Directory).
- Podpora „port security“ funkcionality.
- Podpora zberu dát do NIDS (napr. RSPAN).
- Možnosť vzdialenej aktualizácie firmware .
- Podpora protokolov CDP alebo LLDP.
- Možnosť konfigurácie aspoň 250 a 4000+ rôznych VLAN v závislosti od určenia.
- Podpora štandardu 802.1Q
- Podpora agregácie liniek.
- Downlink porty s minimálnou rýchlosťou 100/1000Mbps.
- Uplink porty s minimálnou rýchlosťou 1000Mbps (v prípade predpokladaných prenosov veľkého objemu dát s rýchlosťou 10Gbps).
- Vyhotovenie, stupeň ochrany a celková odolnosť vyhotovenia switchu musia zodpovedať náročnosti prostredia, v ktorom bude switch umiestnený.
- V prípade použitia switchu, pre zariadenia využívajúce industriálne protokoly (Profinet a pod.) je nutné aby bola zaručená ich natívna podpora samotným switchom.
- Je možné dodať len zariadenia, na ktoré je od výrobcu deklarovaná podpora po dobu 5 rokov od dátumu prevzatia diela a zároveň počas tejto doby musí byť na zariadenia

zakúpená podpora od výrobcu s možnosťou sťahovania nových verzií firmware ak ich výrobca neposkytuje bezplatne na stiahnutie.
- Na switchoch musia ostať voľné min. 2 porty (servis, rezerva).
- Rezervné porty musia byť na manažovateľných switchoch deaktivované.

3.2 Routre

Dodávka routrov je možná len v prípade nevyhnutne nutnej hardvérovej segmentácie siete. Každý router musí obsahovať/podporovať statefull firewall, VRF, VRRP, BGP a OSPF routovacie protokoly. Použitie routrov musí byť v súlade s architektonickými princípmi OT siete MHTH a podlieha schváleniu zo strany MHTH.

3.3 Firewally

Dedikované centrálne OT FW a ich funkcionalita sú poskytované zo strany MHTH. Dodávka FW dodávateľom je zakázaná s výnimkou dedikovaných industriálnych FW a FW obsiahnutých v routroch (viď. Kapitola 3.2). Dodávané industriálne FW musia podporovať BGP a OSPF routovacie protokoly.

3.4 Prevodníky

Zariadenia na prevod signálu z optického vlákna na metalický kábel resp. „vice versa“ môžu byť použité len v technológii pri koncových zariadeniach. Pre prepojenia v rámci serverovne alebo vyhradenej miestnosti musí byť ukončenie optického sieťového kábla priamo na switchi. Pre ostatné prepojenia musí byť ukončenie optického sieťového kábla v opto paneli v rozvádzači pomocou optického SFP modulu, korešpondujúcim typom portu a optického kábla. Môžu sa použiť iba SFP moduly alebo DAC káble, ktoré sú podporované výrobcami na zariadeniach do ktorých sa budú pripájať. Prevodník musí byť v rozvádzači pevne uchytený.

3.5 Kabeláž

3.5.1 Všeobecné bezpečnostné požiadavky

Dodávateľ overí a poskytne dokumentáciu, že fyzické komunikačné kanály sú zabezpečené pred fyzickým narušením. (napr. štandardy bezpečnej kabeláže).

3.5.2 Optické sieťové káble

Dodávané optické sieťové káble musia spĺňať nasledovné požiadavky:
- Single-mode kábel musí byť typu OS1 pre vnútorné a OS2 pre vonkajšie použitie.

Realizačné riešenie návrhu optickej siete musí prejsť schvaľovacím procesom zo strany MHTH v rámci schvaľovania realizačnej dokumentácie.

3.5.3 Optické konektory

Na ukončenie optických káblov sú požadované SC/UPC konektory. Pre pripojenie MAN sietí je možné použiť aj SC/APC.

3.5.4 Metalické sieťové káble

Metalické sieťové káble musia byť kategórie Cat6 a vyššej.

3.6 Bezdrôtové siete

V rámci MHTH sa bezdrôtové lokálne siete v rámci aktuálne OT nepoužívajú. Vybudovanie novej bezdrôtovej siete v rámci dodávky je možné len v prípade, že nie je technicky možné zrealizovať fyzické pripojenie pomocou kábla.

3.7 WLAN

Nové infraštruktúry musia podporovať výhradne IP protokol verzie 4 alebo vyššej. Iné protokoly musia byť odfiltrované, aby sa do siete skupiny mohli dostať iba IP protokoly. Umiestnenie prístupových bodov a vysielací výkon musia byť zvolené tak, aby pokrývali iba želanú oblasť. Používanie bezdrôtových extenderov/bridge-ov je povolené iba ak sú počas rádiového prenosu implementované šifrovanie pripojenia a techniky overovania rovnakej úrovne zabezpečenia ako na access pointe, ku ktorému sa extender/bridge pripája. Bezdrôtové siete musia používať minimálne WPA3-Enterprise s autentifikáciou 802.1X napojenou na Active Directory. Použitie WPA2-Personal alebo nižších štandardov je zakázané. Preklad sieťových adries (NAT) nie je na prístupových bodoch povolený.

3.8 Bluetooth

Používanie Bluetooth na komunikáciu medzi jednotlivými časťami OT systémov je zakázané.

3.9 Konfigurácia

Konfiguráciu dodávaných komponentov sieťových zariadení bude vykonávať dodávateľ na základe schválenej dokumentácie. MHTH následne validuje nastavenú konfiguráciu. Konfigurácia musí zodpovedať bezpečnostným štandardom a všetkým požiadavkám zo strany MHTH.

3.10 Zapojenie

Zapojenie sieťovej infraštruktúry, vrátane kabeláže, bude vykonávať dodávateľ podľa platnej projektovej dokumentácie. V prípade zapájania v serverovniach alebo vyhradených miestnostiach MHTH, bude toto zapojenie vykonávané pod dohľadom zodpovednej osoby, ktorú určí MHTH.

3.11 Zonácia a segmentácia

Zonáciu a segmentáciu sietí navrhuje dodávateľ a schvaľuje MHTH. Dokumentácia k zonácii a segmentácii je súčasťou realizačnej dokumentácie a musí obsahovať sieťový diagram a typy a počty plánovaných pripojených zariadení. Riešenie musí byť navrhnuté s ohľadom na dobrú prax – PERA model a IEC 62443. Dodávateľ je povinný vykonať v rámci realizačnej dokumentácie formálne posúdenie rizík kybernetickej bezpečnosti pre navrhovanú zonáciu a segmentáciu (napr. podľa IEC 62443, vrátane priradenia cieľových bezpečnostných úrovní (SL-T) jednotlivým zónam a conduits a zostavenia CRS). Akákoľvek komunikácia so sieťami mimo lokálnej OT siete musí prebiehať cez DMZ/Proxy, terminovaná je cez FW, ktorý je určený zo strany MHTH na základe odsúhlasenej segmentácie a topológie siete.

3.11.1 VLAN

VLAN a ich adresné rozsahy sú určené zo strany MHTH podľa špecifických potrieb systému definovaných dodávateľom. VLAN sa poskytujú v najmenšom možnom rozsahu s minimálnymi rezervami. VLAN sú navrhované tak, aby sieť bola rozdelená na čo najmenšie logické celky, čo musí byť reflektované aj v požiadavkách od dodávateľa. Všetky VLAN sú ukončené na FW určenom zo strany MHTH a sú navzájom izolované. V prípade nutnosti komunikácie medzi rôznymi VLAN pozri kapitolu 3.11.3.

3.11.2 Komunikačná matica

Súčasťou realizačnej dokumentácie musí byť aj komunikačná matica obsahuje minimálne:

- Zdrojovú a cieľovú IP adresu.
- Konkrétne porty a služby ktoré majú byť otvorené.
- Smer komunikácie.
- Popis komunikácie vrátane uvedenia použitého protokolu a jeho prípadnej verzie.
- Zdôvodnenie nutnosti komunikácie.
- Klasifikáciu prenášaných dát v zmysle Prílohy č. 2 k vyhláške č. 227/2025 Z. z..

Komunikačná matica obsahuje komunikácie medzi všetkými zariadeniami (aj na rovnakom subnete). Komunikačnú maticu navrhuje dodávateľ v rámci prípravy realizačnej dokumentácie a schvaľuje ju MHTH v rámci procesu schvaľovania na základe platných bezpečnostných štandardov. Komunikačná matica musí obsahovať najmenší možný rozsah portov a IP adries nutný na správnu funkcionalitu systému. Vzor komunikačnej matice bude poskytnutý na vyžiadanie.
Komunikačná matica musí byť aktualizovaná pri každej zmene v sieťovej konfigurácii alebo pri pridávaní nových zariadení a v rámci záručnej doby prehodnocovaná najmenej raz ročne.

3.11.3 Prestupy medzi VLAN

Prestupy medzi rôznymi VLAN sú možné len na základe schválenej komunikačnej matice.

3.12 Komunikácia smerom von

Akákoľvek komunikácia smerom von zo siete MHTH, pokiaľ nie je výslovne požadovaná zo strany MHTH, je zakázaná. Procesná komunikácia medzi zariadeniami vo vlastníctve MHTH cez dedikované APN je povolená. Zmluva o poskytovaní komunikačných služieb vrátane APN musí byť uzatvorená priamo medzi MHTH a poskytovateľom služby (mobilným operátorom).

3.13 Komunikácia smerom dnu

Akákoľvek komunikácia smerom dnu do siete MHTH, pokiaľ nie je výslovne požadovaná zo strany MHTH, je zakázaná. Procesná komunikácia medzi zariadeniami vo vlastníctve MHTH cez dedikované APN je povolená. Zmluva o poskytovaní komunikačných služieb vrátane APN musí byť uzatvorená priamo medzi MHTH a poskytovateľom služby (mobilným operátorom).

3.14 Vzdialený prístup

Vzdialený prístup do siete MHTH je možný len na základe platnej zmluvy alebo v prípade plynutia doby záruky, avšak len v takom prípade, že takýto prístup je nevyhnutný na plnenie kontraktuálnych záväzkov zo strany dodávateľa. Spôsob a zabezpečenie takejto komunikácie určuje MHTH. Nutnou podmienkou je platná ZoBOaNP medzi dodávateľom a MHTH vrátane individuálneho informovaného súhlasu pristupujúcich osôb s platnými bezpečnostnými politikami MHTH. MHTH si vyhradzuje možnosť obmedzenia služby vzdialeného prístupu za účelom zabezpečenia bezpečnosti.
Vytváranie akýchkoľvek foriem vzdialeného prístupu bez schválenia zo strany MHTH je prísne zakázané. V prípade vytvárania vzdialeného prístupu do siete MHTH je povinná viacfaktorová autentifikácia (MFA).

3.15 NIDS

Architektúra siete a konfigurácia sieťových komponentov musí byť navrhnutá a realizovaná tak, aby zabezpečovala zber a prenos dát do NIDS určeného zo strany MHTH.

3.16 GSM modemy a pripojenia

Použitie a inštalácia akýchkoľvek GSM modemov mimo požiadaviek vyplývajúcich so zadania je zakázané. Povolené pripojenie je len prostredníctvom schválenej APN v správe MHTH.

4. Komunikačné rozhrania a protokoly

4.1 Všeobecné požiadavky

MHTH vyžaduje použitie zabezpečených protokolov na komunikáciu medzi jednotlivými systémami. Taktiež komunikácia medzi jednotlivými komponentami systému musí byť zabezpečená. Jedinou výnimkou je nutná komunikácia s existujúcimi systémami, ktoré nepodporujú použitie zabezpečených protokolov. To neplatí pre prípad keď daná komunikácia zabezpečuje prenos prihlasovacích údajov alebo informácii s vyššou klasifikáciou ako „interné“. V takom prípade je nutné realizovať zabezpečenie tohto spojenia vhodnými technickými prostriedkami.
Pre všetku šifrovanú komunikáciu je vyžadované použitie TLS verzie 1.2 a vyššie s tým, že pri TLS verzie 1.2 nesmú byť povolené šifrovacie algoritmy, ktoré sú v dobe odovzdania považované za nedostatočné. Použitie TLS verzie 1.3 je preferované. Použitie TLS 1.0 a 1.1 je zakázané. Použitie SSL všetkých verzií je zakázané

4.2 Komunikačná schéma

Súčasťou realizačnej dokumentácie musí byť aj bloková komunikačná schéma, ktorá je grafickou reprezentáciou komunikačnej matice.

4.3 Zoznam obmedzených protokolov

Služba/Protokol	**Popis**
FTP	Zakázané
Telnet	Zakázané
SMTP	Len pre interné e-mailové adresy za predpokladu použitia TLS s možnosťou overovania.
IMAP	Zakázané
POP3	Zakázané
HTTP	Zakázané. Potrebné nahradiť HTTPS
OPC DA	Zakázané. Potrebné nahradiť šifrovaným OPC UA.
MQTT	Len šifrované na porte 8883. Nešifrovaná komunikácia na porte 1883 je zakázaná.
SNMPv1/SNMPv2c	Zakázané.

5. Servery

5.1 Všeobecné požiadavky

Všetky servery v rámci dodávky musia byť virtualizované v rámci internej infraštruktúry MHTH. Automatické spúšťanie vymeniteľného média („Autorun") musí byť deaktivované. Na každom serveri musí byť implementované automatické uzamknutie interaktívnej relácie po preddefinovanej dobe nečinnosti (maximálne 10 minút). Uzamknutie je možné odstrániť iba po riadnom overení používateľa. Automatické uzamknutie musí byť konfigurovateľné/vypínateľné za použitia administrátorského oprávnenia. Nastavenie automatického uzamknutia nie je vyžadované (aj keď funkcionalita samotná musí byť dostupná) pre „Kioskové" riešenia a pre relácie určené pre operátorov v nepretržitej prevádzke.

Všetky servery musia umožňovať vzdialený manažment užívateľov (RADIUS, TACACS+, Active Directory). Konkrétnu inštanciu určí MHTH.

5.2 Sieťové rozhranie

Každý server môže disponovať, až na výnimky uvedené nižšie, len jedným sieťovým rozhraním. Ako komunikačný protokol je povolený len IP protokol verzie 4. Všetky ďalšie komunikačné protokoly musia byť vypnuté. Servery musia používať statické IP adresy. Na serveroch musí byť vypnuté smerovanie a nesmie byť zapnuté preposielanie paketov. Všetky nevyžadované sieťové rozhrania musia byť vypnuté a zablokované.

Zoznam výnimiek pre viac sieťových rozhraní:

- Zabezpečenie vysokej dostupnosti alebo vysokej priepustnosti.
- Zabezpečenie komunikácie pomocou industriálnych protokolov vyžadujúcich dedikované sieťové rozhranie (napr. Profinet).

5.3 Služby

Nainštalované a spustené služby môžu byť len tie, ktoré sú vyžadované pre prevádzku. Kontá služieb používané na tento účel musia mať pridelené minimálne oprávnenia tak aby služba mohla fungovať. Kontá služieb nesmú mať povolenia interaktívne sa prihlásiť na server. Kontá s lokálnymi alebo lokálnymi správcovskými oprávneniami (koreňové, správcovské, kontá správcov domén atď.) sa nesmú používať na spúšťanie aplikácií. Služby, ktoré vyžadujú overenie a požadujú aby boli meno a heslo uložené v nezašifrovanom texte sa nesmú používať a musia byť nahradené zabezpečenými službami. Protokoly sa musia používať v ich najbezpečnejších verziách v dobe nasadenia systému do prevádzky. Konfigurácia povolených služieb servera musí byť jasne a zrozumiteľne zdokumentovaná. Pred uvedením do prevádzky a po inštalácii všetkých aplikácií MHTH skontroluje a zdokumentuje, či neobsahujú nepovolené služby. V prípade, že budú takéto služby identifikované musí ich dodávateľ, ešte pred uvedením diela do prevádzky, na vlastné náklady odstrániť.

5.4 Súborový systém

Oprávnenia systému súborov sa musia nastaviť podľa princípu najnižších oprávnení alebo „need-to-know". Iba správcovia systému a systémové kontá môžu dostať právo na zapisovanie do súborov operačného systému servera. Údaje musia byť udržiavané štruktúrovaným spôsobom, pričom systémové súbory a údajové súbory musia byť uložené v oddelených oblastiach. Aplikácie musia byť nainštalované na inú partíciu ako je systémová, tak aby nemohlo dôjsť k jej neželanému zaplneniu.

5.5 Virtuálne servery

Virtuálne prostredie a inštaláciu virtuálneho servera zabezpečuje a vykonáva MHTH podľa špecifikácií dodaných dodávateľom.

Špecifikácia požiadaviek na virtuálny server v nasledovnom rozsahu musí byť už súčasťou ponuky v prílohe č.2 a následne aj všetkých stupňov dokumentácie:

- Typ a verzia operačného systému.
- Počet vCPU.
- Veľkosť RAM.
- Veľkosť úložiska podľa jednotlivých partícií.
- Počet sieťových rozhraní.
- Požadované výnimky pre AV a FW.
- Zoznam štandardných služieb a rolí servera, vrátane ich konfigurácie, ktoré majú byť nainštalované.
- Zoznam inštalovaného SW vrátane databázových serverov vrátane ich verzií.

V prípade nevyužitia požadovaných zdrojov si MHTH vyhradzuje právo na ich redukciu tak, aby bola stále zachovaná výkonnostná rezerva.

5.6 Fyzické servery

Nakoľko všetky servery musia byť virtualizované, dodávka fyzických serverov nie je povolená. V prípade špecializovaných HW riešení, ktoré nie je možné virtualizovať je potrebné zabezpečiť minimálne nasledovné požiadavky:

- HW komponenty musia byť vymeniteľné za prevádzky (hot-plug/hot-swap). V prípade zlyhania HW riešenia musí byť návrh bez jediného bodu zlyhania architektúry (no single point of failure architecture) pre kritické biznis oblasti.
- Systém musí byť ovládateľný na diaľku (vrátane studeného štartu / zastavenia)
- Pevné disky servera musia byť šifrované.
- Pri fyzických serveroch nesmie byť žiadna značka (tag) alebo označenie obsahujúce citlivé informácie (napr. informáciu o ILO mgmt.), ktoré nesmú byť viditeľné neoprávneným osobám.

6. Databázy a databázové servery

6.1 Všeobecné požiadavky

V prípade, že dodávaný systém potrebuje využívať databázy, tak tieto databázy musia byť umiestnené na databázovom serveri, ktorý určí MHTH. Použitie dedikovaného databázového servera je možné len v nasledovných prípadoch:

- Aplikačný SW vyžaduje pre bezproblémový beh inštaláciu na rovnaký server ako je databázový server a táto podmienka je uvádzaná výrobcom.
- Existuje technické obmedzenie, ktoré to neumožňuje, prípadne výrobca to nedovoľuje. V takom prípade musí byť musí byť obmedzenie riadne zdokumentované a preukázané počas tvorby realizačnej dokumentácie.

6.2 Databázy

V prípade, že súčasťou dodávky je aj databáza, ktorá môže bežať na externom databázovom serveri, tak jej finálne umiestnenie určí MHTH počas procesu prípravy realizačnej dokumentácie, nakoľko pre niektoré typy databázových serverov existujú centrálne riešenia, ktoré sú uprednostňované pred stand-alone riešeniami. Umiestnenie databázy bude ovplyvnené parametrami ako je požadovaná veľkosť a očakávaná záťaž read/write prístupov.

6.3 Databázové servery

Všetky databázové servery musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH. Všetky databázové servery sú spravidla virtualizované vo virtuálnom prostredí MHTH a inštalované na serverový operačný systém. Inštalácia databázového servera spolu s aplikačným SW na jeden server je povolená len v prípade, že ide o nutnú podmienku na bezproblémový beh aplikačného SW udávanú jeho výrobcom. Táto skutočnosť musí byť zdokumentovaná počas tvorby realizačnej dokumentácie a aj vo finálnej dokumentácii.
Špecifikácia požiadaviek na virtuálny databázový server v nasledovnom rozsahu musí byť súčasťou ponuky v prílohe č.2 a následne aj všetkých stupňov dokumentácie:

- Typ a verzia operačného systému.
- Počet vCPU.
- Veľkosť RAM.
- Veľkosť úložiska podľa jednotlivých partícií.
- Počet sieťových rozhraní.
- Požadované výnimky pre AV a FW.
- Zoznam štandardných služieb a rolí servera, vrátane ich konfigurácie, ktoré majú byť nainštalované.

Databázové servery, ktorých licenčný model by vyžadoval licencovanie celého virtuálneho prostredia, nie sú povolené.

7. Klientské stanice

7.1 Všeobecné požiadavky

Všetky klientské stanice musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH. Na každej klientskej stanici musí byť implementované automatické uzamknutie interaktívnej relácie po preddefinovanej dobe nečinnosti (maximálne 10 minút). Uzamknutie je možné odstrániť iba po riadnom overení používateľa. Automatické uzamknutie musí byť konfigurovateľné/vypínateľné za použitia administrátorského oprávnenia. Nastavenie automatického uzamknutia nie je vyžadované (aj keď funkcionalita samotná musí byť

dostupná) pre „Kioskové“ riešenia HMI (Kap. 9.5.2) a pre relácie určené pre operátorov v nepretržitej prevádzke.

7.2 Sieťové rozhranie

Každá klientská stanica môže disponovať (až na výnimky uvedené nižšie), len jedným sieťovým rozhraním. Ako komunikačný protokol je povolený len IP protokol verzie 4. Všetky ďalšie komunikačné protokoly musia byť vypnuté. Procesne kritické klientské stanice musia používať statické IP adresy. Na staniciach musí byť vypnuté smerovanie a nesmie byť zapnuté preposielanie paketov. Všetky nevyžadované sieťové rozhrania musia byť vypnuté.

Zoznam výnimiek:

- Zabezpečenie vysokej dostupnosti alebo vysokej priepustnosti.
- Zabezpečenie komunikácie pomocou industriálnych protokolov vyžadujúcich dedikované sieťové rozhranie (napr. Profinet).

7.3 Služby

Nainštalované a spustené služby môžu byť len tie, ktoré sú vyžadované pre prevádzku. Kontá služieb používané na tento účel musia mať pridelené minimálne oprávnenia tak aby služba mohla fungovať. Kontá služieb nesmú mať povolenia interaktívne sa prihlásiť na klientskú stanicu.
Kontá s lokálnymi alebo lokálnymi správcovskými oprávneniami (koreňové, správcovské, kontá správcov domén atď.) sa nesmú používať na spúšťanie aplikácií. Služby, ktoré vyžadujú overenie a požadujú aby boli meno a heslo uložené v nezašifrovanom texte sa nesmú používať a musia byť nahradené zabezpečenými službami.
Protokoly sa musia používať v ich najbezpečnejších verziách v dobe nasadenia systému do prevádzky. Konfigurácia povolených služieb klientskej stanice musí byť jasne a zrozumiteľne zdokumentovaná. Pred uvedením do prevádzky a po inštalácii všetkých aplikácií MHTH skontroluje a zdokumentuje, či neobsahujú nepovolené služby. V prípade, že budú takéto služby identifikované musí ich dodávateľ, ešte pred uvedením diela do prevádzky, na vlastné náklady odstrániť.

7.4 Súborový systém

Oprávnenia systému súborov sa musia nastaviť podľa princípu najnižších oprávnení alebo „need-to-know“. Iba správcovia systému a systémové kontá môžu dostať právo na zapisovanie do súborov operačného systému servera. Údaje musia byť udržiavané štruktúrovaným spôsobom, pričom systémové súbory a údajové súbory musia byť uložené v oddelených oblastiach.

7.5 Databázové servery

Inštalácia databázových serverov na klientské stanice je zakázaná. Výnimku tvoria len databázové servery, ktoré sú neoddeliteľnou súčasťou aplikačného SW a sú súčasťou inštalačného balíka (vyžadované výrobcom aplikačného SW). Takáto výnimka musí byť riadne zdokumentovaná už vo fáze tvorby realizačnej dokumentácie a preukázaná. Takáto inštalácia podlieha rovnakým pravidlám ako inštalácia na serverový operačný systém. Databázové servery musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH.

7.6 Operátorské stanice

Preferované riešenie vizualizácie riadiaceho systému pre operátorov na velíne je použitie virtuálneho terminálového servera. V prípade, že terminálový server nie je možné

z technického obmedzenia uvádzaného výrobcom použiť, tak pracovné stanice poskytujúce túto službu musia byť virtualizované.

7.7 Inžinierske stanice (EWS)

Všetky inžinierske/konfiguračné stanice musia byť sieťovo oddelené od zvyšku riadiaceho systému. Komunikácia smerom dnu a von musí byť obmedzená na nutné minimum.

7.8 Tenkí klienti

Pre vytvorenie nových operátorských pracovísk je nutné použiť tenkého/zero klienta, ktorý bude sprostredkovávať zabezpečenú užívateľskú reláciu s príslušným serverom/pracovnou stanicou pomocou protokolu RDP alebo HTTPS. Preferovaná konfigurácia tenkého/zero klienta je stiahnutie si konfigurácie pri štarte zo siete (PXE Boot).

Minimálne technické požiadavky:

- Podpora šifrovania SSL/TLS (TLS verzie 1.3 a vyššej).
- Možnosť blokovania periférnych zariadení USB.
- Možnosť zakázať funkciu pre WI-FI.
- Centralizovaná a vzdialená správa tenkých klientov schopných presadzovať bezpečnostné politiky (Device management).
- Možnosť opravy firmvéru vzdialeného tenkého klienta.

8. Automatizačné a ostatné zariadenia a komponenty

8.1 Všeobecné požiadavky

Manažment užívateľov v Active Directory pre tieto zariadenia je povinný v prípade, že to zariadenie umožňuje.

8.2 Sieťové rozhranie

Každé automatizačné či ostatné zariadenie alebo komponent môže disponovať (až na výnimky uvedené nižšie), len jedným sieťovým rozhraním. Ako komunikačný protokol je povolený len IP protokol verzie 4. Všetky ďalšie komunikačné protokoly musia byť vypnuté. Procesne kritické klientské stanice musia používať statické IP adresy. Na staniciach musí byť vypnuté smerovanie a nesmie byť zapnuté preposielanie paketov. Všetky nevyžadované sieťové rozhrania musia byť vypnuté.
Zoznam výnimiek:

- Zabezpečenie redundantného pripojenia fyzickej zariadenia alebo komponentu do siete. Takéto pripojenie je však možné len do jednej VLAN.
- Zabezpečenie aplikačnej redundancie pomocou dedikovanej VLAN. VLAN použitá na zabezpečenie redundancie medzi dvoma zariadeniami alebo komponentami musí byť úplne izolovaná.
- Zabezpečenie komunikácie pomocou industriálnych protokolov vyžadujúcich dedikované sieťové rozhranie (napr. Profinet).

8.3 Služby

Nainštalované a spustené služby môžu byť len tie, ktoré sú vyžadované pre prevádzku. Kontá služieb používané na tento účel musia mať pridelené minimálne oprávnenia tak aby služba mohla fungovať. Kontá služieb nesmú mať povolenia interaktívne sa prihlásiť na zariadenie.
Kontá s lokálnymi alebo správcovskými oprávneniami (koreňové, správcovské atď.) sa nesmú používať na spúšťanie aplikácií.

Služby, ktoré vyžadujú overenie a požadujú aby boli meno a heslo uložené v nezašifrovanom texte sa nesmú používať a musia byť nahradené zabezpečenými službami. Protokoly sa musia používať v ich najbezpečnejších verziách v dobe nasadenia systému do prevádzky.
Konfigurácia povolených služieb servera musí byť jasne a zrozumiteľne zdokumentovaná. Pred uvedením do prevádzky a po inštalácii všetkých aplikácií MHTH skontroluje a zdokumentuje, či neobsahujú nepovolené služby. V prípade, že budú takéto služby identifikované musí ich dodávateľ, ešte pred uvedením diela do prevádzky, na vlastné náklady odstrániť.

8.4 Súborový systém

Oprávnenia systému súborov sa musia nastaviť podľa princípu najnižších oprávnení alebo „need-to-know“. Iba správcovia systému a systémové kontá môžu dostať právo na zapisovanie do súborov operačného systému zariadenia. Údaje musia byť udržiavané štruktúrovaným spôsobom, pričom systémové súbory a údajové súbory musia byť uložené v oddelených oblastiach.

9. Software

9.1 Všeobecné požiadavky

Každý dodávaný SW musí byť legálny, v prípade open-source riešení zabezpečené legálne použitie pre komerčné účely, dodaný spolu s inštalačnými súbormi v použitej verzii, platnou dokumentáciou od výrobcu a podrobným návodom na inštaláciu vrátane potrebnej konfigurácie. Open-source licencia môže byť použitá len taká, ktorá nevyžaduje zverejnenie modifikovaného kódu verejnosti.
SW je dodávaný v poslednej stabilnej verzii. Preferovaná je verzia zabezpečujúca dlhodobú podporu (long term support).
Nutnou súčasťou realizačnej dokumentácie každého SW, ktorý spracováva alebo uchováva dáta je aj klasifikácia spracovávaných alebo uchovávaných dát v zmysle Prílohy č. 2 k vyhláške č. 227/2025 Z. z.

9.2 Podpora

Pre dodávaný SW, vrátane OS/Firmware, musí byť zabezpečená dostupnosť bezpečnostných záplat minimálne po dobu 5 rokov od dátumu prevzatia diela. V prípade, že životný cyklus SW je kratší ako 5 rokov, musí byť súčasťou dodávky aj bezplatná možnosť upgrade na takú verziu aby bolo zabezpečené plnenie tejto požiadavky.

9.3 Operačný systém a firmware

Preferovaná je dodávka operačného systému na báze MS Windows alebo bežných komerčných distribúcií na báze Unix/Linux. Pokiaľ sa na správu využíva webové rozhranie, musí byť toto rozhranie kompatibilné s aktuálne dostupnou verziou MS EDGE.

9.3.1 MS Windows

Všetky zariadenia s operačným systémom na báze MS Windows musia byť pripojené do Active Directory, ktoré určí MHTH. MS Windows musí byť dodaný v poslednej známej LTSC verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.3.2 Unix/Linux

Všetky zariadenia s operačným systémom na báze Unix/Linux musia umožňovať manažment užívateľov v Active Directory, ktorého inštanciu určí MHTH. Autentifikácia a autorizácia musí byť implementovaná bezpečnou cestou v súlade so zákonnými požiadavkami, normami a najlepšou praxou.. Unix/Linux musí byť dodaný v poslednej známej LTS verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.3.3 Iné OS

V prípade, že pre realizáciu dodávaného riešenia je potrebné použiť iný OS ako MS Windows alebo Unix/Linux (napríklad rôzne real-time OS a podobné špecializované typy OS), tak tento OS musí umožňovať manažment užívateľov v Active Directory, ktorého inštanciu určí MHTH. Autentifikácia a autorizácia musí byť implementovaná bezpečnou cestou v súlade so zákonnými požiadavkami, normami a najlepšou praxou. Operačný systém musí byť dodaný v poslednej známej stabilnej verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.3.4 Firmware

Dodávané komponenty obsahujúce firmware musia byť pri odovzdávaní diela aktualizované na aktuálnu stabilnú verziu firmware s aplikovanými bezpečnostnými záplatami. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.4 Aktualizácie OS a firmware

OS a firmware, vrátane BIOSu, musí umožňovať aplikáciu bezpečnostných a funkčných aktualizácií, patchov a service packov vydaných výrobcom, bez toho aby to negatívne ovplyvnilo záruku na dodané dielo aj v prípade, že tieto aktualizácie nevykoná dodávateľ. Možnosť použitia centrálnej správy aktualizácií je preferovaná.

9.5 Aplikačný SW

Aplikačný SW musí byť dodaný v poslednej stabilnej verzii, alebo prípadne v takej verzii, aby výrobca garantoval jeho podporu (minimálne vydávanie bezpečnostných záplat) po dobu minimálne 5 rokov od dátumu prevzatia diela. Medzi aplikačný SW sa radia aj databázové servery. Aplikačný SW musí umožňovať manažment užívateľov pomocou Active Directory, ktoré určí MHTH. Pokiaľ aplikačný SW využíva webové rozhranie, musí byť toto rozhranie kompatibilné s aktuálne dostupnou verziou MS EDGE.

9.5.1 Aktualizácie aplikačného SW

Aplikačný SW musí umožňovať aplikáciu bezpečnostných a funkčných aktualizácií, patchov a service packov vydaných výrobcom, bez toho aby to negatívne ovplyvnilo záruku na dodané dielo aj v prípade, že tieto aktualizácie nevykoná dodávateľ. Táto požiadavka sa týka aj patchovania OS na ktorom aplikačný SW beží a podporných služieb.

9.5.2 Human Machine Interface

Aplikačný SW poskytujúci funkcionalitu HMI alebo inej vizualizácie slúžiacej na sledovanie alebo riadenie výrobných procesov musí umožňovať tzv. „Kiosk mód“ kde prístup na operačný systém hosťujúci aplikačný SW je umožnený len oprávneným používateľom. Neoprávnení používatelia nesmú mať možnosť akokoľvek interagovať s OS alebo inými aplikáciami.

9.5.3 Kompatibilita s aktuálnou virtualizačnou platformou

Dodávateľ musí garantovať kompatibilitu dodávaného aplikačného SW s aktuálne používanou virtualizačnou platformou používaným v MHTH, tak aby bola umožnená virtualizácia. Informácia o type a verzii bude poskytnutá úspešnému uchádzačovi po podpise zmluvy.

9.6 Zákazkový software

Pre dodávaný softvér vyvíjaný na zákazku musí dodávateľ preukázať súlad vývojového procesu s IEC 62443. Dodávateľ je povinný využívať automatizované nástroje na monitorovanie známych zraniteľností (CVE) pre všetky komponenty uvedené v SBOM.

9.7 SBOM

Dodávateľ poskytne pre každý dodaný produkt s digitálnymi prvkami (softvér, firmvér, embedded systémy) Software Bill of Materials (SBOM) – formálny záznam obsahujúci detaily a vzťahy dodávateľského reťazca komponentov obsiahnutých v softvérových prvkoch produktu. SBOM musí byť kryptograficky podpísaný dodávateľom (napr. pomocou Sigstore/cosign alebo PGP alebo KEP/ZEP). Podpis slúži ako referenčný stav pre overenie integrity počas celej doby záruky.
SBOM musí byť dodaný najneskôr pri Factory Acceptance Test (FAT) a aktualizovaný pri každej významnej zmene softvéru alebo firmvéru.

SBOM musí byť v bežne používanom, strojovo čitateľnom formáte. Akceptované formáty:

- SPDX (ISO/IEC 5962) vo formáte JSON alebo XML.
- CycloneDX vo formáte JSON alebo XML.

Formát PDF alebo neštruktúrovaný text nie je akceptovaný.

SBOM musí obsahovať minimálne nasledujúce údaje pre každý komponent:

- Názov komponentu.
- Verzia komponentu.
- Dodávateľ / autor komponentu.
- Jednoznačný identifikátor (napr. CPE, PURL).
- Vzťahy medzi komponentmi (dependency relationships).
- Licenčné informácie (SPDX license identifier).
- Hash / kontrolný súčet (pre overenie integrity).

SBOM musí pokrývať minimálne všetky top-level závislosti produktu. Rekurzívne rozlíšenie závislostí sa odporúča minimálne po prvý externý komponent mimo rozsah dodávky.

SBOM musí zahŕňať všetky softvérové komponenty vrátane firmvéru, RTOS (real-time operating system), bootloaderov a embedded knižníc použitých v dodaných zariadeniach.
V prípade použitia open-source komponentov musí dodávateľ identifikovať ich verzie a monitorovať známe zraniteľnosti.

Dodávateľ musí udržiavať a aktualizovať SBOM počas celého trvania záruky/servisnej zmluvy a informovať MHTH o:

- Každom softvérovom alebo firmvérovom update/patchi.
- Každej zmene závislostí alebo komponentov tretích strán.
- Objavení novej zraniteľnosti ovplyvňujúcej komponenty v SBOM.

Aktualizovaný SBOM musí byť poskytnutý najneskôr do 15 dní od zmeny.

10. Hardware

10.1 Zabezpečenie podpory

Dodávateľ je povinný dodať hardvér v takej verzii, pre ktorú výrobca ku dňu odovzdania do prevádzky garantuje:

- Dostupnosť bezpečnostných aktualizácií a technickej podpory po dobu minimálne 5 rokov od dátumu odovzdania do prevádzky, a
- Dostupnosť kompatibilných náhradných dielov po dobu minimálne 5 rokov od dátumu prevzatia diela.

Dodávaný hardvér musí byť v aktívnej fáze podpory (mainstream/active support). Nie je prípustné dodať model, pre ktorý výrobca ku dňu odovzdania do prevádzky oznámil ukončenie podpory alebo dostupnosti (end-of-sale, end-of-support), a to ani v prípade, že zostatok záruky výrobcu by formálne pokrýval požadovanú 5-ročnú lehotu.
Dodávateľ predloží pri FAT písomné potvrdenie výrobcu alebo úradný produktový lifecycle dokument preukazujúci splnenie tejto podmienky.

10.2 Preukázanie originality

Pri dodávke kritických hardvérových komponentov je dodávateľ povinný poskytnúť mechanizmus preukázania ich originality, aby sa zabránilo nasadeniu falošných alebo klonovaných zariadení. Pre všetky HW komponenty musí byť dodaná informácia o zabezpečení distribučného kanála voči neoprávnenej manipulácii. Pri dodávke každého kritického hardvérového komponentu je dodávateľ povinný predložiť Certificate of Authenticity (COA) vydaný priamo výrobcom komponentu alebo jeho oprávneným zástupcom. COA musí jednoznačne identifikovať komponent (výrobca, model, sériové číslo alebo výrobná šarža) a musí byť predložený najneskôr pri FAT.

10.3 Zabezpečenie distribučného kanála

Pre všetky hardvérové komponenty (kritické aj nekritické) je dodávateľ povinný predložiť písomné vyhlásenie distribútora potvrdzujúce, že:

- Dodávka pochádza z autorizovaného distribučného kanála výrobcu.
- Komponenty neboli počas distribúcie vystavené neoprávnenej manipulácii.
- Distribútor je oprávneným partnerom výrobcu ku dňu dodávky.

Vyhlásenie musí byť podpísané oprávneným zástupcom distribútora a predložené spolu s dodacou dokumentáciou.

10.4 Fyzická integrita

Dodávateľ je povinný dodať komponenty v originálnom, neporušenom obale výrobcu s neporušenými tamper-evident prvkami. Porušenie obalu alebo absencia tamper-evident prvkov zakladá právo MHTH odmietnuť prevzatie príslušného komponentu.

10.5 HBOM

Dodávateľ poskytne pre každý dodaný IT/OT systém Hardware Bill of Materials (HBOM) – štrukturovaný súpis všetkých hardvérových komponentov, modulov a integrovaných obvodov (vrátane ASIC, FPGA, sieťových rozhraní).
HBOM musí byť dodaný najneskôr pri FAT a aktualizovaný pri akejkoľvek zmene hardvérového dizajnu alebo výmene komponentov.

HBOM musí obsahovať minimálne:

- Výrobca, model a produktové číslo každého HW komponentu.
- Sériové číslo alebo iný jednoznačný identifikátor (lot/batch identifikátor).
- Verzia / revízia hardvéru.
- Krajina pôvodu (ak je známa).
- Verzia firmvéru nainštalovaného na komponente.
- Sieťové rozhrania a komunikačné adresy.
- Informácia o konci podpory (end-of-life / end-of-support dátum).
- Referenčný identifikátor komponentu pre krížovú referenciu s SBOM (napr. PURL, CPE)

HBOM musí byť v štrukturovanom, strojovo čitateľnom formáte. Akceptované formáty:

- CycloneDX HBOM (JSON alebo XML).
- Štrukturovaný text (CSV/JSON) kompatibilný s interným systémom správy aktív organizácie.

Formát PDF alebo neštrukturovaný text nie je akceptovaný.

Dodávateľ musí udržiavať a aktualizovať HBOM počas trvania záruky/servisnej zmluvy a informovať MHTH o:

- Zmenách v HW dizajne alebo nahradeniach komponentov.
- Ukončení podpory (end-of-life - EOL) akejkoľvek HW časti (najneskôr do 30 dní od oznámenia výrobcom komponentu, pokiaľ je EOL dodávateľovi vopred známy, upozornenie minimálne 12 mesiacov vopred).
- Objavení bezpečnostných zraniteľností vzťahujúcich sa na HW komponenty.

Aktualizovaný HBOM musí byť poskytnutý najneskôr do 15 dní od zmeny.

10.6 Periférie

Dodávané zariadenia musia umožňovať zabezpečenie dátových rozhraní voči neautorizovanému použitiu. Všetky nepoužívané USB a sieťové porty musia byť softvérovo alebo hardvérovo zabezpečené voči neautorizovanému použitiu.

11. Licencie a podpora

Súčasťou dodávky akéhokoľvek SW alebo HW musia byť aj všetky potrebné licencie (vrátane licencií potrebných na zálohovanie). V prípade časovo obmedzenej licencie je nutné dodať licenciu platnú minimálne po dobu 5 rokov od odovzdania do prevádzky. Všetky špecifické SW alebo HW licencie musia byť registrované na MHTH na konto, ktoré určí MHTH.

V prípade, že je zo strany výrobcu požadovaná platená licenčná/technická podpora (alebo iná forma platenej podpory/služby) pre dostupnosť podpory zo strany výrobcu alebo aktualizácií (vrátane bezpečnostných záplat a funkčných opráv), tak musí byť súčasťou dodávky aj takáto licenčná/technická podpora (alebo iná forma platenej podpory/služby) platná na obdobie minimálne 5 rokov od odovzdania do prevádzky.

12. Cloudové služby a cudzia infraštruktúra

Použitie cloudových služieb, alebo infraštruktúry mimo vlastníctva MHTH je pre OT systémy a technológie zakázané. Výnimku tvoria telekomunikačné služby na prenos dát, ktoré sú

poskytované licencovanými operátormi. Používanie takýchto služieb je možné len za predpokladu, že už existuje priama zmluva medzi MHTH a poskytovateľom služby.

13. Antivírus a zabezpečenie

13.1 Všeobecné požiadavky

Všetky dodávané systémy musia byť v čo najvyššej možnej miere zabezpečené voči neoprávneným zásahom a zneužitiu. Všetky systémy musia mať nainštalovaný antivírusový SW alebo EDR/XDR používaný MHTH. Informácia o type a verzii bude poskytnutá úspešnému uchádzačovi po podpise zmluvy alebo uchádzačovi, ktorý podpíše zmluvu o mlčanlivosti.

13.2 Antivírus, XDR/EDR

V prípade, že pre správny beh dodávaného SW sú nutné výnimky na skenovanie v rámci AV nastavení, tak je potrebné tieto výnimky uviesť už počas tvorby realizačnej dokumentácie. Licencie pre AV zabezpečuje MHTH.

13.3 Lokálny Firewall

Lokálny firewall musí zostať aktivovaný a musí byť nastavený v zmysle schválenej komunikačnej matice (viď Kap. 3.11.2). Pre zariadenia s operačným systémom na báze MS Windows bude použitý integrovaný firewall a pre zariadenia s operačným systémom na báze Unix/Linux je nutné použiť nftables alebo iptables alebo firewalld.

13.4 Minimálne požiadavky na hardening

Dodávateľ je povinný zamedziť možnosti neoprávnenej manipulácie. Dodávateľ odstráni všetky softvérové komponenty, ktoré nie sú potrebné na prevádzku a/alebo údržbu Obstaraného produktu/systému. Ak odstránenie nie je technicky možné, dodávateľ deaktivuje softvér, ktorý nie je potrebný na prevádzku a/alebo údržbu obstaraného produktu. Toto odstránenie nesmie brániť primárnej funkcii obstarávaného produktu. Ak softvér, ktorý nie je potrebný, nie je možné odstrániť alebo deaktivovať, dodávateľ zdokumentuje konkrétne vysvetlenie a poskytne odporúčania na zmiernenie rizika a/alebo špecifické technické zdôvodnenie. Dodávateľ poskytne dokumentáciu o tom, čo je odstránené a/alebo deaktivované. Softvér, ktorý sa má odstrániť a/alebo deaktivovať, zahŕňa, ale nie je obmedzený na:

- Gaming software a ovládače zariadení pre komponenty produktu kt. neboli obstarané/dodané.
- Messaging services (napr. e-mail, instant messenger, zdieľanie súborov typu peer-to-peer).
- Zdrojový kód alebo knižnice, kt. nie sú potrebné na prevádzkové účely.
- Softvérové kompilátory pre programovacie jazyky, ktoré sa nepoužívajú na prevádzkové účely.
- Nepoužívané a nepotrebné sieťové a komunikačné protokoly (DHCP, TELNET, IPv6 atď.).
- Nepoužívané administratívne nástroje, funkcie diagnostiky, správy siete a správy systému.
- Zálohy súborov, databáz a programov používaných iba počas vývoja systému.
- Všetky nepoužité dáta a konfiguračné súbory.
- Pre OS Windows je potrebné použiť NTLM verzie 2 a vyššej.

13.5 Prevencia neoprávnených prístupov

Dodávateľ pred odovzdaním diela overí a zabezpečí, že pre obstaraný produkt nie sú nainštalované neoprávnené pripojenia alebo logovacie zariadenia (napr. keyloggery, trójske kone s vzdialeným prístupom, kamery, mikrofóny, špionážne zariadenia atď.). Overenie je potrebné zdokumentovať a vydokladovať.

13.6 Odstránenie nepoužívaných prístupov

Pred spustením akceptačných testov diela/systému, dodávateľ odstráni alebo deaktivuje všetky účty, ktoré nie sú potrebné pre bežnú prácu alebo údržbu IT/OT systémov alebo produktov.

14. Zálohovanie

Podmienky a požiadavky na dostupnosť sú určené v Zadaní. Na ich základe dodávateľ navrhne plán záloh a údržby všetkých častí dodávky, ktorý bude súčasťou realizačnej dokumentácie a následne aj dokumentácie skutkového stavu. Na základe požiadaviek na dostupnosť a kontinuitu dodávateľ navrhne aj DRP, ktorý bude súčasťou realizačnej dokumentácie a následne aj dokumentácie skutkového stavu. DRP musí byť v rámci dodávky aj riadne otestovaná aby sa potvrdila jej správnosť a vykonateľnosť v zmysle stanovených parametrov RTO a RPO.
Pred uvedením do prevádzky, musí dodávateľ poskytnúť MHTH aktuálne zálohy všetkých komponentov v elektronickej podobe.

14.1 Servery

Zálohovanie serverov bude vykonávané centrálnou službou v kompetencii MHTH. Pred uvedením do prevádzky je dodávateľ povinný v súčinnosti s MHTH validovať funkčnosť automatických záloh. V prípade, že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky. V prípade, že požadované RTO a RPO je nižšie ako zabezpečuje štandardne MHTH, tak súčasťou dodávky musí byť aj potrebný nastroj na zálohovanie.

14.2 Klientské stanice

Pred uvedením do prevádzky, musí dodávateľ poskytnúť MHTH aktuálne zálohy všetkých klientských staníc v elektronickej podobe v takom formáte aký bude odsúhlasený zo strany MHTH. V prípade, že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky.

14.3 Databázy

V prípade, že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky.

14.4 Sieťové komponenty

Zálohovanie konfigurácie sieťových komponentov je v zodpovednosti MHTH. Dodávateľ je povinný zabezpečiť nutnú súčinnosť. V prípade, že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky.

14.5 Automatizačné a ostatné zariadenia a komponenty

Automatizačné a ostatné zariadenia a komponenty ako sú napríklad PLC, konfigurovateľné frekvenčné meniče a podobne, alebo zariadenia a komponenty (HA a SW) nespadajúce do ani jednej vyššie uvedených kategórií. musia umožňovať zálohovanie konfigurácie. V prípade,

že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky.

15. Časová synchronizácia

Všetky zariadenia a systémy sa musia vedieť synchronizovať pomocou protokolu NTP. Zdroj času určí MHTH.

16. Kryptografia

Kryptografické prostriedky sa používajú na zabezpečenie:

- Dôvernosti údajov.
- Integrity údajov.
- Autentizácie odosielateľa (digitálny podpis).
- Nepopierateľnosti vykonanej činnosti (non-repudiation).

Kryptografické prostriedky sa používajú najmä na ochranu citlivých údajov:

- Prenášaných cez nezabezpečené prostredie (napr. internetová alebo e-mailová komunikácia).
- Uložených na lokálnych diskoch (koncové stanice, zdieľané úložiská údajov a pod.).
- Prenosných zariadeniach (notebooky, tablety, smartfóny a pod.).
- Prenosných médiách (CD, DVD, USB a pod.).

Použitý šifrovací algoritmus musí byť vhodne zvolený tak, aby zabezpečil dostatočnú úroveň ochrany údajov. Úroveň zabezpečenia údajov vyplýva z ich citlivosti, resp. klasifikačného stupňa.

Výber použitej kryptografickej metódy závisí najmä na:

- Posúdení rizík spojených s ochranou aktíva.
- Požadovanej úrovni ochrany aktíva.
- Technických možnostiach prevádzkovaných systémov.
- Ekonomickej náročnosti opatrenia vzhľadom na hodnotu chráneného aktíva.

Minimálne požiadavky kryptografickej ochrany aktív podniku sú definované nasledovne:

- Šifrovací algoritmus symetrického šifrovania: AES-256.
- Šifrovací algoritmus asymetrického šifrovania: RSA.
- Dĺžka kryptografického kľúča RSA: najmenej 2048 bitov.
- Exspirácia kryptografického kľúča: 1 rok.
- Funkcia používaná na hashovanie: SHA-256.

Nasadenie kryptografických prostriedkov vykonáva:

- Zamestnanec dodávateľa v prípade externe vyvíjaného alebo nasadzovaného IS alebo RS.
- Špecialista/administrátor úseku informačných technológií MHTH v prípade interných aplikácií alebo nástrojov.

Správu nasadených kryptografických prostriedkov vykonáva špecialista/administrátor úseku informačných technológií MHTH. MHTH požaduje dodržiavať min. Odporúčania dobrej praxe v oblasti kryptografických prostriedkov, uvedených tu:

https://nukib.gov.cz/download/uredni_deska/Minimalni_pozadavky_v4_FINAL.pdf

17. Bezpečnostné logovanie a monitoring

Systémy musia byť konfigurované tak, aby logovali všetky bezpečnostne relevantné udalosti definované nižšie. Systémy, ktoré logujú udalosti, sa musia synchronizovať prostredníctvom vopred dohodnutého referenčného času. Logy musia byť chránené pred neoprávneným prístupom a modifikáciou. Ak logy obsahujú klasifikované informácie, potom môže byť zabezpečený prístup len osobám disponujúcim potrebnou autorizáciou vlastníka informácie.

17.1 Logovanie udalostí

Logovacie zdroje musia byť nakonfigurované tak, aby bolo možné zaznamenávať minimálne nasledujúce bezpečnostne relevantné udalosti:

- Úspešné a neúspešné pokusy o prihlásenia (pre administrátorské aj bežné účty).
- Vytvorenie, zmena, zablokovanie, odblokovanie a vymazanie účtov a rolí.
- Zmeny hesiel a certifikátov.
- Zmeny oprávnení (napr. používateľské práva, oprávnenia k objektom, členstvo v skupinách).
- Spúšťanie a ukončovanie procesov.
- Zmeny systémového času a časovej služby.
- Zmeny v nastaveniach logovania (najme jeho deaktivácia).
- Všetky ostatné udalosti, ktoré osoby zodpovedné za logovacie mechanizmy považujú za dôležité.
- Systémové chyby a zlyhania.
- Užívateľské akcie (platí hlavne pre SCADA a HMI).

Okrem bezpečnostne relevantných udalostí musí byť zaznamenaná aj činnosť samotného logovacieho mechanizmu. Všetky logy by mali byť zapisované do logovacích mechanizmov operačného systému, akými sú Windows Event Log, Unix/Linux syslog, prípadne iné ekvivalentné služby špecifické pre danú platformu.
Logy musia byť uchovávané minimálne 24 mesiacov alebo do ukončenia nasledujúceho auditu kybernetickej bezpečnosti podľa zákona 69/2018 Z. z., podľa toho čo je dlhšie. Integrita logov musí byť chránená pred neautorizovanou modifikáciou (napr. použitím WORM úložiska, digitálneho podpisu alebo presmerovaním do centrálneho SIEM).

17.1.1 Štruktúra logovacích hlásení

Logovacie hlásenia musia obsahovať nasledovné údaje o udalostiach:

- Časovú značku (synchronizovanú).
- Identifikáciu používateľa alebo procesu.
- Zdroj udalosti (napr. IP adresa alebo hostname).
- Výsledok operácie (úspech/neúspech).
- Opis udalosti.

Odporúča sa zahrnúť aj:

- Úroveň závažnosti (severity).
- Kategória (napr. informácia, chyba, výstraha, ...).

Logovacie hlásenia nesmú obsahovať heslá, ich „hashe“ alebo akúkoľvek autentifikačné tajomstvá.

17.1.2 Sledovanie logovacích hlásení

Dodávateľ je povinný v rámci projektu spolupracovať s Oddelením kybernetickej bezpečnosti na napojení systému na nástroje pre kontinuálne monitorovanie hrozieb (napr. SIEM). Logovacie záznamy musia byť odosielané do centrálnych systémov spracovania logov v rámci organizácie MHTH. Spôsob realizácie musí byť popísaný v RD.

17.2 Centrálny monitoring

Servery, klientské stanice a sieťová infraštruktúra musia byť napojené na nástroj centrálneho monitoringu používaného v MHTH. Informácia o požiadavkách na spôsob pripojenia bude poskytnutá úspešnému uchádzačovi po podpise zmluvy.

17.2.1 Servery

Každý server bude monitorovaný príslušným klientom centrálneho monitoringu. MHTH poskytne základnú šablónu monitorovaných parametrov, ktorú dodávateľ upraví tak aby klient vedel vyhodnotiť všetky neštandardné stavy indikujúce poruchu alebo stavy smerujúce k poruche.

17.2.2 Klientské stanice

Každá klientská stanica bude monitorovaná príslušným klientom centrálneho monitoringu. MHTH poskytne základnú šablónu monitorovaných parametrov, ktorú dodávateľ upraví tak aby klient vedel vyhodnotiť všetky neštandardne stavy indikujúce poruchu alebo stavy smerujúce k poruche.

17.2.3 Sieťové komponenty

Všetky switche, routre a prípadne iné konfigurovateľné komponenty musia byť napojené na centrálny monitoring pomocou protokolu SNMP V3.

17.2.4 Ostatné komponenty

Pokiaľ niektorý z dodávaných systémových komponentov nie je uvedený v predchádzajúcich podkapitolách a umožňuje napojenie na centrálny monitoring pomocou protokolu SNMP V3, tak takýto komponent musí byť napojený tiež.

18. Access and identity management

18.1 Všeobecné požiadavky

Všetky prístupy do OS a aplikačného SW musia byť riešené cez RADIUS, TACACS+ alebo Active Directory), ktoré určí MHTH. Vytváranie nových lokálnych servisných prístupov s oprávnením lokálneho administrátora (OS Windows) je v prípade použitia AD zakázané. Ak je v prípade použitia AD, nutné servisné konto s oprávnením lokálneho administrátora, tak je nutné použiť Group Managed Service Accounts (gMSAs). Vytváranie užívateľských lokálnych prístupov je prípade použitia AD zakázané. Prístupy do všetkých systémov a zariadení v rámci dodávky musia byť odovzdané MHTH. Heslá do zabudovaných lokálnych prístupov musia byť pred odovzdaním diela zmenené tak, aby ich jediným držiteľom bola zodpovedná osoba v MHTH. Vyžaduje sa princíp RBAC (Role-based access control), teda vytvárania rolí na základe špecifických požiadaviek na prístupové oprávnenia pre každú rolu zvlášť tak, aby každý užívateľ mal iba ten level oprávnení potrebných na vykonanie vyžadovaných pracovných činností.
Dodávateľ je povinný hlásiť akékoľvek prezradenie alebo kompromitáciu účtov a ich hesiel, aby mohli byť následne zmenené.

Dodávateľ musí riadne zadokumentovať všetky generické a servisné účty a ich zoznam odovzdať MHTH.

18.2 Vytváranie používateľov a skupín v AD

Všetci používatelia a role v AD sú vytvárane zástupcom MHTH na základe požiadaviek dodaných zo strany dodávateľa, ktoré musia zodpovedať bezpečnostným štandardom MHTH.

18.3 Autentifikácia používateľov

Autentifikácia používateľov dodávaných systémov musí byť vykonávaná centrálne za pomoci Active Directory, ktoré určí MHTH. Všetky systémy ktoré to umožňujú, a na ktorých sa vyžaduje manažment používateľov musia, pre tento účel, používať Active Directory.
V prípade výpadku Active Directory, musia mať zariadenia dostupný aj lokálny účet výhradne pre zabezpečenie kontinuity a možnosti obsluhy zariadenia.
Použitie lokálnych účtov je zakázane, mimo vyššie uvedeného prípadu.

18.4 Autorizácia používateľov

Prístup k informáciám, ktoré dodávaný systém spracováva alebo ukladá musí byť nevyhnutne podmienený autentifikáciou a autorizáciou. Pre autorizáciu k dátam v rámci systému platia nasledovné pravidlá. Autorizácia používateľov je vykonávaná na základe ich role, ktorú na danom systéme plnia. Tieto role sa delia na systémové a aplikačné role.

Minimálne delenie rolí je nasledovné:

- **Administrátor operačného systému**

  Takýto účet je autorizovaný na vykonávanie administratívnych zásahov do systému. Takýto administrátor nesmie mať oprávnenie spravovať, resp. používať aplikácie, ktoré môžu byť prevádzkované na systéme.

- **Používateľ operačného systému**

  Táto rola môže byť pridelená používateľovi, ktorý má oprávnenie spravovať súbory a nastavenia aplikácie na úrovni operačného systému. Tento používateľ nesmie mať administrátorské oprávnenia na systém.

- **Systémový používateľ**

  Táto rola môže byť pridelená používateľovi, na základe ktorého sa v rámci operačného systému alebo v rámci aplikácie spúšťa služba, ktorá vyžaduje neinteraktívnu identifikáciu a autentifikáciu používateľa. Tento používateľ môže mať oprávnenie na vykonávanie administratívnych alebo aplikačných úloh, ktoré sa vykonávajú automaticky. Tento používateľ nesmie byť použitý na interaktívne prihlásenie do systému alebo aplikácie.

- **Aplikačný administrátor**

  Táto rola môže byť pridelená používateľovi, ktorý má oprávnenie spravovať aplikáciu. Takýto používateľ nesmie mať oprávnenie na bežné používane aplikácie. Taktiež nesmie mať oprávnenie na správu používateľov, rolí a oprávnení v rámci aplikácie.

- **Aplikačný administrátor oprávnení**

  Táto rola môže byť pridelená používateľovi, ktorý má v rámci aplikácie oprávnenie spravovať používateľské účty a role, prideľovať a odoberať oprávnenia pre

používateľov a role. Takýto používateľ nesmie mať oprávnenie na bežné používane aplikácie.

- **Aplikačný používateľ**

  Táto rola môže byť pridelená používateľovi, ktorý aplikáciu používa na účely, pre ktoré bola aplikácia vytvorená. Tento používateľ nesmie mať oprávnenia na správu aplikácie a ani na správu používateľov.

Manažment jednotlivých rolí je na základe členstva užívateľských účtov v skupinách Active Directory.

18.5 Zvýšenie oprávnení (Privilege escalation)

Dodávateľ zabezpečí ochranu pred neoprávneným zvýšením oprávnení.

18.6 Prednastavené účty

Dodávateľ zmení predvolené nastavenia účtu na nastavenia špecifické pre organizáciu (napr. dĺžka, zložitosť, história a konfigurácie) alebo zabezpečí podporu organizácie pri týchto zmenách. Dodávateľ nezverejní zmenené informácie o účte. Dodávateľ poskytne organizácii nové informácie o účte prostredníctvom chráneného mechanizmu.

18.7 Ochrana prístupových údajov

Produkt v nasadenej konfigurácii nesmie prenášať ani zdieľať používateľské poverenia v nešifrovanej forme (plaintext). Dodávateľ nesmie uchovávať poverenia používateľov v otvorenom texte. Tieto musia byť chránené pomocou moderných kryptografických metód (napr. silný hashing so soľou). Akákoľvek výnimka z tohto pravidla musí byť podložená analýzou rizík a výsledkami penetračného testovania, ktoré potvrdia adekvátnu kompenzačnú ochranu. Výnimka musí byť časovo obmedzená a podlieha prehodnoteniu pri každej hlavnej verzii produktu alebo každej významnej zmene vo verzií produktu. Dodávateľ povolí výhradne komunikačné protokoly zabezpečujúce šifrovanie prenosu prihlasovacích údajov (napr. SSH, TLS v aktuálne podporovaných verziách).

18.8 Továrenské prístupové údaje (Default credentials) a „hardcoded“ poverenia

Produkt nesmie byť dodaný s aktívnymi továrenskými (default) prihlasovacími údajmi. Všetky default účty musia byť pred odovzdaním buď deaktivované, alebo musia mať zmenené prihlasovacie údaje na hodnoty unikátne pre dané nasadenie.
Je zakázané uchovávať akékoľvek poverenia (heslá, API kľúče, tokeny, certifikáty súkromných kľúčov) priamo v zdrojovom kóde, konfiguračných súboroch verzionovaných v repozitári alebo v SBOM. Poverenia musia byť spravované prostredníctvom dedikovaného mechanizmu správy tajomstiev (secrets management).

18.9 Manažment hesiel

Dodávané produkty, ktorý má konfigurovateľnú správu hesla účtu musí umožňovať minimálne nasledovné:

- Zmeny hesiel (vrátane predvolených hesiel).
- Výber dĺžky hesla.
- Frekvencia zmeny hesla.
- Nastavenie zložitosti požadovaného hesla.
- Počet pokusov o prihlásenie pred uzamknutím .
- Odhlásenie z neaktívnej relácie.
- Zamknutie obrazovky podľa aplikácie.

- Odvodenie hesla od používateľského mena.
- Odmietnutie opakovaného alebo použitia rovnakého hesla.

18.10 Súbežné prihlásenia (Concurrent logins)

Pokiaľ nie je v zadaní stanovené inak, dodávateľ nepovolí viacnásobné súbežné prihlásenie pomocou rovnakých autentifikačných poverení (generické účty), neumožní aplikáciám uchovávať prihlasovacie údaje medzi jednotlivými reláciami, neposkytne akúkoľvek funkciu automatického dopĺňania počas prihlasovania alebo neumožní anonymné prihlásenie/prihlásenie hosťa.

18.11 Odovzdanie prístupov

Dodávateľ zdokumentuje a poskytne MHTH všetky prístupy k SW a HW zariadeniam, vrátane servisných/núdzových, rovnako ku všetkým dodaným IT/OT komponentom. V rámci dokumentácie musí byť jasne identifikovateľné na aký účel príslušný prístup slúži, kto je vlastníkom, akého systému alebo jeho časti sa týka a aký je rozsah oprávnení.
Dodávateľ nesmie mať po odovzdaní projektu prístup k týmto heslám bez výslovného súhlasu zo strany MHTH.

19. Ochrana dát a ich sanitizácia

Dodávateľ je povinný vykonať bezpečné a trvalé vymazanie citlivých dát (konfigurácie, heslá, IP adresy) z hardvéru a softvéru, ktorý dodávateľ mení z dôvodu poruchy, odstraňuje zo systému alebo si ho berie na diagnostiku mimo MHTH. Bezpečná sanitácia musí byť vykonaná podľa uznávaných štandardov (napr. NIST SP 800-88). Použitá metóda a výsledok musia byť zdokumentované a odovzdané MHTH.

20. Riadenie zmien

Akákoľvek zmena v konfigurácii, softvéri, hardvéri alebo sieťovej architektúre dodávaného systému po schválení realizačnej dokumentácie musí podliehať formálnemu procesu riadenia zmien schválenému zo strany MHTH. Každá zmena musí byť pred schválením posúdená z hľadiska bezpečnostného dopadu a zdokumentovaná. Pred nasadením do produkčnej prevádzky aj otestovaná.

21. Posudzovanie zraniteľností

Dodávateľ je povinný pred odovzdaním diela vykonať skenovanie zraniteľností všetkých dodávaných komponentov a výsledky poskytnúť MHTH. Metóda a spôsob vykonania skenovania zraniteľností musí byť dopredu odsúhlasená zo strany MHTH a vykonáva sa výlučne za súčinnosti zo strany MHTH. Skenovanie zraniteľností musí byť navrhnuté tak, aby nedošlo k negatívnemu ovplyvneniu bežiacej prevádzky.
Počas záručnej doby je dodávateľ povinný monitorovať známe zraniteľnosti komponentov (aj podľa obsahu v SBOM) a informovať MHTH najneskôr do 48 hodín od ich zverejnenia.

22. Požiadavky na RIS

22.1 Všeobecné požiadavky na RIS

Systém pozostáva zo štandardného hardvéru, systémového softvéru a firmvéru výrobcu, ktorý musí byť nakonfigurovaný tak, aby spĺňal všetky opísané požiadavky. Architektúra systému sa skladá z technológie založenej na normách pre funkčnú a kybernetickú bezpečnosť. Ak je v zadaní požiadavka na vypracovanie HAZOP, ktorý určí potrebu SIL pre niektoré z obvodov, musia byť tieto požiadavky na SIL dodržané v celom rozsahu(vstupné merania, logic solver, výstupné akčné členy). Nasadenie a zmeny v SIS musí byť vykonané len osobou s príslušným oprávnením podľa normy STN EN 61508/ 61511.

22.2 Požiadavky na SIS

V prípade dodávky SIS alebo zásahu do neho je potrebné dodržiavať nasledovné požiadavky:

- Fyzický/Softvérový zámok pre konfiguráciu (Configuration mode): SIS musí obsahovať hardvérové/softvérové rozhranie (napr. kľúčový prepínač, špeciálne heslo), ktorým sa dá fyzicky/softvérovo uzamknúť a zakázať konfiguračný režim. Musí byť zabezpečené, že kľúč/heslo sú prístupné len povereným osobám.
- Je prísne zakázaný vzdialený prístupu na SIS EWS: Pri inžinierskych staniciach SIS (SIS EWS) nie je dovolené využívať metódy vzdialeného prístupu (napr. cez RDP, VNC). Prístup na SIS EWS, do konfiguračného módu resp. do konfiguračného SW, môže mať len dedikovaný užívateľ.
- SIS EWS musí byť samostatná stanica. Pri existujúcich zdieľaných EWS je nutné zabezpečiť oddelenie užívateľov a ich prístup ku častiam SIS od ostatných aplikácií.
- Prísne zakázané bezdrôtové pripojenia. Zákaz používania akýchkoľvek bezdrôtových zariadení ako integrálnej súčasti ochranných funkcií SIS.

22.3 Požiadavky na dizajn RIS

Pri návrhu dizajnu RIS musia byť zohľadnené najmä, avšak nielen, podmienky obsiahnuté v nasledovných podkapitolách.

22.4 Výkon, odozva a veľkosť RIS

Odozva systému je čas medzi zmenou na vstupnej veličine, reakciou riadiaceho algoritmu jeho a zmenou na výstupnom zariadení. Odozva systému pozostáva z nasledujúcich krokov:

- Konverzia analógového signálu(4-20 mA) na digitálny a jeho zápis na I/O kartu.
- Spracovanie vstupného digitálneho signálu v CPU.
- Spracovanie riadiaceho algoritmu.
- Spracovanie signálu z riadiaceho algoritmu a jeho zápis na I/O kartu.
- Konverzia digitálneho signálu na analógový signál(4-20 mA).

Maximálny čas odozvy vychádza z technologických požiadaviek podľa potrieb bezpečného a kontinuálneho riadenia procesov, prípadne požiadaviek dodávateľa subsystémov. Ak nie je určené inak, maximálna odozva pre rôzne typy signálov je nasledovná:

Meranie tlaku kvapalín	0,5s
Meranie tlak plynov	0,5s
Merane diferenčného tlaku	0,5s
Meranie prietoku	0,5s
Meranie teploty	1s
Meranie hladiny	1s
Iné merania	1s
Špeciálne rýchle riadenie	0,25s

Spracovanie digitálnych meraní 0,5s

Spracovanie signálov z komunikačných kariet musí byť v čo najkratšom cykle, ktoré dané zariadenia umožňujú tak, aby nedochádzalo ku zbytočným oneskoreniam.

22.5 Rezervy a rozšíriteľnosť systému

RIS musí byť dodaný s minimálnymi rezervami 10% a rozšíriteľnosťou o minimálne 20%. Tieto hodnoty sa týkajú voľných nodov, IO slot, IO kariet, výkonu elektrických zdrojov, terminálových svoriek, miesta v káblových žľabov, miesta v kabinetoch, výkonu na CPU a komunikačných kartách. V prípade úprav na existujúcom systéme, nesmie klesnúť rezerva a rozšíriteľnosť o vyššie uvedené hodnoty. V prípade že by k tomu došlo je nutné vopred žiadať schválenie od objednávateľa.

22.6 Single loop integrity

Single loop integrity znamená princíp, že chyba jedného elementu nemôže ovplyvniť celý systém, resp. viac ako jednu riadiacu slučku. Pri votingoch – výbere napr. 2oo3 a iných, musia byť tieto merania oddelené nielen na úrovni kariet ale podľa možnosti aj nodov. V prípade ak sa používa jeden element vo viacerých systémoch/slučkách, musí byť navrhnutá a použitá redundancia napr. CPU, IO karty, napájacie zdroje, operátorské stanice.

22.7 Požiadavky na vstupno výstupné karty – IO

Dodaný RIS musí podporovať modulárne použitie rôznych IO kariet(AI, DI, AO, DO, Serial atď.) v redundantnej alebo single konfigurácií. V prípade ovládania záskokových zariadení(napr. čerpadlo A/B), je možné použiť single IO kartu, avšak zariadenia nemôžu byť nakonfigurované na jeden IO karte. Analógové IO karty musia podporovať HART, Foundation Fieldbus komunikáciu. Vstupná analógová karta musí umožňovať zapojenie aktívneho(4 vodič) aj pasívneho (2 vodič) vysielača.

Systém musí umožňovať výmenu karty za chodu tzv. hot swapping. Výmena karty musí prebehnúť bez odpojenia/zapojenia jednotlivých vodičov na IO kartu. Karty musia byť odolné voči skratu a statickým výbojom.

Interná zbernica systému musí byť galvanicky oddelená. Tak isto jednotlivé IO body musia byť na karte samostatne oddelené, tak aby nedošlo pri zlyhaní jedného kanálu, ku zlyhaniu celej karty. V prípade použitia externého oddeľovača medzi poľom a systémom, je požadované použitie oddeľovača len na jedno pripojenie. V prípade nutnosti použitia multi kanálového oddeľovača, nesmú byť naň zapojené signály z jednej slučky.

IO karty musia umožňovať diagnostiku jednotlivých kanálov a sledovať stavy jednotlivých obvodov a to minimálne:

- Analógový vstup – meranie mimo rozsah, detekcia odpojenej vstupnej slučky.
- Analógový výstup – detekcia odpojenej výstupnej slučky.
- Digitálne signály – detekcia prerušeného vedenia a detekcia skratu.

S ohľadom na zabezpečenie maximálnej dostupnosti musia byť vstupno-výstupné signály, ktorých poruchou môže dôjsť ku výpadkom v riadenom procese, zdvojené(redundantné) a úrovni IO modulov. Obslužné signály nemusia byť redundantné.

22.8 Historizácia

Dodávaný riadiaci systém musí umožňovať konfiguráciu rozsahu a periódy vzorkovania historizovaných hodnôt. Historizovanie musí byť nastavené tak, aby boli historizované minimálne všetky procesné hodnoty, povely, udalosti a alarmy súvisiace s riadeným procesom

s takou vzorkovacou periódou, ktorá umožní bezproblémovú spätnú analýzu prevádzkových stavov a porúch..

22.9 Ochrana pred stratou dát

Dodávaný riadiaci systém musí poskytovať mechanizmus proti strate dát (napríklad "Store & Forward") pre procesné dáta, udalosti a alarmy, ktorý zabezpečí zachovanie dát pri dočasnej nedostupnosti komunikácie medzi procesnou úrovňou systému a historianom (historickou DB) a ich následné doručenie do historianu (historickej DB) bez straty významu a bez porušenia poradia (zachovanie časových značiek).

22.10 Vizualizácia a grafické rozhranie

Pri tvorbe grafického rozhrania musí dodávateľ dodržiavať základné požiadavky, lokálne požiadavky, tak ako aj zohľadňovať požiadavky vyplývajúce z IEC 63303.

Základné požiadavky na grafické rozhranie:

- Rozloženie zobrazenia musí byť konzistentné s akceptovaným mentálnym modelom procesu.
- Kde je to možné, tok procesu má byť zľava doprava, plyny smerom nahor a kvapaliny smerom nadol. Rozloženie nemusí nevyhnutne kopírovať usporiadanie P&ID, ak sa mentálny model operátora líši.
- Grafika nesmie obsahovať zbytočné detaily a vizuálny balast. Žiadne samoúčelné animácie (otáčajúce sa turbíny, horiaci oheň). Animácie sa majú používať iba na zvýraznenie abnormálnych situácií. Zariadenia majú byť zobrazené jednoduchými 2D symbolmi s nízkym kontrastom. Farba pozadia musí byť neutrálna.
- Na každom zobrazení musí byť prítomná trvalo viditeľná navigačná lišta a banner so súhrnom alarmov, ktoré umožnia operátorovi prejsť na ľubovoľnú úroveň hierarchie a zobraziť počet/prioritu aktívnych alarmov bez opustenia aktuálnej obrazovky.
- Jasné, sýte farby (ako červená, oranžová, žltá, azúrová) musia byť vyhradené výlučne pre alarmy a abnormálne stavy. Tieto farby sa nesmú používať na žiadny iný účel.
- Procesné hodnoty (PV), žiadané hodnoty (SP) a regulačné veličiny (CV) musia byť škálované v konzistentných inžinierskych jednotkách. Inžinierske jednotky musia byť zobrazené pri každej hodnote, jednoznačné a konzistentné na všetkých obrazovkách. Taktiež musí byť zabezpečená aj jasná a konzistentná indikácia kvality zobrazovanej hodnoty.
- Procesné hodnoty majú byť znázornené v kontexte, nie ako izolované čísla. Analógové indikátory (stĺpcové grafy, ukazovatele) majú zobrazovať aktuálnu hodnotu vzhľadom na normálny prevádzkový rozsah, alarmové limity a prahy blokovaní (interlock). Normálny/požadovaný rozsah má byť vizuálne vyznačený (napr. svetlo tieňovanou zónou).
- Vstupné polia musia byť obmedzené na platné prevádzkové rozsahy hodnôt. Vstupné polia musia byť vizuálne odlíšiteľné od statického textu a živých dát (podľa konvencií farieb). Pre akcie s významnými dôsledkami musia byť vyžadované potvrdzovacie dialógy, aby sa predišlo neúmyselnej aktivácii.
- Systém musí generovať alarm pri fyzikálne nemožných stavoch vstupno/výstupných premenných (napr. súčasne aktívne párové signály OTVOR+ZATVOR) a pri odchýlkach od očakávaných časov pri fyzickej činnosti (prekročená doba behu a pod.) alebo pri neočakávanej nečinnosti procesu.
- Alarmy na stanoviskách s permanentnou obsluhou musia byť signalizované aj zvukovo aj vizuálne dostatočne veľkou zmenou tak, aby sa upútala pozornosť operátora
- Procesné hodnoty musia byť zobrazované a povely vykonávané takmer v reálnom čase. Obnovovacie frekvencie zobrazenia dát a rýchlosť načítavania stránok musia byť primerané dynamike monitorovaného procesu.

23. Požiadavky na zabezpečenie a kontrolu prostredia

23.1 Všeobecné požiadavky

V prípade budovania nových objektov alebo rekonštrukcie existujúcich musí byť v rámci dodávky zabezpečené plnenie bezpečnostných opatrení pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení podľa §20 ods. 2 písm. o) Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v rozsahu opatrení podľa prílohy č. 1 k Vyhláške Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach.
Všetky elektronické systémy zabezpečujúce tieto požiadavky musia byť kompatibilné s existujúcou infraštruktúrou v rámci MHTH a musí byť v rámci dodávky zabezpečená ich integrácia do nej.

23.2 Špecifické požiadavky na fyzické zabezpečenie rozvádzačov

Všetky rozvádzače a skrine, v ktorých je umiestnená akákoľvek časť OT systému alebo infraštruktúry musia byť uzamykateľné a musia mať implementovanú signalizáciu otvorenia dverí, tak aby bolo možné monitorovať každý prístup. Tato informácia musí byť zaslaná ako aj do lokálneho riadiaceho systému, tak aj do nadradeného riadiaceho systému ako alarm.

23.3 Špecifické požiadavky na kontrolu prostredia rozvádzačov

Všetky rozvádzače a skrine, v ktorých je umiestnená akákoľvek časť OT systému alebo infraštruktúry musia mať zabezpečené sledovanie a udržiavane prevádzkovej teploty v rozmedzí 15-35°C počas celoročnej prevádzky pokiaľ nie je výrobcom zariadenia požadovaný prísnejší interval teplôt. Hodnota teploty musí byť prenášaná ako aj do lokálneho riadiaceho systému, tak aj do nadradeného riadiaceho systému. Informácia o porušení želaného teplotného rozsahu, poruche senzora a prípadnej poruche chladiaceho/ohrievacieho zariadenia (ak je použité) musí byť zaslaná ako aj do lokálneho riadiaceho systému, tak aj do nadradeného riadiaceho systému ako alarm.
Taktiež musí byť zabezpečená ochrana proti vnikaniu prachu do uzatvoreného rozvádzača alebo skrine napríklad použitím vhodných filtrov a tesnení.

23.4 Požiadavky na monitorovacie kamerové systémy (MKS)

Minimálne požiadavky na kamery:

- Vysoké rozlíšenie obrazu (minimálne 4 Mpx).
- Prenos cez sieťové pripojenie (IP kamery).
- Funkciu zmeny polohy snímania (natáčania) kamier.
- Umožňujú šifrovaný prenos údajov, ktorý musí byť implementovaný.
- Infračervený dosvit min 50 metrov.
- POE.
- Obrazové funkcie ako WDR 120 dB, 3DNR, BLC, HLC.
- Krytie IP 67.
- Integrovane funkcie (IVS, People counting, Face detection).
- Odolnosť voči teplotám, prípadne vibráciám podľa miesta umiestnenia.
- Pokročilé detekčné funkcie (SMD - rozlíšenie ľudských tvarov a tvarov vozidiel, Tripwire alebo Area intrusion- možnosť ohraničenia perimetra, priestoru, pričom vyšle upozoznenie len v prípade nežiadúceho pohybu osôb alebo vozidiel v ohraničenom priestore).

Minimálne požiadavky na NVR:

- Redundantné IP sieťové rozhranie.

- Počet kanálov podľa zadania. V prípade že nie je definovaný tak minimálne pokrývajúci všetky kamery v rámci dodávky + 10% rezerva.
- Záznam / živý obraz / prehrávanie v 4K.
- Podporované formáty H.264 /H.265 / MLPEG.
- záznam max. do 1024 Mbps.
- Maximálne rozlíšenie 32 Mpx na kameru a viac
- Podpora ONVIF, podpora IP PTZ.
- Videoanalytické funkcie.
- Veľkosť úložiska podľa zadania. V prípade, že nie je definované, tak veľkosť úložiska musí byť taká, aby pojala záznam na 15 dní pre maximálny počet pripojiteľných kamier (aj v prípade, že nie sú pripojene všetky porty).
- Funkcionalita automatického mazania záznamov po určitom počte dní pričom počet je užívateľsky konfigurovateľný.
- Raid 0 / 1 / 5 / 6 / 10 (podpora HDD Hot-swap).
- Časová synchronizácia pomocou externého NTP.

Pripojenie kamier:
Access switch (prístupový prepínač), do ktorého sú kamery pripojené musí byť do zvyšku siete pripojený redundantným spôsobom. Napájanie kamier musí byť realizované pomocou POE.

Umiestnenie NVR:
NVR musí byť umiestnené v serverovni/počítačovej miestnosti, ktorú určí MHTH.

Funkčné rozdelenie NVR
NVR pre kamery zabezpečujúce primárne funkcionalitu fyzickej objektovej bezpečnosti a NVR pre kamery zabezpečujúce primárne dohľad výrobného procesu musia byť fyzicky oddelené.

Integrovateľnosť:
Všetky kamery a záznamové zariadene (NVR) MKS musia byť integrovateľné do Integračného bezpečnostného systému (IBS) MHTH.
Kamery a záznamové zariadenie (NVR) MKS, ktoré sú používané na dohľad výrobného procesu musia byť integrovateľné aj do HMI pre operátorov technológie.
Integrovateľnosťou sa rozumie okrem kompatibility hardvéru aj potrebný rozsah licencií.

24. Požiadavky na rozvádzače a MaR

24.1 Všeobecné požiadavky na rozvádzače

Rozvádzače pre RIS a elektro zariadenia musia byť v modulárnom vyhotovení, ktoré umožňuje doplnenie výbavy rozvádzača. Dvere rozvádzača musia byť uzamykateľné zámkom s kľúčom a vo dverách je inštalovaný držiak na dokumentáciu. Rozvádzače musia byť označené bezpečnostnými nálepkami(blesk, zákaz hasenia vodou a penovými prístrojmi atď.). Krytie rozvádzačov je minimálne IP54.
Vstup káblov do rozvádzačov je zdola. Káble musia byť pri prestupe pevne uchytené príchytkami SONAP. Prestupy káblov do rozvádzača musia byť utesnené voči prachu a vlhkosti a certifikovanými protipožiarnymi zábranami. To neplatí ak je rozvádzač umiestnený na zvýšenej podlahe v elektrickej rozvodni a celá miestnosť je jeden požiarny úsek.

Pripojenie poľovej inštrumentácie do RIS bude riešené cez samostatný Marshalling kabinet. Do tohto kabinetu budú privedené poľové káble a jednotlivé žily budú vyvedené na terminálové svorky. Z pripojovacích svoriek bude urobený prepoj na pripojovacie dosky podľa typu signálu t.j. AI/AO/DI/DO. Pripojovacie dosky budú napojené na IO karty systémovými káblami. Káble do priemeru 1,5mm^2 budú pripojené pomocou pružinových svoriek. Káble nad 1,5mm^2 vrátane, budú pripojené pomocou skrutkovej svorkovnice. Vodič a káble ktoré sú pod napätím nad 24V budú tiež pripojené pomocou skrutkovej svorkovnice.

24.2 Požiadavky na uloženie a oddelenie káblov

Pri ukladaní a zapájaní káblov je nutné oddelenie jednotlivých káblov kvôli možnému ovplyvňovaniu elektromagnetickými silami. Káble s rôznymi napätiami a prúdovými sústavami sa musia ukladať do samostatných skupín, ktoré sú oddelené od seba medzerami. Medzi káblami s napätím do 1 kV a nad 1 kV, musí byť aspoň 25 centimetrová medzera, ak už nie sú oddelené mechanicky pevnou priehradkou s výškou presahujúcou obidve skupiny káblov, ktorá odolá elektrickému oblúku. Pri ukladaní káblov v zvislej rovine musia byť káble s vyšším napätím nad káblami s nižším napätím. High voltage cables (vysokonapäťové káble), Low voltage cables (nízkonapäťové káble), Control and Signalling cables (ovládacie a signalizačné káble) a ďalšie Pri kábloch (High voltage - vysokonapäťové káble, Low voltage - nízkonapäťové káble, Control and Signalling - ovládacie a signalizačné káble), ktoré musia byť pri trasovaní káblov v lávkach oddelené prepážkami, je nutné dbať na to, aby sa medzi sebou tieto skupiny káblov neprehadzovali. Pri rekonštrukcii trás elektrických rozvodov, je nutné počítať s rezervou pre uloženie oznamovacích rozvodov, rozvodov počítačových sietí a pod. a aj možnosťou nového spôsobu prevádzky objektu s ohľadom na predpokladané priestory s možnosťou samostatného merania a riadenia každého subjektu.

24.3 Požiadavky na značenie káblov

Značenie káblov sa vykonáva prostredníctvom štítkov. Štítky musia byť v trvácnom a odolnom vyhotovení a musia byť pevne pripevnené ku káblu takým spôsobom, aby pri bežnej manipulácii s káblom štítok neodpadol alebo sa neposunul. Štítky musia mať strojový popis. Ručné značenie nie je dovolené. Štítky budú umiestnené na obidvoch koncoch kábla, v miestach odbočenia, v miestach prestupu a priebežne po celej trase kábla každých 20m. Štítky vo vnútornom prostredí, bez pôsobenia iných vonkajších vplyvov, budú vložené do plastové púzdra, ktoré sa umiestni na kábel. Štítky použité vo vonkajšom prostredí, musia byť v nerezovom prevedení a popis musí byť v nezmazateľnom prevedení (gravírovanie).
Štítok musí obsahovať nasledovné údaje:

- Číslo kábla.
- Odkiaľ kábel vedie.
- Kam kábel smeruje.

Označenie jednotlivých žíl kábla sa vykonáva primárne pomocou zmršťovacej popisovacej bužírky. Popis pozostáva z nasledovných údajov:

- Označenie zariadenia.
- Odkiaľ kábel vedie.
- Kam kábel smeruje.

Všetky označenia káblov a žíl musia byť uložené tak, aby boli čitateľné bez manipulácie s káblom. Iné spôsoby označovania a použitých štítkov musia byť schválené pred realizáciou.

25. Požiadavky na realizačnú dokumentáciu

Požiadavky na RD majú zabezpečovať, že projekt bude realizovaný podľa plánov a Zadania a bude spĺňať požiadavky na efektívnosť, bezpečnosť a monitorovanie počas jeho prevádzky a zároveň bude spĺňať požiadavky na kybernetickú bezpečnosť už vo fáze projektovania. RD v závislosti na rozsahu projektu a dodávky, musí obsahovať a zahrňovať vydokladovanie plnenia požiadaviek vyplývajúcich z tohto dokumentu a nižšie uvedené body:

- **Systémová architektúra RIS**

Dokumentácia musí obsahovať kompletný prehľad o systémovej architektúre vrátane všetkých komponentov, ich vzájomných prepojení a funkcionalít. Zmeny alebo doplnenia musia byť označené, aby sa uľahčila identifikácia nových alebo upravených častí systému.

- **Opis dodaného projektu alebo systému z hľadiska HW, IO, napájania, zberníc, operátorských pracovísk, inžinierskej stanice a pod.**

  Dokumentácia musí obsahovať popis hardvérovej konfigurácie zahrnujúci všetky zariadenia, vstupy/výstupy (IO), komunikačné zbernice, napájanie, architektúru operátorských a inžinierskych staníc ktoré sa používajú na monitorovanie a ovládanie systému vrátane verzií použitého firmwaru, softwaru a licencií.

- **Metódy integrácie subsystémov, použité komunikačné zbernice, pripojenie na NRS, resp. integrácia do NRS**

  Dokumentácia musí obsahovať spôsob integrácie rôznych subsystémov do hlavného systému, vrátane použitých komunikačných zberníc (napr. Profibus, Modbus, Ethernet/IP) a ich pripojenia k nadradenému riadiacemu systému NRS.

- **Konvencia názvoslovia tagov**

  Dokumentácia musí obsahovať popis jednotného a jasného názvoslovia pre tagy (identifikátory signálov), ktoré sa používajú v celom systéme, aby sa zaručila konzistencia a zrozumiteľnosť. Preferovaný systém značenia je KKS.

- **Hierarchické rozdelenie aplikácie na jednotlivé procesné celky, jednotky, zariadenia atď.**

  Dokumentácia musí obsahovať hierarchiu systémových komponentov (procesy, jednotky, zariadenia, linky) s dôrazom na logickú organizáciu a prepojenia medzi rôznymi úrovňami systému.

- **Popis použitých typicalov pre regulačné slučky a monitorovanie signálov**

  Dokumentácia musí obsahovať opisy bežne používaných typicalov (typických nastavení a konfigurácií) regulačných slučiek a monitorovacích funkcií, ktoré sa využívajú v rámci systému.

- **Popis použitých typicalov pre ovládanie zariadení (klapky, čerpadlá, motory atď.)**

  Dokumentácia musí obsahovať opis použitých typicalov pre ovládanie zariadení ako sú klapky, čerpadlá, motory a ďalšie, vrátane základných ovládacích a bezpečnostných stratégií.

- **Návrhy grafických obrazoviek vrátane popisu jednotlivých symbolov, farebných označení, pop up grafické prvkov atď.**

  Dokumentácia musí obsahovať zhrnutie návrhu grafických obrazoviek pre operátorské pracoviská, vrátane popisu symbolov, farieb, ktoré sa používajú na indikáciu rôznych stavov (napr. zelené/červené indikácie pre normálny/stresový stav), a špecifických požiadaviek na pop-up grafické prvky.

- **Zoznam alokovaných I/O**

  Dokumentácia musí obsahovať zoznam všetkých alokovaných I/O bodov (vstupy a výstupy) pre daný systém, s podrobnými informáciami o tom, ktoré zariadenia sú pripojené k jednotlivým I/O(rozsahy, inžienierske jednotky, alarmové a blokovacie hodnoty, binárne stavy a pod.).

- **Očakávané zaťaženie riadiacich jednotiek a komunikačných liniek**

  Dokumentácia musí obsahovať odhadovanú záťaž, ktorú bude systém vyžadovať od riadiacich jednotiek a komunikačných liniek, aby sa zabezpečila ich optimálna výkonnosť a aby sa predišlo preťaženiu.

- **Spôsob alarmovania**

  Dokumentácia musí obsahovať detailný popis spôsobu správy alarmov, vrátane konfigurácie varovaní a ich priorít, spôsobu notifikácie operátorov a možných reakcií na rôzne druhy alarmov.

- **Spôsob historizácie**

  Dokumentácia musí obsahovať metódy, ktoré sa používajú na zaznamenávanie historických údajov a signálov z procesu pre neskoršiu analýzu alebo optimalizáciu. Taktiež musí obsahovať zoznam historizovaných premenných vrátane periodicity a ukladaných metadát.

- **Zoznam regulačných a riadiacich slučiek**

  Dokumentácia musí obsahovať zoznam všetkých regulačných, riadiacich a blokačných slučiek implementovaných v systéme, vrátane parametrov a nastavení.

- **Zoznam ostatných slučiek**

  Dokumentácia musí obsahovať zoznam ostatných slučiek alebo funkcií, ktoré sa používajú, ale nie sú priamo súčasťou regulácie, riadenia alebo blokovania.

- **Opis špeciálnych algoritmov (napr. sekvenčné riadenie, blokády, netypické riešenia)**

  Dokumentácia musí obsahovať popis špeciálnych algoritmov, ako je sekvenčné riadenie, ktoré sa používajú na riadenie procesov a vyžadujú netypické alebo zložité logiky.

- **Opis logiky a výpočtov**

  Dokumentácia musí obsahovať popis matematických modelov, výpočtových metód a logických schém, ktoré sa používajú na riadenie systému.

- **Opis nových alebo neštandardných funkcií operátora**

  Dokumentácia musí obsahovať popis nových alebo špecifických funkcií, ktoré sú určené na zjednodušenie práce operátora alebo na zvýšenie flexibility systému.

- **Spôsob reportovania**

  Dokumentácia musí obsahovať popis spôsobu generovania správ, vrátane formátu, rozdelenia údajov a spôsobu distribúcie týchto správ pre ďalšie spracovanie alebo archiváciu.

- **Komunikačná matica**

  Dokumentácia musí obsahovať komunikačnú maticu v zmysle tohto dokumentu.

- **Bezpečnostné opatrenia a manažment prístupov**

  Dokumentácia musí obsahovať všetky bezpečnostné opatrenia a nastavenia vyplývajúce z požiadaviek MHTH vrátane nastavenia všetkých prístupov a ich manažmentu.

- **Popis spôsobu aktualizácie systémových komponentov**

  Dokumentácia musí obsahovať popis procesu aktualizácie jednotlivých komponentov dodávaného OT systému spolu s informáciou o spôsobe získavania aktualizácií

- **Popis zálohovania a obnovy systémových komponentov**

  Návrh konceptu a postupu zálohovania a obnovy jednotlivých komponentov dodávaného OT systému tak, aby boli splnené požiadavky na dostupnosť a rýchlosť obnovy zo strany MHTH a právnych noriem, ktorým MHTH podlieha. Zároveň sú zahrnuté bezpečnostné opatrenia pri zaobchádzaní so zálohovanými údajmi.

- **Disaster recovery plan (DRP).**

  Dokumentácia musí obsahovať DRP, testovacie scenáre a protokoly ktoré musia overiť správnosť DRP. Počas testovania DRP sa overí čas obnovy RTO a objem stratených dát RPO.

- **Dokumentácia výrobcu (Vendor dokumentácia)**

  Kompletná vendor dokumentácia na všetky dodané súčasti OT systému. V prípade že vendor dokumentácia nie je v slovenskom alebo českom jazyku, môže byť dodaná v anglickom jazyku.

26. Požiadavky na dokumentáciu skutkového vyhotovenia

DSV obsahuje všetky zaznamenané zmeny oproti ktoré nastali počas FAT a SAT. Všetky návody a manuály musia byť dodané v slovenskom jazyku. DSV obsahuje naviac oproti DRS nasledovné dokumenty:

- **Printout projektu z riadiaceho systému**

  Printout musí byť v elektronickej forme, v ktorej sa dá textovo vyhľadávať. Printout musí obsahovať kompletný export nastavení a konfigurácie systému, vrátane printoutu blokačných, regulačných, sekvenčných logík, nastavenich IO bodov, sériové čísla a verzie firmwaru všetkých modulov.

- **Návod na používanie a obsluhu RS**

  Návod na obsluhu obsahuje popis bezpečného a správneho používania riadiaceho systému počas bežnej prevádzky. Sú v ňom uvedené pokyny na prihlásenie do systému, ovládanie používateľského rozhrania (napr. dotykovej obrazovky, tlačidiel alebo HMI panelu), kontrolu aktuálneho stavu zariadení a sledovanie prevádzkových hlásení a upozornení. Návod ďalej obsahuje postupy na nastavovanie prevádzkových parametrov, prepínanie režimov (automatický/manuálny), zobrazovanie trendov, historických údajov a alarmových záznamov.

- **Návod na ovládanie technologického zariadenia**

  Návod na obsluhu technologických zariadení, ako sú čerpadlá, kotly, klapky a regulačné prvky, obsahuje pokyny na bezpečné a správne používanie týchto zariadení počas ich prevádzky. Uvádzajú sa v ňom postupy na spustenie a zastavenie zariadenia, kontrolu funkčnosti a sledovanie prevádzkových stavov. Popísané sú možnosti nastavovania prevádzkových parametrov, prepínania režimov (napr. ručný/automatický), reakcie na hlásenia alebo poruchové stavy a zobrazovanie údajov na ovládacích paneloch. Návod kladie dôraz na dodržiavanie bezpečnostných opatrení a správne zaobchádzanie s jednotlivými prvkami zariadení v súlade s rozsahom oprávnení obsluhy.

- **Manuál na servis a údržbu riadiaceho systému (RS)**

  Manuál na servis a údržbu riadiaceho systému obsahuje pokyny na vykonávanie pravidelnej a preventívnej údržby, diagnostiky a riešenia porúch systému. Uvádzajú sa v ňom odporúčané intervaly údržby, kontrolné body a úkony, ktoré majú byť vykonané na zabezpečenie spoľahlivej a bezpečnej prevádzky systému. Popísané sú postupy pri výmene komponentov, aktualizácii softvéru a identifikácia a odstránenie bežných chýb. Manuál kladie dôraz na dodržiavanie bezpečnostných zásad, správnu dokumentáciu zásahov a oprávnenie personálu vykonávajúceho servisné úkony.

- **Manuál na zálohovanie a obnovu riadiaceho systému (RS)**

  Manuál na zálohovanie a obnovu riadiaceho systému obsahuje podrobné pokyny na pravidelné zálohovanie konfigurácií, nastavení a dôležitých dát systému. Uvádzajú sa v ňom postupy na vykonávanie zálohovania softvérových a systémových konfigurácií, ako aj nastavenie záložných kópií. Manuál popisuje rôzne metódy zálohovania a odporúčané intervaly pre tieto úkony. Ďalej sú v ňom uvedené kroky na obnovu systému zo zálohy v prípade poruchy alebo straty dát, vrátane testovania integrity záloh a overenia obnovy funkčnosti systému. Zároveň sú zahrnuté bezpečnostné opatrenia pri zaobchádzaní so zálohovanými údajmi.

27. Požiadavky na testovanie a protokoly

27.1 Všeobecné požiadavky

Účelom testov FAT, SAT je zaistiť, že RIS a pripojené subsystémy sú navrhnuté, nainštalované a nakonfigurované v súlade so špecifikáciou. Skúšky sa vykonávajú v priestoroch dodávateľa - FAT a opakujú sa po ukončení montážnych prác v priestoroch objednávateľa - SAT. Dodávateľ musí pred dodaním ku dodávateľovi nainštalovať a prevádzkovať kompletný riadiaci systém a jeho pripojené subsystémy vo svojich priestoroch. Dodávateľ RIS vykoná pred FAT svoj vlastný štandardný interný test a predloží záznamy o testovaní objednávateľovi. Interná skúška dodávateľa musí zahŕňať kompletnú kontrolu systému doplnenú o hardvér, softvér a riadiace funkcie všetkých subsystémov (napr. PLC, SIS atď.), pričom osobitnú pozornosť treba venovať komunikácii pripojených systémov. Súčasťou FAT a SAT je aj testovanie aplikačného softvéru a riadiacich funkcií na základe údajov poskytnutých v projekte alebo Zadaní
Dodávateľ RIS musí prevádzkovať celý systém nepretržite počas najmenej 48 hodín. Počas tohto obdobia sa vykonajú skúšky hardvéru. FAT sa vykonáva za prítomnosti objednávateľa, alebo jeho zástupcov.
Dodávateľ systému poskytne vhodné testovacie zariadenia, testovacie systémy a kvalifikovaný personál, ktorý bude pokračovať v testoch podľa harmonogramu. O každej skúške sa vypracuje protokol.
Účasť zástupcov objednávateľa v žiadnom prípade nezbavuje dodávateľa systému jeho záručných povinností týkajúcich sa kvality materiálu, inštalácie, výroby a prevádzkyschopnosti.

27.2 Testovacia dokumentácia

4 týždne pred plánovaným začiatkom testovania, odovzdá dodávateľ objednávateľovi, na schválenie podrobný postup jednotlivých testov vrátane protokolov kde sa budú zaznamenávať výsledky testovania.
Zistené diskrepancie (odchýlky, chyby, zmeny, nefunkčnosti a pod.) eviduje dodávateľ v osobitnom zozname spolu s detailnejším opisom tak, aby bolo zrejmé v čom spočíva diskrepancia. Všetky diskrepancie musia byť vyriešené pred ukončením testovania(FAT,SAT). Vyriešené diskrepancie musia byť znova otestované (skontrolované) a výsledok zapísaný.

27.3 HW FAT

Kontrola FAT HW sa vykonáva na reálnom funkčnom systéme, ktorý bude následne nasadený v prevádzke. Počas kontroly a testovania HW dodávky RIS budú vykonané nasledovné testovania a kontroly:

- **Kontrola množstva a typu nainštalovaného hardvéru podľa špecifikácie DRS a zmluvy o dielo.**

  Overenie, že všetok inštalovaný hardvér zodpovedá špecifikáciám uvedeným v projektovej dokumentácii a v zmluve. Toto zahŕňa potvrdenie o správnosti modelov, verzií, revízií firmvéru a počtu zariadení, ktoré boli dodané.

- **Kontrola množstva a typu náhradných dielov**

  Overenie, že dodávka obsahuje požadované náhradné diely ako sú náhradné moduly, karty, senzory, kabeláže a iné komponenty, ktoré sú nevyhnutné pre správnu funkčnosť systému.

- **Kontrola dokumentácie, certifikátov a softvérových licencií**

  Overenie, že všetky relevantné dokumenty (certifikáty ku jednotlivým dielom, softvérové licencie, bezpečnostné osvedčenia, revízne správy) boli dodané a sú v súlade s požiadavkami projektu.

- **Vizuálna kontrola systému, kontrola konštrukčnej a mechanickej kompletnosti, systémovej integrity a poškodenia**

  Overenie všetkých komponentov systému na prítomnosť viditeľných poškodení, defektov alebo mechanických problémov, ako aj overenie, že všetky časti systému sú správne nainštalované a plne funkčné.

- **Kontrola zapojenia subsystémov**

  Overenie správnosti zapojenia všetkých subsystémov podľa projektových schém. To bude zahŕňať kontrolu prepojení medzi riadiacimi jednotkami, I/O modulmi, senzormi, aktuátormi a ďalšími subsystémami.

- **Kontrola napájania systému podľa schémy napájania**

  Overenie správnosti napájania systému podľa predpísanej schémy, vrátane zabezpečenia správnej polohy pripojení a správnych parametrov napájacích zdrojov.

- **Kontrola systémového alarmu výpadku UPS**

  Overenie správnosti alarmov a reakcií systému pri výpadku napájania, vrátane detekcie problémov s napájaním a aktivácie záložného UPS systému. Systém musí byť schopný detekovať a alarmovať každý výpadok.

- **Kontrola chladenia a teplôt kabinetov**

  Overenie efektívnosti chladenia v rámci systému, vrátane merania teplôt v kabinetoch a overenie, že teplotné parametre sú v rámci schválených limitov, aby sa predišlo prehriatiu a poškodeniu hardvéru.

- **Kontrola uzemnenia RIS podľa schém uzemnenia a tienenia**

Overenie, že uzemnenie a tienenie riadiaceho systému (RIS) je správne implementované podľa predpísaných schém, aby sa minimalizovalo riziko elektromagnetických rušení a zabezpečila bezpečnosť systému.

- **Kontrola označenia káblov, pripojovacie dosky svoriek, RIS (štítky káblov atď.)**

  Overenie že všetky káble, svorky, pripojovacie dosky a ďalšie komponenty sú správne označené podľa predpísaných štandardov a schém, aby sa zaručila správnosť zapojení a uľahčil sa neskorší servis a údržba.

- **Kontrola systémovej kabeláže riadiaceho systému**

  Overenie stavu fyzickej kabeláže, vrátane zabezpečenia správneho ukladania káblov, ich správneho smerovania a ochrany pred mechanickým poškodením.

- **Kontrola oddelenia kabeláže (z hľadiska ochrany, oddelenia a triedenia)**

  Overenie že kabeláž je správne oddelená podľa požiadaviek projektu, najmä v prípade vysoko citlivých alebo bezpečnostných obvodov, aby sa minimalizovali možné interferencie medzi signálmi.

- **Kontrola označenia a rozdelenia svorkovníc a vnútornej kabeláže**

  Overenie správneho označenia svorkovníc a vnútornej kabeláže, aby bola zabezpečená ich správna identifikácia a ľahká údržba.

- **Kontrola vstupov a výstupov podľa výkresov**

  Overenie funkčnosti IO modulov, aby sa overilo, že každé IO je správne zapojené a funkčné. Tento test zabezpečuje, že všetky vstupy a výstupy systému pracujú podľa špecifikácie.

- **Kontrola redundancie**

  Overenie redundancie(záskoku) systémových mechanizmov (napr. CPU, IO moduly, redundantné napájanie, redundantné komunikačné linky, záložné systémy), aby sa overilo, že systém je schopný automaticky prejsť na záskok v prípade poruchy bez prerušenia prevádzky.

27.4 SW FAT

Kontrolu SW počas FAT, možno vykonať aj na testovacom systéme, pokiaľ nie je dostupný reálny systém. Požiadavky na testovanie zabezpečujú, že softvér riadiaceho systému je nielen funkčný, ale aj bezpečný a pripravený na nasadenie do prevádzky, pričom poskytujú možnosť na odhalenie chýb alebo nedostatkov pred finálnym nasadením.
Minimálne požiadavky na SW FAT zahŕňajú nasledujúce detaily:

- **Kontrola systémových funkcií RIS**

  Overenie základných funkcií riadiaceho systému podľa predpísaného protokolu dodávateľa, vrátane funkcií obsluhy, alarmovania, hlásení a ďalších kľúčových funkcií systému.

- **Kontrola konfigurácie I/O**

  Overenie správnej konfigurácie vstupov a výstupov (I/O) podľa nasledujúcich parametrov:

  - AI (Analog Inputs): Kontrola pozície I/O, rozsahu merania, jednotiek, linearizácie vstupov, správneho nastavenia alarmov a ďalších parametrov.

- AO (Analog Outputs): Kontrola pozície I/O, smeru výstupu (FO/FC), stavu "bezpečný" (safe), aby sa zabezpečila správnosť výstupov.
- DI (Digital Inputs): Overenie pozície I/O, stavov signálov a správnosti nastavenia alarmov.
- DO (Digital Outputs): Kontrola pozície I/O, stavov, správneho stavu "bezpečný" (safe state), ktorý zabezpečuje bezpečnosť systému.

- **Kontrola riadiacich algoritmov**

  Overenie správnej implementácie riadiacich algoritmov v systéme:

  - Kontrola zapojenia funkčných blokov (napr. kaskádové zapojenie riadiacich blokov), ktoré zaisťujú správne fungovanie regulácie a riadenia.
  - Kontrola nastavení funkčných blokov, ako sú parametre PID, smer riadenia (napr. priamy alebo inverzný), nastavenia alarmov a ďalších parametrov.
  - Kontrola logiky riadenia podľa dokumentácie, vrátane overenia správnosti implementovaných logických schém v aplikácii.
  - Kontrola logiky sekvenčného riadenia, aby sa zabezpečila správna implementácia fázových alebo sekvenčných operácií v systéme.

- **Kontrola prepojení subsystémov v súlade podľa sieťovej architektúry**

  Overenie správnosti prepojení medzi subsystémami podľa schém sieťovej architektúry, vrátane zabezpečenia správnej komunikácie medzi jednotlivými komponentmi systému.

- **Kontrola prepojení bezpečnostného systému SIS (napr. SOE, alarmy...)**

  Overenie prepojení bezpečnostného systému (SIS) do NRS, vrátane kontroly správnosti implementácie SOE (Sequence of Events) a bezpečnostných alarmov, ktoré zaisťujú ochranu systému.

- **Kontrola faceplatov**

  Overenie správnosti a funkčnosti faceplatov, ktoré používateľ používa na interakciu so systémom. To zahŕňa kontrolu vzhľadu, prístupových práv a kompatibility s riadiacimi funkciami.

- **Kontrola dynamického a statického obsahu HMI**

  Overenie dynamického a statického obsahu HMI (Human-Machine Interface), vrátane správnosti vizuálneho zobrazenia, interakcie a záznamu informácií v reálnom čase.

- **Kontrola dynamického a statického obsahu alarmov a eventov**

  Overenie správneho zobrazenia a fungovania alarmov a udalostí (eventov) na HMI, vrátane testovania správnych reakcií na zmeny v stave systému a generovanie alarmov v prípade porúch alebo neštandardných podmienok.

- **Kontrola bezpečnosti (CFAT)**
  Ešte pred začatím CFAT musí dodávateľ na systém nainštalovať všetky záplaty operačného systému, aplikácií, balíky Service Pack a iné certifikované aktualizácie. Zároveň musí byť vytvorená a zdokumentovaná základná konfigurácia (baseline). Dodávateľ musí zabezpečiť, aby počas tejto fázy boli aplikované vhodné bezpečnostné kontroly, a aby neboli technikmi úmyselne obchádzané len s cieľom "rýchlo sfunkčniť systém". CFAT sa skladá z nasledovných kontrol:

- Malvér v dodávaných zariadeniach: Dodávateľ overí a preukáže (napr. skenovaním pred dodaním), že všetky dodávané zariadenia (vrátane staníc a PLC) sú pri dodaní do MHTH čisté a bez známeho malvéru
- Validácia bezpečnostných požiadaviek: Overenie, či implementované technické a organizačné opatrenia spĺňajú požiadavky definované v tomto dokumente, ZoBOaNP a súvisiacich dokumentoch.
- Kontrola originality a dodávateľského reťazca: Overenie preukázania originality a zabezpečenia dodávateľského reťazca voči neoprávnenej manipulácii.

27.5 SAT

SAT - Site acceptance test sa vykonáva na reálnom funkčnom systéme ktorý je nainštalovaný, oživený sú zapojené všetky obvody a komunikačné linky. Počas kontroly a testovania HW dodávky RIS budú vykonané nasledovné testovania a kontroly:

- **Vizuálna kontrola systému, kontrola konštrukčnej a mechanickej kompletnosti, systémovej integrity a poškodenia**

  Overenie všetkých komponentov systému na prítomnosť viditeľných poškodení, defektov alebo mechanických problémov, ako aj overenie, že všetky časti systému sú správne nainštalované a plne funkčné a neboli pri preprave a montáži poškodené.

- **Kontrola napájania systému podľa schémy napájania**

  Overenie správnosti napájania systému podľa predpísanej schémy, vrátane zabezpečenia správnej polohy pripojení a správnych parametrov napájacích zdrojov.

- **Kontrola zapojenia subsystémov**

  Overenie správnosti zapojenia všetkých subsystémov podľa projektových schém. To bude zahŕňať kontrolu prepojení medzi riadiacimi jednotkami, I/O modulmi, senzormi, aktuátormi a ďalšími subsystémami.

- **Kontrola redundancie**

  Overenie redundancie(záskoku) systémových mechanizmov (napr. CPU, IO moduly, redundantné napájanie, redundantné komunikačné linky, záložné systémy), aby sa overilo, že systém je správne zapojený a schopný automaticky prejsť na záskok v prípade poruchy bez prerušenia prevádzky.

- **Kontrola obvodov – Loop check**
  - Kontrola všetkých analógových obvodov v rozsahoch minimálne 0%,50% a 100% zadávačom priamo zo snímača, vrátane kontroly a skúšky rozsahu, inžinierskych jednotiek, alarmových a tripovacích hodnôt. Kontrola týchto alarmov a eventov v HMI, prípadne v nadradenom riadiacom systéme.
  - Kontrola všetkých digitálnych obvodov priamo zo snímača a kontrola správnosti jednotlivých stavov a alarmov. Kontrola týchto alarmov a eventov v HMI, prípadne v nadradenom riadiacom systéme.
  - Kontrola komunikácie s riadiacim systémom alebo inými subsystémami. Kontrola všetkých signálov/adries ktoré sú komunikované medzi systémami, vrátane kontroly týchto signálov v HMI.

- **Kontrola systémových funkcií RIS**

  Overenie základných funkcií riadiaceho systému podľa predpísaného protokolu dodávateľa, vrátane funkcií obsluhy, alarmovania, hlásení a ďalších kľúčových funkcií systému.

- **Kontrola riadiacich algoritmov**

  Overenie správnej implementácie riadiacich algoritmov v systéme a ich skúška vrátane snímačov, akčných členov, vizualizácie, alarmovania. To pozostáva z nasledovných kontrol:

  - Kontrola zapojenia funkčných blokov (napr. kaskádové zapojenie riadiacich blokov), ktoré zaisťujú správne fungovanie regulácie a riadenia.
  - Kontrola nastavení funkčných blokov, ako sú parametre PID, smer riadenia (napr. priamy alebo inverzný), nastavenia alarmov a ďalších parametrov.
  - Kontrola logiky riadenia podľa dokumentácie, vrátane overenia správnosti implementovaných logických schém v aplikácii.
  - Kontrola logiky sekvenčného riadenia, aby sa zabezpečila správna implementácia fázových alebo sekvenčných operácií v systéme.

- **Kontrola bezpečnosti (CSAT)**

  CSAT sa vykonáva po úplnom dokončení prevádzkových a inštalačných testov, ale ešte **pred** samotným uvedením procesu do produkčnej prevádzky a skladá sa z nasledovných kontrol:

  - Validácia bezpečnostných požiadaviek: Overenie, či implementované technické a organizačné opatrenia spĺňajú požiadavky definované v tomto dokumente, ZoBOaNP a súvisiacich dokumentoch.
  - Katalogizácia a overenie integrity: Overenie integrity, pričom sa kontrolujú predprodukčné konfigurácie, nastavenia a verzie softvéru či firmvéru. Tieto sa porovnávajú so známou a overenou verziou, tzv. „zlatým diskom“ (gold disk).
  - Aktívne bezpečnostné testy: Vykonanie špecifických bezpečnostných testov, ako sú skenovanie zraniteľností, penetračné testy, testy systémov na detekciu prienikov a testovanie kontroly prístupu.

- **Overenie DRP**

  Počas SAT musí prebehnúť overenie DRP scenárov ktoré sú súčasťou RD. Test prebieha počas vopred schváleného scenára a meria sa maximálny čas obnovenia systému - RTO a maximálny prípustný objem stratených dát - RPO. Odchýlky, nedostatky alebo odporúčania zistené počas testu sa musia zaznamenať do testovacieho protokolu a na základe týchto zistení sa vytvoria návrhy na aktualizáciu DRP. Aktualizované DRP bude súčasťou DSV - dokumentácie skutkového vyhotovenia. DRP musí prebehnúť po odstránení všetkých nedorobkov, aby bolo možné validovať finálny stav diela. Počas záručnej doby diela, dodávateľ opakuje test DRP každých 12 mesiacov, prípadne sa test DRP opakuje za asistencie dodávateľa. Mimoriadne sa testuje DRP pri významnej zmene v infraštruktúre, alebo po bezpečnostnom incidente.

28. Požiadavky na programovanie a skriptovanie

28.1 Všeobecné požiadavky

Dodávateľ poskytne štandardné zabezpečenie v softvéri a zabezpečí ochranu proti:

- Buffer Overflows- pretečeniu vyrovnávacej pamäte, v ktorej sú vstupné polia vyplnené dlhými sekvenciami údajov, ktoré prepĺňajú vyrovnávaciu pamäť programu, čo poskytne ovládanie programu vzdialenému používateľovi.
- Insertion a Injection - vloženie/podhodenie údajov, pri ktorých sú vstupné polia vyplnené riadiacimi alebo príkazovými sekvenciami vloženými rôznymi spôsobmi, ktoré však aplikácia akceptuje, prípadne ich prenesie do operačného systému, a ktoré umožňujú spúšťanie privilegovaných škodlivých a neautorizovaných programov, príp. ktoré môžu byť spustené vzdialene.

28.2 Bezpečné programovacie postupy

V prípade dodávky softvéru musia byť zabezpečené nasledujúce bezpečnostné požiadavky:

- Kontrola vstupov na primerané zadávateľné hodnoty
- Šifrovanie dátových súborov
- Potrebné pochopiť bezpečnostné dopady OS a iných knižníc tretích strán
- Potrebné uistiť sa, že operačné systémy a iné knižnice tretích strán majú/existuje politika aktualizácií
- Zakázať pretečenie vyrovnávacej pamäte
- Verifikovať nezmeniteľnosť logov (nepopierateľnosť, auditovateľnosť)
- Používať end-to-end autentifikáciu a kontrolu integrity dátovej komunikácie medzi procesmi
- Potrebné overiť, či nie sú v kóde vložené alebo zdokumentované žiadne heslá a šifrovacie kľúče v clear-text forme
- Požadované používať bezpečný dizajn a kontrolu kódu (napr. OWASP).

28.3 Požiadavky na dokumentáciu

Každý kód (program/skript) vytvorený v rámci dodávky musí byť náležite zdokumentovaný. Každá ucelená časť kódu alebo funkcia musí obsahovať popis svojej funkcionality a vstupno/výstupných parametrov.

28.3.1 Dokumentácia hlavičky

Dokumentácia hlavičky musí byť umiestnená na začiatku každého zdrojového súboru (s výnimkou nevyhnutných systémových direktív, napr. shebang).
Dokumentácia musí obsahovať informácie o:

- Názov a stručný popis účelu programu/skriptu.
- Prevádzkové poznámky (odporúčania pre používanie, obmedzenia, pravidlá nasadenia).
- Identifikáciu autora (meno/spoločnosť) a dátum vytvorenia (RRRR-MM-DD).
- Podrobný popis (správanie, závislosti od iných modulov, prístup k externým zdrojom ako DB, PLC a pod.).
- Históriu verzií (každá zmena musí obsahovať číslo verzie, autora zmeny, dátum a stručný popis úprav). Formát histórie verzií:<verzia>: <autor> @ <dátum zmeny> - <stručný opis zmien>
- Dokumentáciu rozhraní (popis globálnych premenných a kľúčových dátových štruktúr).

28.4 Lokálne premenné a funkcie

Každá funkcia musí byť dokumentovaná priamo v mieste jej definície. Dokumentovanie bežných lokálnych premenných v hlavičke súboru sa nevyžaduje, ak je ich význam zrejmý z kontextu kódu. Kľúčové premenné však musia byť opatrené komentárom priamo v kóde.

28.5 Dodatočné požiadavky na programovanie PLC

Pri programovaní PLC riadiacich výrobné procesy je odporúčané dodržiavať najlepšiu prax definovanú v aktuálnom dokumente Secure PLC Coding Practices: Top 20 list dostupnom na stránkach PLC Security. Link: Top_20_Secure_PLC_Coding_Practices_V1.0.pdf