



POŽADAVKY NA KYBERNETICKOU BEZPEČNOST ŘÍDICÍCH SYSTÉMŮ A OT TECHNOLOGIÍ

VVC, Modernizace řídicích systémů VD a PK

verze 250812

OBSAH

ČÁST I. OBECNÁ UJEDNÁNÍ	6
1 Účel dokumentu a projektové cíle	6
1.1 Projektové cíle v oblasti kybernetické bezpečnosti řídicích systémů	6
2 Definice používané v tomto dokumentu	7
3 Vztah k bezpečnosti zdraví a práce	11
3.1 Přednost BOZP při řešení kybernetické bezpečnosti	11
3.2 Informování Objednatele při narušení BOZP	11
3.3 Kybernetické incidenty s dopadem na BOZP	12
4 Závazné legislativní a normativní rámce	12
4.1 Související právní rámce	12
4.2 Závazné právní předpisy a normy	12
4.3 Možnosti odchýlení se od stanovených požadavků	13
4.4 Nové požadavky ze strany oprávněných orgánů	13
4.5 Změnové řízení při výskytu nových požadavků	14
4.6 Požadavky na dokumentaci změn	14
4.7 Související standardy kybernetické bezpečnosti	15
5 Související dokumentace	16
5.1 Dokumenty, provázanost a jejich hierarchie	16
5.2 Právo na úpravu dokumentace během realizace	16
5.3 Odpovědnost za správu a doplnění dokumentace	16
ČÁST II. POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI NA ZHOTOVITELE	17
6 Požadavky na kybernetickou bezpečnost při přípravě projektu	17
6.1 Princip Secure by Design	18
6.2 Organizační způsobilost	18
6.3 Důvěrnost informací a režim NDA	18
6.4 Požadavky na personální zajištění zhotovitele	19
6.5 Podzhotovitelé	19
7 Požadavky na kybernetickou bezpečnost v průběhu implementace	20
7.1 Požadavky na kybernetickou bezpečnost v průběhu implementace řídicích systémů	20
7.2 Dodávaná zařízení a komponenty	20
8 Požadavky na kybernetickou bezpečnost na zhotovitele po implementaci	21
8.1 Školení objednatelů	21
8.2 Zkoušky a ověření kybernetické bezpečnosti	22
8.3 Provozní podpora po implementaci	22
8.4 Dokumentace řídicích systémů a její předání objednateli	23
8.5 Podpora při řešení bezpečnostních incidentů	24

9	Ukončení projektu	24
ČÁST III. POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI NA ŘÍDICÍ SYSTÉMY A PROVOZNÍ TECHNOLOGIE		26
10	Technické požadavky kybernetické bezpečnosti	26
10.1	Fyzická bezpečnost	26
10.2	Bezpečnost komunikačních sítí	27
10.3	Správa a ověřování identit	30
10.4	Řízení přístupových oprávnění	31
10.5	Aplikační bezpečnost	32
10.6	Kryptografické algoritmy	32
10.7	Zajišťování dostupnosti řídicích systémů	33
11	Licence a přístupová práva k systémům OT a bezpečnostnímu software	34
11.1	Obecně	34
11.2	Povaha a Doba trvání licence; odměna za licenci	34
12	Kompenzační opatření	35

ČÁST I. OBECNÁ UJEDNÁNÍ

1 ÚČEL DOKUMENTU A PROJEKTOVÉ CÍLE

Tento dokument stanovuje závazné požadavky Objednatele na zajištění kybernetické bezpečnosti řídicích systémů, jejich částí a dalších OT systémů a souvisejících technologií (např. kamerových, komunikačních a bezpečnostních systémů), které jsou součástí technologické infrastruktury Vodního díla. Jedná se zejména o zařízení a systémy zajišťující automatizované řízení, dohled, sběr dat a přímé ovládání fyzických procesů – tedy systémy, jejichž kompromitace může vést k přímému narušení provozní kontinuity, ohrožení bezpečnosti osob či environmentálním škodám.

Tento dokument se vztahuje na všechny fáze životního cyklu těchto řídicích systémů – od návrhu a implementace přes zprovoznění, provoz a údržbu až po případnou dekomisi. Jeho účelem je zajistit, aby architektura, technologie i provozní opatření odpovídala aktuálním požadavkům kybernetické bezpečnosti, principům „Secure by Design“ a legislativním a standardizačním rámcům (např. zákon č. 181/2014 Sb., vyhlášky o bezpečnostních opatřeních, IEC 62443).

Bezpečnost je chápána jako nedílná a neoddělitelná součást správného fungování technických aktiv. Bez jejího naplnění nelze považovat systém za provozuschopný, bezpečný ani efektivně spravovatelný.

1.1 PROJEKTOVÉ CÍLE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI ŘÍDICÍCH SYSTÉMŮ

Zhotovitel je povinen při realizaci řídicího systému navrhnout, implementovat a konfigurovat řídicí systémy tak, aby bezpečnost byla integrální součástí každého návrhového rozhodnutí, nikoliv dodatečným nebo dílčím opatřením. Bezpečnostní opatření musí být navržena s ohledem na jejich vliv na funkčnost, provozní dostupnost a správu zařízení, a musí být v každém bodě technicky a provozně ospravedlnitelná.

Dokument slouží jako výchozí rámec pro naplnění následujících cílů v oblasti kybernetické bezpečnosti řídicích systémů:

- (a) Ochrana před relevantními kybernetickými hrozbami (včetně fyzického a vzdáleného přístupu), a to prostřednictvím návrhu segmentované síťové architektury, řízení přístupových práv, detekce bezpečnostních událostí a prevence laterálního pohybu v síti.
- (b) Návrh systémové architektury podle zásad Secure by Design, s důrazem na minimalizaci rizik lidské chyby, bezpečné výchozí konfigurace, technické a procesní řízení změn a auditovatelnost všech přístupů a operací.
- (c) Zajištění provozní spolehlivosti a dlouhodobé správy bezpečnosti, včetně mechanismů pro správu zranitelností, pravidelné aktualizace firmwaru a softwaru, monitoring bezpečnostního stavu a řízení incidentů.
- (d) Omezení závislosti na konkrétním dodavateli či technologii, a to prostřednictvím nasazení standardních protokolů, otevřených rozhraní a transparentního provozního modelu s předanou dokumentací a znalostní základnou.
- (e) Zajištění souladu s bezpečnostními politikami Objednatele a připravenosti na legislativní a technologické změny (např. NIS2, nové požadavky NBÚ, revize standardů IEC 62443),

s cílem zajistit dlouhodobou kompatibilitu řešení a snižovat náklady na jeho budoucí úpravy.

2 DEFINICE POUŽÍVANÉ V TOMTO DOKUMENTU

V tomto dokumentu jsou používány tyto definice a zkratky:

- (a) **„2FA/MFA“** (tzv. 2 factor authentication/multi factor authentication) – dvou faktorové/více faktorové ověřování zahrnuje dva nebo více kroků nebo procesů k identifikaci uživatele.
- (b) **„ACL“** (tzv. Access Control List) – je seznam pravidel, který určuje, které subjekty (uživatelé, skupiny, procesy, zařízení) mají oprávnění přistupovat k určitému objektu.
- (c) **„Technické aktivum“** (tzv. – Technical Asset) – je v kontextu kybernetické bezpečnosti řídicích systémů jakýkoli technologický prvek, který je součástí řídicího systému a má hodnotu pro organizaci z hlediska funkčnosti, provozu nebo bezpečnosti dle dokumentu *TPO_OTP_003 5.6 Řídicí systém*. Narušení, ztráta nebo zneužití tohoto aktiva může negativně ovlivnit dostupnost, integritu nebo důvěrnost provozních procesů. Mezi technická patří také kamerové systémy (tzv. CCTV), komunikační systémy, bezpečnostní a poplachové systémy a další systémy pro automatizaci budov, které řídí například osvětlení, vytápění, ventilaci nebo klimatizaci a další.
- (d) **„API“** (tzv. Application Programming Interface) – je soubor definovaných pravidel, protokolů a nástrojů, které umožňují komunikaci a výměnu dat mezi různými softwarovými aplikacemi.
- (e) **„ARP“** (tzv. Address Resolution Protocol) – je síťový protokol používaný k překladi logické IP adresy na fyzickou MAC adresu zařízení v rámci stejné lokální sítě (LAN).
- (f) **„Bezpečnostní perimetr“** je pomyslná nebo fyzická hranice, která odděluje chráněný prostor od okolí a slouží k ochraně majetku, informací nebo systémů před nežádoucím přístupem nebo narušením. V kontextu fyzické bezpečnosti se jedná o ohraničení pozemku či objektu, kde jsou instalovány technologie a systémy pro detekci narušení.
- (g) **„Bezpečnostní zóna“** – je logicky nebo fyzicky oddělená část sítě nebo systému, ve které jsou shromážděna aktiva, která mají podobné požadavky na úroveň důvěry, bezpečnosti a ochrany.
- (h) **„BOZP“** – bezpečnost a ochrana zdraví při práci.
- (i) **„Brute Force“** (tzv. útok hrubou silou) – je typ kybernetického útoku, při kterém se útočník systematicky pokouší uhodnout heslo, šifrovací klíč nebo jiný autentizační údaj tím, že zkouší všechny možné kombinace, dokud nenalezne správnou.
- (j) **„CVE“** (tzv. Common Vulnerabilities and Exposures) – běžné zranitelnosti a vystavení se hrozbám je číselné označení záznamu v databázi, která poskytuje definice veřejně dostupných zranitelností v oblasti kybernetické bezpečnosti.
- (k) **„ČSN“** (tzv. české technické normy) – stanovují základní požadavky na kvalitu a bezpečnost, slučitelnost, zaměnitelnost, ochranu zdraví a ochranu životního prostředí a vyjadřují požadavky na výrobky, procesy nebo služby, které zajistí splnění požadavků vhodnosti pro určený účel.
- (l) **„DCS“** (tzv. Distributed Control System) – distribuovaný řídicí systém, který využívá data šířená v reálném čase bez centrálního uzlu; běžně se používá při výrobě energie, rafinaci ropy, čištění odpadních vod nebo v chemickém průmyslu.

- (m) **„Dílo“** je stavba, technologické zařízení, softwarové vybavení, dočasná díla a případné další součásti Díla tak, jak jsou popsány v příslušné smlouvě o dílo.
- (n) **„Dekomise“** – vyřazení z provozu (z angl. Decomission); poslední fáze obvyklého životního cyklu řídicího systému.
- (o) **„DNS“** (tzv. Domain Name System) je internetová služba, která překládá doménová jména na IP adresy.
- (p) **„DOCX“** je souborový formát pro textové dokumenty, který používá aplikace Microsoft Word (od verze 2007).
- (q) **„DoS“** (tzv. Denial of Service) – je typ kybernetického útoku, jehož cílem je znepřístupnit službu, systém nebo síť legitimním uživatelům tím, že je přetížen požadavky, které systém nedokáže efektivně zpracovat.
- (r) **„DDoS“** (tzv. Distributed Denial of Service) – je rozšířenou formou DoS útoku, při níž útočník využívá velké množství kompromitovaných zařízení, aby koordinovaně zahltila cílový systém nebo síť.
- (s) **„End of Support“** – označuje okamžik, kdy výrobce softwaru nebo hardwaru ukončí technickou podporu, aktualizace a bezpečnostní záplaty pro daný produkt nebo systém.
- (t) **„ENISA“** (tzv. European Network and Information Security Agency) – Evropská agentura pro bezpečnost sítí a informací je jedna z agentur Evropské unie, jejímž úkolem je zlepšovat informační bezpečnost v rámci Evropské unie.
- (u) **„ERP“** (tzv. Enterprise Resource Planning) – je integrovaný informační systém, který slouží k plánování a řízení podnikových zdrojů a procesů napříč celou organizací.
- (v) **„ETSI“** (tzv. Evropský institut pro telekomunikační normy) je nezávislá evropská normalizační organizace, která vyvíjí globálně uznávané standardy pro oblast informačních a komunikačních technologií.
- (w) **„HMI“** (tzv. Human-Machine Interface) – rozhraní, které zpřístupňuje data z databáze obsluze (operátorovi).
- (x) **„IACS“** (tzv. Industrial Automation and Control Systems) – viz řídicí systém.
- (y) **„ICS“** (tzv. Industrial Control Systems) – viz řídicí systém.
- (z) **„IDMZ“** – je průmyslová demilitarizovaná zóna, která slouží jako bezpečnostní přechodová vrstva mezi IT a OT prostředím. Jejím hlavním cílem je řídit, kontrolovat a zabezpečit komunikaci mezi podnikovými systémy.
- (aa) **„IEC“** (tzv. International Electrotechnical Commission) – organizace, která vypracovává a publikuje mezinárodní normy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory.
- (bb) **„I/O“** (tzv. Input/Output) – označuje všechny formy komunikace mezi systémem a jeho okolím, tedy příjem dat (vstup) a odesílání dat (výstup).
- (cc) **„IP adresa“** – je jedinečný číselný identifikátor, který slouží k označení zařízení v počítačové síti, a umožňuje směrování a doručování dat mezi zařízeními.
- (dd) **„ISO“** (tzv. International Organization for Standardization) – mezinárodní organizace pro normalizaci.
- (ee) **„ISMS“** (tzv. Information Security Management System) je zkratka pro Systém řízení informační bezpečnosti. Jedná se o soubor pravidel, procesů, zásad, opatření

a technologií, jejichž cílem je systematicky řídit rizika spojená s ochranou informací a zajistit důvěrnost, integritu a dostupnost informací v organizaci.

- (ff) **„Konduit“** – logická nebo fyzická komunikační cesta, která spojuje dvě nebo více zón (segmentů) v síti provozních technologií.
- (gg) **„MAC adresa“** (Media Access Control Address) Je jedinečný fyzický identifikátor síťového rozhraní zařízení, přiřazený výrobcem.
- (hh) **„MES“** (tzv. Manufacturing Execution System) – je zkratka pro výrobní informační systém, který řídí, monitoruje a optimalizuje výrobní procesy v reálném čase.
- (ii) **„MITM“** (tzv. man-in-the-middle) – je forma kybernetického útoku, při které se útočník skrytě vloží mezi dvě komunikující strany a odposlouchává, mění nebo přesměrovává přenášená data bez vědomí obou stran.
- (jj) **„Modbus RTU“** – je komunikační protokol pracující na sériovém přenosu dat, který je široce používán v průmyslové automatizaci pro komunikaci mezi řídicími systémy.
- (kk) **„Modbus TCP/IP“** – je průmyslový komunikační protokol, který umožňuje přenos dat po Ethernetových sítích pomocí standardního protokolu TCP/IP.
- (ll) **„NBÚ“** (tzv. Národní bezpečnostní úřad) - je ústřední správní úřad České republiky, který zajišťuje úkoly v oblasti ochrany utajovaných informací, bezpečnostní způsobilosti osob a podnikatelů, a dále plní důležitou roli v oblasti kybernetické bezpečnosti.
- (mm) **„NDA“** (tzv. Non-Disclosure Agreement) – je dohoda o mlčenlivosti.
- (nn) **„NIS2“** (tzv. Network and Information Security 2) – je směrnice Evropské unie, která má za cíl posílit kybernetickou bezpečnost organizací poskytujících klíčové služby pro společnost.
- (oo) **„NÚKIB“** (tzv. Národní úřad pro kybernetickou a informační bezpečnost) – je ústředním správním úřadem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.
- (pp) **„OPC UA“** (tzv. Open Platform Communications Unified Architecture) – je otevřený, platformě nezávislý komunikační standard, který umožňuje bezpečnou, spolehlivou a strukturovanou výměnu dat mezi zařízeními, systémy a aplikacemi v průmyslové automatizaci.
- (qq) **„OT“** (tzv. Operational Technologies – provozní technologies) – je soubor technických prostředků, hardwaru a softwaru, který slouží k řízení, monitorování a automatizaci fyzických procesů a prostředí v reálném čase. Mezi OT patří také kamerový systém.
- (rr) **„PDF“** (tzv. Portable Document Format) – přenositelný formát dokumentu.
- (ss) **„PID“** (tzv. Proportional-Integral-Derivative Controller) proporcionálně–integračně–derivační regulátor, což je typ zpětnovazebního regulačního algoritmu, který se široce používá v průmyslové automatizaci.
- (tt) **„PERA model“** (tzv. Purdue Enterprise Reference Architecture model) – referenční model architektury pro průmyslové řídicí systémy, který rozděluje síťovou infrastrukturu do úrovní, aby bylo možné jasně definovat hranice mezi podnikovými IT systémy a jednotlivými provozními technologiemi. Model tak slouží jako základ pro návrh segmentace sítí, řízení přístupů a dalších bezpečnostních opatření.

- (uu) **„PMS“** (tzv. Production Management Systém) – je informační systém pro řízení a optimalizaci výroby na úrovni závodu.
- (vv) **„PO“** – požární ochrana.
- (ww) **„Principle of least privilege“** (tzv. Princip nejnižších privilegií) - označení pro metodu, při které jsou kvůli informační bezpečnosti přidělována uživatelům, programům či procesům nejnížší možná oprávnění, která umožní jeho správnou funkci.
- (xx) **„Průmyslová, řídicí a obdobná specifická technická aktiva“** – viz. řídicí systém.
- (yy) **„RBAC“** (tzv. Role-Based Access Control) – metoda regulace přístupu k počítačovým nebo síťovým zdrojům na základě rolí jednotlivých uživatelů.
- (zz) **„RTU“** (tzv. Remote Terminal Unit) – je vzdálená řídicí a sběrná jednotka, která se používá v průmyslové automatizaci pro monitorování a ovládání zařízení na vzdálených nebo distribuovaných stanovištích
- (aaa) **„Řídicí systém“** jsou technická programovatelná zařízení (hardware, firmware a software) používaná převážně k řízení, monitorování a automatizaci fyzických a technologických procesů v reálném čase. Definice „řídicí systém“ je ekvivalentní s pojmy jako OT systém nebo IACS (tzv. Industrial Automation Control System). Mezi řídicí systémy patří například SCADA, DCS, BAS, PLC, RTU, PID, IED a další. Kategorizace řídicích systémů vychází z modelu PERA dle normy IEC 62443, který tvoří základ bezpečné architektury průmyslových řídicích systémů. Klíčové je stanovení komponent řídicího systému a jeho hranic s ohledem na jejich zařazení do jednotlivých úrovní modelu PERA. V rámci tohoto projektu se pracuje s úrovněmi 0 až 3 – řídicí systém tak obsahuje fyzické zařízení (tzv. úroveň 0 – typicky čidla a aktuátory), obsahuje úroveň základního řízení (tzv. úroveň 1 - typicky PLC), dohledovou úroveň (tzv. úroveň 2 – typicky HMI) a serverovou část (tzv. úroveň 3 - typicky SCADA server). Řídicí systém je oddělen demilitarizovanou zónou od klasických IT systémů.
- (bbb) **„Secure by Design“** (tzv. bezpečnost v rámci návrhu) – je označení IT/OT systém, který byl navržen od základu tak, aby byl bezpečný. Znamená to, že návrhový vzor je volen tak, aby jeho znalost (tj. znalost principů práce IT/OT systému) neohrozila bezpečnost.
- (ccc) **„SLA“** (tzv. Service Level Agreement) – je dohoda o úrovni poskytovaných služeb, formální smluvní dokument, který definuje úroveň, rozsah, kvalitu a dostupnost poskytované služby, včetně odpovědností a sankcí při nedodržení sjednaných podmínek.
- (ddd) **„SL-T“** (tzv. Target Security Level) – označuje cílovou úroveň bezpečnosti, kterou má systém, zóna nebo komponenta dosáhnout.
- (eee) **„Smluvní podmínky“** jsou Smluvní podmínky pro dodávku technologických zařízení a projektování-výstavbu elektro – a strojně-technologického díla a pozemních a inženýrských staveb projektovaných zhotovitelem; Smluvní podmínky zahrnují tzv. Obecné podmínky ve znění tzv. Zvláštních podmínek tak, jak byly součástí smlouvy mezi Zhotovitelem a Objednatelem.
- (fff) **„SMTP“** (tzv. Simple Mail Transfer Protocol) – je základní internetový protokol pro odesílání e-mailů mezi poštovními servery a z poštovních klientů na servery.
- (ggg) **„SFTP“** (tzv. SSH File Transfer Protocol) – je bezpečný protokol pro přenos souborů, který zajišťuje šifrovaný přenos dat i autentizaci.
- (hhh) **„SIL“** (tzv. Safety Integrity Level) – je kvantitativní měřítko úrovně bezpečnostní integrity bezpečnostních funkcí v automatizovaných systémech.

- (iii) **„Visio“** – je grafický nástroj pro vytváření schémat, diagramů a technických výkresů
- (jjj) **„VFD“** (tzv. Variable Frequency Drive) – je měnič frekvence, je elektronické zařízení používané k řízení otáček a točivého momentu elektromotoru prostřednictvím regulace frekvence a napětí napájení motoru.
- (kkk) **„Vodní dílo“** – je soubor konstrukcí na vodním toku a v jeho přímém okolí, které svým koordinovaným (funkce řízení) spolupůsobením zajišťují mimo jiné dostatečnou plavební hloubku (funkce vzdutí) a / nebo umožňují plavební prostupnost toku (funkce proplavení). Součástí vodního díla se zde rozumí i konstrukce a budovy technologického, servisního a personálního zázemí (funkce podpůrná).
- (III) **„VPN“** (tzv. Virtual Private Network) – virtuální privátní síť, chrání své uživatele šifrováním jejich dat a maskováním jejich IP adres.
- (mmm) **„WAF“** (tzv. Web Application Firewall) – je specializovaný bezpečnostní systém, který chrání webové aplikace před škodlivými požadavky a útoky na aplikační vrstvě.
- (nnn) **„XLSX“** – je souborový formát pro tabulky vytvořené v Microsoft Excelu
- (ooo) **„Zadávací dokumentace“** – je soubor dokumentů, údajů, požadavků a technických podmínek Objednatele vymezujících předmět veřejné zakázky v podrobnostech nezbytných pro jeho vyprojektování, provedení a dokončení.
- (ppp) **„ŽP“** – životní prostředí

3 VZTAH K BEZPEČNOSTI ZDRAVÍ A PRÁCE

3.1 PŘEDNOST BOZP PŘI ŘEŠENÍ KYBERNETICKÉ BEZPEČNOSTI

Při implementaci jakýchkoliv opatření kybernetické bezpečnosti u řídicích systémů musí mít za všech okolností přednost ochrana života, zdraví osob a životního prostředí. Všechna opatření v oblasti kybernetické bezpečnosti musí být navržena, realizována a provozována v souladu s platnými předpisy v oblasti bezpečnosti práce (BOZP), požární ochrany (PO) a ochrany životního prostředí (ŽP).

Dojde-li k jakémukoliv konfliktu mezi požadavkem na kybernetické bezpečnosti a požadavky BOZP, PO nebo ŽP, má přednost plnění zákonných a provozních požadavků na BOZP, PO a ŽP. Kybernetická bezpečnost musí být vždy implementována tak, aby žádným způsobem nesnižovala bezpečnost pracovního prostředí ani funkční spolehlivost technických zařízení z hlediska BOZP.

3.2 INFORMOVÁNÍ OBJEDNATELE PŘI NARUŠENÍ BOZP

Zhotovitel je povinen zajistit, aby jakákoliv navržená bezpečnostní opatření, konfigurace nebo technologický zásah neohrozily život nebo zdraví osob ani integritu provozního prostředí. Pokud Zhotovitel nebo jím pověřený pracovník zjistí, že navržené nebo požadované opatření může mít potenciálně negativní dopad na BOZP, PO nebo ŽP:

- (a) nesmí být takové opatření realizováno;
- (b) musí být neprodleně informován Objednatel;
- (c) Zhotovitel je povinen aktivně vyhodnotit kybernetická rizika ve vztahu k BOZP a navrhnout alternativní řešení, které bude bezpečné z hlediska provozu i kybernetické bezpečnosti;

- (d) pokud daná oblast není dostatečně upravena ve smluvní nebo technické dokumentaci, musí Zhotovitel vždy iniciativně kontaktovat Objednatele za účelem projednání dalšího postupu.

3.3 KYBERNETICKÉ INCIDENTY S DOPADEM NA BOZP

V případě kybernetické události, incidentu nebo selhání bezpečnostního opatření související s řídicími systémy, které by mohlo:

- (a) ohrozit zdraví nebo životy osob;
- (b) ohrozit bezpečnost práce na místě;
- (c) narušit ochranu provozního nebo životního prostředí.

Zhotovitel je povinen:

- (a) okamžitě informovat Objednatele o reálném nebo potenciálním dopadu;
- (b) zahájit nápravná opatření k zajištění bezpečnosti prostředí a osob;
- (c) poskytnout Objednateli součinnost při řešení incidentu dle stanoveného eskalačního postupu a v souladu s provozními předpisy vodního díla.

V krizových nebo nejasných situacích musí Zhotovitel vždy upřednostnit ochranu osob a provozní bezpečnost před jakýmkoliv standardními postupy kybernetického bezpečnosti.

4 ZÁVAZNÉ LEGISLATIVNÍ A NORMATIVNÍ RÁMCE

4.1 SOUVISEJÍCÍ PRÁVNÍ RÁMCE

Zhotovitel je povinen navrhnout a implementovat v plném souladu se všemi platnými a účinnými právními předpisy, technickými normami a závaznými metodickými dokumenty v oblasti kybernetické bezpečnosti.

Tento právní a normativní rámec tvoří závazný základ pro bezpečnostních opatření a vztahuje se na celý životní cyklus realizovaného řešení – od návrhu přes implementaci, testování, uvedení do provozu až po údržbu a případné vyřazení z provozu.

4.2 ZÁVAZNÉ PRÁVNÍ PŘEDPISY A NORMY

Zejména následující právní předpisy a normy jsou pro Zhotovitele závazné z hlediska implementace kybernetické bezpečnosti pro řídicí systémy a doprovodné OT technologie:

- (a) zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů;
- (b) tzv. nový zákon o kybernetické bezpečnosti (sněmovní tisk č. 759, předpokládaná účinnost 1. 11. 2025¹);
- (c) související prováděcí vyhlášky vydané Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB);
- (d) evropské a mezinárodní rámce, pokud jsou na základě zákona nebo vnitřních pravidel Objednatele relevantní, např.:

¹ Tzv. nový zákon o kybernetické bezpečnosti je pro Zhotovitele závazný i tehdy, pokud k jeho účinnosti dojde po tzv. Základním datu ve smyslu Pod-čl. 1.1.3.1 Smluvních podmínek.

- (i) doporučení a metodiky ENISA (Evropská agentura pro kybernetickou bezpečnost);
 - příslušné části normativní řady ČSN EN IEC 62443 na které se tato legislativa odkazuje (zejména 2-1, 2-4, 3-2 a 3-3);
 - normy ISO/IEC 27001, 27005, 27019, pokud se vztahují k řízení rizik související se s kybernetickou bezpečností řídicích systémů.

Zhotovitel odpovídá za to, že plnění bude navrženo a realizováno tak, aby bylo v každém okamžiku v souladu s aktuálně účinnou právní úpravou. V případě, že během realizace Vodního díla vstoupí v účinnost nové právní předpisy nebo dojde k aktualizaci závazných norem, je Zhotovitel povinen v souladu se smlouvou jejich požadavky do řešení promítnout (typicky prostřednictvím Článku 13 [Variace a úpravy] Smluvních podmínek).

4.3 MOŽNOSTI ODCHÝLENÍ SE OD STANOVENÝCH POŽADAVKŮ

Od bezpečnostních požadavků uvedených v tomto dokumentu je možné se odchýlit pouze za splnění všech následujících podmínek:

- (a) odchylka byla předem písemně schválena Objednatelem, a to na základě zdůvodněné žádosti Zhotovitele;
- (b) navržené řešení prokazatelně zajišťuje ekvivalentní nebo vyšší úroveň bezpečnosti než požadovaná specifikace, a toto tvrzení je podloženo technickou dokumentací a odborným zdůvodněním;
- (c) odchylka vychází z doporučení nebo metodických pokynů vydaných uznávanou odbornou autoritou (např. NÚKIB, ENISA, ISA/IEC, nebo obdobnou mezinárodní institucí), které jsou relevantní pro daný typ opatření
- (d) pokud navrhované řešení prokazatelně zajistí vyšší nebo ekvivalentní úroveň kybernetické bezpečnosti, a toto bude řádně zdokumentováno;
- (e) na základě doporučení a metodiky NÚKIB, ENISA a dalších uznávaných autorit, pokud jsou relevantní pro realizaci bezpečnostního požadavku.

4.4 NOVÉ POŽADAVKY ZE STRANY OPRÁVNĚNÝCH ORGÁNŮ

V případě, že v průběhu realizace řídicího systému dojde ke vzniku nových požadavků na oblast kybernetické bezpečnosti ze strany oprávněných orgánů veřejné moci týkající se tohoto projektu, je Zhotovitel povinen tyto požadavky respektovat, bezodkladně zohlednit a v souladu se smlouvou (typicky prostřednictvím Článku 13 [Variace a úpravy] Smluvních podmínek) začlenit do realizace řídicího systému. Tímto se rozumí zejména:

- (a) stanoviska, metodická doporučení, rozhodnutí či jiné závazné nebo směrodatné výstupy vydané Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB);
- (b) nové nebo aktualizované požadavky vyplývající z činnosti jiných příslušných státních nebo dozorových orgánů (např. NBÚ, Ministerstvo vnitra, EU agentury, orgány krizového řízení);
- (c) aktualizace zákonných povinností nebo bezpečnostních standardů, které se vztahují na realizované řídicí systémy nebo na Objednatele jakožto provozovatele řídicího systému či kritické infrastruktury;

- (d) další požadavky v oblasti kybernetické bezpečnosti, které mohou mít vliv na návrh realizace řídicího systému mohou vyplynout z jednání o předběžných nabídkách, z bezpečnostních auditů, nebo ze změn právních či technických předpisů.

Tato povinnost platí i v případě, že požadavky byly adresovány primárně Objednateli, nikoliv přímo Zhotoviteli. V takovém případě poskytne Objednatel Zhotoviteli nezbytnou součinnost, včetně předání dokumentace, vysvětlení kontextu a definování rozsahu dopadů na předmět plnění.

4.5 ZMĚNOVÉ ŘÍZENÍ PŘI VÝSKYTU NOVÝCH POŽADAVKŮ

V případě, že v průběhu realizace řídicích systémů dojde ke vzniku nových požadavků ze strany oprávněných orgánů veřejné moci (viz část I., 4.4 [Nové požadavky ze strany oprávněných orgánů]), je Zhotovitel povinen postupem podle smlouvy zajistit:

- (a) vyhodnocení dopadu nových požadavků na rozsah, architekturu, harmonogram a náklady realizace řídicích systémů;
- (b) návrh technického řešení, které zabezpečí naplnění nových požadavků v souladu s existujícím konceptem kybernetické bezpečnosti, právním rámcem a smlouvou. Návrh musí být v rozsahu umožňujícím jeho odborné posouzení;
- (c) doplnění nebo aktualizaci projektové dokumentace, bezpečnostní architektury, analýz rizik, návrhu bezpečnostních opatření a dalších souvisejících výstupů, pokud se na ně nové požadavky vztahují.

4.6 POŽADAVKY NA DOKUMENTACI ZMĚN

Každá změna navržená nebo realizovaná v rámci řídicích systémů, která má dopad na kybernetickou bezpečnost, architekturu systému, technické řešení nebo smluvní plnění, musí být řádně a úplně zdokumentována. Dokumentace změn je nedílnou součástí výstupů Zhotovitele a slouží jako základní podklad pro technickou, provozní a bezpečnostní správu systému po předání řídicích systémů. Zhotovitel je povinen zajistit, že každá změna bude doložena těmito prvky:

- (a) identifikace změny:
 - jedinečné označení změny,
 - název změny, stručný popis a důvod změny (např. změna v důsledku nové vyhlášky NÚKIB);
 - datum návrhu a realizace změny;
- (b) popis dopadu změny:
 - specifikace dotčených částí systému (např. konkrétní síťový segment, bezpečnostní zóna, zařízení, dokumentace);
 - vyhodnocení dopadu na bezpečnostní opatření, provoz, rizika a soulad s právními předpisy;
 - identifikace, zda změna vyžaduje schválení Objednatele;
- (c) aktualizovaná dokumentace:

- nové nebo upravené verze technické a bezpečnostní dokumentace (např. síťová architektura, zóny a konduity, seznam technických aktiv a komponent, řízení přístupů);
 - aktualizace provozních scénářů, pokud změna ovlivňuje funkčnost;
- (d) schvalovací záznam:
- záznam o schválení změny Objednatelům (včetně podpisu, datace nebo elektronického potvrzení);
 - pokud změna nevyžaduje schválení, uvedení odůvodnění a jméno odpovědné osoby za rozhodnutí.

Tato dokumentační povinnost platí i pro změny vyvolané vnějšími vlivy – např. rozhodnutími orgánů veřejné moci, aktualizacemi právních předpisů, nebo zjištěním nových kybernetických rizik během realizace projektu.

4.7 SOUVISEJÍCÍ STANDARDY KYBERNETICKÉ BEZPEČNOSTI

Pro účely návrhu, implementace a provozní správy kybernetické bezpečnosti řídicích systémů je Zhotovitel povinen zohlednit a ve všech relevantních oblastech se opírat o uznávané mezinárodní a evropské standardy v oblasti kybernetické a informační bezpečnosti:

- (a) ČSN EN IEC 62443-3-2:2021 „*Bezpečnost pro průmyslové automatizační a řídicí systémy – Část 3-2: Bezpečnostní analýza rizik pro systém*“ → stanovuje metodiku pro hodnocení rizik v prostředí IACS (tzv. Industrial Automation and Control Systems) a jejich přenos do požadavků na zabezpečení systému;
- (b) ČSN EN IEC 62443-3-3:2013 „*Bezpečnost pro průmyslové automatizační a řídicí systémy – Část 3-3: Systémové bezpečnostní požadavky a bezpečnostní úrovně*“ → definuje požadovaná opatření v závislosti na stanovené cílové bezpečnostní úrovni (SL-T), včetně logického oddělení, řízení přístupů, detekce a reakce;
- (c) ČSN EN IEC 62443-4-2:2019 „*Bezpečnost pro průmyslové automatizační a řídicí systémy – Část 4-2: Technické požadavky na komponenty IACS*“ → určuje minimální bezpečnostní parametry pro jednotlivé typy zařízení (např. PLC, HMI, komunikační brány), které budou nasazeny v rámci systému;
- (d) ČSN EN ISO/IEC 27001:2023 „*Informační technologie – Bezpečnostní techniky – Systémy řízení informační bezpečnosti – Požadavky*“ → poskytuje rámec pro zavedení systému řízení bezpečnosti informací (ISMS), relevantní zejména pro integrační, provozní nebo dohledové části řešení;
- (e) Další normy řady ISO/IEC 27000, IEC 62443, případně doporučení ENISA, ETSI, pokud jsou relevantní pro specifické části technického řešení nebo odpovídají charakteru prostředí (např. segmentace sítě, detekce anomálií, vzdálený přístup, zálohování, krizové řízení apod.);

Standardy uvedené v tomto článku slouží jako odborný a technický rámec pro doplnění, konkretizaci a zdůvodnění bezpečnostních opatření pro realizované řídicí systémy. Pokud není v této dokumentaci stanoveno jinak, má jejich uplatnění doporučující charakter, avšak v případě absence podrobné specifikace požadavků jsou považovány za výchozí referenci.

5 SOUVISEJÍCÍ DOKUMENTACE

5.1 DOKUMENTY, PROVÁZANOST A JEJICH HIERARCHIE

Tento dokument tvoří nedílnou součást Zadávací dokumentace a je obsahově i významově propojen s dalšími jejími částmi. Všechny dokumenty Zadávací dokumentace musí být při návrhu, realizaci a vyhodnocování bezpečnostních opatření chápány jako vzájemně provázané, přičemž výkladové nesrovnalosti musí být řešeny v souladu s touto stanovenou hierarchií závaznosti:

- (a) zákonné a normativní požadavky, jak jsou uvedeny v odstavci 2 "*Závazné právní předpisy a normy* „– zejména právní předpisy, závazné vyhlášky, mezinárodní a národní standardy, které mají právní nebo technickou závaznost pro daný typ řešení, a nadřazené dokumenty Zadávací dokumentace;
- (b) tento dokument, tj. dokument specifikující požadavky na kybernetickou bezpečnost technických a řídicích systémů;
- (c) ostatní dokumenty Zadávací dokumentace.

5.2 PRÁVO NA ÚPRAVU DOKUMENTACE BĚHEM REALIZACE

Objednatel si vyhrazuje právo v průběhu realizace projektu aktualizovat, zpřesnit nebo rozšířit kterékoliv části Zadávací dokumentace, včetně tohoto dokumentu, a to postupem podle smlouvy (viz zejména Článek 13 [Variace a úpravy] Smluvních podmínek).

5.3 ODPOVĚDNOST ZA SPRÁVU A DOPLNĚNÍ DOKUMENTACE

Objednatel odpovídá za zpřístupnění a aktualizaci dokumentů, které jsou jeho interním výstupem nebo součástí řízené dokumentace.

Zhotovitel je povinen na požádání doložit, že výchozí podklady při návrhu a realizaci zohlednil.

Pokud Zhotovitel zjistí nesrovnalost nebo nedostatečnost podkladu, je povinen tuto skutečnost oznámit Objednateli a vyžádat si doplnění, objasnění nebo souhlas s alternativním postupem.

ČÁST II. POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI NA ZHOTOVITELE

Tato část specifikuje souhrnné požadavky na Zhotovitele v oblasti kybernetické bezpečnosti, které se vztahují k celému průběhu realizace řídicích systémů, jejich částí a dalších OT systémů na vodním díle (např. kamerových systémů, bezpečnostních systémů apod.). Cílem je zajistit, aby kybernetická bezpečnost byla systémově řízena, průběžně zajišťována a důsledně kontrolována ve všech fázích projektu – od přípravy až po předání, provozní podporu a uzavření smluvního vztahu. Struktura této části odpovídá fázím životního cyklu projektu a zahrnuje následující logicky navazující fáze:

- **požadavky na kybernetickou bezpečnost při přípravě projektu²** – zahrnuje např. povinnosti v oblasti školení, předložení metodiky řízení bezpečnosti, jmenování odpovědných osob, uzavření NDA, provedení úvodní analýzy rizik a harmonogramu bezpečnostních činností (viz část II, sekce 6 [Požadavky na kybernetickou bezpečnost při přípravě projektu]);
- **požadavky na kybernetickou bezpečnost v průběhu implementace řídicích systémů** – zahrnuje např. návrh bezpečnostní architektury, zón a conduitů, kontrolu implementace bezpečnostních opatření, provedení zkoušek funkčnosti a bezpečnosti, aktualizaci rizik a dokumentace (viz část II, sekce 7 [Požadavky na kybernetickou bezpečnost v průběhu implementace]);
- **požadavky na kybernetickou bezpečnost po implementaci řídicích systémů³** – zahrnuje např. zajištění předání bezpečnostní dokumentace, ukončení přístupů, výmaz citlivých dat, poskytování provozní podpory v režimu bezpečnostní shody, případné SLA pro reakci na incidenty (viz část II, sekce 8 [Požadavky na kybernetickou bezpečnost na zhotovitele po implementaci]);
- **požadavky na kybernetickou bezpečnost při ukončení projektu** – zahrnuje např. deaktivaci uživatelských účtů a přístupových prostředků Zhotovitele a subdodavatelů, ukončení všech aktivních síťových spojení a vzdálených přístupů včetně VPN a servisních kanálů, zabezpečení odstranění dat Objednatele na systémech Zhotovitele (viz část II, sekce 9 [Ukončení projektu]).

6 POŽADAVKY NA KYBERNETICKOU BEZPEČNOST PŘI PŘÍPRAVĚ PROJEKTU

Tato část zahrnuje požadavky na organizaci Zhotovitele, tedy jeho celkovou bezpečnostní způsobilost, interní procesy a schopnost nést odpovědnost za kybernetickou bezpečnost řídicích systémů včetně řetězce podzhotovitelů.

² V kontextu smlouvy o dílo, resp. Díla jako celku, se jedná o fázi projektování, jak je popsána v Části III dokumentu Požadavky objednatele, který je součástí smlouvy.

³ V kontextu smlouvy o dílo, resp. Díla jako celku, se jedná o fázi, kdy dochází k dokončení Díla a navazuje plnění ze servisní smlouvy, která je součástí Zadávací dokumentace.

6.1 PRINCIP SECURE BY DESIGN

Princip Secure by Design znamená, že bezpečnost je systematicky integrována do všech fází návrhu, realizace i následného provozu řídicích systémů. Namísto dodatečného doplňování bezpečnostních opatření po dokončení je bezpečnost považována za základní součást architektury řešení již od samého počátku.

Zhotovitel je povinen navrhnout a implementovat řídicí systémy tak, aby byla bezpečnost nedílnou součástí každého návrhového rozhodnutí, použité technologie i implementovaného procesu. Očekává se jeho aktivní zapojení, spolupráce s objednatelem a schopnost promítnout bezpečnostní principy do návrhu, vývoje i uvádění do provozu.

V rámci přístupu Secure by Design má zhotovitel prostor využít svou odbornost a zkušenosti při hledání optimálních řešení, která nejen plní požadovanou funkci, ale zároveň minimalizují rizika v oblasti kybernetické a provozní bezpečnosti. Rozsah a způsob aplikace principu Secure by Design je závazný pro všechny části řídicího systému. Konkrétní požadavky a podmínky uplatnění tohoto principu jsou dále specifikovány v dalších částech smluvní dokumentace. Řídicí systém musí být primárně navržen a implementován tak, aby splňoval zásady bezpečné architektury řídicích systémů v souladu se sekci 10 [Technické požadavky kybernetické bezpečnosti].

6.2 ORGANIZAČNÍ ZPŮSOBILOST

Zhotovitel musí na výzvu Správce stavby prokázat, že jako organizace disponuje systémovým přístupem k implementaci kybernetické bezpečnosti, schopností řídit bezpečnostní rizika a schopností nést odpovědnost za bezpečnost celého řešení.

Organizace Zhotovitele musí splňovat následující podmínky:

- (a) Zhotovitel musí mít nejpozději do 1 roku od účinnosti smlouvy zavedený a certifikovaný systém řízení bezpečnosti informací certifikovaný dle ISO/IEC 27001 (tzv. ISMS), jehož implementaci a platnost je povinen Objednateli prokázat;
- (b) v případě vývoje a implementace řídicích systémů musí Zhotovitel prokázat znalost řady norem IEC 62443, jak je uvedeno v odstavci 4.7 [Související standardy kybernetické bezpečnosti].

6.3 DŮVĚRNOST INFORMACÍ A REŽIM NDA

Veškeré informace, výstupy a dokumentace související s návrhem a implementací řídicích systémů v oblasti kybernetické bezpečnosti podléhají režimu důvěrnosti a nejsou veřejně přístupné.

Zhotovitel bere na vědomí, že:

- (a) dokumenty a informace týkající se bezpečnostní architektury, analýzy rizik, seznamů zranitelností, síťové infrastruktury, návrhů zón a konduitů, přístupových práv, záznamů o incidentech a dalších bezpečnostních mechanismů představují citlivé údaje, které mohou mít charakter utajovaných, provozně důvěrných nebo jinak chráněných informací;
- (b) přístup k těmto informacím může být umožněn výhradně osobám, které jsou k tomu určeny a schváleny Objednatelem, a které uzavřely příslušnou dohodu o mlčenlivosti (tzv. NDA).

Podmínky přístupu k informacím:

- (a) přístup k dokumentům a informacím týkajícím se kybernetické bezpečnosti bude Zhotoviteli (včetně jeho Poddodavatelů, zaměstnanců nebo jiných spolupracujících osob) umožněn pouze po předchozím uzavření NDA v rozsahu stanoveném Objednatelem;
- (b) vzor dohody o mlčenlivosti je součástí Zadávací dokumentace;
- (c) Zhotovitel odpovídá za to, že tuto dohodu uzavřou všechny osoby, které budou mít přístup k důvěrným informacím v rámci plnění zakázky;
- (d) jakékoliv neoprávněné zpřístupnění, ztráta, zneužití nebo šíření těchto informací bude považováno za závažné porušení smlouvy a může vést k právním a smluvním postihům.

6.4 POŽADAVKY NA PERSONÁLNÍ ZAJIŠTĚNÍ ZHOTOVITELE

Pracovníci Zhotovitele, kteří se účastní na návrhu a implementaci řídicích systémů, musí mít odpovídající odborné znalosti a být pravidelně školeni v oblasti OT kybernetické bezpečnosti.

Personální zajištění Zhotovitele musí splňovat následující požadavky:

- (a) definovat jasnou strukturu odpovědností a rolí v oblasti kybernetické bezpečnosti a jmenovat pracovníka odpovědného za kybernetickou bezpečnost řídicích systémů, který musí mít prokazatelnou odbornou kvalifikaci v OT kybernetické bezpečnosti (např. certifikaci řady IEC 62443 Design Specialist, vyšší nebo obdobnou);
- (b) všichni pracovníci podílející se na vyprojektování, provedení nebo dokončení řídicích systémů musí absolvovat školení zaměřené na kybernetickou bezpečnost řídicích systémů prostředí;
- (c) evidence školení a kvalifikací musí být kdykoliv dostupná ke kontrole Objednatelem;
- (d) v případě odchodu pracovníka během projektu musí být zajištěno předání jeho znalostí nástupci a zachování kvalifikace nástupce;
- (e) všichni pracovníci musí být prokazatelně vázáni k mlčenlivosti a ochraně důvěrných informací.

6.5 PODZHOTOVITELÉ

Zhotovitel plně přebírá odpovědnost v oblasti kybernetické bezpečnosti za činnost Podzhotovitelů, kteří se účastní na návrhu a implementaci řídicích systémů a zajistil, že na ně budou přeneseny stejné bezpečnostní požadavky, které platí pro něj samotného.

Na všechny podzhotovitele se vztahují stejné bezpečnostní požadavky jako na Zhotovitele, včetně požadavků stanovených tímto dokumentem, interními politikami Objednatele a příslušnými právními předpisy. Podzhotovitel musí splňovat následující požadavky:

- (a) Každý podzhotovitel musí být:
 - (i) prověřen z hlediska bezpečnostní způsobilosti;
 - (ii) písemně zavázán prostřednictvím smlouvy, která přenáší odpovědnost a konkrétní bezpečnostní povinnosti na Zhotovitele;
 - (iii) seznámen s bezpečnostními standardy Objednatele a musí je dodržovat;
- (b) Podzhotovitelé musí:
 - (i) podepsat bezpečnostní dohodu o mlčenlivosti (NDA);

- (ii) podepsat případně další dokumenty požadované objednatelem (např. prohlášení o školení, přístupová oprávnění);
 - (iii) na požádání tuto evidenci zpřístupnit objednateli;
- (c) Jakákoliv změna podzhotovitele nebo přidání nové osoby s přístupem k řídicím systémům musí být:
 - (i) předem oznámena Objednateli;
 - (ii) schválena z hlediska bezpečnosti;
 - (iii) doložena dokumentací podle požadavků výše.
- (d) V případě, že podzhotovitel poruší bezpečnostní pravidla nebo způsobí incident, nese odpovědnost Zhotovitel, a to v plném rozsahu – včetně nápravných opatření, odpovědnosti za škodu a spolupráce při vyšetřování.

7 POŽADAVKY NA KYBERNETICKOU BEZPEČNOST V PRŮBĚHU IMPLEMENTACE

7.1 POŽADAVKY NA KYBERNETICKOU BEZPEČNOST V PRŮBĚHU IMPLEMENTACE ŘÍDICÍCH SYSTÉMŮ

Zhotovitel musí v rámci projektu uplatnit strukturované řízení bezpečnosti, včetně návrhu, schválení a realizace opatření podle platných norem.

- (a) Zhotovitel musí v průběhu návrhu a implementace řídicích systémů splňovat následující požadavky:
- (b) dodržovat všechny požadavky uvedené v tomto dokumentu, včetně standardů, politik, směrnic a provozní dokumentace Objednatele týkající se OT i IT kybernetické bezpečnosti;
- (c) integrovat kybernetickou bezpečnost jako součást návrhu, implementace, testování i provozu systému;
- (d) uplatňovat zásady „Secure by Design“ ve všech fázích projektu;
- (e) průběžně komunikovat s Objednatelem a účastnit se pravidelných i ad hoc jednání o stavu bezpečnostní implementace, rizicích, rozhodovacích bodech a plánovaných změnách a na vyžádání zpracovat a s předstihem předložit podklady pro tato jednání;
- (f) poskytovat potřebnou součinnost pracovníkům Objednatele, odborným konzultantům nebo orgánům veřejné moci během auditů, inspekcí a dalších kontrolních činností souvisejících s bezpečností řídicích systémů;
- (g) zavést systém řízení změn a zajistit, že každá změna řídicích systémů bude zdokumentována, posouzena z hlediska kybernetické bezpečnosti a schválena odpovědnou osobou.

7.2 DODÁVANÁ ZAŘÍZENÍ A KOMPONENTY

Veškerá zařízení, komponenty a softwarové prvky dodané v rámci řídicích systémů musí splňovat požadavky Objednatele na provoz v OT prostředí a zároveň být v souladu se rámci uvedeným v sekci 4 [Závazné legislativní a normativní rámce] a s technickými požadavky kybernetické bezpečnosti v sekci 10 [Technické požadavky kybernetické bezpečnosti].

Zhotovitel je povinen vyhovět následujícím požadavkům:

- (a) všechna zařízení a komponenty musí být určena pro provoz v prostředí OT a odpovídat provozním, environmentálním a síťovým podmínkám daného místa nasazení;
- (b) Zhotovitel musí být schopen doložit, že zařízení, software a firmware byly prověřeny z hlediska bezpečnosti, integrity a důvěryhodnosti výrobce a že dodávané komponenty v rámci smlouvy jsou aktuální k datu dodání a že neobsahují známé kritické zranitelnosti. Tuto skutečnost lze doložit například výstupem z CVSS databáze, ze skeneru zranitelností (např. Nessus, OpenVas) či jiným vhodným způsobem tak, aby v případě potřeby bylo možné zkontrolovat aktuálnost dodávaných komponent a zda neobsahují bezpečnostní zranitelnosti v době dodání;
- (c) konfigurace zařízení musí umožnit jejich zařazení do bezpečnostních zón a konduktů dle architektury řídicího systému včetně řízení komunikace v souladu se zásadou nejmenších privilegií (tzv. least privilege) a omezením neautorizovaného provozu; zónová architektura vychází z principů definovaných v normě IEC 62443, přičemž bezpečnostní zóna představuje logicky nebo fyzicky vymezenou část infrastruktury s jednotnými bezpečnostními požadavky a úrovní důvěry; v rámci daného řešení se předpokládá minimálně čtyřzónová segmentace: IT DMZ (hlavní perimetrická ochrana vodního díla), IT zóna (systémy podnikové informatiky), OT DMZ (perimetrická ochrana řídicích systémů) a OT zóna (řídicí a provozní technologie); na základě architektonického návrhu může být Zhotovitelem realizována i podrobnější segmentace, například oddělení jednotlivých řídicích systémů v rámci OT zóny;
- (d) na žádost Objednatele je Zhotovitel povinen doložit původ zařízení a jeho dodavatele k zajištění důvěryhodnosti zařízení vzhledem k rizikům spojeným s dodávkami z třetích zemí; Zhotovitel nepoužije zařízení ani jednotlivé komponenty takových výrobců, na které bylo v minulosti NÚKIB vydáno varování nebo byly obdobným dokumentem označeny jako potenciálně rizikové z hlediska kybernetické bezpečnosti.

8 POŽADAVKY NA KYBERNETICKOU BEZPEČNOST NA ZHOTOVITELE PO IMPLEMENTACI

Tato sekce zahrnuje požadavky související s dokončením Díla a provozem, vyhodnocením a udržováním řídicího systému z bezpečnostního hlediska po uvedení do provozu.

8.1 ŠKOLENÍ OBJEDNATELE

Zhotovitel je povinen v rámci Díla vyškolit personál Objednatele pro bezpečný a správný provoz nově dodaných řídicích systémů.

- (a) Zhotovitel musí zajistit zaškolení personálu Objednatele na uživatelské i administrátorské úrovni;
- (b) Zhotovitel musí zajistit zaškolení personálu Objednatele ve vztahu k reakci na bezpečnostní incidenty, jejich obnovy a další nouzové scénáře a postupy v souvislosti s řídicími systémy;
- (c) dokumentace ke školení (agenda, prezenční listiny, materiály) musí být archivována a předána Objednateli.

8.2 ZKOUŠKY A OVĚŘENÍ KYBERNETICKÉ BEZPEČNOSTI

Zhotovitel je povinen v rámci Díla provést přijímací zkoušky řídicích systémů se zaměřením na ověření funkčnosti a účinnosti bezpečnostních opatření dle požadavků Objednatele a v souladu s legislativním a normativním rámcem dle sekce 4 [Závazné legislativní a normativní rámce]. Tyto zkoušky slouží k prokázání, že systém splňuje stanovenou bezpečnostní úroveň a je odolný vůči relevantním kybernetickým hrozbám. V rámci zkoušek musí Zhotovitel zajistit následující:

- (a) provedení přijímacích akceptačních testů bezpečnostních funkcí systému, včetně ověření segmentace sítě, správného rozdělení bezpečnostních zón a konduitů, nastavení firewallů a řízení komunikace mezi jednotlivými částmi OT sítě;
- (b) ověření správné konfigurace přístupových práv lokálního i vzdáleného připojení a autentizačních mechanismů (včetně více faktorové autentizace, správy uživatelů, zásad minimálních oprávnění a evidence přístupů);
- (c) poskytnout součinnost při provedení testů odolnosti systému vůči základním typům kybernetických útoků a realizace penetračního testování na straně Objednatele, jehož cílem je simulace reálných útokových scénářů zaměřených na identifikaci zranitelností systému; testování bude zahrnovat pokusy o neoprávněný přístup (např. brute force útoky, získání přihlašovacích údajů), útoky typu man-in-the-middle (MITM), útoky na dostupnost služeb (např. DoS/DDoS), zneužití špatně nakonfigurovaných služeb nebo otevřených portů, stejně jako prověření fyzických přístupů, zabezpečení vzdálené správy a rozhraní mezi IT a OT prostředím; testování provádí Objednatel nebo jím pověřený subjekt; součinnost Zhotovitele zahrnuje zejména zajištění přístupů, technických informací a přítomnosti odpovědných osob v průběhu testování; výsledkem testování musí být přehled zjištěných slabín a doporučení pro jejich odstranění; Zhotovitel se v návaznosti na servisní smlouvu zavazuje odstranit zjištěné zranitelnosti v časových lhůtách doporučených ve výstupní zprávě z penetračního testování;
- (d) že všechny nalezené bezpečnostní zranitelnosti budou před finální přejímkou zdokumentovány, klasifikovány podle závažnosti a buď odstraněny, nebo bude navrženo kompenzační opatření schválené Objednatelem.

8.3 PROVOZNÍ PODPORA PO IMPLEMENTACI

Po předání řídicích systémů do provozu je Zhotovitel povinen na základě servisní smlouvy zajistit přiměřenou podporu pro udržení bezpečnosti a funkčnosti dodaných řídicích systémů. Tato podpora zahrnuje poskytování aktualizací, řešení bezpečnostních událostí, asistenci při změnách nebo rozšířeních systému a průběžné informování o zjištěných rizicích a ukončení podpory použitých komponent. Podpora musí být poskytována v souladu s požadavky Objednatele a platnými bezpečnostními zásadami.

Forma a rozsah této podpory jsou upřesněny v servisní smlouvě, která je součástí Zadávací dokumentace.

Zhotovitel (pokud uzavře příslušnou servisní smlouvu) musí splňovat následující požadavky na podporu systému po implementaci:

- (a) Zhotovitel musí postupovat v souladu s dokumentací Objednatele a poskytovat technickou asistenci při řešení provozních problémů;
- (b) Zhotovitel je povinen zajistit zvýšenou úroveň technické a bezpečnostní podpory v období bezprostředně po uvedení OT systému do provozu za účelem průběžného sledování

chování systému, zajištění jeho stabilního a bezpečného provozu a bezodkladného řešení všech vzniklých problémů;

- (c) po celou dobu účinnosti servisní smlouvy zachovávat důvěrnost, integritu a dostupnost všech informací, se kterými zhotovitel během podpory pracuje;
- (d) poskytovat součinnost při vyhodnocování stavu bezpečnostních opatření a v případě zjištění nedostatků musí navrhnout korektivní nebo kompenzační opatření;
- (e) provádět funkční a bezpečnostní aktualizace softwaru, firmwaru a konfigurací prostřednictvím řízeného a testovaného procesu v kontrolovaném prostředí s minimálním dopadem na dostupnost řídicích systémů;
- (f) spolupracovat při změnách konfigurace nebo při rozšíření řídicích systémů;
- (g) všechny změny vykonávat prostřednictvím systému řízení změn a vést záznamy o provedených změnách, zásazích, aktualizacích a doporučeních, které byly v rámci podpory realizovány;
- (h) upozorňovat na blížící se konec životního cyklu (tzv. End of Support) klíčových komponent a doporučit další kroky.

8.4 DOKUMENTACE ŘÍDICÍCH SYSTÉMŮ A JEJÍ PŘEDÁNÍ OBJEDNATELI

Po implementaci řídicích systémů (avšak stále v rámci Díla) je Zhotovitel povinen předat Objednateli kompletní a srozumitelnou dokumentaci řídicího systému ve formátu umožňujícím její další využití, správu a bezpečný samostatný provoz.

Dokumentace musí splňovat následující požadavky (resp. obsahovat následující informace):

- (a) kompletní technická a bezpečnostní dokumentace řídicího systému včetně topologie sítě, zónové architektury, síťového schématu, seznamu dílčích komponent, seznam souvisejících aktiv, seznam sériových čísel, verzí firmwaru a další identifikační údaje
- (b) konfigurace bezpečnostních a přístupových pravidel síťových prvků;
- (c) přehled všech přístupových účtů, oprávnění a přístupových údajů včetně evidence uživatelských a servisních účtů a nastavení autentizačních mechanismů;
- (d) výsledky testování, kontrol a přejímacích zkoušek, včetně logování, výstupů z testů zranitelností a penetračního testování s doložením nápravných opatření;
- (e) dokumentace plán obnovy provozu řídicího systému po kybernetickém útoku nebo technickém selhání; plán obnovy provozu (Disaster Recovery Plan – DRP) je strukturovaný dokument, který stanovuje postupy a odpovědnosti pro obnovu funkčnosti řídicího systému do předem definovaného stavu po mimořádné události; plán musí zahrnovat identifikaci kritických komponent a jejich závislostí, scénáře selhání (kybernetické incidenty, hardwarové závady, ztráta konfigurace apod.), postupy pro zálohování a obnovu dat, stanovení priorit obnovy, odpovědnosti jednotlivých rolí, komunikační kanály a rozhodovací procesy; dále musí obsahovat časové parametry obnovy (RTO – Recovery Time Objective, RPO – Recovery Point Objective a MTD – Maximum Tolerable Downtime vypočítané v součinnosti s Objednatelem), přehled potřebných nástrojů a přístupových oprávnění, jakož i harmonogram pravidelného testování a revize plánu; plán musí být provádán s celkovým systémem řízení kontinuity provozu a schválen odpovědnou osobou;

- (f) provozní příručka a doporučené postupy pro správu a údržbu řídicích systémů, plán aktualizací, kontakty na technickou podporu a návrh systematické pravidelné údržby komponent;
- (g) na předchozí písemnou žádost Objednatele potvrzení, že žádná data, konfigurace nebo přístupy nezůstaly neoprávněně na straně Zhotovitele, Podzhotovitelů a jejich zaměstnanců, pokud nemají být zachovány pro plnění servisní smlouvy.

8.5 PODPORA PŘI ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Po předání řídicích systémů do provozu je nezbytné, aby Zhotovitel na základě servisní smlouvy zajišťoval efektivní podporu, rychlou odezvu a odbornou spolupráci při řešení incidentů.

Zhotovitel je povinen v souladu se servisní smlouvou dodržet následující požadavky na podporu při řešení bezpečnostních incidentů:

- (a) Zhotovitel musí postupovat dle plánu řízení bezpečnostních incidentů a plánu obnovy dodaných pro řídicí systém v rámci dokumentace dle odstavce 8.4 [Dokumentace řídicích systémů a její předání objednateli];
- (b) Zhotovitel je povinen zajistit adekvátní podporu pro každý bezpečnostní incident nahlášený Objednatelem bez zbytečného odkladu nebo jak je definováno v SLA.

9 UKONČENÍ PROJEKTU

Zhotovitel je povinen zajistit, aby ukončení jeho činností neohrozilo kybernetickou bezpečnost ani provozní kontinuitu řídicích systémů Objednatele. Před ukončením smluvního vztahu⁴ musí být realizována a prokazatelně zdokumentována všechna opatření k zabezpečení dat, přístupů, dokumentace a systémové správy. Proces ukončení musí být řízený, auditovatelný a transparentní, a to i v případě, že nedochází k okamžitému převzetí systému jiným dodavatelem nebo k předání do vlastní správy Objednatele.

Zhotovitel je povinen při ukončení plnění provést minimálně následující kroky:

- (a) deaktivovat veškeré uživatelské účty Zhotovitele a Podzhotovitelů, které byly vytvořeny nebo využívány v rámci realizace řídicích systémů;
- (b) odebrat přístupové prostředky jako jsou kryptografické klíče, tokeny, certifikáty, SSH přístupy a jiné autentizační prvky;
- (c) ukončit všechna aktivní síťová spojení a vzdálené přístupy, včetně VPN tunelů, servisních kanálů a přístupů prostřednictvím IDMZ nebo jiných rozhraní;
- (d) zajistit, aby nebyly ponechány žádné aktivní nebo neauditované zbytkové přístupy ze strany Zhotovitele nebo jeho subdodavatelů.
- (e) Pokud nebylo výslovně dohodnuto jinak, musí Zhotovitel:
 - (i) trvale odstranit nebo anonymizovat veškerá data Objednatele, která byla zpracovávána nebo uchovávána na systémech Zhotovitele;
 - (ii) zajistit vymazání všech záloh, pracovních kopií, dočasných souborů, souborů v testovacích nebo vývojových prostředích;

⁴ Objednatel předpokládá, že uvedené povinnosti budou aktivovány v čase, kdy bude plněna jen servisní smlouva (smlouva o dílo již bude splněna – Dílo bude dokončeno a předáno Objednateli).

- (iii) vyčistit e-mailovou komunikaci obsahující provozní nebo bezpečnostní informace, které nejsou nezbytné pro právní účely;
 - (iv) postup provést v souladu s platnými právními předpisy, zejména zákonem o kybernetické bezpečnosti, zákonem o ochraně osobních údajů a případnými vnitřními předpisy Objednatele.
- (f) Zhotovitel je povinen po dobu stanovenou Objednatelem nebo v přiměřeném rozsahu poskytnout součinnost při přechodu na jiného dodavatele nebo na vlastní správu Objednatele, a to zejména formou:
 - (i) účasti na předávacím jednání a spolupráce při ověření úplnosti výstupů;
 - (ii) předání všech relevantních konfiguračních a provozních dat;
 - (iii) poskytování technické konzultace a podpory v přechodném období;
 - (iv) zajištění kontinuity provozu systému během přechodu, a to bez přerušení, zpoždění nebo rizika narušení bezpečnosti.
- (g) Zhotovitel je povinen předložit Objednateli kompletní dokumentaci o realizaci všech bezpečnostních kroků při ukončení spolupráce, zejména:
 - (h) prohlášení o deaktivaci všech přístupů Zhotovitele a jeho zástupců do systémů, sítí a dat Objednatele;
 - (i) záznam o odstranění nebo anonymizaci dat, včetně identifikace datových úložišť, rozsahu a způsobu provedení;
 - (j) seznam předané dokumentace, technických výstupů a administrativních záznamů;
 - (k) jmenný seznam osob, které měly přístup k systémům, včetně jejich identifikace a rozsahu oprávnění.

ČÁST III. POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI NA ŘÍDICÍ SYSTÉMY A PROVOZNÍ TECHNOLOGIE

Tato část stanovuje soubor technických požadavků kybernetické bezpečnosti, které musí být zohledněny při návrhu, implementaci a provozu řídicích systémů, jejich částí a dalších OT systémů (např. kamerových systémů). Cílem je zajistit, aby řídicí systémy byly navrženy a provozovány způsobem, který minimalizuje rizika narušení důvěrnosti, integrity a dostupnosti provozu Vodního díla, a to především díky zajištění striktního oddělení lokálního IT prostředí od centrálního pomocí DMZ, od prostředí třetích stran a internetu a zároveň oddělením IT a OT prostředí s řídicími systémy pomocí IDMZ a jednotlivých řídicích systémů od sebe.

Zhotovitel musí pro zajištění kybernetické bezpečnosti řídicích systémů zavést bezpečnostní opatření, zařízení a nástroje, které zajistí:

- (a) omezení fyzického přístupu k řídicím systémům, omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům;
- (b) segmentaci komunikačních sítí řídicích systémů od jiných prostředí a segmentaci těchto komunikačních sítí podle odstavce 10.2 „*Bezpečnost komunikačních sítí*“ a souvisejícími principy segmentace dle normy ČSN IEC 62443;
- (c) omezení vzdálených přístupů a vzdálené správy řídicích systémů;
- (d) ochranu jednotlivých řídicích systémů před využitím známých hrozeb a zranitelností;
- (e) obnovitelnost dostupnosti řídicích systémů pomocí předem definovaného mechanismu zálohování tak, aby šly provést činnosti související s obnovením dostupnosti řídicího systému k plné funkčnosti systému po výpadku, poruše nebo kybernetickém incidentu (tyto činnosti mohou být sjednány na základě servisní smlouvy).

10 TECHNICKÉ POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI

10.1 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost je nedílnou součástí komplexního zabezpečení řídicího systému. Z tohoto důvodu musí být v rámci zabezpečení řídicích systémů zajištěna odpovídající úroveň fyzické bezpečnosti, která bude chránit řídicí systémy, zařízení a podpůrnou infrastrukturu před fyzickým narušením, krádeží, poškozením nebo zneužitím. Zhotovitel je povinen v návrhu i realizaci řídicích systémů zajistit splnění následujících požadavků:

- (a) řídicí systémy musí být zajištěny proti poškození, krádeži nebo zneužití nebo přerušení poskytování služby spojené se systémem, uzamčením rozvodných skříní a všech dalších míst, kde se systémy nebo jejich části nacházejí pro zamezení fyzického poškození (související povinnosti Zhotovitele jsou definovány smlouvou, zejména TPO v rámci Požadavků objednatele);
- (b) řídicí systémy musí mít stanoven fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a data, nebo ve které jsou umístěna technická aktiva řídicího systému;

- (c) jednotlivé fyzické bezpečnostní perimetry řídicího systému podle písmena (b) musí být zdokumentovány a s ohledem na důležitost umístěných technických aktiv být také rozdělené dle potřeby na jednotlivé úrovně fyzické ochrany;
- (d) řídicí systémy a jeho části musí být v rámci každého fyzického bezpečnostního perimetru, stanoveného podle písmene (c), chráněny odpovídajícími fyzickými bezpečnostními opatřeními, která odpovídají stanovené úrovni fyzické ochrany;
- (e) k zamezení neoprávněnému vstupu;
- (f) k zamezení poškození a neoprávněným zásahům;
- (g) k zajištění fyzické ochrany na úrovni objektů a v rámci objektů.
- (h) pro zajištění detekce narušení fyzického bezpečnostního perimetru musí být zajištěné evidování vstupů a přístupů do fyzického bezpečnostního perimetru.

10.2 BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ

Zhotovitel je povinen navrhnout a implementovat architekturu komunikační sítě řídicích systémů tak, aby byla v souladu s požadavky na kybernetickou bezpečnost, a zároveň umožňovala bezpečný, řízený a auditovatelný provoz v celém rozsahu technických prostředí souvisejících se systémem.

Síťová architektura musí odpovídat základním principům segmentace, řízení přístupů do jednotlivých zón a důvěryhodného přenosu dat mezi jednotlivými zónami a vrstvami systému. Systémy nesmí být realizovány jako tzv. „flat network“ – každý řídicí systém a jejich komponenty musí být jednoznačně zařazeny do odpovídající bezpečnostní zóny a segmentovány.

Řídicí systém musí splňovat následující požadavky v oblasti bezpečnosti komunikačních sítí:

- (a) Komunikační síť řídicích systémů musí být segmentována na samostatné bezpečnostní zóny. Zároveň musí být zajištěno, aby mezi zónami probíhala komunikace pouze přes řízené a bezpečnostně kontrolované konduity a všechna připojení pro vzdálený přístup, aktualizace nebo diagnostiku musí procházet řízenými body a být auditovatelná.
- (b) Tyto zóny musí být navrženy a implementovány tak, aby následující prostředí byla oddělena do konkrétních jednotlivých zón:
- (c) provozní prostředí jednotlivých řídicích systémů od sebe navzájem, kde zóny s řídicími systémy vysoké důležitosti pro provoz Vodního díla musí být navíc chráněné průmyslovým firewallem;
- (d) lokální IT prostředí od centrálního IT prostředí a internetu pomocí demilitarizované zóny (tzv. DMZ);
- (e) provozní prostředí obsahující řídicí systémy a další OT technologie od lokálního IT prostředí pomocí průmyslové demilitarizované zóny (tzv. IDMZ);
- (f) zálohovací prostředí (např. zálohovací servery, úložiště);
- (g) veškeré IP adresní rozsahy jsou definovány Objednatelem. Zhotovitel není oprávněn samostatně definovat a přidělovat IP adresy nebo adresní rozsahy bez předchozího schválení Objednatelem.
- (h) DMZ bude sloužit jako bezpečnostní brána mezi lokálními IT systémy centrálními IT systémy, IT systémy třetích stran a internetem. Tato speciální zóna musí mít následující parametry:

- (i) webový server pro poskytování webových stránek a aplikací přístupných z internetu (např. zákaznické portály, HMI přes web rozhraní);
- (j) DNS server (veřejný; není součástí Díla) pro zajištění překladu doménových jmen na IP adresy pro služby dostupné z internetu;
- (k) VPN brána umožňující bezpečný vzdálený přístup zaměstnancům nebo partnerům pomocí šifrovaného VPN spojení;
- (l) SFTP server pro bezpečné výměny souborů s externími subjekty;
- (m) reverse proxy/Web Application Firewall (tzv. WAF) pro přeposílání požadavků z internetu na vnitřní aplikace. Objednatel požaduje, aby reverse proxy/Web Application Firewall byl provozován v prostředí operačního systému Windows nebo jako hardwarové zařízení/appliance. Provoz v režimu cloudové služby mimo infrastrukturu Objednatele není akceptován;
- (n) server pro autentizaci a zajištění ověřování uživatelů IT systémů (Active Directory Domain Services – AD DS);
- (o) autentizaci a zajištění ověřování uživatelů řídicích systémů (OT);
- (p) provoz řídicího systému nesmí být závislý na dostupnosti cloudových služeb. Veškeré klíčové funkce včetně autentizace uživatelů, provozu systému a správy oprávnění musí být plně funkční i při výpadku připojení k internetu nebo nedostupnosti cloudových platforem;
- (q) autentizační mechanismus (např. Domain Controller) musí být umístěn v rámci lokální infrastruktury Objednatele;
- (r) přístupový server (není součástí Díla) musí sloužit jako centralizovaný, kontrolovaný, monitorovaný a auditovatelný bod pro veškerý vzdálený administrativní přístup do interní infrastruktury Objednatele; veškeré přístupy musí být autorizovány, logovány a v případě potřeby i zaznamenávány pro účely zpětné kontroly a bezpečnostního auditu;
- (s) v kontextu státních správců vodních cest (např. Systém říčních informačních služeb provozovaný Státní plavební správou apod.), se zde integrují i rozhraní pro výměnu dat s centrálním dopravním managementem. Systém musí být schopen komunikovat s centrálními systémy státu, typicky pomocí definovaného API nebo datových rozhraní. Musí být v souladu s technickými i bezpečnostními požadavky (např. formát XML, REST/SOAP, šifrování, autentizace).
- (t) IDMZ představuje bezpečnostní přechodovou zónu mezi OT systémy a podnikovými IT systémy. Tato vrstva slouží jako ochranná brána, která kontroluje a omezuje komunikaci mezi OT a IT prostředím, čímž zajišťuje bezpečné propojení a minimalizuje riziko šíření kybernetických hrozeb.
- (u) V rámci IDMZ jsou umístěny klíčové integrační body, které umožňují přístup IT systémů k datům a službám řídicích systémů. IDMZ také zajišťuje jednosměrný tok dat tam, kde je to z hlediska bezpečnosti potřeba, a umožňuje audit a kontrolu všech přístupů mezi doménami. IDMZ významně přispívá k zachování integrity a dostupnosti OT systémů, protože izoluje kritická zařízení od potenciálně méně zabezpečeného IT prostředí, a zároveň umožňuje nezbytnou interoperabilitu a správu systému v souladu s bezpečnostními standardy
- (v) IDMZ musí mít následující parametry:

- (w) základem architektury je dvojice firewallů (jeden firewall zajistí Zhotovitel v rámci Díla, druhý firewall zajistí Objednatel mimo Dílo), které kontrolují, filtrují a řídí komunikaci mezi OT a IT sítěmi. Firewally musí být plně kompatibilní a schopné bezproblémové integrace se stávající IT infrastrukturou Objednatele. Součástí implementace je napojení na stávající firewallovou infrastrukturu založenou na zařízeních FortiNet FortiGate, která jsou centralizovaně spravována pomocí nástroje FortiManager a monitorována nástrojem FortiAnalyzer. Konfigurace bezpečnostních pravidel a další nastavení firewallů musí být pravidelně konzultována s Objednatelem, aby byla zajištěna správná a bezpečná integrace s existujícími systémy;
- (x) přístupový server (není součástí Díla) je uvažován jako centralizovaný bezpečnostní bod, který zabezpečuje přístup k OT systémům prostřednictvím vícefaktorové autentizace (MFA), detailního logování a monitorování všech přístupů a aktivit. Veškerý vzdálený přístup musí být řízen na základě přísných přístupových politik a všechny činnosti musí být auditovatelné pro účely bezpečnostních kontrol a forenzní analýzy, kterou zajišťuje Objednatel. Dále musí být přístupový server pravidelně aktualizován a zabezpečen proti známým zranitelnostem, s minimálním přístupem k síťovým zdrojům nezbytným pro správu OT systémů;
- (y) reportingové rozhraní pro nadřazené systémy bez nutnosti přímého propojení s primárními řídicími systémy (např. replika datového serveru k řídicímu systému – databázový server, který shromažďuje a ukládá data z řídicích systémů pro využití IT systémy), rozhraní musí mít zajištěný jednosměrný tok dat pro zvýšení bezpečnosti;
- (z) IDMZ musí být monitorována a spravována specializovaným nástrojem, který zajišťuje aktuálnost bezpečnostních pravidel a konfigurací.
- (aa) Zhotovitel je povinen navrhnout a nakonfigurovat síťové komponenty (např. přepínače, směrovače, brány) tak, aby v případě budoucí potřeby umožňovaly:
 - (i) monitorování veškeré síťové komunikace;
 - (ii) řízení povolených toků na základě zdrojové a cílové zóny, IP adresy, portů a protokolů;
 - (iii) detekci nepovolené nebo podezřelé komunikace, včetně komunikace porušující definovaná síťová pravidla, pokusů o přístup z neautorizovaných IP adres, neobvyklých komunikačních vzorců, změn protokolů, nadměrného provozu, skenování portů nebo jiných aktivit indikujících průnik, laterální pohyb nebo přípravu útoku; systém musí umožňovat v případě potřeby zachytávání a vyhodnocování těchto událostí v reálném čase, s možností jejich předávání do SIEM (tzv. Security Information and Event Management) systému pro korelaci, archivaci a forenzní analýzu; detekce musí být implementován včetně provozu směřujícího na síťové brány, firewally a segmentační body;
 - (iv) omezení broadcastů a multicastů mimo určené segmenty;
 - (v) povolení komunikace mezi zónami pouze prostřednictvím konduktů, ve kterých je zajištěno řízení přístupů pomocí průmyslových firewallů pro významné systémy a pomocí ACL (tzv. Access Control List) pro méně významné systémy;
 - (vi) předem definované protokolové omezení (např. pouze Modbus RTU a MODBUS TCP/IP);
 - (vii) detekce a logování;
 - (viii) případně šifrování.

- (bb) Vzdálený přístup ke komunikační síti musí být umožněn výhradně prostřednictvím předem schválených a řízených přístupových kanálů (mimo rámec Díla);
- (cc) pravidla pro vzdálenou správu řídicích systémů (např. PLC, HMI, SCADA serverů) musí být stanovená, dokumentovaná a technicky prosazena tak, aby nedocházelo k neautorizovanému nebo neauditovanému přístupu;
- (dd) komunikační síť musí být nakonfigurována tak, aby umožňovala pouze ty komunikační toky, které jsou nezbytné pro zajištění funkčnosti řídicích systémů. Veškeré nadbytečné nebo nevyužívané porty, protokoly a služby musí být zakázány;
- (ee) pro veškerý přenos informací a dat v rámci komunikační sítě, kde hrozí riziko narušení důvěrnosti nebo integrity přenášených dat, musí být využity kryptografické algoritmy odpovídající aktuálním doporučením národního regulátora (viz odstavec 10.9 „Kryptografické algoritmy“);
- (ff) Šifrování musí být aplikováno zejména na:
 - (gg) vzdálený přístup;
 - (hh) správu zařízení;
 - (ii) přenos konfiguračních dat;
 - (jj) synchronizaci času a logů;

10.3 SPRÁVA A OVĚŘOVÁNÍ IDENTIT

Z hlediska správy a ověřování identit musí řídicí systém splňovat následující požadavky:

- (a) řídicí systém musí mít implementován nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv služby spojené se systémem;
- (b) řídicí systém musí prostřednictvím nástroje pro správu a ověření identity administrátorů, uživatelů a technických aktiv zajistit:
 - (i) ověření identity před zahájením aktivit-řízení počtu možných neúspěšných pokusů o přihlášení;
 - (ii) odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu;
 - (iii) opětovné ověření identity po stanovené době nečinnosti-dodržení důvěrnosti při vytváření výchozích autentizačních údajů při obnově přístupu;
 - (iv) centralizovanou správu identit s ohledem na vazby mezi aktivy;
- (c) řídicí systém musí mít implementován pro ověření identity administrátorů, uživatelů a technických aktiv (např. operátorských stanic) autentizační mechanismus založený na více faktorové autentizaci s nejméně dvěma různými typy faktorů;
- (d) v případě že některá část řídicího systému nesplňuje požadavek (c) musí být vedena evidence technických aktiv, účtů a autentizačních mechanismů, které tyto požadavky nesplňují, včetně odůvodnění;
- (e) pokud není více faktorová autentizace pro daný řídicí systém možná implementovat, musí systém využívat autentizaci pomocí kryptografických klíčů nebo certifikátů;
- (f) pokud pro daný řídicí systém není možná autentizace pomocí kryptografických klíčů nebo certifikátů, musí mít systém implementován nástroj pro autentizaci pomocí identifikátoru účtu a hesla, přičemž tento nástroj musí vynucovat:

- (i) délku hesla alespoň:
 - (ii) 12 znaků pro účty uživatelů;
 - (iii) 17 znaků pro účty administrátorů;
 - (iv) 22 znaků pro účty technických aktiv.
 - (v) bezodkladnou změnu výchozího hesla technických aktiv na nové náhodně generované heslo složené z malých a velkých písmen, číslic a speciálních znaků;
 - (vi) neomezování použití malých a velkých písmen, číslic a speciálních znaků;
 - (vii) umožnění změny hesla uživatelům a administrátorům, přičemž období mezi dvěma změnami nesmí být kratší než 30 minut;
 - (viii) povinnou změnu hesla maximálně po 18 měsících;
 - (ix) zabránění:
 - (x) volbě hesel ze slovníku nejčastěji používaných hesel;
 - (xi) tvoření hesel na základě opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo podobného způsobu;
 - (xii) opětovnému použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.
- (g) v řídicím systému musí být umožněno vygenerování náhodného výchozí hesla nebo identifikátoru sloužícímu k vytvoření nebo obnově přístupu v souladu s pravidly uvedenými v písmenu (f);
- (h) v řídicím systému musí být umožněno zneplatnění hesla nebo identifikátoru sloužícímu k vytvoření nebo obnově přístupu po jeho prvním použití, nebo nejpozději do 24 hodin od jeho vytvoření;
- (i) řídicí systém musí pro administrátorský účet určený zejména pro případ obnovy po kybernetickém bezpečnostním incidentu vynucovat:
- (i) bezodkladnou změnu výchozího hesla;
 - (ii) vytvoření hesla náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků;
 - (iii) délku hesla alespoň 22 znaků;
 - (iv) bezpečné uložení hesla-manipulaci s účtem a jeho heslem pouze pověřenými osobami v nezbytně nutných případech;
 - (v) změnu hesla po jeho použití nebo nejpozději po 18 měsících.
- (j) Evidenci manipulace a pokusů o manipulaci s tímto účtem a jeho heslem

10.4 ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Řízení přístupových oprávnění k řídicím systémům představuje klíčový prvek zabezpečení. Jeho správná implementace zajišťuje, že jednotlivé osoby nebo systémy mají přístup pouze k těm systémovým prostředkům a funkcím, které nezbytně potřebují pro výkon své role, a pouze v nezbytném rozsahu. Přístupová oprávnění musí být technicky vynucena, jednoznačně evidována a pravidelně revidována.

Zhotovitel je povinen zajistit, aby řídicí systémy v oblasti řízení přístupových oprávnění splňoval následující požadavky:

- (a) řídicí systém musí využívat nástroj pro správu přístupových oprávnění, který umožní:
 - (i) evidenci oprávnění ve vazbě na konkrétní uživatele, účty, technická aktiva a jejich provozní nebo bezpečnostní roli;
 - (ii) řízení přístupových práv v návaznosti na logickou nebo fyzickou topologii systému (např. členění dle bezpečnostních zón, síťových segmentů, technologických oblastí apod.);
 - (iii) podporu auditu přístupových změn (kdo, kdy, komu a proč přiřadil nebo odebral oprávnění).
- (b) řídicí systém musí umožňovat řízení oprávnění k jednotlivým technickým aktivům na základě oprávnění s možností přesného nastavení přístupových práv, včetně:
 - (i) přístupu (např. možnost přihlásit se, ovládat HMI nebo SCADA rozhraní);
 - (ii) čtení dat (např. přístup ke konfiguracím, historickým záznamům, telemetrii);
 - (iii) zápisu nebo modifikace (např. provádění změn konfigurací, zásah do řízení);
 - (iv) změny oprávnění (pouze vyhrazené role mohou nastavovat oprávnění jiným subjektům).
 - (v) Každé přístupové oprávnění musí být jednoznačně přiřazeno konkrétnímu uživatelskému účtu nebo systému a musí být udělováno dle principu nejmenšího možného oprávnění (least privilege) a role-based access control (tzv. RBAC).

10.5 APLIKAČNÍ BEZPEČNOST

Z hlediska aplikační bezpečnosti, musí řídicí systém splňovat následující požadavky:

- (a) Zhotovitel musí zajistit aplikování bezpečnostních aktualizací použitých aplikací před samotnou instalací řídicího systému a jeho částí;
- (b) řídicí systém musí zajistit ochranu obsažených informací, transakcí a přenášných identifikátorů relací před neoprávněnou činností a popřením provedených činností pomocí metody tzv. whitelistingu – musí být povoleny pouze oprávněné aplikace související s řídicím systémem, všechny ostatní musí být zakázány.

10.6 KRYPTOGRAFICKÉ ALGORITMY

Z hlediska kryptografických algoritmů, musí řídicí systém pro přenos a uložení důvěrných dat splňovat následující požadavky:

- (a) řídicí systém musí pro zajištění ochrany technických aktiv a jejich komunikace:
 - (i) používat aktuálně odolné kryptografické algoritmy;
 - (ii) prosazovat bezpečné nakládání s kryptografickými algoritmy;
 - (iii) zohledňovat doporučení a metodiky v oblasti kryptografických algoritmů vydané NÚKIB, zveřejněné na jeho internetových stránkách;
- (b) řídicí systém musí v souladu s písmenem (a) zajistit bezpečnou:
 - (i) hlasovou, audiovizuální a textovou komunikaci, včetně e-mailové komunikace;

- (ii) nouzovou komunikaci v rámci organizace;
- (c) řídicí systém musí v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě:
 - (i) používat pouze aktuálně odolné kryptografické klíče a certifikáty;
 - (ii) používat systém správy klíčů a certifikátů, který:
 - (iii) zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
 - (iv) umožní kontrolu a audit;
 - (v) zajistí důvěrnost a integritu kryptografických klíčů.
 - (vi) pro více detailní přehled na minimální požadavky na kryptografické algoritmy je možné nahlédnout do dokumentu vydaným NÚKIB.⁵

10.7 ZAJIŠŤOVÁNÍ DOSTUPNOSTI ŘÍDICÍCH SYSTÉMŮ

Z hlediska zajišťování dostupnosti řídicích systémů, musí řídicí systémy splňovat následující požadavky:

- (a) řídicí systém musí mít implementovány bezpečnostní opatření pro zajišťování dostupnosti Vodního díla spojené se systémem, kterými zajistí:
 - (i) odolnost řídicího systému vůči hrozbám a zranitelnostem, které by mohly snížit jeho dostupnost, musí být zajištěna prostřednictvím technických a organizačních opatření směřujících k minimalizaci rizik narušení provozu; součástí těchto opatření je tzv. hardening systému, tedy soubor konfiguračních a bezpečnostních zásahů vedoucích k omezení zneužitelných prvků a zvýšení celkové bezpečnostní odolnosti; mezi základní kroky patří správné nastavení firewallů, aplikace principu nejmenších privilegií (tzv. least privilege), uzavření všech nevyužívaných síťových portů, zavedení silných autentizačních mechanismů (např. komplexní hesla), odstranění nebo deaktivace nepotřebných služeb, a pravidelná kontrola systémových a síťových konfigurací; tato opatření musí být systematicky dokumentována, uplatňována v rámci životního cyklu systému (tedy i v rámci servisní smlouvy) a pravidelně revidována s ohledem na nové hrozby a technologický vývoj;
 - (ii) redundanci vybraných klíčových technických aktiv nezbytných pro zajištění dostupnosti řídicího systému;
- (b) řídicí systém musí pro zajištění dostupnosti služby v souladu s písmem (a) umožňovat vytvářet pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy služby v případě kybernetického bezpečnostního incidentu (to platí pro PC, servery i PLC a další relevantní aktiva, jež jsou součástí řídicího systému);
- (c) řídicí systém musí u vytvořených záloh umožnit:
 - (i) pravidelné testování integrity, dostupnosti a obnovitelnosti záloh;
 - (ii) poskytnout dostatečné informace k souvisejícímu zdokumentování výsledků testování těchto záloh;

⁵ MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY: doporučení v oblasti kryptografické bezpečnosti. NÚKIB, 2025.

- (iii) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, zejména šifrováním v souladu s odstavcem 10.9 „*Kryptografické algoritmy*“;
- (iv) ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti v souladu s pravidlem 3-2-1, což znamená, že z každé zálohované sady dat musí existovat minimálně tři kopie (jedna primární a dvě záložní), tyto kopie musí být uloženy alespoň na dvou různých fyzicky odlišných úložných médiích a jedna z těchto kopií musí být navíc umístěna mimo hlavní lokalitu, kde se řídicí systém nachází;
- (d) řídicí systém musí za účelem omezení šíření kybernetického bezpečnostního incidentu a snížení jeho dopadu oddělovat zálohovací prostředí od jiných prostředí podle odstavce 10.2 „*Bezpečnost komunikačních sítí*“.

11 LICENCE A PŘÍSTUPOVÁ PRÁVA K SYSTÉMŮM OT A BEZPEČNOSTNÍMU SOFTWARE

11.1 OBECNĚ

V případě, že součástí řídicích systémů zařízení a komponenty, jejichž provoz, zabezpečení nebo správa je zajištěna prostřednictvím softwaru – zejména softwaru pro řízení přístupů, monitoring, detekci hrozeb, správu konfigurace nebo centralizovanou správu aktiv – je Zhotovitel povinen nejpozději k datu dokončení příslušného řídicího systému poskytnout Objednateli platnou licenci k uvedenému softwaru, zajistit dostupnost všech nezbytných aktualizací, oprav, bezpečnostních záplat a podpory, předat kompletní uživatelskou a systémovou dokumentaci, včetně instalačních balíčků, konfiguračních manuálů a přístupových údajů (v případě softwarových platforem, které vyžadují správu přes webové nebo jiné administrační rozhraní).

Poskytnutá licence musí opravňovat Objednatele, případně jím smluvně určenou třetí osobu, k plnému provozu, správě, administraci, údržbě a případnému rozvoji kybernetické bezpečnosti řídicích systémů, a to v rozsahu nezbytném pro:

- (a) zajištění kontinuální bezpečnosti provozu;
- (b) naplňování požadavků právních předpisů (např. zákon o kybernetické bezpečnosti) – související dopady na práva a povinnosti stran jsou popsány ve smlouvě nebo servisní smlouvě;
- (c) zachování samostatnosti Objednatele v oblasti správy systému po ukončení závazků Zhotovitele.

V případech, kdy je software dodán jako tzv. „krabicové řešení“ nebo je součástí firmwaru technologických zařízení (např. PLC, RTU, HMI, bezpečnostní brány apod.), se uplatní licenční podmínky dané výrobcem, které však nesmí omezit Objednatele v nezbytných úkonech pro zabezpečení a provozuschopný chod systému.

11.2 POVAHA A DOBA TRVÁNÍ LICENCE; ODMĚNA ZA LICENCI

Zhotovitel musí Objednateli poskytnout v rámci Díla licenci minimálně v souladu s následujícími požadavky:

- (a) v rámci Datového centra musí Zhotovitel poskytnout nevýhradní licence pro servery a správu;

- (b) v rámci Vodních děl musí Zhotovitel poskytnout licence pro datové servery, operátorská PC a dohledová PC;
- (c) nevýhradní licence pro servisní zařízení.

Počty licencí a jejich konkrétní specifikace jsou uvedeny v tzv. Návrhu zhotovitele, který je součástí smlouvy o dílo. Pokud není v Návrhu zhotovitele v konkrétním případě stanoveno jinak, je licence poskytnuta na dobu neurčitou a odměna za ni je zahrnuta ve smluvní částce za řídicí systém (v tzv. Přijaté smluvní částce v kontextu Smluvních podmínek). Pokud je v Návrhu zhotovitele v konkrétním případě stanoveno, že je licence poskytnuta na 1 rok, je ve smluvní částce za řídicí systém zahrnuta odměna za 1 rok trvání takové licence.

V případě firmware nebo uzavřeného systému se za akceptovatelnou považuje licence s trváním odpovídajícím životnosti zařízení. Zhotovitel je povinen upozornit Objednatele na takové časové omezení a poskytnout doporučení, jak bude zabezpečena případná náhrada nebo aktualizace tohoto firmwaru nebo uzavřeného systému.

Veškeré náklady spojené s poskytnutím licencí, zajištěním přístupů k administračním rozhraním a nastavením, přístupem k provozním API a konfiguračním rozhraním, musí být zahrnuty ve smluvní částce za řídicí systém. Zhotovitel nemá nárok na další úhradu, pokud není výslovně dohodnuto jinak.

12 KOMPENZAČNÍ OPATŘENÍ

Primárním cílem tohoto dokumentu je stanovení závazných požadavků Objednatele na zajištění kybernetické bezpečnosti řídicích systémů, jejich částí, dalších OT systémů a souvisejících technologií. V případě, že pro část řídicího systému není možné zcela naplnit uvedené bezpečnostní požadavky uvedené v sekci 10 „Technické požadavky kybernetické bezpečnosti“ lze tyto bezpečnostní požadavky nahradit v souladu s IEC 62443-3-3 a bezpečnostní politikou tzv. kompenzačními opatřeními.

Kompenzační opatření musí být v souladu se smlouvou použita k zajištění potřebné bezpečnostní funkce tak, aby byla splněna požadovaná úroveň bezpečnosti. Zahrnutí kompenzačních opatření musí být doprovázeno odpovídající dokumentací, aby bylo možné zajistit kontrolu, které konkrétní bezpečnostní požadavky jsou řešeny kompenzačně, a že výsledná dosažená bezpečnostní úroveň řídicího systému odpovídá požadované úrovni bezpečnosti.

V případě použití kompenzačních opatření je Zhotovitel povinen:

- (a) tuto skutečnost předem specifikovat, navrhnout řešení kompenzačního opatření, a to oznámit Objednateli;
- (b) implementovat kompenzační opatření postupem podle smlouvy (viz zejména Článek 13 [Variace a úpravy] Smluvních podmínek).