

PeMaR

Ing. Michael Pekárek
Habrová 3100/21
415 01 Teplice
tel.: 602475156
E-mail: pekym@seznam.cz

Odběratel: PS projekty spol. s r.o., 14.října 291/4, 41501 Teplice

**Aquacentrum Teplice p.o. - Venkovní úpravy
D1. Dokumentace inženýrského objektu
D1:IO 203 Přeložka horkovodu**

**D1: IO 203.3 OPS Palackého 2887
D1: IO 203.3.2 - Měření a regulace**

Dokumentace provádění stavby

Seznam dokumentace:

1. Technická zpráva
2. Výkaz výměr
3. Vstupy a výstupy
4. Schéma MaR
5. Půdorys a řez
6. Seznam dokumentace

Zakázkové číslo: 12/P/23
Zpracoval: Ing. Pekárek
IČO: 46067442

Paré číslo: 1

PeMaR

Ing. Michael Pekárek
Habrová 3100/21
415 01 Teplice
tel.: 602475156
E-mail: pekym@seznam.cz

Odběratel: PS projekty spol. s r.o., 14.října 291/4, 41501 Teplice

**Aquacentrum Teplice p.o. - Venkovní úpravy
D1. Dokumentace inženýrského objektu
D1:IO 203 Přeložka horkovodu**

**D1: IO 203.3 OPS Palackého 2887
D1: IO 203.3.2 - Měření a regulace**

Dokumentace provádění stavby

Technická zpráva

Zakázkové číslo: 12/P/23
Zpracoval: Ing. Pekárek
IČO: 46067442

Poř. číslo: 1

Technická zpráva

1.) Všeobecná část:

1.1. Úvod

Předmětem projektu je řízení objektové předávací stanice. Stanice je osazena výměníkem přípravy ÚT a výměníkem přípravy teplé vody s akumulací nádrží a nabíjecím čerpadlem. OPS zásobuje objekt topnou vodou ÚT čerpadlem s řízenými otáčkami. Příprava teplé vody je vybavena nabíjecím a cirkulačním čerpadlem. Tlak topného systému je udržován ze zpátečky horkovodu solenoidovým ventilem. V OPS je osazen kombinovaný rozvaděč měření a regulace, který mimo řídicí jednotku obsahuje též zařízení pro přenos dat do dispečinku ČEZ Teplárenská.

Technická dokumentace obsahuje:

- osazení čidel pro potřebu řízení technologie
- nový kombinovaný rozvaděč
- řídicí jednotku
- přenosové zařízení

1.2. Výchozí podklady

- podklady strojní části
- požadavky provozovatele
- prohlídka stávajícího stavu

1.3. Řídicí jednotka

Ve stanici je navržena podle potřeb a funkce technologického zařízení a umožňuje řídit provoz objektové předávací stanice.

2. Základní technické údaje

2.1. Použitá napěťová soustava: 1 NPE 50 Hz 230V/TN-S, 24DC PELV, 24VAC PELV

2.2. Celkový instalovaný výkon zařízení měření a regulace zařízení je zanedbatelný

2.3. Prostředí v prostoru technologie stanice dle ČSN 332000-3 normální AA5 - teplota okolí +5°C až 40°C, AD1 - výskyt vody zanedbatelný, BC1 - bez dotyku s potenciálem země

Prostor dle ČSN 332000-5-51 ed.3 normální bez nebezpečných prostor.

2.4. Ochrana před nebezpečným dotykovým napětím je uvažována dle ČSN 332000-4-41 ed.2 automatickým odpojením od zdroje v síti TN-C-S.

2.5. Přívod do rozvaděče je řešen z elektroměrového rozvaděče, který bude doplněn o nové měření elektrické energie. Přihlášku nového jednofázového odběru zajistí investor u ČEZ distribuce.

3. Popis technického řešení

3.1. Sdružený rozvaděč je řešen jako skříňový, který obsahuje řídicí jednotku, ovládací panel, ovládací a signalizační prvky. Do rozvaděče bude umístěno přenosového zařízení sloužící pro komunikaci s dispečinkem ČEZ Teplárenská a.s.. Vlastní přenosové zařízení, převodník MBus/Ethernet, switch jsou součástí projektu měření a regulace. Přenos je zajištěn pomocí optického kabelu, který je připojen z rozvodny zrušené výměňkové stanice u Aquacentra.

3.2. Základní okruhy

- | | |
|------|---------------------------|
| TI | 1 - Měření teplot |
| PI | 2 - Měření tlaků |
| A-OC | 3 - Poruchová signalizace |

TC	4 - Regulace teploty ÚT
PS	5 - Udržování tlaku ÚT
OC	6 - Ovládání čerpadla ÚT
TC	7 - Regulace teploty TV
OC	8 - Ovládání čerpadel TV
FTdQ	9 - Měření spotřeby tepla a průtoku
RA	10 - Příslušenství rozvaděče DT1
Y	11 - Řídící jednotka
X	12 - Přenosové zařízení

3.3. Popis funkce základních okruhů

TI 1 - Měření teplot

Teploty jsou snímány odporovými teploměry Pt1000, které jsou vedeny na analogové vstupy a zpracovány v řídicím systému. Je uvažováno s měřením teploty vstupu horké vody, teploty ÚT a teplé vody i teploty kondenzátu.

Sledované teploty:

- T HV vstup OPS
- T HV výstup OPS
- T ÚT výstup výměník
- T ÚT vratná
- T teplé vody výměník
- T výstup za AN
- T teplé vody AN dolní
- T teplé vody AN horní
- T cirkulace TV
- T TV před výměníkem
- T venkovní

PI 2 - Měření tlaku

Měření tlaků ve výměňkové stanici je navrženo snímači tlaku s napěťovým výstupem 0...10V. Je sledován tlak vstupu přívodu a vratné horké vody, tlaky topného systému a studené vody.

Sledované tlaky:

- P vstupu HV přívod
- P vstupu HV vratná
- P top.systému ÚT vratná
- P top.systému ÚT náběh
- P studené vody

A-OC 3 - Poruchová signalizace

Mimo poruchových stavů snímaných vlastním řídicím systémem je objektová předávací stanice vybavena snímáním poruchových stavů, které jsou hlídány havarijní smyčkou. K odstavení výměňkové stanice dojde havarijní funkcí regulačních ventilů na přívodu horké vody do výměníků přípravy topné (ÚT) i teplé vody.

Každé havarijní odstavení nutno odblokovat obsluhou. U mezních hodnot sledovaných řídicím systémem dojde rovněž k odstavení příslušné části výměňkové stanice, avšak je povoleno jedno automatické najetí se signalizací poruchového stavu hlídaného řídicím systémem. Při opětovné poruše dojde k trvalému odstavení přípravy ÚT nebo TV dle charakteru poruchy, které je možno vybavit obsluhou z dispečinku.

Poruchové stavy snímané sledované řídicím systémem:

- pokles přetlaku (ÚT)
- teplota TV výstup + 65°C při sanitizaci +75°C
- teplota ÚT na výstupu výměníků + 80°C
- ztráta napájení
- zaplavení OPS
- uzavírá ventil přípravy ÚT (1)
- uzavírá ventil přípravy TV (6)
- uzavírá ventil přípravy ÚT (1)
- odstaví chod OPS (1,6)
- odstaví chod OPS (1,6)

Po pominutí těchto uvedených poruch dojde k opětovnému najetí provozu výměňkové stanice.

Poruchové stavy hlídáné poruchovou signalizací. Po odstavení výměňkové stanice nebo pouze části výměňkové stanice poruchovou signalizací možno technologii zprovoznit pouze ze stanice obsluhou.

Snímané hodnoty jsou vedeny na vstup jak na vstup řídicí jednotky, tak na příslušné ventily:

- teplota prostoru OPS +40°C
- teplota ÚT na výstupu výměníku +85°C
- teplota TV na výstupu výměníku
- pokles přetlaku ÚT
- ruční odstavení stanice
- odstaví chod OPS (1,6)
- uzavírá ventil přípravy ÚT (1)
- uzavírá ventil přípravy TV (6)
- uzavírá ventil přípravy ÚT (1)
- odstaví chod OPS (1,6)

TC 4 - Regulace teploty ÚT

Regulace teploty ÚT je prováděna v závislosti na venkovní teplotě a teplotě výstupní ÚT výměníku. Teploty jsou snímány odporovými teploměry a zpracovány v řídicím systému. Podle vzniklé regulační odchylky je ovládán regulační ventil na přívodu horké vody do výměníku. Z displeje bude možno korigovat topnou křivku. Akčními členem toho okruhu je regulační ventil s havarijní funkcí s napěťovým řízením.

K uzavření ventilu (1) dojde, pokud při provozu topného systému bude překročena výstupní teplota ÚT. Při poklesu přetlaku v topném systému uzavírá regulační ventil a vypíná čerpadlo ÚT. Mezní hodnoty výstupní teploty a tlaku ÚT jsou sledovány řídicím systémem na základě údaje čidel, které slouží i pro regulaci nebo z okruhu poruchové signalizace havarijními prvky. Oběhové čerpadlo v případě překročení teploty zůstává v provozu.

PS 5 - Udržování tlaku ÚT

Udržování tlaku topného systému je zajištěno na základě snímače tlaku solenoidovým ventilem přepouštěním z vratné vody horkovodu. Při poklesu tlaku dojde k otevření solenoidového ventilu a uzavření při dosažení požadovaného tlaku. Doplnění topného systému je blokováno časově základní doba nastavení 5 min., po překročení této doby je dojde k přerušení doplňování.

OC 6 - Ovládání čerpadla ÚT

Řízení oběhového čerpadla ÚT je řešeno na základě diferenčního tlaku na výstupu z výměňkové stanice. Ovládání chodu čerpadla je buďto ruční nebo automatické řídicím systémem. Ruční ovládání slouží jenom pro odzkoušení funkčnosti zařízení. Chod čerpadla je řízen na základě požadovaného diferenčního tlaku pomocí napěťového vstupu. K odstavení chodu čerpadla dojde při odstavení výměňkové stanice s časovým doběhem nebo při poruchovém stavu poklesu tlaku topného systému nebo ztrátě jedné přívodní fáze. V letním provozu je čerpadlo vypnuto a jeho provoz je řízen týdenním časovým režimem (protočení čerpadla po stanovenou dobu), za předpokladu tlaku v topném systému. Časový režim je nastavován z displeje.

TC 7 - Regulace teploty TV

Regulace prováděna na konstantní výstupní teplotu na výstupu z výměníku ohřevu 55°C. Teplota teplé vody je snímána odporovým teploměrem. Signál je zpracován v řídicím systému a podle vzniklé regulační odchylky je ovládán regulační ventil (6) na přívodu horké vody do výměníku TV regulačním ventilem s havarijní funkcí a napěťovým řízením.

V době sanitace připravována teplota TV o teplotě 70°C. Sanitace je prováděna obsluhou.

Nutno přenastavit havarijní termostat.

OC 8 - Ovládání čerpadel TV

Ovládání čerpadel je buďto ruční nebo automatické řídicím systémem. Ruční ovládání slouží jenom pro odzkoušení funkčnosti zařízení. Ovládání a napájení je zajištěno z rozvaděče měření a regulace. Nabíjecí čerpadlo přípravy teplé vody (10) je ovládáno na základě teplot v akumulární nádrži. Při poklesu žádané teploty na horním čidle v akumulární nádrži dojde k sepnutí nabíjecího čerpadla, které je vypnuto při dosažení žádané teploty na spodním čidle AN.

Z rozvaděče je rovněž ovládáno cirkulační čerpadlo (9). Sledována je teplota cirkulace. Čerpadlo je možno řídit časovým režimem avšak je nutno zajistit jeho chod v době sanitace.

FTdQ 9 – Měření spotřeby tepla a průtoků

Měřiče tepla s MBus výstupem jsou osazeny na zpátečce ÚT (5) a na zpátečce horké vody z výměníku TV (12). Na přívodu studené vody je osazen průtokoměr s MBus výstupem zajišťující měření množství studené vody (11). Další vodoměr je osazen na doplňování vody ze zpátečky horkovodu (13).

RA 10 - Příslušenství rozvaděče DT1

Řídicí jednotka je umístěna v kombinovaném rozváděči BA. Na dveřích rozvaděče jsou osazeny ovládací prvky a ovládací jednotka. Přívod do rozvaděče 1x230V, 50Hz, 25A řešen ze stávajícího elektroměrného rozvaděče v rámci tohoto projektu. V rozvaděči umístěna řídicí jednotka, ovládací panel, vyhodnocovací jednotka snímače hladiny zaplavení, pomocná relé, napájecí zdroje 24VAC a 24VDC. V rozvaděči bude umístěno přenosové zařízení jako je switch, převodník MBus/ethernet a optický rozvaděč pro ukončení optického kabelu. Rozvaděč bude vybaven kontaktním čidlem pro kontrolu otevření dveří se signalizací do operátorské stanice na centrálním dispečinku.

Y 15 - Řídicí jednotka

Řídicí jednotka je podpůrným aktivem ISZS (Informační systém základní služby), práce na tomto systému se považují za práce na KII/ISZS a musí splňovat požadavky uvedené v SKČ_ST_0027 - Standard informační a kybernetické bezpečnosti. Smlouva s dodavatelem musí obsahovat požadavky definované v příloze SKČ_ST_0027 VP H – Bezpečnostní požadavky pro dodávky dle ZoKB.

Realizace systému SKŘ musí splňovat podmínky uvedené v příloze „D7 Informatika - požadavky IKB - TAS.docx“

Ve výměníkové stanici bude osazena kompaktní řídicí jednotka 16xAI,8xAO,32xDI a 32xDO s výstupem ethernet doplněná o modul 8xAI. Řídicí jednotka je doplněna o ovládací barevný 7“ dotykový displej. V rámci unifikace je požadováno použití řídicích systémů výrobce Domat Control Systém s.r.o. s komunikací BacNET IP. Proces tvorby a ověření SW musí probíhat řízeným způsobem v souladu s SKČ_ME_0230 – Bezpečný vývoj software.

Zhotovitel musí poskytnout a předat SW a HW prostředky nezbytné k obnově zařízení po poruše, tj. ke kompletní reinstalaci SW ze záložních médií, jeho konfiguraci a spuštění, případně další nástroje nezbytné pro předepsanou údržbu zařízení.

Jako jeden z výstupů procesu tvorby a ověření zhotovitelem instalovaného SW budou kromě dokumentace díla zhotovitelem předány i datové nosiče se systémovými aplikačním SW, a to včetně administrátorských hesel. Pro stanice na bázi PLC a DCS navíc i záložní média s obrazy disků a zdrojové formy aplikačního SW.

Jednotlivé verze nově instalovaného SW musí být zhotovitelem řádně evidovány a zálohovány. Funkčnost nového SW zhotovitel otestuje v rámci zkušebního provozu. Zhotovitel předá programové kódy k PLC v editovatelné a komentované verzi protokolárně pracovníkům Oddělení ICT a KB. Do doby předání programových kódů bude automaticky uplatněna pozastávka

10% z ceny díly.

X 16 - Přenosové zařízení

Do sdruženého rozvaděče DT1 osazeno přenosové zařízení, které se skládá z převodníku MBus/Ethernet a switchu se dvěma porty SFP pro optický kabel. Jeden port složí pro napojení komunikace této OPS a na druhý bude napojena OPS Aquacentra. Komunikace přes ethernet protokolem BacNET IP. Tvorbu a zprovoznění vizualizace zajistí Oddělení ICT a KB (TAS), zhotovitel v rámci tvorby SW pro PLC předá komunikační tabulku ve verzi schválené TAS (na vyžádání předáme) – oddělení ICT a KB (BacNET adresy budou odpovídat standardu TAS) před zprovozněním stanice a oživováním komunikace na dispečink. Dále zhotovitel po oživení stanice zjistí ověření funkce jednotlivých okruhů MaR a poruchových hlášení na dispečerské pracoviště ve spolupráci s Oddělením ICT a KB. Hranicí dodávek je komunikační rozhraní PLC a předaná komunikační tabulka obsahující potřebné údaje pro tvorbu dispečerské SCADA aplikace. IP adresy pro jednotlivá zařízení dodá na výzvu Oddělení ICT a KB.

Vlastníkem programového kódu a všech programových licencí k provozovanému informačnímu systému kritické informační infrastruktury/informačního systému základní služby (PLC) je objednatel, pokud není ve smlouvě uvedeno jinak nebo je obecně závaznými právními předpisy stanoveno jinak. Zhotovitel předá programové kódy k PLC v editovatelné a komentované verzi protokolárně pracovníkům oddělení ICT a KB.

3.4. Kabeláž

Hlavní kabelová trasa je vedena v drátovém kabelovém žlabu na konzolách nebo na pomocných ocelových konstrukcích z ocelových žárově zinkovaných nosných prvků. Podružné trasy mohou být vedeny v ochranných trubkách.

3.5. Požadavky na ostatní profese

V rámci strojní části je zajištěna dodávka a montáž regulačních ventilů, čerpadel a osazeny návarky odběrů tlaků a teplot na strojní technologii. Optický kabel je řešen v rámci horkovodu.

3.6. Hranice dodávky části měření a regulace

Projekt měření a regulace řeší řízení provozu objektové předávací stanice, zajišťuje sběr dat a přenosové zařízení. Součástí projektu je i napájecí kabel z elektroměrného rozvaděče, který bude doplněn o nové měření elektrické energie, které zajistí odběratel.

3.7. Úřední zkoušky

Návrh technického řešení je vypracován v souladu s platnými normami ČSN. Práce elektro v rozvaděcích a práce na elektrickém zařízení smí provádět pouze osoba s kvalifikací „znalá“ přezkoušená ze základních elektrotechnických a bezpečnostních předpisů dle vyhlášky 250/2021Sb, paragraf 6. Na zařízení musí být prováděna pravidelná údržba a prohlídky dle platných norem a předpisů. Revize nutno provádět v intervalu dvou let. Osoby určené k obsluze el.zařízení musí být náležitě a prokazatelně proškoleny a obeznámeny s provozním zařízením a nebezpečím, jež může vzniknout při práci – ČSN EN 501 10-1 ed.2.

Zařízení bude provozováno dle provozního řádu, který si zpracuje provozovatel. Pomůcky určené k obsluze provozu a zajištění bezpečnosti podle ČSN 381081 musí být zajištěny před uvedením zařízení do zkušebního provozu.

Ochranné a pracovní pomůcky musí být udržovány provozuschopné a mimo použití vždy řádně uloženy na přístupných místech. Ochranné a pracovní pomůcky nejsou součástí dodávky el.zařízení.

Provozovatel zhotoví pro objekt požární předpisy, s kterými seznámí příslušné pracovníky. V požárních předpisech bude určeno, které části el.zařízení a jak se budou při požáru vypínat. Předpokladem pro řádný a trvalý provoz el.zařízení je správná obsluha a údržba el.zařízení dle

příslušných norem a pokynů výrobců.

Jejich ustanovení je nutno dodržovat i při prováděcích pracích. Změny je možno provést po dohodě s projektantem. Před kolaudací je prováděcí podnik povinen dodržet ustanovení norem ČSN o výchozí revizi. Technická zpráva doplňuje výkresovou část projektové dokumentace a je její součástí.

* Nařízení vlády č.494/2000 Sb., kterým se stanoví způsob evidence, hlášení a zasílání záznamu o úrazu

* Nařízení vlády č.9/2013 Sb., kterou se stanoví způsob ochrany zdraví při práci

* Vyhláška ČUBP a ČBÚ č. 50/1978 o odborné způsobilosti v elektrotechnice, ve znění vyhl. 98/1982 Sb.

* Vyhláška ČUBP č.48/1982 Sb., kterou se stanoví základní požadavky k zajištění bezpečnosti práce technických zařízení, ve znění vyhl. Č.352/2000Sb.

* Zákon č.309/2006 Sb., o bezpečnosti práce a technických zařízení při stavebních pracích.

* Vyhláška MPSV 73/2010 Sb., kterou se určují vyhrazená elektrická zařízení a stanoví některé podmínky k zajištění jejich bezpečnosti. ČSN EN 50110-1 ed.3 Obsluha a práce na elektrických zařízeních – Část 1: Obecné požadavky

* BOZP dodavatele

Provedení montážních prací a použitý materiál odpovídá platným ČSN:

ČSN 33 0165/EN 60446/ Elektrické předpisy. Značení vodičů barvami nebo číslicemi.
Prováděcí ustanovení

ČSN 33 1500 Elektrické předpisy. Revize elektrických zařízení

ČSN 33 2000-1 ed.2 Elektrické instalace nízkého napětí – Část 1: Základní hlediska, stanovení základních charakteristik

ČSN 33 2000-4-41-ed.2 Elektrické instalace nízkého napětí – Část 4-41: Ochranná opatření pro zajištění bezpečnosti – Ochrana před úrazem elektrickým proudem

ČSN 33 2000-4-42-ed.2 Elektrotechnické předpisy. Elektrická zařízení Část 4: Bezpečnost. Kapitola 42: Ochrana před účinky tepla

ČSN 33 2000-4-43 ed.2 El.instalace nn – Část 4-43: Bezpečnost - Ochrana před nadproudy

ČSN 33 2000-4-443 ed.2 Elektrické instalace budov. Bezpečnost – Ochrana před rušivým napětím a elektromagnetickým rušením. Kapitola 443: Ochrana proti atmosférickým nebo spínacím přepětím

ČSN 33 2000-4-444 Elektrické instalace nízkého napětí – Část 4-444: Bezpečnost – Ochrana před napětíovým a elektromagnetickým rušením

ČSN 33 2000-4-46 ed.2 Elektrotechnické předpisy. Elektrická zařízení. Část 4: Bezpečnost. Kapitola 46: Odpojování a spínání

ČSN 33 2000-4-473 Elektrotechnické předpisy. Elektrická zařízení. Část 4: Bezpečnost. Kapitola 47: Použití ochranných opatření pro zajištění bezpečnosti. Opatření proti nadproudům

ČSN 33 2000-7-729 Elektrické instalace nízkého napětí – Část 7-729: Zařízení jednoúčelová a ve zvláštních objektech – Uličky pro obsluhu nebo údržbu

ČSN 33 2000-5-51 ed.3 Elektrické instalace nízkého napětí – Část 5-51: Výběr a stavba elektrických zařízení – Všeobecné předpisy

ČSN 33 2000-5-52 ed.2 Elektrotechnické předpisy. Elektrická zařízení. Část 5: Výběr a stavba elektrických zařízení. Kapitola 52: Výběr soustav a stavba vedení

ČSN 33 2000-5-534 Elektrická instalace nízkého napětí – Část 5-53: Odpojování, spínání a řízení Oddíl 534: Přepětíová ochranná zařízení

ČSN 33 2000-5-54 ed.3 Elektrické instalace nízkého napětí – Část 5-54: Výběr a stavba el.

zařízení. Uzemnění, ochr.vodiče a vodiče ochr. Pospojování

- ČSN 33-2000-5-56 ed.2 Elektrické instalace nízkého napětí – Část 5-56: Výběr a stavba elektrických zařízení – Zařízení pro bezpečnostní účely
- ČSN 33 2000-6 Elektrické instalace nízkého napětí – Část 6: Revize
- ČSN 33 3051 Ochrany elektrických strojů a rozvodných zařízení
- ČSN 33 2130 ed.2 Elektrické instalace nízkého napětí – Vnitřní elektrické rozvody
- ČSN 33 3210 Elektrotechnické předpisy. Rozvodná zařízení. Společná ustanovení
- ČSN 33 120 Elektrotechnické předpisy. Normalizovaná napětí
- IEC ČSN 33 3015 Elektrotechnické předpisy. El.stanice a el.zařízení. Zásady dimenzování podle elektrodynamické a tepelné odolnosti při zkratech
- ČSN 34 1610 Elektrický silnoproudý rozvod v průmyslových provozovnách
- ČSN EN 61140 ed.2 Ochrana před úrazem elektrickým proudem – společná hlediska pro instalaci zařízení
- ČSN EN 61439-1 ed.2 Rozvaděče nízkého napětí – Část 1: Všeobecná část

Informatika a telekomunikace

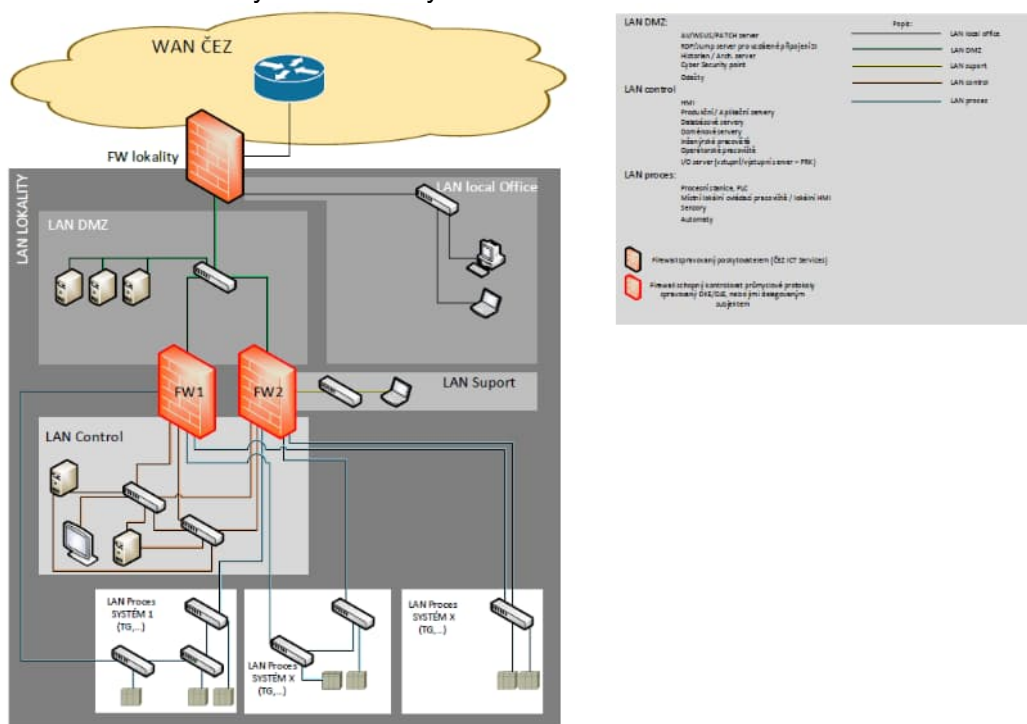
Nově instalovaná PLC a operátorská stanice budou součástí vlastní nezávislé automatizační sítě.

Realizace má dopad na kybernetickou bezpečnost. Dotčené systémy jsou součástí ISZS. Řešení a realizace musí splňovat požadavky uvedené v SKČ_ST_0027 - Standard informační a kybernetické bezpečnosti. Smlouva s dodavatelem musí obsahovat požadavky definované v příloze SKČ_ST_0027 VP H – Bezpečnostní požadavky pro dodávky dle ZoKB. Před uvedením do provozu bude provedena nezávislá kontrola zabezpečení systému útvarem IKB TAS (DOKE) nebo centrálním útvarem IKB.

Architektura sítě

Návrh síťové infrastruktury bude v souladu s SKČ_ME_0231 Síťová bezpečnost (zejména napojení OT systémů viz příloha č. 3 této metodiky).

Pro návrh síťové architektury je doporučeno vycházet například ze standardu ISA/IEC 62443 Industrial network and system security viz. obr. níže.



Segmentace sítě

- Bude použita segmentace sítě s využitím VLAN a rozdělením dle účelu systému. Tyto sítě budou mít svůj vlastní adresní rozsah, který nebude jinde v lokalitě použit a bude z privátního rozsahu.
- Všechny prostupy mezi VLANy budou routované a řízené skrze FW a schválená komunikační pravidla. Součástí předávací dokumentace bude seznam všech využitých VLAN, IP rozsahů a komunikačních pravidel.
- Na FW budou pravidla nastavena, dle zásady "co není dovoleno je zakázáno", tj. poslední pravidlo bude DENY. FW pravidla budou obsahovat pouze definice nutného provozu pro řádné fungování systému. Pravidla FW budou schválena architektem KB.

- Pouze aktivní prvky typu router nebo FW mohou mít více aktivních ethernetových rozhraní zapojených do různých sítí. Stanice budou mít vždy připojené ethernetové rozhraní pouze do jedné sítě, je zakázáno připojovat ke stanici více než jednu ethernetovou síť s různou IP adresací (např.: síť aplikační a technologické).
- V případě potřeby připojení zařízení do sítě ŘS, které není součástí ŘS (např.: nb/pc dodavatele) je nutné vytvořit dedikovanou VLAN s omezeným přístupem do této sítě. Tímto způsobem je dovoleno pouze provádět konfiguraci systému. Přenos souborů (např.: instalačních, konfiguračních) musí probíhat zabezpečenou formou přes přenosové médium v stejném režimu jako je popsáno u TRIS (viz. výše) nebo skrze terminálový server, který je umístěn v technologické DMZ (jump server).
- Design sítě musí být konzultován a schválen útvarem IKB TAS (DOKE) nebo centrálním útvarem IKB.

Oddělení sítí

- Nesmí existovat přímý prostup do internetu, přímý vzdálený přístup ani přístup do sítě ŘS z korporátní sítě. Okolní systémy je nutné oddělit a řídit komunikace skrze FW, dodané FW musí být integrované do stávajícího managementu FW DOKE / TAS. Vazby do jiných technologických sítí mohou být odděleny jednostupňově na úrovni FW, korporátní síť musí být oddělena dvoustupňově pomocí DMZ, viz výše. To se vztahuje i na vazby na stávající technologické systémy, se kterými bude nový systém integrován.
- Vazby do jiných technologických sítí mohou být odděleny jednostupňově na úrovni FW.
- Nesmí existovat přímý prostup do sítě ŘS z korporátní sítě. Pro komunikaci s korporátní sítí musí být využito DMZ (demilitarizovaná zóna). Vzdálený přístup není požadován.
- Servisní a dohledové prostupy musí být realizovány také přes DMZ. Pro vzdálené přístupy bude využito terminálového serveru (Jump serveru), který bude v DMZ.
- Všechna komunikační pravidla budou schválena útvarem IKB TAS (DOKE) nebo centrálním útvarem IKB.
- Technologická komunikace po vyhrazených spojích pro potřeby dispečerského řízení elektráren, které jsou zajišťovány dceřinými společnostmi, nemusí být speciálně chráněny, doporučuje se však použít VPN kanál – minimálně musí zařízení být schopno VPN tunel ustavit.
- Technologická komunikace na cizí subjekty musí být zabezpečena (sériová komunikace bod-bod nebo síťová komunikace v souladu s požadavky stanovenými v technickém řešení
- Dodávané firewallové řešení musí být kompatibilní a napojené na management řešení DOKE minimálně v rozsahu firewallů na perimetru ŘS (řízení komunikace z/do ŘS). V TAS (DOKE) ČEZ je vybrána technologie výrobce FORTINET. Pro oddělení je postačující např. typ Fortigate 60, případně Fortigate 80, který má SFP porty. Provozovaným managementem je řešení FortiManager. Zařízení musí být dodáno s poslední verzí v době nákupu, musí mít zakoupenou podporu výrobce na 5 let (na úrovni supportu Enterprise Protection s podporou SCADA a OT protokolů).
- FW pravidla budou obsahovat pouze definice nutného provozu pro řádné fungování systému.
- Na FW budou pravidla nastavena dle zásady "co není dovoleno je zakázáno" tj. poslední pravidlo bude DENY.
- Pro návrh síťové architektury doporučujeme vycházet například ze standardu ISA/IEC 62443 Industrial network and system security.

Dohled nad sítí

- Logování bezpečnostních událostí bude co do rozsahu a retence v souladu s SKČ_ST_0027 Standard informační a kybernetické bezpečnosti a vyhláškou 82/2018 Sb. Budou logovány události minimálně na úrovni:
 - Bezpečnostní infrastruktury (firewall, IPS, antivirová ochrana, terminálový server),
 - Veškeré přístupy na aktivní prvky a terminálový server budou logovány, a to jak úspěšné, tak neúspěšné,
 - Operační systémy (pracovní stanice, servery),
 - Aplikační vrstva (zejména přístupy a změny oprávnění),
 - Procesní stanice.
- Logy se budou sbírat a vyhodnocovat centrálně a je požadováno zajistit jejich předávání do korporátního bezpečnostního dohledu iSOC. Logy budou zasílány přes DMZ.
- V případě žádosti IKB bude nastaven jeden port na vybraných aktivních prvcích (switche, FW, routery) do režimu mirror (SPAN) a bude umožněno k těmto prvkům připojit IDS/IPS a monitorovat a logovat provoz.
- U všech firewallů a aktivních prvků musí být zajištěn alespoň přístup pro čtení logů a konfigurací pro oprávněné osoby (zejména SI). Pro samotné logy musí být umožněno předávání protokolem syslog do bezpečnostního dohledu SOC, sběr logů bude zajištěn přes DMZ.

Zálohování

- Veškeré starší verze SW musí být archivovány včetně podpůrné dokumentace, konfiguračních parametrů atp.
- Budou implementovány a popsány postupy pro zálohování a obnovení funkčnosti.
- Obnovení funkčnosti systému ze zálohy bude otestováno.
- Zhotovitel nejpozději ke dni předání Díla vytvoří aktuální zálohy SW. Tyto zálohy budou uloženy na nezávislém externím uložišti (např. DVD). Zhotovitel zpracuje postupy pro zálohování a obnovení systému. Četnost záloh a rozsah záloh budou definovány na základě provedené bezpečnostní klasifikace.
- Zálohovaná data doporučujeme šifrovat, musí být umístěna na jiném mediu a místě než produkční data.
- Záloha SW vlastního PC smí být na stanici umístěna jen v případě, že se jedná o fyzicky odpojenou kopii disku dotčeného stroje.
- Zhotovitel zpracuje postupy pro zálohování a obnovení systému. Četnost záloh a rozsah záloh budou definovány na základě provedené bezpečnostní klasifikace.

Řízení zranitelností

- Bude definována politika pro řízení zranitelností a aktualizací, a to minimálně na úrovni hraničních prvků, ideálně na úrovni všech zařízení.
- Bude definován způsob a četnost a bezpečný způsob aktualizací.
- Tam, kde nebude možná z technických důvodů pravidelná aktualizace, budou definována náhradní opatření (kontrola vstupů, oddělení sítě, řízení přístupu).

Ochrana proti malware

- Musí být zajištěna ochrana vybraných komponent systému ICT/ICS (např.: koncová zařízení, servery, sdílená datová úložiště) antivirovým programem nebo jiným opatřením proti škodlivému kódu.
- Antivirový program musí být pravidelně bezpečným způsobem aktualizován vč. virových definic:
- Pokud bude docházet k stahování virových definic a aktualizací operačních systémů, je nutné definovat roli Security Serveru (bude plnit pouze funkci aktualizace) a umístit ho do DMZ. Pokud bude docházet k aktualizacím skrze flash USB paměť, je nutné, aby byly soubory nahrávány řízeně na aktualizovaném PC s aktualizovanou AVO.
- Pokud bude docházet k aktualizacím skrze flash USB paměť, je nutné, aby byly soubory nahrávány řízeně na aktualizovaném PC s aktualizovanou AVO. Seznam veškerých připojovaných zařízení bude řádně evidován. Ukládání dat na tato média bude probíhat po prověření na škodlivý kód a pouze na speciálním pracovišti k tomuto určeném. Na toto pracoviště budou data přenášena nebo ukládána řízeným bezpečným způsobem. Před nasazením do produkčního prostředí musí být programový kód řádně otestován, jednotlivé verze řádně evidovány a zálohovány.
- Bude definováno, kdo zodpovídá za aktualizace a s jakou periodou bude prováděno.
- Pro antivirovou ochranu budou definované pravidelné skeny a bude aktivní rezidentní ochrana tam, kde je to možné.
- Pro zařízení bez možnosti nasazení aktivní antivirové ochrany budou definována náhradní opatření (oddělení, kontrola vstupů, řízení přístupu, offline skeny apod.).
- Plány pro zotavení (DRP) musejí brát v potaz dopady škodlivých programů.

Provozní bezpečnost

- Pouze aktivní prvky typu router nebo FW mohou mít více rozhraní do více sítí. Servery budou mít vždy přístup pouze do jedné sítě (kromě případů redundantního připojení) a nebudou spojovacím článkem mezi sítěmi (jako např. aplikační a automatizační síť).
- Nová zařízení (PC, síťové prvky) budou instalována v souladu s hardeningovými politikami ČEZ (tj. např. zakázání nevyužívaných služeb, protokolů a portů, odstranění default uživatelů a změna default hesel apod.) schválenými architektem kybernetické bezpečnosti, nově instalovaná PC budou zabezpečena systémem hesel vč. BIOS, bude zabráněno přístupu obsluhy do systémového nastavení aplikace i OS.
- Na aktivních prvcích budou deaktivovány nevyužívané služby a porty, nebudou využívány nezabezpečené protokoly (FTP, Telnet, http, SNMP v1 a 2) a budou změněna defaultní hesla. Bude proveden zákaz nebo logické oddělení nevyužívaných portů na aktivních prvcích, bude nastaveno oprávnění pro přístup na aktivní prvky.
- Bude definována politika ochrany proti malware. Pro antivirovou ochranu bude definován bezpečný způsob pravidelné aktualizace (samotný antivirový program vč. virových definic) a pravidelné skeny, bude aktivní rezidentní ochrana tam, kde je to možné. Pro zařízení bez možnosti nasazení aktivní antivirové ochrany budou definována náhradní opatření (oddělení, kontrola vstupů, řízení přístupu, offline skeny apod.). Plány pro zotavení (DRP) musejí brát v potaz dopady škodlivých programů.
- Bude definována politika řízení zranitelností, a to minimálně na úrovni hraničních prvků, ideálně na úrovni všech zařízení. Bude definován způsob a četnost a bezpečný způsob

aktualizací. Tam, kde nebude možná z technických důvodů pravidelná aktualizace, budou definována náhradní opatření (kontrola vstupů, oddělení sítě, řízení přístupu).

- Využití nezabezpečených protokolů je zakázáno (FTP, Telnet, http, SNMP v1 a 2 apod.).
- Předání SW od zhotovitele musí proběhnout bezpečnou formou.
- Nový software bude před instalací otestován na výskyt malwaru a jiného škodlivého kódu.
- Při realizaci změny nesmí být k TŘIS připojováno žádné neautorizované a neschválené zařízení (notebook) ani žádné neproověřené přenosné médium.
- Budou implementovány a popsány postupy pro zálohování a obnovení funkčnosti systému

Umístění prvků

- Rozvaděče, ve kterých jsou umístěné aktivní prvky SKŘ, musí být vybavené kontaktním čidlem pro kontrolu otevření dveří se signalizací do operátorské stanice.
- Ve skříních SKŘ nesmí být umístovány zařízení, která nesouvisí s tímto SKŘ (jedná se například o switche, převodníky zařízení, které nespádají do správy SKŘ).
- Do sítě SKŘ nesmí být provedena žádná připojení pomocí nezabezpečených bezdrátových zařízení jako je např. WiFi, Bluetooth apod., včetně periferních zařízení.
- Bude nasazena mechanická ochrana rozhraní proti nepovolenému použití – nepoužívané USB porty PC stanic budou osazeny mechanickou ochranou.

Bezpečnostní dohled

- Logování bezpečnostních událostí bude co do rozsahu a retence v souladu s vyhláškou 82/2018 Sb. Budou logovány události na úrovni operačních systémů, síťových prvků a PLC.
- Bezpečnostní infrastruktury (firewally, IPS, antivirová ochrana, terminálový server)
- Přístupy na síťové prvky
- Operační systémy (pracovní stanice, servery)
- Aplikační vrstva (zejména přístupy a změny oprávnění)
- Procesní stanice
- Logy se budou sbírat a vyhodnocovat centrálně a je požadováno zajistit jejich předávání do korporátního bezpečnostního dohledu iSOC. Logy budou zasílány přes DMZ.

Řízení přístupu

- Řízení přístupu bude definováno v autorizačním konceptu, který bude součástí dodané dokumentace. Autentizace a autorizace bude řízena:
 - na úrovni operačních systémů,
 - na úrovni aplikace,
 - na úrovni přístupu k aktivním prvkům.
- Rozvaděče, ve kterých jsou umístěné aktivní prvky SKŘ, musí být vybavené kontaktním čidlem pro kontrolu otevření dveří se signalizací do operátorské stanice.
- Ve skříních SKŘ nesmí být umístovány zařízení, která nesouvisí s tímto SKŘ (jedná se například o switche, převodníky zařízení, které nespádají do správy SKŘ).
- Do sítě SKŘ nesmí být provedena žádná připojení pomocí nezabezpečeného bezdrátových zařízení jako je např. WiFi, Bluetooth apod., včetně periferních zařízení.
- Objednatel vybaví veškerá zařízení obsahující USB porty (včetně USB-C) mechanickými zámkami USB (záslepkami, zámkami připojených zařízení) kompatibilními s již používanými zámkami a klíči od společnosti Smart Keeper.

- Řízení přístupu bude definováno v autorizačním konceptu, který bude součástí dodané dokumentace. Autentizace a autorizace bude řízena na úrovni operačních systémů, na úrovni aplikace i na úrovni přístupu k aktivním prvkům nebo firewallu.
- Autentizace bude řízena pomocí personifikovaných účtů. Sdílené účty jsou přípustné pouze u operátorských pracovišť s trvalou obsluhou 24x7. Tyto účty nesmí mít zvýšená oprávnění. Privilegované účty musí být personifikované. Defaultní účty jako Administrator a Guest budou zakázány. Účty typu Host jsou přípustné pouze na aplikační úrovni, viz dále.
- Komplexita hesla musí být v souladu s vyhláškou 82/2018 Sb.
- Na aplikační úrovni bude aplikována kontrola přístupu do aplikace pomocí účtu (korporátní jméno a heslo).
- Inženýrské stanice jsou využívány výhradně pro inženýrské a servisní účely. Na aplikační úrovni budou zachovány role a uživatelské účty dle stávající koncepce.
- Kontrola přístupu pomocí jména a hesla musí být aplikována i na síťových prvcích jakou jsou switche, routery, firewally atd.
- Uživatelský/administrátorský přístup bude chráněn pomocí uživatelského účtu a hesla. Hesla budou v systému uložena v šifrované podobě. Pro administraci systémů ICT/ICS musí být využívány pouze personifikované administrátorské účty speciálních tříd k tomu určených-QS, QR. Sdílené účty mohou být použity pouze u operátorských rolí na pracovišti s nepřetržitou obsluhou a nesmí mít oprávnění pro změny konfigurace systému a aplikací.

Síťová a IKB dokumentace

Součástí předávací dokumentace k síti bude:

- schéma logické a fyzické topologie sítě a vazeb na okolní systémy,
- adresní plán sítě,
- seznam všech využitých VLAN, fyzických sítí,
- komunikační pravidla, routovací tabulky a využité protokoly.
- Bude vytvořen autorizační koncept pro přístup k systému.
- Budou popsány postupy pro zálohování systému.
- Bude popsána politika ochrany proti malware.
- Bude popsána politika pro řízení zranitelností a aktualizací.
- Budou popsány plány pro zotavení a obnovení funkčnosti systému (DRP – Disaster Recovery Plan).
- Bude aktualizovaná provozně technická dokumentace SKŘ.

Požadavky na zpracování software

- Proces tvorby a ověření SW musí probíhat řízeným způsobem v souladu s plány jakosti výrobce (dle ČSN ISO/IEC/IEEE 90003_Softwarové inženýrství – Směrnice pro použití ISO 9001:2015 na počítačový software).
- Zhotovitel musí poskytnout a předat SW či HW prostředky nezbytné k obnově zařízení po poruše, tj. ke kompletní reinstalaci SW ze záložních médií, jeho konfiguraci a spuštění a případně i další nástroje nezbytné pro předepsanou údržbu zařízení.
- Jako jeden z výstupů procesu tvorby a ověření Zhotovitelem instalovaného SW budou kromě dokumentace Díla Zhotovitelem předány i datové nosiče se systémovým a aplikačním SW, a to včetně administrátorských hesel; pro stanice na bázi PLC a DCS navíc i záložní média s obrazy disků a zdrojové formy aplikačního SW.
- Jednotlivé verze nově instalovaného SW musí být Zhotovitelem řádně evidovány a zálohovány. Funkčnost nového SW Zhotovitel otestuje v rámci zkušebního provozu.

Další požadavky

- Při realizaci nesmí být k TRIS připojováno žádné neautorizované a neschválené zařízení (notebook) ani žádné neproověřené přenosné médium. Všechna použitá média budou evidována. Ukládání dat na tato média bude probíhat po prověření na škodlivý kód a pouze na speciálním pracovišti k tomuto určeném. Předání SW od zhotovitele musí proběhnout bezpečnou formou. Před nasazením do produkčního prostředí musí být programový kód řádně otestován, jednotlivé verze řádně evidovány a zálohovány.
- V případě potřeby připojení zařízení do sítě RS, které není součástí RS (např.: NB/PC dodavatele) je nutné vytvořit dedikovanou VLAN s omezeným přístupem do této sítě. Tímto způsobem je dovoleno pouze provádět konfiguraci systému. Přenos souborů (např.: instalačních, konfiguračních) musí probíhat zabezpečenou formou přes přenosové médium v stejném režimu jako je popsáno u TRIS (viz. výše) nebo skrze terminálový server, který je umístěn v technologické DMZ (jump server).
- Zhotovitel zajistí, aby k datu předání díla neobsahoval řídicí systém SW, který není součástí dodávky, a aby na discích neležely soubory ani adresáře, které nejsou součástí nebo provozním produktem nasazeného operačního systému nebo nasazené aplikace. Veškeré pomocné soubory a adresáře vzniklé během nasazování aplikace musí být průběžně odstraňovány.
- Nejpozději k datu předání budou z operačních systémů stanic RS odstraněny všechny předchozí „body obnovení“ a bude vytvořen nový s posledním provozním stavem. Teprve následně bude vytvořena záloha disku.
- Basic design musí být konzultován a schválen architektem IKB. Součástí basic designu musí být podrobná schémata včetně definování jednotlivých sítí a podsítí. Schéma bude obsahovat adresní plán, routovací tabulky a komunikační pravidla mezi jednotlivými sítěmi, včetně a využitých protokolů a definování předávacích míst (router, firewall, ...).
- Před uvedením zařízení do provozu bude provedena nezávislá kontrola zabezpečení systému útvarem IKB TAS (DOKE) nebo centrálním útvarem IKB.

Požadavky na PKZ

- 1 Vstupní kontrola
 - 1.1 Kontrola provedení školení dle CYBEX
 - 1.2 Kontrola registrovaných zařízení dodavatele
 - 1.3 Kontrola provedení konzultace designu a kompatibility architektury s IKB TAS (DOKE) nebo centrálním útvarem IKB
- 2 Kontrola v rámci realizace
 - 2.1 Kontrola architektury sítě
 - 2.2 Kontrola dohledu nad sítí
 - 2.3 Kontrola zálohování
 - 2.4 Kontrola řízení zranitelností
 - 2.5 Kontrola ochrany proti malware
 - 2.6 Kontrola provozní bezpečnosti
 - 2.7 Kontrola řízení přístupu
- 3 Výstupní kontrola
 - 3.1 Kontrola síťové a IKB dokumentace
 - 3.2 Finální kontrola díla (včetně PTD)