Zadávací dokumentace

Audit a dokumentace ICT a MaR

Hlavní cíle auditu a dokumentace ICT a MaR

Cíly auditu a dokumentace ICT a MaR jsou zejména zabezpečení provozu objednatele při jakékoliv poruše software, nebo hardware, zabezpečení proti napadení ICT a MaR objednatele, a to jak z vnější sítě, tak z vnitřní sítě s ohledem zejména na odepření služeb, neoprávněné získávání dat objednatele, neoprávněný přístup k systémům a technologiím objednatele, poškozením software, nebo hardware objednatele. Audit dále navrhne a popíše opatření, jak k tomuto požadovanému stavu dojít.

Jednotná terminologie

Pro účely tohoto dokumentu jsou vymezeny následující názvy a pojmy (názvosloví).

AB – administrativní budova, sídlo společnosti Žatecká teplárenská, a. s.

Centrální SCADA systém – soubor HW a SW objednatele, který umožňuje obsluhám přístup k dozoru a ovládání výrobních a podpůrných technologií a který provádí distribuci dat mezi uživateli a řídicími systémy a který provádí nadřazené regulace technologií.

Datový rozvaděč – technické zařízení, kde jsou umístěny prvky ICT (servery, aktivní prvky, routery, firewally...)

DB-Net – sériový komunikační protokol AMiT.

DB-Net/IP – průmyslová komunikační sběrnice na základě ethernetu AMiT.

Firmware – nízkoúrovňové programové vybavení zařízení od výrobce, které není uživatelsky dostupné (embedded software).

FM – frekvenční měnič.

ICT – informační a komunikační technologie firmy.

ISP – poskytovatel připojení k síti internet.

KKS – systém jednotného značení zařízení energetických výroben.

Komunikace – proces přenosu dat různými fyzickými prostředky a protokoly.

Komunikační převodník – převodník signálu, nebo komunikace na komunikaci.

Komunikační rozvaděč – technické zařízení, kde dochází k propojení, opakování, galvanickému oddělení, nebo konverzi komunikace, nebo signálu.

LDS – lokální distribuční síť. Objednatel provádí dálkový odečet energie a vody.

MAN – metropolitní počítačová síť.

MaR – měření a regulace. Obor zabývající se komplexně řízením technologií pomocí elektrických, elektronických a ICT prvků.

MODBUS – otevřený protokol pro vzájemnou komunikaci různých zařízení, a to jak sériovou, nebo TCP/IP verzí.

M-BUS – komunikační protokol určený především pro dálkový odečet hodnot z různých měřičů energií, tepla, vody atd. Má vlastní fyzické provedení.

Perč I – soubor budov a technologií výtopny Perč dle situačního nákresu.

Perč II ORC – soubor budov a technologií teplárny Perč dle situačního nákresu.

Poseidon – systém bezdrátových prostředků Enika.

Pracovní stanice – stolní počítač, notebook, tablet a jiná zařízení pomocí kterých je umožněn přístup do podnikové a technologické sítě.

PROFIBUS – průmyslová sériová komunikační sběrnice.

PROFINET – průmyslová komunikační sběrnice na základě ethernetu.

Řídicí systém (ŘS) – volně programovatelné zařízení, které ovládá nějaký technologický proces.

Rozvaděč MaR – technické elektrické zařízení, které je souborem elektrických a elektronických komponent a prvků, které spolu řídí technologii, nebo část technologie.

SCADA – software umožňující dispečerské řízení a sběr dat.

SCZT – soustava centrálního zásobování teplem.

Sériová komunikace – veškerá komunikace prováděná linkami RS232, RS485, RS422, M-BUS atd. a to včetně jejich konverzí na jiné formy komunikace. V Žatecké teplárenské, a. s. se jedná zejména o DB-Net, Profibus, Modbus, M-BUS, Siox. Pro účely tohoto dokumentu a díla je pod tento pojem zahrnuta i případná paralelní komunikace.

SIOX – asynchronní sériová komunikační sběrnice.

SNMP – internetový protokol převážně sloužící ke správě počítačových sítí.

Subnet – je myšlena část vnitřní sítě. která je vymezena účelem, nebo fyzicky, nebo IP adresací, nebo jako VLAN.

Vnější síť – vnější ICT infrastruktura, ke které je připojená ICT objednatele.

Vnitřní síť – veškerá ICT infrastruktura v majetku objednatele.

VPN – virtuální privátní síť.

VS – výměníková stanice slouží k předávání tepla odběratelům, nebo do dalších částí teplárenské sítě. Podle druhu provedení jde také o KPS, DPS, PS, kdy se jedná vždy i v těchto případech o výměníkovou stanici.

WiFi – standard pro bezdrátovou komunikaci.

1 Vymezení rozsahu díla

Dodavatel díla provede z horizontálního hlediska dokumentaci na veškerá zařízení, která jsou propojená sériovou komunikací, bezdrátovou komunikací, nebo TCP/IP komunikací. Jedná se o soubor řídicích systémů, převodníků, serverů, pracovních stanic, frekvenčních měničů, aktivních prvků atd. která komunikují mezi sebou, s centrálními SCADA systémy, uživatelsky, nebo je k nim přistupováno komunikačně jiným způsobem. Zařízení objednatele se nachází ve třech definovaných prostorech:

1.1 Zdroj

Veškerá zařízení ICT a MaR v rámci budov a technologií výroben Perč I a Perč II ORC včetně LDS. Areál se nachází mimo město Žatec u silnice č. 227 směr Žatec – Holedeč, přibližně 1,5 km od Žatce. Jedná se oplocený prostor se soustavou budov, vnitřního a venkovního zařízení. V areálu se nachází serverovna s několika servery a aktivními prvky, přibližně 4 datové rozvaděče, 3 rozvodny NN se zařízeními MaR a 10 samostatných rozvaděčů MaR. V celém areálu je přibližně 20 řídicích systémů, 20 komunikačních převodníků, 40 frekvenčních měničů. Pro dohled nad technologiemi jsou nasazeny 4 vizualizační systémy různých výrobců. V areálu se nachází zejména:

- centrální SCADA systém
- kamerový systém
- subnet filtrů odprášení
- subnet kotlů K1 a K2
- LDS sběrný dvůr
- subnet Perč I
- subnet Perč II ORC
- bezdrátová síť Poseidon
- podnikový systém
- serverovna
- a další

1.2 SCZT

Veškerá zařízení ICT a Mar v rámci SCZT a MAN Žatecké teplárenské, a. s. ve městě Žatci. Zařízení, nebo zakončení komunikačních tras se nachází zejména ve výměníkových stanicích, podzemních šachtách, kolektorech, topných kanálech, pronajatých prostorách atd. Výměníkových stanic s nějakou formou komunikace, nebo sdílením dat je přibližně do 150. Délka komunikačních sítí (metalických, nebo optických tras) je přibližně 24 km a jejich zakončení je přibližně na 150 místech. V soustavě je použito přibližně 20 LTE routerů. Tato zařízení obsahují zejména:

- kabelové metalické a optické trasy
- trasy zemních chrániček bez využití
- LTE komunikace
- sériové komunikace
- ethernet komunikace
- rozvaděče datové, komunikační a MaR

- měřiče tepla (seznam předá objednatel)
- a další

1.3 AB

Administrativní budova se nachází v areálu výroben Perč, nicméně je brána jako samostatný celek. V budově se nachází zejména aktivní síťové prvky, záložní NAS atd. Dokumentace pracovních stanic v této budově již proběhla a bude pro účely tohoto díla předána objednatelem dodavateli pro začlenění do díla a naplnění ostatních cílů díla.

2 Požadované úrovně

Dodavatel díla provede dokumentaci z vertikálního hlediska na všechna ICT a MaR zařízení do úrovně všech forem sériové komunikace, nebo TCP/IP komunikace (včetně bezdrátových). Nižší úrovně komunikace jako např. 4–20 mA, HART snímače teplot, tlaku apod. nejsou předmětem díla.

2.1 Internet

Dodavatel díla provede dokumentaci všech připojení k internetu z podnikové a technologické sítě. Dokumentace bude taktéž obsahovat veškeré komunikační kanály rozdělené na permanentní a náhodné. Permanentní jsou ta, která využívají prostředky MaR k periodické komunikaci mezi sebou anebo s nadřazeným systémem. Náhodná jsou ta, kdy dochází k občasnému nepravidelnému připojení, a to zejména obsluh, servisních techniků, programátorů apod. Dále dokumentace musí rozlišit úroveň připojení, zda se jedná o přímé spojení (porty), nebo o VPN, včetně popisu a konfigurace. Záznamy budou obsahovat, pokud budou dostupné i tyto informace:

- Způsob připojení a ISP (přibližně 30 různých připojení)
- Technické a výkonové parametry
- Použitá technologie
- IP adresace
- Otevřené porty a jejich účel
- VPN a jejich účel

2.2 Interní sítě

Dodavatel díla provede dokumentaci všech interních komunikačních sítí MAN, LAN a sériových sítí. Předmětem dokumentace budou:

- Sériové linky
- Ethernetové sítě
- Bezdrátové sítě (WiFi, Poseidon...)
- Protokoly
- Aktivní prvky (převodníky, opakovače, galvanická oddělení, routery, switche...)
- IP adresace

- Schéma topologie
- Blokové schéma datových, komunikačních a MaR rozvaděčů
- WiFi (AP, bridge...)
- Servery
- Úložiště
- Pracovní stanice
- Počítačové periferie se síťovou komunikací (LAN, WiFi)
- Ostatní (EZS, docházkový systém, EPS...)

3 Software

V rámci tohoto díla bude zdokumentován veškerý software pracovních stanic, serverů, řídicích systémů a jiných volně programovatelných zařízení. Dílo se nevztahuje na firmware a software, který je součástí zařízení od výrobce a neumožňuje jakýkoliv zásah uživatele (typicky například firmware pevného disku, čipu WiFi, GPS čipu a obdobných). Na firmware a software, které podléhá jakýmkoliv funkčním, nebo bezpečnostním aktualizacím se předmět díla vztahuje (řídicí systémy, převodníky, aktivní síťové prvky...) Záznamy budou obsahovat, pokud budou dostupné i tyto informace:

3.1 Software

- Operační systémy
- Virtualizace
- Obchodní systémy
- Kancelářské systémy
- Antivirové systémy
- Ovladače a drivery, které nejsou součástí OS, jsou dodatečně instalované a jsou nutné pro chod aplikací (typicky ovladače virtuálních sériových, nebo jiných portů, ovladače pro komunikaci s UPS apod.)
- Runtime licence
- Cloud agenty
- Aplikační software řídicích systémů

3.2 Informace o software

- Název
- Výrobce
- Verzi
- Dostupnost zdrojového kódu
- Místo zálohy
- Zabezpečení obnovení
- Nutnost a aktuálnost aktualizace
- Datová provázanost s ostatními SW
- Kontakt na servis, nebo podporu
- Kontakt na programátora

- Dostupnost vývojového prostředí
- Časová dostupnost servisu, nebo podpory
- Priorita funkčnosti

3.3 Priority funkčnosti

Na veškeré auditované a dokumentované zařízení bude v rámci díla stanovena priorita funkčnosti. Ta stanoví, jak dlouho může být zařízení nefunkční, tak, aby nebyla ohrožena výroba, nebo chod podniku. Priority funkčnosti budou stanoveny ve spolupráci s objednatelem, kdy ten v rámci kontrolních dní schválí zařazení jednotlivých zařízení ve vytvořené škále (předběžně navrhovaná škála):

- ihned – zařízení musí být v nejkratším možném dostupném čase funkční
- do 24 hodin
- do 5 pracovních dní
- do začátku topné sezóny
- není kritické

3.4 Software vazby

Dodavatel díla provede dokumentaci software vazeb. Tím je myšleno komunikační provázání mezi zařízeními, nebo software, kdy se předávají periodicky nějaká data, nebo soubory a tato vazba slouží ke sdílení informací, konvergenci, zvýšení robustnosti systému, zálohování atd. Software vazby budou v rámci díla členěny na:

- SCADA – ŘS
- SCADA – SCADA
- ŘS – ŘS
- ostatní (klienti IS, zálohování, přesuny a zrcadlení dat...)

4 Značení KKS

- Všechna fyzická zařízení podléhající dokumentaci dle tohoto díla dodavatel označí standardním kódem KKS.
- Strukturu KKS vytvoří a dodá dodavatel díla. Strukturu vytvoří od 1. do 3. stupně s tím, že řídicí systémy a další elektronické prvky, které jsou tvořeny modulárně, nebo doplněny o interní rozšiřující prvky jsou chápány jako jeden celek 3. stupně.
- Označeny budou veškeré aktivní prvky, které komunikují, nebo zprostředkovávají komunikaci.
- Označeny budou veškeré metalické a optické trasy, a to na obou svých koncích.
- Značení bude trvalé a odpovídající prostředí, ve kterém bude použito, tak aby byla zajištěna jeho funkčnost po celou dobu životnosti označeného prvku, nebo zařízení.

5 Prezentace výsledků

Výstupem dokumentační části díla bude elektronická evidence založená na databázovém systému umožňující permanentní udržování aktuálního stavu. Záznamy budou obsahovat veškeré informace s předchozích kapitol vymezení díla 1.3 a 1.4 a informace o software z kapitol 1.5 Pro datové vazby dle kapitoly 1.5.4 budou provedeny samostatné záznamy. Záznamy budou obsahovat, pokud budou dostupné i tyto informace:

- Název zařízení
- Typ zařízení
- Výrobce zařízení
- Sériové číslo zařízení
- Fotografie zařízení
- Konfigurace zařízení
    - IP konfigurace (IP, maska, GW, DNS, DHCP, porty...)
    - sériová konfigurace (adresa, parita, stopbity, počet bitů, rychlost...)
    - VPN (protokol, server, heslo, uživatel...)
    - ostatní (protokol, port, uživatel, heslo, SNMP...)
- Dodavatel software
- Verze firmware, operačního systému.
- Servisní zajištění, support a platnost.
- Umístění (místo, ulice, č. p., označení výměníkové stanice, místnost, rozvaděč...)
- Trasa v případě kabelu (situační plánek)
- Datová komunikace

5.1 Fyzická databáze

Databáze dokumentace bude dodána v takové formě, aby mohla být nasazena na stávající serverová řešení společnosti a bude v architektuře Windows. Přístup do databáze bude buď přímým otevřením, nebo formou tenkého klienta, a to výhradně libovolného webového prohlížeče bez nutnosti instalace jakéhokoliv doplňku prohlížeče. Součástí nabídky samostatně bude i správa, zálohování a aktualizace databáze.

5.2 Datová struktura

Dodavatel díla navrhne datovou strukturu, která bude součástí nabídky a bude dále sloužit k prezentaci a uložení vypracovaných dat. Během díla bude jakoukoliv změnu struktury dodavatel díla předkládat objednateli k novému odsouhlasení s označením verze dokumentu obsahujícím pravidelné stoupající číslování. Změnu struktury může vyvolat i objednatel a řídí se stejným postupem.

5.3 Filtrace a prohledávání záznamů

Dodaná elektronická dokumentace bude mimo struktury umožňovat prohledávání záznamů pomocí hledání záznamů a filtrace záznamů. Hledáním záznamů se myslí programová technika, kdy bude záznam možno vyhledat zadáním klíčových slov a filtrací záznamů se myslí programová technika, kdy

bude výstupem výpis záznamů splňující zadané kritérium. Zařízení bude možné filtrovat i podle stavu a použitelnosti dle kapitoly 1.14.

5.4 Mapa ICT

Dodaná elektronická dokumentace od dodavatele bude obsahovat zákresy všech komunikačních sítí v situačních schématech, nebo mapách. Mapy pro zákresy na území soustavy CZT dodá odběratel.

5.5 Aktualizace záznamů

Po celou dobu dodání díla až do jeho finálního předání budou záznamy v databázi dokumentace udržovány aktuální a pokud budou v rámci činnosti objednatele provedeny nějaké změny, tak dodavatel zajistí jejich aktualizaci. Pro tento proces navrhne dodavatel metodický pokyn, který bude schválen objednatelem a podle kterého bude postupováno při zajištění aktuálnosti a konzistence záznamů v dokumentaci, a to i po dokončení díla.

6 Bezpečnostní audit

Dodavatel díla provede kontrolu zabezpečení podnikové a technologické sítě včetně následných návrhů opatření. Kontrola bude provedena s ohledem zejména na:

- Průnik a funkci IDS
- Neautorizovaný přístup do sítí zevnitř i z venku
- Odepření kritické služby
- Aktualizace a bezpečnostní záplaty
- Zálohování a obnovení po výpadku
- Dálkové přístupy
- Směrnice podniku, interní předpisy a normy a soulad s těmito předpisy.
- Směrnice GDPR a soulad se směrnicí
- Ostatní

Kontrola bude rozšířená o sběr objektivizovaných bezpečnostně-provozních dat z kritických systémů podnikové a technologické sítě, a to po dobu 14 dnů v reálném provozu. Kritické systémy a termín budou definovány a odsouhlaseny dodavatelem a objednatelem v rámci kontrolního dne. Výstupem bude komplexní zpráva, která provede vyhodnocení objektivizovaných bezpečnostně-provozních dat, popíše aktuální bezpečnostní stav a navrhne technická, organizační a procesní opatření. Pokud budou současná technická zařízení v souladu s požadavky na zabezpečení dle cílů tohoto díla, tak další navrhovaná technická opatření musí brát v úvahu unifikaci a tím zohlednit případné technické návrhy na stejné platformě. V oblasti organizační a procesní dodavatel navrhne doplnění vnitřních směrnic, provozních řádů, metodických pokynů nebo jiných dokumentů pro naplnění cílů tohoto díla.

6.1 Stav a použitelnost

Dodavatel díla vytvoří seznam jednotlivých prvků a sítí, které jsou technicky, ekonomicky a v dalším horizontu vývoje vědy a techniky, GDPR, morálního a technického stáří, možnosti aktualizace a reakce

na bezpečnostní hrozby nevhodné, nebo nepoužitelné. Tato část díla se týká jak pro programovou, tak pro fyzickou vrstvu. Seznam bude vhodně prezentován v dodané elektronické dokumentaci, například upozorněním při vyhledání zařízení. Zároveň o tom bude vytvořen samostatný dokument, který bude předán v rámci předání díla. Dodavatel se zaměří i na tyto prvky a vlastnosti, pokud budou relevantní.

- Poškození, která znemožňují použití v prostředí, nebo nesplňují IPxx dle výrobce.
- Nemožnost servisu, nebo aktualizace z důvodu zániku výrobce.
- Nemožnost servisu, nebo aktualizace z důvodu následné ztráty funkce zařízení, nebo software.
- Poškození, nebo stáří, nebo důvod k vyřazení dle návodu výrobce u prvků zabezpečujících. ochranu zařízení a komunikačních linek (přepěťové ochrany třídy D).

6.2 Návrh koncepce

Dodavatel navrhne koncepci dalšího směřování ICT a MaR společnosti v budoucnosti, tak aby byla zajištěna zejména tato kritéria:

- Ekonomická výhodnost,
- technické řešení reflektující trendy a vývoj na poli vědy a techniky,
- legislativní prostředí, a to zejména v otázkách kybernetické bezpečnosti a GDPR,
- stabilita výrobců a dodavatelů materiálu a služeb.

Výsledkem bude dokument, který popíše dle priorit největší hrozby pro ICT a MaR objednatele a navrhne jejich řešení, tak aby byly naplněny hlavní cíle tohoto auditu a dokumentace ICT a MaR.

6.3 Ostatní

Dokumentace a audit se týkají pouze zařízení a majetku Žatecké teplárenské, a.s.

Použitá terminologie vychází z potřeb tohoto díla a v případě rozporu s obecnou terminologií platí přiměřeně názvosloví definované v tomto dokumentu