Tento metodický pokyn je řídicím dokumentem společnosti NET4GAS, s.r.o.

Postupování třetím osobám je možné pouze se souhlasem jednatele společnosti nebo vlastníka procesu.

	Zpracoval	Přezkoumal po věcné stránce	Přezkoumal po formální stránce	Schválil
Funkce	Manažer, SCADA provozní technologie	Ředitel, Provoz soustavy	Specialista, Kancelář vedení společnosti	Ředitel, Informační technologie
Jméno	Zdeněk Vondrouš	Ing. Petr Koutný	Daniela Kašparová	Ing. Zdeněk Haloda
Podpis	v. r.	v. r.	v. r.	v. r.
Datum	30.06.2015	30.06.2015	30.06.2015	08.07.2015

Změnový list

Označení části textu*	**Popis změny**
	Základní – výchozí verze dokumentu

** příp. odkaz na kapitolu, odstavec, …*

Rozdělovník

a) Typový:

- Jednatel společnosti - Výkonný ředitel, Finance
- Ředitel, Provoz soustavy
- Ředitel, Informační technologie
- Zpracovatel
- Specialista, Kancelář vedení společnosti - správce řízené dokumentace
- Zaměstnanci společnosti NET4GAS, s.r.o.

b) Individuální:

Útvar	Funkce
Provoz soustavy	Manažer, SCADA
Provoz soustavy	Manažer, lokální ŘS, STO
Technická podpora	Specialista - telemetrie
Informační technologie	Projektový manažer
Informační technologie	Manažer, IT Infrastruktura
Informační technologie	Bezpečnostní manažer

Obsah

A Účel

Tento dokument poskytuje přehled pravidel a zásad pro bezpečnou práci uživatele a správce ŘS či SCADA systému (dále jen „Pracovník“) v prostředí ICS společnosti NET4GAS, s.r.o. (dále jen „Společnost“), Dokument stanovuje pro Pracovníky základní zásady bezpečného používání prostředků ICS.

B Rozsah platnosti a kontrola

Tento řídicí dokument platí pro Společnost a subjekty, které se zavázaly dodržovat bezpečnostní politiku a Bezpečnostní opatření Společnosti v oblasti ICS.

Kontrolu plnění tohoto metodického pokynu jsou oprávněni provádět pracovníci určení Manažerem, SCADA provozní technologie, nebo Manažerem, IT infrastruktura.

Za revizi a změny tohoto metodického pokynu a postupů v něm uvedených zodpovídá ve společnosti NET4GAS, s.r.o., vlastník procesu.

C Definice pojmů a zkratek

Pojem / Zkratka	Definice
ASDU	Application Service Data Unit (viz ČSN EN 60870-5-104)
CCTV	Kamerový systém
CD, DVD	Datové nosiče
DC Praha	Dispečerské centrum Praha – centrální dispečink společnosti NET4GAS, s.r.o.
DN4G	Dispečink přepravní soustavy NET4GAS, s.r.o., určený k řízení přepravy plynu
DPD	Databáze provozních dat
EPS	Elektrická požární signalizace - vyhrazené požárně bezpečnostní zařízení splňující podmínky obecně závazných předpisů na úseku požární ochrany a norem (Vyhláška č. 246/2001Sb., ČSN EN 54, ČSN 730875, ČSN 342710)
Ethernet	Přenosový protokol
FER	Frontend komunikační server pro komunikaci s podřízenými stanicemi
FW	Firewall
GPRS	General Packet Radio Service – přenos Ethernet rámců v prostředí mobilních telefonních sítí
HLNT	Název řídicího systému High-Leit NT od firmy IDS GmbH
HPS	Hraniční předávací stanice
HSB	Role serveru řídicího systému, kdy čeká na výpadek LR serveru (Hot-StandBy stav)
HW	Hardware
IEC 60870-5-104	Norma definující a popisující komunikační protokol užívaný pro dálkové řízení a sběr dat označená jako IEC 60870-5-104:2006 nebo ČSN EN 60870-5-104 ed. 2
InSQL	Industrial SQL server – uložiště lokálních provozních dat
ICS	Industrial Control System – řídicí systém
KS	Kompresní stanice
LŘS	Lokální řídicí systém
MPLS	Multiprotocol Label Switching-síťová technologie založená na směrování (přepínání) paketů podle značek
MP, metodický pokyn	Typ řídicího dokumentu, poskytuje detailní informaci o tom, jak opakovaně provádět konkrétní činnosti
N4G nebo též „Společnost“	NET4GAS, s.r.o.
NET4GAS	Společnost NET4GAS, s.r.o.

OPC DA 2.0	Způsob předávání realtime dat pomocí standardu OPC (Ole for Process Control) DA (data Acces) 2.0 (verze)
PDS	Plynové detekční systémy
Podřízená stanice	Kterákoliv stanice, ze které ŘS DN4G sbírá data, nebo ji řídí. (Viz telemetrie, VPS a PRS)
PRS	Předávací a regulační stanice
Přenosová relace	Seznam přenášených veličin, jejich adres, jednotek apod. mezi ŘS DN4G a podřízenou stanicí
PZTS	Poplachové zabezpečovací a tísňové systémy, dříve EZS (elektronické zabezpečovací zařízení)
ŘS	Řídicí systém
SCADA	Systémy pro průmyslové řízení a sběr dat (Supervisory Control And Data Acquisition)
setpoint	Žádaná hodnota
SKV	Systém kontroly vstupu
SLA	Service Level Agreement – servisní smlouva s externím dodavatelem servisu a služeb
SM, směrnice	Typ řídicího dokumentu - určuje metody, pravidla, postupy, prostředky pro výkon činností v procesech a jejich součinnost
Správce ŘS DN4G	Vyhrazení pracovníci zodpovědní za provoz a údržbu ŘS DN4G
SQL	Structured Query Language
STO	Systémy technické ochrany objektů (CCTV, PZTS, SKV, systémy perimetrické ochrany a související technická zařízení) - soubor technických prostředků instalovaných jako součást fyzické ochrany
SW	Software
TA	Technologické aplikace
TDC	Technologické datové centrum
Telemetrie	zařízení zajišťující přenos měřených fyzikálních veličin a stavových informací ze sledovaného technologického procesu (ve smyslu tohoto MP, jinak „Telemechanika“) včetně přenosu povelů a parametrů k akčním členům řízené technologie. Dálkový přenos je realizován s využitím různých přenosových médií
VPS	Vnitrostátní předávací stanice
WAN	Wide Area Network
WS	Work Station – operátorský terminál dispečera

D Popis procesů a pravidel

Společnost provozuje část kritické infrastruktury státu a je držitelem výhradní licence pro přepravu plynu (TSO) v České republice. Provozuje více než 3600 km plynovodů a její přepravní soustava je zárukou bezpečnosti a spolehlivosti, provozní dokonalosti a inovativních řešení, které respektují závazek vůči budoucím generacím. Soustava Společnosti propojuje trhy do všech světových stran přeshraničními propoji. Společnost tak přispívá zvýšení energetické bezpečnosti nejen v České republice, ale v celém středoevropském regionu.

Ochrana Informačních Aktiv je zásadním principem i cílem Společnosti v oblasti bezpečnosti. Z tohoto pohledu podléhá Společnost regulaci a musí vyhovět mnoha zákonným normám a předpisům.

Tento metodický pokyn se zabývá ochranou Informačních Aktiv ICS a ochranou vlastního zpracování Informačních Aktiv v rámci ICS.

Veškeré nakládání s Informačními Aktivy je Pracovník povinen podřídit pravidlům stanovených pro danou klasifikaci informací podle stupně jejich důvěrnosti. Třídu důvěrnosti informace stanoví vlastník Informačního aktiva. Tato pravidla definuje směrnice Společnosti „*Bezpečnostní pravidla pro ochranu informací*“. Tato směrnice stanoví následující klasifikaci informačních aktiv podle stupně jejich důvěrnosti na Strategické, Určené, Interní a Veřejné. Pro každou z těchto klasifikačních tříd jsou ve zmíněné směrnici mimo jiné zavedena pravidla nakládání s informacemi patřícími do dané třídy/úrovně klasifikace.

D.1 Obecné postupy a pravidla pro ICS

Oblast bezpečnosti je v rámci Společnosti popsána řadou dokumentů. Pracovníci jsou povinni mimo tohoto metodického pokynu respektovat a postupovat v souladu s tím, co je uvedeno v následujících dokumentech (metodický pokyn je v tomto ohledu pouze upřesněním v konkrétních oblastech zajištění bezpečnosti pro ICS doplněným o technické detaily). Pracovníci musí při každodenní práci mimo jiné dodržovat bezpečnostní zásady popsané v následujících interních řídicích dokumentech Společnosti (dále jen nadřazená bezpečnostní dokumentace):

- "*Bezpečnostní řád NET4GAS s.r.o.*“
- „*Bezpečnostní pravidla pro ochranu informací*“
- „*Ochrana dat*“ - Metodický pokyn pro práci s klasifikovanou informací
- „*Bezpečnostní politika IT*“ IT-SECPOL
- *„Řízení fyzické bezpečnosti v NET4GAS, s.r.o.“*
- *„SCADA provozní technologie“*
- *„Havarijní plán přepravní soustavy NET4GAS, s.r.o.“*
- *„Provoz a správa řídicího systému DN4G“*
- *„Komunikace řídicího systému Dispečinku N4G a podřízených stanic“*
- *„Provoz a údržba lokálních řídicích systémů“*
- *„Provoz a údržba řídicího systému přepravní soustavy“*

V následujících kapitolách je popsán seznam bezpečnostních požadavků a pravidel pro ICS. Pravidla jsou rozdělena do následujících oblastí:

- Základní rozdíly mezi běžným ICT/IS a prostředím ŘS a SCADA systémů (ICS)
- Vymezení ICS (ŘS a SCADA systémů) Společnosti
- Data
- SW a aplikace
- Zabezpečení platformy
- Zabezpečení komunikace
- Ochrana před škodlivým SW a zlomyslnou činností
- Povolené užití aktiv ŘS a SCADA systémů
- Řízení přístupu

- Hlášení
- Fyzická bezpečnost
- Manuální provoz, havarijní plán a obnovení provozu
- Výjimky

D.2 Základní rozdíly mezi běžným ICT/IS a prostředím ŘS a SCADA systémů (ICS)

Tento metodický pokyn je součástí Bezpečnostní politiky IT (dále jen IT-SECPOL). Prostředí ICS se od běžného prostředí ICT/IS i přes použití prakticky totožných technologií významně liší. Pochopení těchto rozdílů mezi ICT/IS a ICS prostředím je klíčové pro naplnění bezpečnosti v rámci celé Společnosti. Základní rozdíly jsou shrnuty v následující tabulce (viz tabulka D.2-1).

Oblast	ICT/IS	ICS
Priorita	Prioritou je důvěrnost a integrita.	Prioritou je BOZP a ochrana vlastního průmyslového procesu.
Rizika	Hlavním rizikem jsou prostoje v obchodním procesu.	Hlavní rizikem je ztráta života, zničení zařízení, poškození životního prostředí, a omezení nebo přerušení transportu zemního plynu.
Změny	Prostředí neustálého vývoje, rozvoje, úprav, změn s vysokou frekvencí realizace. Mnoho změn je prováděno automaticky.	Prostředí stability a řízeného technického procesu změn. Minimální provádění změn a každá změna nese vysoké náklady spočívající v otestování integrity a dopadů do celého ICS. Časová realizace i velmi jednoduchých změn je v řádu až několika týdnů s násobně vyšším finančním nákladem než v případě ICT/IS.
Životní cyklus	Životní cyklus použitých komponent je typicky 3-5 let.	Životní cyklus použitých komponent (vyjma standardních IT komponent jako PC, či server) je typicky 10-15 let.
Dodavatelé a podpora	Diversifikované portfolio vzájemně relativně zaměnitelných dodavatelů.	Po celý životní cyklus typicky existuje jen jeden dodavatel pro vlastní systém. Vzhledem k délce životního cyklu často nejsou další jednotlivé komponenty ICS již v podpoře původního dodavatele (např. operační systémy či jednotlivá zařízení).
Konsekvence použití dalších bezpečnostních opatření.	Bezpečnostní řešení, požadavky a opatření jsou typicky navrhována s ohledem na běžný ICT/IT systém. Tato řešení typicky nemají významnější dopady do vlastní funkce ICT/IS.	Bezpečnostní řešení a opatření užitá v ICT/IS musí být řádně otestována, tak aby negativně neovlivňovala funkci a provoz ICS. ICS zařízení mají relativně limitované zdroje (paměť, výkon) a jejich řádný provoz významným způsobem ovlivňují i komunikační parametry sítě (zpoždění, jitter atd.). Vypršení certifikátů, blokace účtů po opakovaném nesprávném přihlášení jsou z pohledu vlastního provozu ICS neakceptovatelným rizikem kontinuity průmyslového procesu.
Zaměření architektury bezpečnosti	Obrana ICT zařízení a informací na nich uložených nebo jimi přenášených.	Primární ochrana koncových zařízení ovládajících vlastní průmyslový proces (PLC atd.). Vzhledem k charakteru ICS prostředí je nutno významně omezit fyzický i logický přístup do ICS (významnost kontroly a zabezpečení perimetru ICS).

Tabulka D.2-1 Shrnutí rozdílů mezi ICT/IS a ICS

Výstižnou a shrnující je do značném míry analogie ICS Společnosti s uzavřenou pilotní kabinou dopravního letadla. Chrání se obsah ICS/pilotní kabiny před neautorizovaným přístupem, ale v případě, kdy je autorizovaný pilot v uzavřené pilotní kabině, tak může prakticky svobodně ovládat veškerá zařízení zde umístěná. Zařízení v ovládací kabině neobsahují zámek blokující přístup pilota. Ochranné mechanismy primárně chrání před chybou či nechtěným provedením úkonu. Pilotu není odepřen či blokován přístup k zařízení po třech neúspěšných pokusech o ovládání přístroje. Zařízení v pilotní kabině se nemění/nemodernizují příliš často (funkčně ani vizuálně). Primárně dochází k striktnímu omezování, kdo, jak, kdy, v jaké roli a za jakých podmínek může přistupovat do ICS/pilotní kabiny.

D.3 Vymezení ICS (ŘS a SCADA systémů) Společnosti

D.3.1 Organizace

Odpovědnost za ICS náleží v rámci Společnosti útvaru Provoz soustavy.

Role a odpovědnosti pro provoz a údržbu ICS jsou uvedeny v nadřazené dokumentaci tj.:

- obecně ve směrnici *„SCADA provozní technologie“*,
- pro řídicí systém přepravní soustavy jsou uvedeny v metodickém pokynu *„Provoz a správa řídicího systému DN4G“*,
- pro lokální řídicí systémy jsou uvedeny v metodickém pokynu *„Provoz a údržba lokálních řídicích systémů“*
- pro řízení komunikace Dispečinku a podřízených stanic v metodickém pokynu *„Komunikace řídicího systému Dispečinku N4G a podřízených stanic“.*

D.3.2 Architektura

Architektura ICS a definice hranic ICS jsou uvedeny v nadřazené dokumentaci tj.:

- pro řídicí systém přepravní soustavy jsou uvedeny v metodickém pokynu *„Provoz a údržba řídicího systému přepravní soustavy“*,
- pro jednotlivé lokální řídicí systémy jsou uvedeny v přílohách metodického pokynu *„Provoz a údržba lokálních řídicích systémů“*

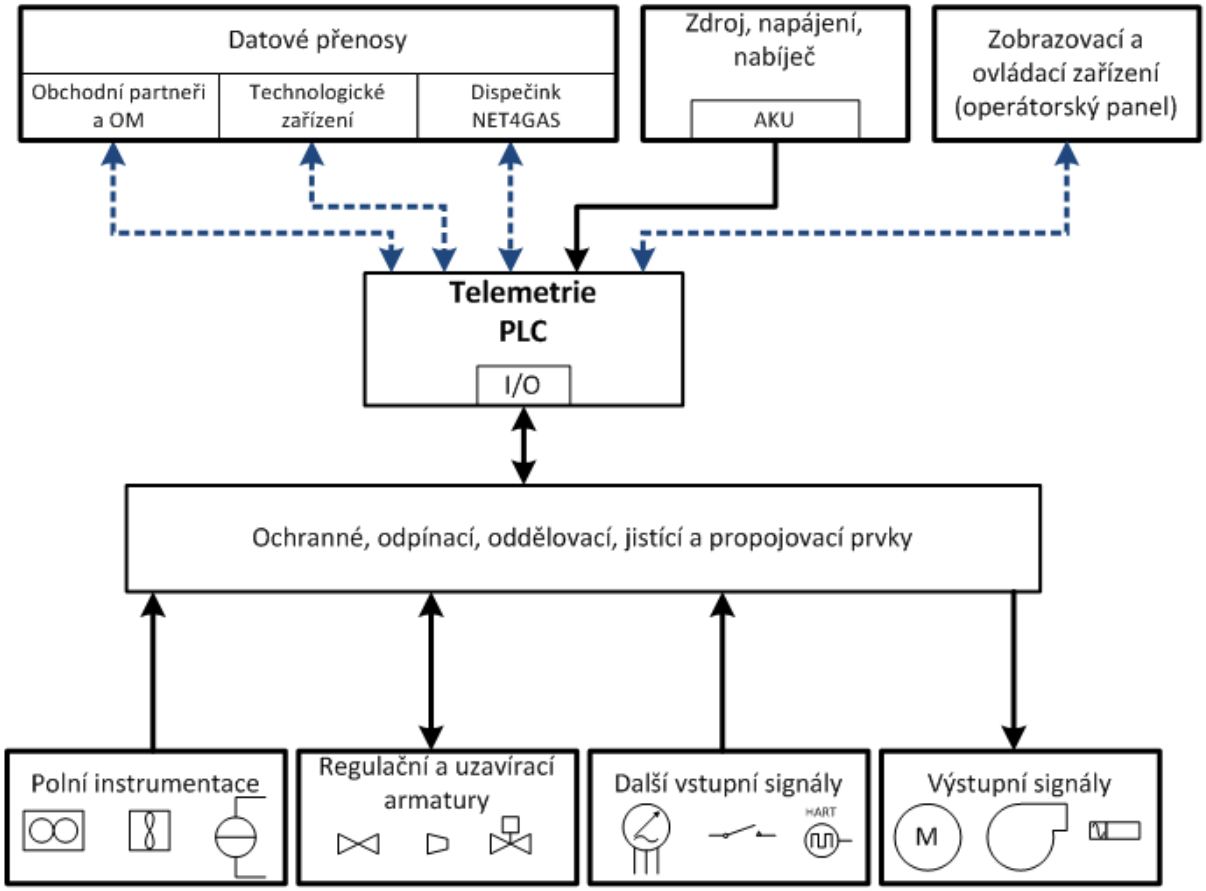

Schéma D3-1 Obecná struktura řídicího systému na externí lokalitě

D.4 Data

D.4.1 Politika zálohování a obnovy dat

Politiky zálohování a obnovy dat jsou uvedeny v nadřazené dokumentaci tj.:

- pro řídicí systém přepravní soustavy jsou uvedeny v metodickém pokynu *„Provoz a správa řídicího systému DN4G“*,
- pro jednotlivé lokální řídicí systémy je zálohování prováděno v souladu s provozními potřebami, které určuje správce lokálního řídicího systému (tj. Klíčový uživatel, Specialista, Lokální řídicí systémy, STO) v dané lokalitě. Lokální řídicí systém neuchovává žádná unikátní data mimo vlastní konfigurace systému. Změny konfigurace systému nejsou frekventované a po každé takové změně je řádně zálohován aktuální stav i konfigurace daného lokálního řídicího systému. Uložení záloh, provedení zálohy a obnovy je zajištěno buď smluvně prostřednictvím dodavatele daného systému, nebo prostřednictvím správce lokálního řídicího systému.

D.4.2 Životní cyklus dat

D.4.2.1 Data řídicího systému Dispečinku

D.4.2.1.1 Vznik dat řídicího systému Dispečinku N4G

Data řídicího systému Dispečinku vznikají několika způsoby:

- Komunikací s lokálními ŘS, či PLC umístěných na technologických objektech NET4GAS (lokální úroveň) protokolem IEC60870-5-104.
- Ručním zadáním v HMI SCADA systému HIGH-LEIT NT.

- Početními, nebo logickými operacemi ve SCADA systému HIGH-LEIT NT (vypočtené proměnné)
- Komunikací v reálném čase s řídicími centry GASPartnerů (TASE.2), nebo cyklickým importem dat od partnerů.

D.4.2.1.2 Prezentace dat v HMI řídicího systému Dispečinku N4G

Data, která ve SCADA systému, vznikla (viz D.4.2.1.1) jsou prezentovaná na operátorských pracovištích HMI SCADA systému HIGH-LEIT NT a na panelu velkoplošného zobrazení (BARCO). Prezentace dat je provedena jak klasickým technologickým schématem s animacemi, tak také přehlednými tabulkami s jednotlivými hodnotami. SCADA systém zároveň zaznamenává veškeré signály přicházející z technologie, provádí jejich zpracování (kontrola plausibility, aritmetické operace apod.) a vyhodnocuje alarmové, výstražné stavy a události.

D.4.2.1.3 Přenos dat na dispečink N4G (nejvyšší nadřazená úroveň)

Data, která v lokálním řídicím systému (tj. např. PLC) vznikla a další data, která vznikla jako logické proměnné nebo výsledky matematických operací v PLC, jsou přenášena do centrálního SCADA systému HIGH-LEIT NT protokolem IEC60870-5-104. Z centrálního SCADA systému lze technologické objekty také ovládat pomocí povelů a setpointů. Řízení typu Closed loop není v NET4GAS vzhledem k povaze a typu řízení implementováno.

D.4.2.1.4 Ukládání dat v řídicím systému dispečinku N4G

V rámci SCADA systému dispečinku HIGH-LEIT jsou data ukládána do dvou databází

1. Proprietární binární databáze SCADA systému HIGH-LEIT - Proprietární databáze SCADA systému se dále dělí na:
    a) Změnový archiv
    b) 1 minutový archiv
    c) 3-minutový archiv
    d) 15-minutový archiv
    e) Hodinový archiv
    f) Denní archiv
    g) Měsíční archiv
    h) Roční archiv

    Databáze je uložená na serverech SCADA systému HIGH-LEIT v DMZ_SCADA a není dostupná pro aplikace a uživatele mimo SCADA_DMZ.
2. Relační databáze Oracle - Relační databáze je uložena na databázovém serveru v DMZ_SRV a je pro aplikace a uživatele v administrativní síti dostupná. Do relační databáze se ukládají všechny typy archivů kromě změnového.

D.4.2.1.5 Destrukce starých dat řídicího systému Dispečinku N4G

Všechna data z řídicího systému jsou vzhledem k dostupné diskové kapacitě uchovávána a neprobíhá jejich destrukce.

D.4.2.2 Data lokálních řídicích systémů (KS a HPS)

D.4.2.2.1 Vznik dat lokálních řídicích systémů

Data lokálních řídicích systémů (KS a HPS), vznikají několika způsoby.

1. Měřením fyzických veličin (binární signál 24VDC, analogový signál např. 4÷20mA, frekvenční vstupy, čítače).
2. Komunikací se zařízeními a akčními členy polní instrumentace průmyslovým protokolem (Profibus DP, Modbus, Powerlink, HART apod.)

3. Komunikací se zařízeními OM a dalšími (přepočítávač, zdroj napájení, UPS apod.) na technologických objektech NET4GAS (lokální úroveň).
4. Komunikací s řídicím systémem (PLC) třetích stran (navazující distribuční společnosti, provozovatel elektráren apod.) standardními protokoly (Modbus RTU/TCP, PROFIBUS DP apod.)
5. Vypočtené, či odvozené proměnné, které vznikají buď pomocí logických operací, nebo aritmetických operací, nebo jejich kombinací.
6. Ručním zadáním v HMI lokálního řídicího systému.

D.4.2.2.2 Přenos dat KS a HPS do nadřazené úrovně (HMI velín)

Data, která v lokálním řídicím systému vznikla (viz D.4.2.2.1) jsou prezentovaná na HMI lokálního řídicího systému (operátorská stanice). Prezentace dat je provedena jak klasickým technologickým schématem s animacemi, tak také přehlednou tabulkou s jednotlivými hodnotami. Z HMI lze technologii také ovládat. Lokální řídicí systém zároveň zaznamenává veškeré signály přicházející z technologie, provádí jejich zpracování (kontrola plausibility, aritmetické operace apod.) a ukládá lokálně vybraná data pro historické trendy. Lokální řídicí systém vyhodnocuje alarmové, výstražné stavy, havarijní stavy a události prezentované na HMI lokálního řídicího systému. Komunikace s místním HMI je pomocí standardních protokolů (Modbus RTU/TCP, Powerlink, RS485 apod.).

D.4.2.2.3 Přenos dat KS a HPS na Dispečink N4G (nejvyšší nadřazená úroveň)

Data, která v lokálním řídicím systému (tj. např. PLC) vznikla a další data, která vznikla jako logické proměnné, nebo výsledky matematických operací jsou také přenášena do centrálního SCADA systému HIGH-LEIT NT protokolem IEC60870-5-104. Výjimkou jsou data z kompresních stanic. Zde záleží na systému, který KS řídí. Pro ŘS PAC je využit protokol Microtel pro vzdálenou obousměrnou komunikaci s DC Praha. KS se systémem UniControls přenášejí jednosměrně data protokolem Modbus TCP/IP (implementace do systému HIGH-LEIT). Z centrálního SCADA systému lze technologické objekty také ovládat viz D.4.2.1.1.

D.4.2.2.4 Ukládání dat v lokálních řídicích systémech (KS a HPS)

Způsob ukládání dat je závislý na typu LŘS:

- LŘS PAC – jsou ukládaná data pouze na vyšší úrovni řízení (halové). Zde je možno vytvořit omezenou množinu proměnných, které se ukládají. Ukládání proměnných probíhá zápisem do lokálního souboru na disk. Každý den vzniká nový datový soubor. Uložená data lze prohlížet pomocí trendů, které jsou implementovány v HMI.
- LŘS UniControls – pracuje s daty, která se ukládají v proprietární databázi systému UniCap. Data se ukládají změnově po dobu cca 1 týdne. Starší data se průměrují do delších časových intervalů v rámci úspory prostředků databáze.
- Veškeré systémy – ukládání dat do lokálního InSQL Wonderware. Ukládána je množina vybraných proměnných obsahující i vypočtené hodnoty. Tato databáze je změnová. Přístup k DB je formou Query, Trendů nebo prostřednictvím WIS (Wonderware Information Server).

D.4.2.2.5 Destrukce starých dat lokálních řídicích systémů

Destrukce starých dat probíhá formou kruhové databáze. V případě systému PAC dochází k umazávání nejstarších trendových souborů. V případě UniControls jsou starší primární data umazána a nahrazena průměrem za delší období.

D.4.2.3 Data řídicích systémů TU, PS, RU, VPS

D.4.2.3.1 Vznik dat řídicího systému TU, PS, RU, VPS

Data řídicího systému TU, PS, RU VPC, vznikají několika způsoby:

1. Měřením fyzických veličin (binární signál 24VDC, analogový signál např. 4÷20mA).
2. Komunikací se zařízeními a akčními členy polní instrumentace průmyslovým protokolem (Profibus DP, Modbus, Powerlink, HART apod.)

3. Komunikací se zařízeními OM a dalšími (přepočítávač, zdroj napájení, UPS apod.) na technologických objektech NET4GAS (lokální úroveň).
4. Komunikací s řídicím systémem (PLC) třetích stran (navazující distribuční společnosti, provozovatel elektráren apod.) standardními protokoly (Modbus RTU/TCP, PROFIBUS DP apod.)
5. Vypočtené, či odvozené proměnné, které vznikají buď pomocí logických operací, nebo aritmetických operací, nebo jejich kombinací.

D.4.2.3.2 Přenos dat TU, PS, RU, VPS do nadřazené úrovně (HMI v rozvaděči MaR)

Data, která v lokálním řídicím systému (tj. např. PLC) vznikla viz D.4.2.3.1 jsou prezentovaná na lokálním zobrazovacím zařízení (lokální zobrazovací panel HMI). Prezentace dat je provedena jak klasickým technologickým schématem s animacemi, tak také přehlednou tabulkou s jednotlivými hodnotami. Z místního HMI lze technologii také za určitých podmínek ovládat. Komunikace s místním HMI je pomocí standardních protokolů (Modbus RTU/TCP, Powerlink apod.).

D.4.2.3.3 Přenos dat TU, PS, RU, VPS na dispečink N4G (nejvyšší nadřazená úroveň)

Data, která v lokálním řídicím systému (tj. např. PLC) vznikla a další data, která vznikla jako logické proměnné, nebo výsledky matematických operací jsou také přenášena do centrálního SCADA systému HIGH-LEIT NT protokolem IEC60870-5-104. Z centrálního SCADA systému lze technologické objekty také ovládat.

D.4.2.3.4 Ukládání dat v řídicím systému TU, PS, RU, VPS

V řídicím systému TU, RU, PS a VPS nejsou data lokálně historizována. Jediný záznamník dat je zde „buffer“ pro archivaci neodeslaných, resp. nepotvrzených telegramů, který slouží jako prevence proti ztrátě dat v případě výpadku spojení s DN4G a za normálního bezchybného provozu je prázdný.

D.5 SW a aplikace

D.5.1 SCADA aplikace

D.5.1.1 Aplikace řídicího systému dispečinku

Řídicí systém dispečinku se skládá z následujících aplikací (je provozován na OS z rodiny MS Windows):

a) SCADA HIGHLEIT NT - jádro SCADA systému
b) ACOS X4 - nástroj pro export/import offline dat ze SCADA systému (aplikace je provozována na aplikačním serveru JBoss 4.2GA)
c) SIMONE online - podpora dispečerského řízení (výpočet akumulace, simulace stavů plynárenské soustavy apod.)
d) ACOS NMS - směnový deník dispečinku NET4GAS
e) SISCO TASE.2 GW - poskytuje rozhraní mezi SCADA systémem HIGH-LEIT NT a komunikací TASE.2 (ICCP)
f) Oracle DB - slouží pro ukládání dat přístupných pro NET4GAS
g) WEB server HLNT - read-only tenký klient řídicího systému dispečinku

D.5.1.2 Aplikace lokálních řídicích systémů (KS a HPS)

a) ŘS KS typu PAC používají pro svůj běh real-time systém AMX68. Pro HMI operátorské pracoviště je využit systém Windex, který je spuštěn v prostředí DOS 6.22. Žádné další aplikace pro chod LŘS systému nejsou zapotřebí.
b) LŘS UniControls a LŘS HPS pro svůj běh využívají OS reálného času. HMI je vždy na platformě MS Windows.

D.5.1.3 Aplikace řídicích systémů TU, PS, RU, VPS

Řídicí systémy TU, PS, RU, VPS nepoužívají pro svůj běh žádné specifické aplikace. Pro svůj běh využívají zpravidla operačních systémů reálného času (OS9, Linux nebo proprietární OS).

Programování těchto systémů se provádí dle normy IEC 1131-3 pomocí aplikací uvedených v kapitole D.5.2.3 tohoto metodického pokynu.

D.5.2 Podpůrné systémy a aplikace

D.5.2.1 Řídicí systém dispečinku

Podpůrné aplikace a systémy řídicího systému dispečinku jsou principiálně jeho součástí, ale z hlediska zabezpečení a funkcionality se považují jako podpůrné následující aplikace a systémy a jsou také uvedeny v kapitole D.5.1.1. Jako podpůrné jsou chápány a považovány z toho důvodu, že pro chod samotného řídicího systému (základní SCADA funkce) nejsou nezbytné a pro řídicí systém poskytují určitá rozhraní a rozšiřující funkčnosti. Podpůrné systémy a aplikace jsou:

- ACOS X4 - nástroj pro export/import offline dat ze SCADA systému (provozován na aplikačním serveru JBoss 4.2GA)
- ACOS NMS - směnový deník Dispečinku NET4GAS
- SISCO TASE.2 GW - poskytuje rozhraní mezi SCADA systémem HIGH-LEIT NT a komunikací TASE.2 (ICCP)
- Oracle DB - slouží pro ukládání dat přístupných pro NET4GAS
- WEB server HLNT - read-only tenký klient řídicího systému Dispečink.

D.5.2.2 Diagnostické pracoviště pro lokální řídicí systémy

- Vývojová stanice pro LŘS PAC – slouží pro emulaci a trasování programu před ostrým nasazením na lokalitě. Vytvořený speciálně kompilovaný program se nahraje pomocí rozhraní LPT do RAM procesoru. Pomocí programu Siera lze provádět debug programu s emulací vstupních proměnných. K diagnostické skříni lze také připojit HMI (přes RS232) – operátorskou stanici a graficky ovládat emulovaný program. Takto lze odladit program procesoru i grafickou nadstavbu HMI.
- Ostatní systémy LŘS jsou spravovány servisními organizacemi s pomocí jejich vlastních diagnostických prostředků.

D.5.2.3 Diagnostické pracoviště pro ŘS TU, PS, RU, VPS

Diagnostické pracoviště je speciální stanice, která je určená pro vzdálenou diagnostiku a programování PLC. Pracoviště je umístěno přímo v síti VPN TLM. Diagnostika a programování se provádí pomocí aplikací, které jsou na této stanici nainstalovány.

a) PERTINAX - SW slouží pro programování a diagnostiku PLC.
b) Automation Studio - SW slouží pro programování a diagnostiku PLC a tvorbu vizualizace.
c) UNICAP - SW slouží pro programování a diagnostiku PLC.
d) EASYBUILDER - SW slouží pro tvorbu vizualizace HMI

Dále se na tomto pracovišti provádí diagnostika komunikace na úrovni jednotlivých ethernetových paketů. Pro tento účel je do této stanice na separátním fyzickém rozhraní přiveden span port ze sítě VPN TLM a TLM DMZ. Na tomto rozhraní je provoz jednosměrně zrcadlen. Pro diagnostiku komunikace se používá SW

a) WireShark - Používá se na diagnostiku a analýzu provozu sítě VPN TLM a TLM DMZ, který je jednosměrně zrcadlen na separátním fyzickém rozhraní (samostatná síťová karta).
b) telnet [součást OS] - Používá se pro testování navazování tcp spojení v síti VPN TLM a TLM DMZ.
c) ping (ICMP) [součást OS] - Používá se pro zjišťování dostupnosti a stavu řídicích systémů v síti VPN TLM a TLM DMZ.

d) tracert [součást OS] - Používá se pro zjištění na kterém hopu se paket zastaví a kde je pravděpodobně závada na komunikaci.

D.6 Zabezpečení platformy

D.6.1 Zabezpečení Serverů

Bezpečnostní požadavky jsou vždy součástí projektové dokumentace daného systému. Pro řídicí systém Dispečinku N4G je zabezpečení celého systému uvedeno v Projektové dokumentaci, „Kniha 13 – Zabezpečení systému“, která obsahuje následující části:

- Bezpečná architektura systému
- Záplaty, management záplat
- Poskytování resp. uvolňování bezpečnostních záplat pro všechny komponenty systému
- Podpora systémových komponent třetích stran poskytovaná dodavatelem systému
- Šifrování citlivých dat při jejich ukládání a přenosu
- Bezpečné mazání citlivých dat
- Standardy šifrování
- Interní / externí bezpečnostní testy a testy požadavků a související dokumentace
- Bezpečná standardní konfigurace a první instalace resp. (opakované) uvedení do provozu
- Test integrity
- Dokumentace
    - Dokumentace designu, popis bezpečnostních systémových komponent a specifikace implementace
    - Administrátorská a uživatelská dokumentace
    - Dokumentace nastavení a systémových hlášení relevantních pro bezpečnost
    - Dokumentace předpokladů a požadavků prostředí na bezpečný provoz systému
- Oblast základního systému
    - Základní zálohování a zvyšování odolnosti systému
    - Antivirový software
    - Autentifikace uživatele
- Oblast sítí a komunikace
    - Koncepce bezpečné sítě a způsob komunikace
        - Uplatněné protokoly a technologie
        - Bezpečná struktura sítě
        - Dokumentace struktury a konfigurace sítě
    - Bezpečné procesy údržby a vzdálený přístup
        - Zabezpečený vzdálený přístup
        - Požadavky kladené na procesy údržby
    - Rádiové technologie: Potřeby a bezpečnostní požadavky
- Oblast aplikací
    - Správa uživatelů
        - Koncepce rolí
        - Autentifikace a přihlášení uživatele
    - Autorizace akcí na uživatelské a systémové úrovni
    - Aplikační protokoly
    - Webové aplikace
    - Protokolování, audit trails, timestamps, koncepce alarmů

  - Self test, chování Fail safe a Fail secure
  - Kontrola integrity relevantních dat
- Vývoj, test a rollout
  - Bezpečné vývojové standardy, řízení kvality a procesy uvolňování
  - Bezpečná úložiště a přenos dat
  - Bezpečné vývojové, testovací a staging systémy, kontrola integrity
  - Bezpečné procesy aktualizace a údržby
  - Konfigurační a změnový management, možnosti rollbacku
  - Ošetření bezpečnostních mezer
  - Uložení zdrojových kódů
- Backup, Recovery a plánování nouzových případů
  - Backup: koncepce, postup, dokumentace, testy
  - Koncepce nouzových případů a plánování opakovaného spuštění

D.6.2 Zabezpečení ICS/SCADA koncových zařízení (PLC/IED/RTU)

Zabezpečení ICS/SCADA koncových zařízení je vždy provedeno v rámci dodávky daného systému či dodávky jednotlivého zařízení dle možností dodávaného systému či koncového zařízení a aktuálních požadavků na zabezpečení daného systému či zařízení. Pro nově navrhované a dodávané systémy či zařízení je při jejich výběru vždy posuzován aspekt bezpečnosti a v rámci IT projektového řízení je řádně prosazována informační bezpečnost viz nadřazená bezpečnostní dokumentace *„Bezpečnostní politika IT / IT-SECPOL“* a kapitola nazvaná Prosazování informační bezpečnosti v rámci IT projektového řízení.

D.7 Zabezpečení komunikace

Vnitřní komunikační infrastruktura Společnosti je z pohledu bezpečnosti rozdělena do základní logických bezpečnostních zón. Jednotlivé zóny jsou definovány dle kritičnosti funkcí zařízení zapojených do dané zóny z pohledu bezpečnosti přepravní soustavy.

Základní logické bezpečnostní zóny vnitřní komunikační infrastruktury ŘS a SCADA jsou:

- **Zelená zóna** – administrativní/business síť (např. propojovací síť, RTG).
- **Žlutá zóna** – demilitarizovaná zóna technologické sítě (např. LANT, DMZ PC, DMZ SRV)
- **Červená zóna** - obsahující vlastní technologické sítě ICS společnosti (např. SCADA, TLM, či sítě Lokálních řídicích systémů)

WAN síť je tvořena několika navzájem propojenými páteřními kruhy, které jsou realizovány propojením jednotlivých směrovačů na lokalitách. Všechny tyto MPLS směrovače, tvořící páteřní sekci sítě, pracují v P/PE režimu, tedy realizují tranzitní provoz metodou LSP přepínání a zároveň terminují logicky oddělené uživatelské síťové entity, v tomto případě L3 MPLS VPN sítě. Dále je páteřní WAN síť tvořena přístupovými sekcemi, které jsou tvořeny propojením jednotlivých směrovačů pracujících v CE režimu. Každá přístupová sekce je připojena na dva různé PE směrovače páteřní sekce sítě. Transportní technologií primárně použitou pro přenos dat v páteřní síti je MPLS (MultiProtocol Label Switching). MPLS poskytuje metodu převádění/směrování paketů, která umožňuje tvorbu uživatelských VPN a explicitní směrování provozu řízené provozovatelem sítě. VPN zde mají podobu směrovaných L3 sítí oddělených na logické úrovni. Na síti je provozováno několik služeb, každá služba je realizována samostatnou L3 MPLS VPN na páteřních PE směrovačích a příslušnou VLAN na L2 přístupové vrstvě.

Komunikace mezi jednotlivými L3 MPLS VPN a logickými bezpečnostními zónami se realizuje na interních firewall farmách umístěných v lokalitách Praha, Kavčí Hory a Kouřim. Zelená zóna je v rámci dalších technických prostředků a zařízení tzv. „administrativního IT“ dále uvnitř zóny i na své perimetru chráněna (např. prostřednictvím dalších firewallů, IDS/IPS systémů, systémů pro kontrolu obsahu, demilitarizovanou zónou obsahující služby dostupné z Internetu atd.)

Zařízení umístěná do žluté a červené zóny jsou součástí tzv. „technologického IT“. Komunikace na rozhraní tzv. „technologického IT“ a tzv. „administrativního IT“ je popsána v rámci kapitoly D.7.2 Komunikace na technologickém perimetru.

Schéma logických bezpečnostních zón viz Schéma D.7-1.

Popis významných technologických sítí:

- Business/Administrativní část (zelená zóna):
  - LANT_DMZ
- Demilitarizované technologické sítě (žlutá zóna):
  - DMZ PC – síť určená pro technologické pracovní stanice (postupně dochází k eliminaci technologických pracovních stanic připojených do této sítě)
  - DMZ SRV – demilitarizovaná zóna pro SCADA řídicí systém
  - DMZ TLM – demilitarizovaná zóna pro telemetrii
  - LANT – komunikační síť lokálních řídicích systémů (obsahuje zařízení umožňující komunikaci mimo síť lokálního řídicího systému)
  - TASE2 – komunikační síť pro výměnu informací s partnery protokolem ICCP TASE.2 dle IEC 60870-6
- Vlastní technologické sítě (červená zóna)
  - SCADA – síť řídicího systému
  - TLM – sběrná sít telemetrie pro SCADA řídicí systém
  - Sítě lokálních řídicích systémů (Local ICS Network)

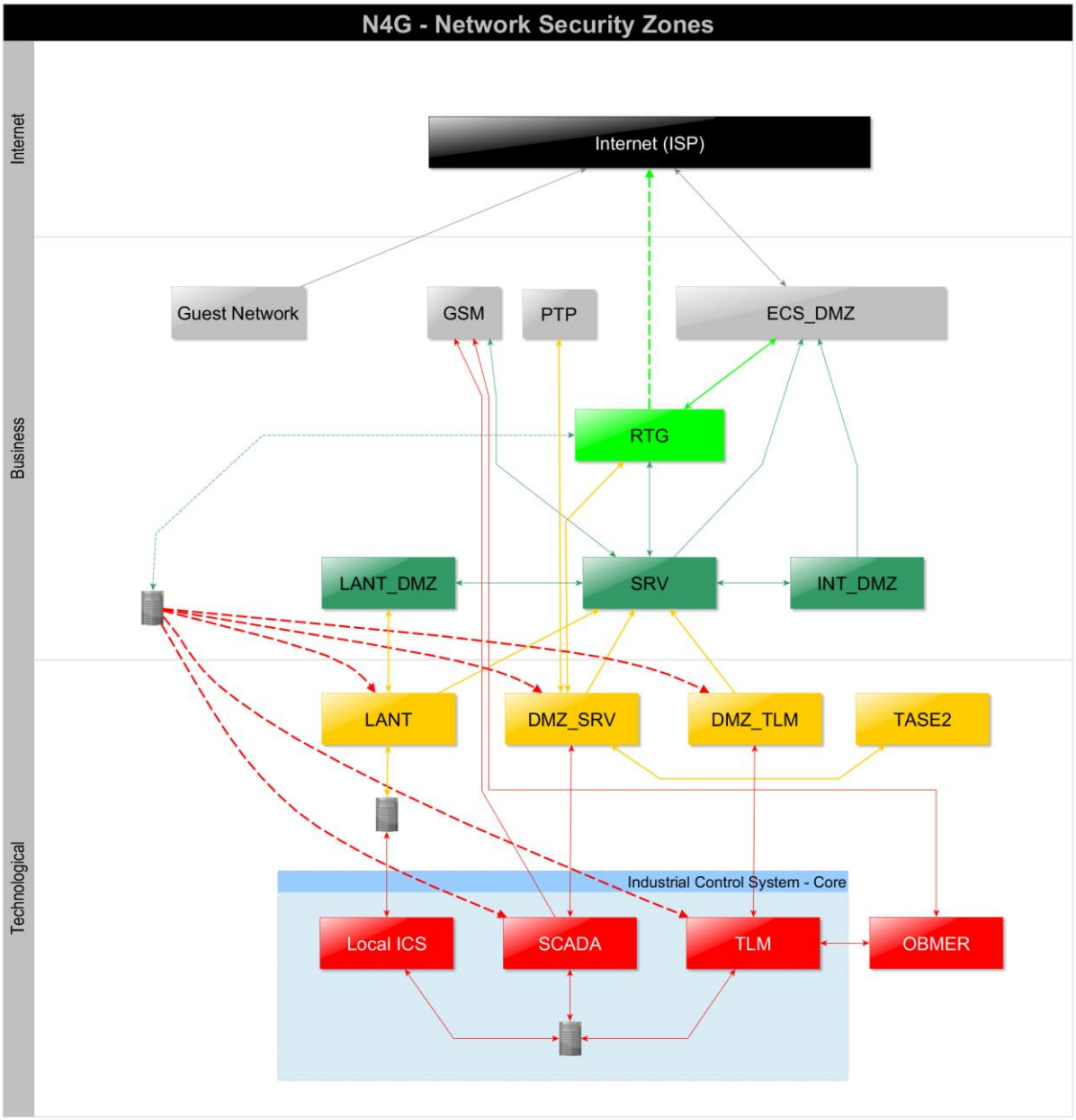

Schéma D.7-1 – Logické bezpečnostní zóny

Přímá komunikace zařízení se zařízením umístěným do červené zóny je možná pouze s:

- jiným zařízením umístěným do červené zóny ve stejné L3 MPLS VPN,
- zařízením umístěným do demilitarizované zóny technologické sítě tj. náležící DMZ v žluté zóně:
  - LANT pro sítě Lokálních řídicích systémů
  - DMZ PC a DMZ SRV pro SCADA síť
  - DMZ TLM pro TLM síť
- „dual-homed“ zařízením připojeným do SCADA, TLM a Local ICS sítí,
- zařízením připojeným prostřednictví VPN klienta společnosti k zařízení VPN Gateway (viz dále kapitola D.7.3 Vzdálené přístupy).

Povolené toky dat a inicializace spojení mezi jednotlivými sítěmi (L3_MPLS_VPN) jsou zobrazeny na schématu D.7-1 pomocí šipek. Pro jakoukoliv jinou komunikaci či tok dat musí existovat schválená výjimka viz kapitola D.14 Výjimky.

D.7.1 Bezdrátové připojení

Bezdrátové sítě jsou pro použití v technologických sítích tj. sítích v červené a žluté zóně obecně zakázány s následujícími výjimkami:

- Povolena je komunikace z vzdálených izolovaných lokalit připojených prostřednictvím datových přenosů veřejné mobilní sítě (GPRS) v kombinaci s užitím adekvátní ochrany šifrování dat přenášených prostřednictvím veřejné mobilní sítě.
- Komunikace bezdrátových snímačů prostřednictvím protokolu WirelessHART chráněná symetrickou šifrou AES s délkou klíče minimálně 128 bitů.

D.7.2 Komunikace na technologickém perimetru

Povolená komunikace a toky dat na technologickém perimetru tj. mezi zařízeními umístěnými do tzv. „administrativního IT“ a zařízeními umístěnými do tzv. „technologického IT“ je zobrazena ve schématu D.7-2. Pro jakoukoliv jinou komunikaci či tok dat musí existovat schválená výjimka viz kapitola D.14 Výjimky.

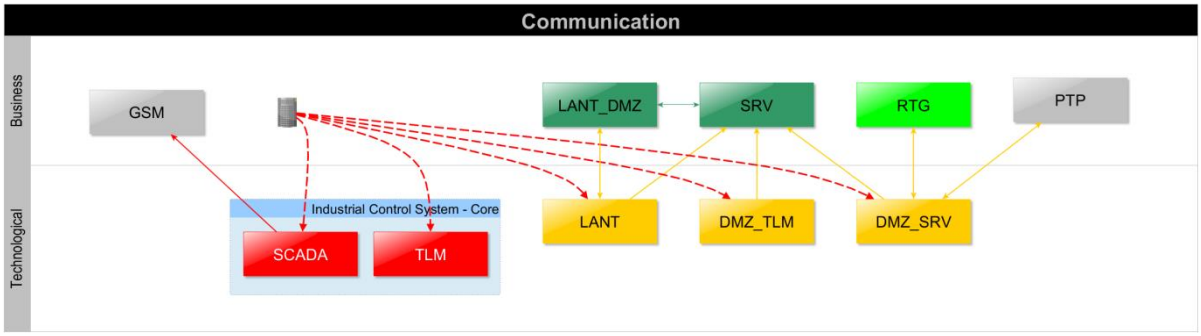

Schéma D.7-2 – Komunikace na technologickém perimetru

Povoleny jsou následující toky dat:

1. **Vzdálený přístup prostřednictvím VPN do technologické části sítě prostřednictvím tzv. „jump boxu“** viz kapitoly D.7.3 Vzdálené přístupy, D.7.4 Připojení externistů a externích subjektů.
2. **Přenos dat z technologických demilitarizovaných zón prostřednictvím administrativní sítě** viz nadřízená bezpečnostní dokumentace tj. např. „Komunikace řídicího systému Dispečinku N4G a podřízených stanic“ či v případě DMZ SRV viz Metodický pokyn *„Provoz a správa řídicího systému DN4G“* kapitola Výměna provozní dat mezi ŘS DN4G a partnery.
3. **Komunikace zařízení umístěných do LANT_DMZ s vybranými zařízeními umístěnými v rámci LANT**. Komunikace je povolena jen prostřednictvím explicitně povolených protokolů a jen pro vyjmenované zařízení v rámci LANT.
4. **Komunikace s DMZ_SRV.** Komunikace přes technologický perimetr do DMZ_SRV je povolena pouze pro zařízení umístěná v rámci sítí SRV, RTG a PTP a to primárně na publikační rozhraní „frontend“ SCADA serverů (tj. např. readonly „kukátko“).
5. **Komunikace do sítě GSM** (síť, ve které jsou zakončeny propoje se vzdálenými lokalitami prostřednictvím sítě jiných telekomunikačních operátorů např. Nowire).

D.7.3 Vzdálené přístupy

Vzdálené přístupy do technologických sítí jsou zprostředkovány prostřednictvím VPN brány (VPN Gateway) umístěné v administrativní části síťové infrastruktury. Zprostředkování vzdáleného přístupu je znázorněno na schématu D.7-3A a D.7-3B.

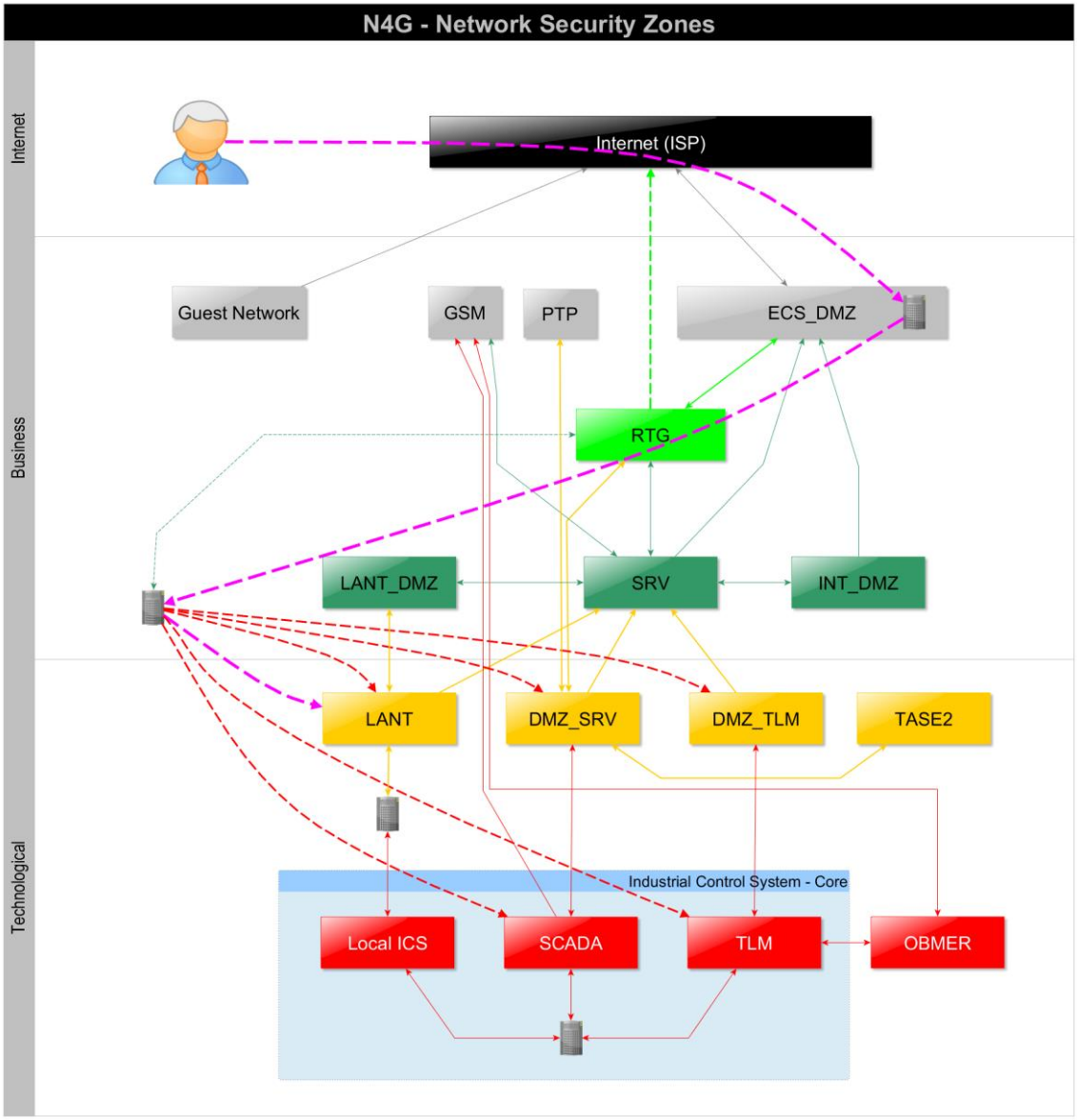

Schéma D.7-3A – Zprostředkování vzdáleného přístupu a zóny

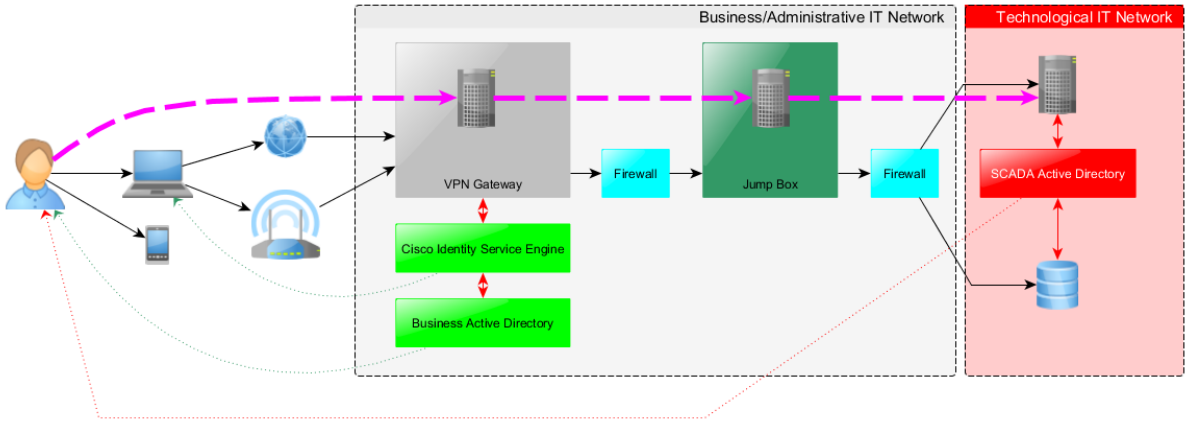

Schéma D.7-3B – Zprostředkování vzdáleného přístupu v jednotlivých krocích

Zprostředkování vzdáleného přístupu do technologických sítí se odehrává v následujících krocích:

1. **Pracovník** (Uživatel) oprávněný k vzdálenému přístupu se prostřednictvím autorizovaného zařízení připojeného do Internetu či zabezpečené WiFi sítě Společnosti spojí prostřednictvím VPN SW klienta s VPN bránou (VPN Gateway).
2. **VPN Gateway** umístěná v administrativní části síťové infrastruktury prostřednictvím dalších služeb a zařízení administrativní sítě (Cisco ISE, AD atd.) provede:
   - autentizaci – uživatele na úrovni přístupu k ICT/IS (administrativní části infrastruktury tj. Business Active Directory),
   - autorizaci – uživatele k přístupu do technologických sítí,
   - ověření povoleného kontextu - přístupu prostřednictvím schváleného zařízení/kontextu.
3. **Interní firewall farmy** následně propustí povolenou příchozí RDP komunikaci z VPN spojení vzdáleného uživatele na schválený tzv. „Jump box“.
4. **Prostřednictvím** tzv. „Jump boxu“ komunikuje pracovník s dalšími zařízeními umístěnými v cílové technologické síti. Komunikace „Jump boxu“ do červené zóny je omezena na nezbytně nutnou prostřednictvím interního firewallu.
5. **Autentizace a autorizace uživatele v rámci technologické sítě** (při přístupu k cílům/službám/, serverům/zařízením) je provedena na základě údajů uložených v SCADA Active Directory či lokálně uloženým AAA (autentizace, autorizace, accounting) záznamům v rámci daného lokálního řídicího systému.

Povolený kontext vzdáleného přístupu je kontext splňující veškeré následující podmínky:

- Pracovník a zařízení, ze kterého přistupuje, jsou autorizováni ke vzdálenému přístupu.
- Zařízení, ze kterého přistupuje Pracovník, musí vyhovovat následujícím bodům:
  - Disponovat instalovaným a aktualizovaným nástrojem na obranu před škodlivým SW.
  - Disponovat zapnutým a řádně nakonfigurovaným personálním firewallem.
  - Řádně aktualizovaný základní SW (např. operační systém).
  - Splnit tzv. „health check“ (kontrolu zdraví) koncového zařízení definovaného v rámci minimálních standardů pro ICT/IS (viz. v případě notebooku Desktop standardy).
  - Omezení Konektivity – nepovolit připojení přímo na internet … vždy pouze prostředím Společnosti či via VPN klient na VPN Gateway.

Pravidla pro tzv. Jump box:

- Uživatelský účet pracovníka nedisponuje silným tj. administrátorským oprávněním pro Jump box, ke kterému je oprávněn se vzdáleně připojit.
- Veškerá aktivita uživatelů tzv. „Jump boxu“ je monitorována, zaznamenávána a archivována minimálně po dobu 3 měsíců.
- Komunikace tzv. „Jump boxu“ v rámci dané technologické sítě je omezena na komunikaci nezbytně nutnou pro výkon práce.
- Dle charakteru přístupů a činností jednotlivých pracovníků může být z bezpečnostních či praktických důvodů vhodné umístění individuálních „Jump box“ serverů či užití virtualizačních technologií.
- Příchozí komunikace prostřednictvím vzdáleného přístupu na „Jump box“ je povolena pouze prostřednictvím RDP se zakázaným přenosem souborů.

D.7.4 Připojení externistů a externích subjektů

Zprostředkování vzdáleného přístupu externistům a externím subjektům se odehrává v obdobných krocích jako v případě přístupu Pracovníků z řad zaměstnanců Společnosti (viz kapitola D.7.3 Vzdálené přístupy) s tím rozdílem, že komunikace je povolena pouze na tzv. „Jump box“, který je zpřístupněn pouze na vyžádání.

Zprostředkování vzdáleného přístupu a jeho řádné ukončení probíhá v tomto případě následujícím způsobem:

1. **Externista** či Pracovník externího subjektu telefonicky požádá svou kontaktní osobu z řad zaměstnanců Společnosti o vzdálený přístup a povolení komunikace přes tzv. „Jump box“ (alternativně zapnutí/zapojení tzv. „Jump boxu“).
2. **Odpovědná osoba** na straně Společnosti ověří oprávněnost požadavku na vzdálený přístup. Dle oprávněnosti následně provede **povolení komunikace** přes (alternativně zapnutí/zapojení) tzv. **„Jump boxu“** a potvrdí externistovi nebo Pracovníkovi externího subjektu povolení přístupu včetně časového limitu na provedení prací či naopak zamítne vzdálený přístup (v případě zamítnutí je zprostředkování vzdáleného přístupu zastaveno).
3. **Externista** či Pracovník externího subjektu pokračuje navázáním vzdáleného připojení na tzv. „Jump box“ tj. postupuje dále v souladu s postupem uvedeným v kapitole D.7.3 Vzdálené přístupy.
4. O **ukončení** práce a ukončení vzdáleného přístupu informuje externista či Pracovník externího subjektu svou kontaktní osobu z řad zaměstnanců Společnosti.
5. **Odpovědná osoba** na straně Společnosti provede **zneplatnění povolení** komunikace externisty přes tzv. **„Jump boxu“** (alternativně odpojení/vypnutí Jump boxu). V případě kdy vyprší lhůta na provedení prací stanovená v bodě 2, tak odpovědná osoba kontaktuje externistu či Pracovníka externího subjektu za účelem získání vyjádření k ukončení vzdáleného přístupu. Oprávněná osoba na straně Společnosti je oprávněna kdykoliv jednostranně ukončit vzdálené připojení a však v případě takového jednostranného ukončení musí zvážit potenciální riziko a dopady takového ukončení na zařízení umístěná v technologické síti (např. probíhající podpora, upgrade, maintenance zařízení externím subjektem).

D.8 Ochrana před škodlivým SW a zlomyslnou činností

D.8.1 Ochrana proti škodlivému kódu a programům

Obecně jsou i pro ICS platná ustanovení „*Bezpečnostní politiky IT / IT-SECPOL*“ (viz nadřazená bezpečnostní dokumentace) s následující výjimkou. V případě ICS má správce systému SCADA přístup do konzole antivirového software a může zde měnit nastavení skupiny aktiv ICS pod kontrolou antivirového systému podle aktuálních provozních potřeb.

D.8.2 Zaznamenávání událostí

Pro kritickou informační infrastrukturu tj. Řídicí systém DN4G a lokální řídicí systémy hraničních předávacích stanic (HSK a LAN) je zajištěno zaznamenávání událostí následujícím způsobem:

- Bezpečnostní logy se automatizovaně ukládají na koncovém zařízení nebo mimo něj.
- Správci provádí kontrolu aplikačních a systémových logů koncových zařízení dle provozních potřeb.
- Útvar IT ve spolupráci s oddělením SCADA provozní technologie zajišťuje automatizované odesílání logů na definovaná úložiště mimo Aktivum ICS, kde byl log pořízen. Na toto definované úložiště nemají přístup správci, kteří vykonávají správu aktiva ICS, na kterém byly logy pořízeny.

D.8.3 Ochrana před využitím známých zranitelností

Oddělení SCADA provozní technologie zajišťuje vlastními silami nebo prostřednictvím Dodavatelů, či Bezpečnostního manažera, sledování technických slabin a známých zranitelností pro provozovaná aktiva ICS. Správci SCADA sledují zveřejněné slabiny používaných operačních systémů, databází a dalších komponent ICS. Oddělení SCADA provozní technologie po zjištění slabiny využitelné v prostředí ICS přijímá nápravná opaření prostřednictvím správců SCADA. Za opatření je zodpovědný Manažer, SCADA provozní technologie pro aktiva ICS Řídicího systému DN4G i pro aktiva ICS Lokálního řídicího systému.

D.8.4 Omezení přístupu, propojení a vzdáleného přístupu k ICS

Omezení fyzického přístupu k aktivům ICS je popsáno v rámci nadřazené bezpečnostní dokumentace viz kapitola D.12 Fyzická bezpečnost. Omezení propojení a vzdáleného přístupu k aktivům ICS je popsáno v rámci kapitoly D.7 Zabezpečení komunikace. Řízení vlastního přístupu Pracovníků je popsáno v rámci kapitoly D.10 Řízení přístupu .

D.8.5 Detekce narušení či neobvyklé komunikace

Detekce narušení či neobvyklé komunikace je primárně řešena na úrovni „přístupové“ bezpečnostní zóny tj. zelené zóny tzv. „administrativního IT“ a na úrovni správy LAN/WAN sítí společnosti. V rámci technologických sítí tj. žluté a červené bezpečnostní zóny nejsou v tomto ohledu přijata další bezpečnostní opatření detekce narušení či neobvyklé komunikace. Základní bezpečnostní opatření jsou popsána v rámci nadřazené bezpečnostní dokumentace viz *„Bezpečnostní politika IT / IT-SECPOL“*.

D.9 Povolené užití aktiv ŘS a SCADA systémů

Povolené užití aktiv Řídicích systémů a SCADA systému je uvedeno v nadřazené dokumentaci tj.:

- obecně ve Směrnici *„SCADA provozní technologie“*,
- pro řídící systém přepravní soustavy je dále uvedeno v metodické pokynu *„Provoz a správa řídicího systému DN4G“*,
- pro lokální řídicí systémy je dále uvedeno v metodickém pokynu *„Provoz a údržba lokálních řídicích systémů“*
- pro řízení komunikace Dispečinku a podřízených stanic je dále uvedeno v metodickém pokynu *„Komunikace řídicího systému Dispečinku N4G a podřízených stanic“.*

D.10 Řízení přístupu

Obecně jsou i v rámci ICS platná ustanovení „*Bezpečnostní politiky IT / IT-SECPOL*“ (viz nadřazená bezpečnostní dokumentace) týkající se řízení přístupu s výjimkami či upřesněními uvedenými v následujících podkapitolách.

D.10.1 Řízení přístupu k ŘS a SCADA systémům

Řízení přístupu ke službám a zdrojům uvnitř ICS je založeno na záznamech a konfiguraci SCADA Active Directory či na lokálně uložených AAA (autentizace, autorizace, accounting) záznamech v rámci daného lokálního řídicího systému. Administrativní/business Active Directory je využíváno pouze pro služby poskytované v rámci administrativní části infrastruktury Společnosti a nikoliv pro služby uvnitř ICS. Z pohledu ICS jsou záznamy administrativního/business Active Directory užívány zejména pro ověření uživatele při zprostředkování vzdáleného přístupu prostřednictvím tzv. „administrativního IT“ na hranici ICS.

D.10.2 Řízení přístupu a vzdálené přístupy

Vzdálený přístup je v případě ICS popsán v rámci následujících kapitol tohoto dokumentu:

- D.7.3 Vzdálené přístupy,
- D.7.4 Připojení externistů a externích subjektů.

V případě déle trvajícího vzdáleného připojení do ICS dochází k:

- upozornění pracovníka přistupujícího vzdáleně po 24 hodinách od navázání spojení a k
- automatickému ukončení vzdáleného připojení po 3 dnech tj. po 72 hodinách od navázání takového připojení.

D.10.3 Koncové zařízení ponechané bez dozoru

Opatření a postupy uvedené v „*Metodickém pokynu IT-SECPOL pro Uživatele*“ týkající se přerušení a ukončení práce neplatí v červené logické bezpečnostní zóně ICS, zde by tato opatření/postupy mohly ohrozit bezpečnost technologie pro přepravu plynu. Mimo červenou bezpečnostní zónu jsou povinni Pracovníci v tomto ohledu dodržovat postupy uvedené v „*Metodickém pokynu IT-SECPOL pro Uživatele*“ týkající se přerušení a ukončení práce.

D.11 Hlášení bezpečnostních událostí a incidentů

Bezpečnostní události a incidenty jsou hlášeny v souladu s metodickým pokynem pro daný typ systému tj. pro:

- Řídicí systém DN4G – v souladu s metodickým pokynem „*Provoz a správa řídicího systému DN4G“*,
- Lokální řídicí systém – v souladu s metodickým pokynem pro *„Provoz a údržbu lokálních řídicích systémů“*.

D.12 Fyzická bezpečnost

Politika fyzické bezpečnosti Společnosti včetně ICS je stanovena v rámci nadřazené bezpečnostní dokumentace. Fyzická bezpečnost budov a místností ve Společnosti je řešena směrnicí „*Řízení fyzické bezpečnosti v NET4GAS, s.r.o.*“ a jejími navazujícími metodickým pokyny.

D.13 Manuální provoz, havarijní plán a obnovení provozu

V případě výskytu výpadku služeb či některé části ICS se pro řešení výpadku a obnovu provozu uplatňují postupy uvedené v nadřízené bezpečnostní dokumentaci, tj. postupuje se následujícím způsobem:

- výpadky a obnova provozu v rámci Řídicího systému DN4G jsou řešeny v souladu s postupem uvedeným v metodickém pokynu *„Provoz a správa řídicího systému DN4G“*,
- výpadky a obnova provozu v rámci Lokálního řídicího systému jsou řešeny v souladu s postupem uvedeným v metodickém pokynu *„Provoz a údržbu lokálních řídicích systémů“,*
- pokud se jedná o mimořádnou situaci (dle definice v rámci *Havarijního plánu přepravní soustavy*) postupuje se při řešení výpadku a obnově v souladu s postupy uvedenými ve směrnici *„Havarijní plánem přepravní soustavy NET4GAS, s.r.o.“*).

D.14 Výjimky

Případné výjimky z pravidel obsažených v tomto dokumentu musí být s vysvětlením jejich opodstatnění předloženy ke zvážení Manažerovi, SCADA provozní technologie, který může pro jejich posouzení iniciovat proces analýzy rizik. Manažerem, SCADA provozní technologie nebo jím určená osoba provádí evidenci výjimek. Výjimka může být udělena jen v odůvodněných případech. Pokud jsou výjimky uděleny, musí být minimálně každých 6 měsíců přezkoumány, zda nepominuly důvody pro jejich udělení a zda se nemění úroveň rizik. Neakceptovatelné zvýšení rizik je důvodem pro neudělení nebo zrušení výjimky.

Základní pravidla životního cyklu výjimky:

- Každá žádost o výjimku musí být evidována. Žádost o výjimku může podat kdokoliv.
- Výjimky z pravidel obsažených v tomto metodickém pokynu:
    - spočívající v posunutí termínů realizace konkrétního opatření až na dvojnásobek předepsané lhůty pro provedení schvaluje Manažer, SCADA provozní technologie;
    - jejíž bezprostřední neudělení by mohlo omezit či ohrozit přepravní soustavu či běh průmyslového procesu schvaluje Manažer, SCADA provozní technologie;
    - obecně schvaluje vlastník procesu.
- Výjimky z celé souboru opatření a pravidel IT-SECPOL (tj. směrnice a všech navazujících metodických pokynů) v případě, kdy není v nadřízené bezpečnostní dokumentaci či v tomto dokumentu uveden pro konkrétní typ výjimky schvalovatel, obecně schvaluje Bezpečnostní výbor ICT/IS.
- V případě, že je výjimka z IT-SECPOL nezbytně nutná pro zajištění bezpečnosti přepravní soustavy v daný okamžik, tak je Dispečink oprávněn v daný okamžik potupovat v rozporu s IT-SECPOL a tento svůj postup neprodleně nahlásí Manažerovi, SCADA provozní technologie. Manažer, SCADA provozní technologie, zajistí bez zbytečného odkladu předání informací o tomto postupu Bezpečnostnímu výboru ICT/IS.

E Související dokumentace

E.1 Vystavené dokumenty a záznamy

Název dokumentu	Forma („P“ – papírová / „E“ – elektronická)	Zpracovatel	Místo uložení	Doba uchování
-	-	-	-	-
-	-	-	-	-

E.2 Navazující dokumentace

E.2.1 Základní obecně závazné právní předpisy

Rozumí se ve znění pozdějších předpisů, tj. včetně všech novelizací, kterými se tyto zákony mění a doplňují:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- Zákon č. 262/2006 Sb., zákoník práce

E.2.2 Externí technické předpisy

Žádné.

E.2.3 Řídicí dokumenty Společnosti

Řád:

- Organizační řád NET4GAS, s.r.o.
- Podpisový řád NET4GAS, s.r.o.
- Pracovní řád NET4GAS, s.r.o.
- Bezpečnostní řád NET4GAS s.r.o.

Směrnice:

- SM_I04_03_03 Havarijní plán přepravní soustavy NET4GAS, s.r.o
- SM_I04_04_01 Řízení fyzické bezpečnosti v NET4GAS, s.r.o.
- SM_I04_07_01 Bezpečnostní pravidla pro ochranu informací
- SM_F03_00 SCADA provozní technologie
- N4G_SM_A09_02 Řízení rizik v NET4GAS, s.r.o. (SM_C02_00)

Metodický pokyn:

- MP_C10_08_05 Ochrana dat (MP_I04_06_01_06)
- N4G_MP_A09_02_01 Řízení rizik v NET4GAS, s.r.o. (MP_C02_00_01)
- MP_H01_00_02 Vzdělávání a rozvoj zaměstnanců
- MP_F03_00_01 Provoz a správa řídicího systému DN4G
- MP_F03_00_02 Provoz a údržba řídicího systému přepravní soustavy
- MP_F03_00_03 Komunikace řídicího systému Dispečinku N4G a podřízených stanic
- MP_F03_00_04 Provoz a údržba lokálních řídicích systémů

Bezpečnostní dokumentace dále určená přímo pro ICT/IS:

- SM_I04_06_02 Bezpečnostní politika IT / IT-SECPOL
- MP_I04_06_02_01 Metodický pokyn IT-SECPOL pro Uživatele
- MP_I04_06_02_02 Metodický pokyn IT-SECPOL pro Dodavatele
- MP_I04_06_02_03 Metodický pokyn IT-SECPOL pro ŘS a SCADA systémy
- MP_C10_08_06 Ochrana koncových stanic (MP_I04_06_01_05)
- MP_H04_01_01_02 Řešení IT požadavků v rámci úseku Informační technologie NET4GAS, s.r.o.
- MP_H04_01_01_03 Řešení IT incidentů v rámci úseku Informační technologie NET4GAS, s.r.o
- SM_I04_06_01 Bezpečnostní pravidla pro práci s výpočetní technikou
- SM_I02_00 Směrnice nákupu a logistiky

POZNÁMKA: Čísla řídicí dokumentace uvedená v závorce odpovídají novému procesnímu uskupení.

F Závěrečná a přechodná ustanovení

Tento metodický pokyn nabývá účinnosti dnem jeho vydání.

P Přílohy

P.1 NET4GAS, s.r.o., Projektová dokumentace Kniha 13 – Zabezpečení systému

TRAN1_000_SPC_IB_004_K13_L.pdf