Datum vytištění: 17. 2. 2025

Rozsah platnosti:

ORLEN Unipetrol RPA s.r.o.

N NORMA

STANDARDY DCS, ESD a PLC

Sailer Digitálně podepsal Sailer Datum: 2025.02.17 12:15:37 +01'00'

Schválil:	Ing. Jan Sailer Ph.D., Technický ředitel
Platnost od:	1.1.2025
Správce dokumentu:	Zdeňka Mašková, Sekce podpory údržby
Zpracovatel:	Martin Jarý, Inženýr řídicích systémů II

Seznam změn

Číslo změny	Číslo strany		Předmět změny	Platnost od	Zpracovatel
	vyjmuté	vložené			
1			Zakomponování PPÚ-504 v rámci projektu Harmonizace PPÚ a N norem, celková revize dokumentu a převod do nové šablony	30.12.2024	Jarý M.
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Upozornění: Změnové řízení je prováděno dle směrnice 821.

Obsah

1 Rozsah platnosti

Norma N 11 023 obsahuje základní požadavky, které jsou uplatňovány při výběru a návrhu řídicích systémů typu DCS, ESD a PLC společnosti ORLEN UNIPETROL RPA s.r.o. umístěných v areálu Litvínov-Záluží a Kralup.

2 Úvod

Tato norma je závazná pro všechny subjekty, které se podílejí na provozu, montážích, údržbě a revizi dotčených řídicích systémů typu DCS, ESD a PLC a dalších zařízení uvedených v textu.

Tato norma platí jak pro nově instalované řídicí systémy, tak i pro rozšíření stávajících.

Tato norma je pravidelně aktualizována zhruba jednou za rok.

Tato norma obsahuje následující kapitoly:

Kapitola	Popis
Kapitola 2 Úvod	Vysvětluje účel normy, pro koho je závazná a popisuje její obecnou strukturu.
Kapitola 3 Pojmy a zkratky	Vysvětluje pojmy a zkratky použité v dokumentu.
Kapitola 4 Požadavky na systémy DCS a ESD	Obsahuje podrobné požadavky na systémy typu DCS a ESD zejména z hlediska hardware, software, licencí, dokumentace, školení.
Kapitola 5 Požadavky na systémy PLC	Obsahuje podrobné požadavky na systémy typu PLC zejména z hlediska hardware, software, licencí, dokumentace, školení.
Kapitola 6 Obecné požadavky	Obsahuje požadavky platné obecně pro řídicí systémy, zejména značení položek.
Kapitola 7 Související normy a předpisy	Obsahuje přehled souvisejících norem a dalších závazných předpisů.

3 Pojmy a zkratky

3.1 Obecné pojmy

Společnost	Orlen Unipetrol RPA s.r.o.
Kontraktor	dodavatel DCS/ESD/PLC či generální dodavatel stavby, jejíž součástí je DCS/ESD/PLC dodávané subdodavatelem.

3.2 Zkratky

zkratka	význam	poznámka
A/D	Analog/Digital	analogově/číslicový
APC	Advanced Process Control	systém vyššího řízení
ARC	Advanced Regulatory Control	složitější regulace
ASŘTP	Automatizované Systémy Řízení Technologických Procesů	lokální odbor údržby ASŘTP a digitalizace
ASW	Application SoftWare	aplikační software
CRAC	Computer Room Air Conditioning	systém přesné klimatizace serveroven
DCS	Distributed Control System	distribuovaný řídicí systém
DMZ	Demilitarized Zone	v počítačové bezpečnosti fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od ostatních zařízení
DWG	DraWinG	formát souborů AutoCAD
EPS	Elektrická Požární Signalizace	
ESD	Emergency Shutdown	havarijní blokovací systém pro nouzové vypnutí (součást SIS)
FAT	Factory Acceptance Test	test ve výrobním/vývojovém závodě dodavatele
FBD	Function Block Diagram	grafický jazyk pro tvorbu programů pro programovatelné logické automaty
FDS	Functional Design Specification	dokument určující funkce, které musí systém nebo komponenta vykonávat
HART	Highway Addressable Remote Transducer	digitální komunikace po proudové smyčce
HAZOP	HAZard and OPErability	analýza nebezpečnosti a provozovatelnosti
HMI	Human-Machine Interface	vizualizace a ovládání
HW	HardWare	
I/O	Input/Output	vstupně/výstupní moduly DCS/ESD/PLC

IPS	Instrumented Protective System (obdoba ESD)	bezpečnostní systém složený ze samostatné a nezávislé kombinace senzorů a zařízení navržených pro dosažení stanoveného rizika
KVM	Keyboard-Video-Mouse	
MCC	Motor Control Center	
OPC	OLE for Process Control	komunikační protokol OPC
P&ID	Piping & Instrumentation Diagram	
PC	Personal Computer	osobní počítač
PDF	Portable Document Format	formát souborů Adobe Acrobat
PDU	Power Distribution Unit	lišta pro distribuci napájení v rozvaděči
PID	Proportional – Integral – Derivative	PID regulátor
PLC	Programmable Logic Controller	programovatelný logický kontrolér
SAT	Site Acceptance Test	test na jednotce Orlen Unipetrol RPA
SIF	Safety Instrumented Function	
SIL	Safety Integrity Level	definováno v IEC61508, IEC61511
SIS	Safety Instrumented System	bezpečnostní systém složený ze samostatné a nezávislé kombinace senzorů a zařízení navržených pro dosažení stanoveného rizika
SW	SoftWare	

4 Požadavky na systémy DCS a ESD

4.1 Úvod

Kapitola 4 této normy obsahuje základní požadavky na DCS/ESD dodávané do Společnosti. Při výběru pro konkrétní aplikaci je možné dohodnout dílčí specifika odlišná od této normy. Veškeré takové změny musí být konzultovány s ASŘTP a jím schváleny.

Na Jednotkách Rafinérie Litvínov a Kralupy se místo ESD používá zkratka IPS ve stejném významu.

Ačkoli jsou požadavky v tomto dokumentu obecné, tedy nejsou určené pro žádný konkrétní DCS/ESD, kontraktor je musí považovat za specifikaci pro konkrétní nabízený či dodávaný DCS/ESD.

Dodaný DCS/ESD musí splňovat veškeré platné technické normy v oblasti napájení, barevného značení, jiskrové bezpečnosti apod.

Česká pobočka výrobce dodávaného DCS/ESD systému musí jako budoucí smluvní udržovatel být součástí investičního projektu a podílet se na návrhu a systémové konfiguraci DCS/ESD.

4.2 Role útvaru ASŘTP

ASŘTP v rámci Společnosti určuje dlouhodobou strategii pořizování a údržby DCS/ESD, podílí se na všech investičních akcích či akcích údržby, kde je součástí dodávky DCS/ESD nebo úpravy ve stávajícím.

ASŘTP je při výběrových řízeních na dodávku DCS/ESD a její následné realizaci jediným odborným útvarem, který rozhoduje o technických specifikacích a požadavcích a o tom, zda je nabízený či dodávaný DCS/ESD splňuje.

Aplikační software (ASW) není součástí dodávky kontraktora. ASW tvoří ASŘTP na základě dokumentace Kontraktora a konkrétní právní forma této spolupráce musí být definována smluvně.

Na Jednotkách Rafinérie Litvínov a Kralupy je ASW součástí dodávky kontraktora.

4.3 Vendor list

Je-li vyhlášeno výběrové řízení, jehož předmětem nebo součástí dodávky je nový řídicí systém DCS/ESD, platí dále uvedený vendor list. Nabídky jednotlivých uchazečů tedy mohou zahrnovat různé DCS/ESD odpovídající dále uvedenému vendor listu. V okamžiku podpisu smlouvy však již musí být jasné, který konkrétní systém bude dodán a jeho specifikace (výrobce, řada) musí být ve smlouvě uvedena.

Do Společnosti smí být dodán DCS výhradně od následujících výrobců a typů:

4.3.1 ABB

Řada:	ABB System 800xA
Kontroléry:	řada AC800M
I/O:	S800/900, Select I/O

4.3.2 Emerson Process Management

Řada: DeltaV
Kontroléry: SQ, MQ, SX, MX, PK kontroler
I/O: řada S nebo M, Intelligent Marshalling (CHARM)

4.3.3 Honeywell

Řada: Experion PKS
Kontroléry: C300, ControlEdge
I/O: Series C

Do Společnosti smí být dodán ESD výhradně od následujících výrobců a typů:

4.3.4 HIMA Paul Hildebrandt GmbH

Řada: HIMax, HIQuad, HIMatrix, Planar4

4.3.5 Honeywell

Řada: Safety Manager SC
Kontroléry: S300
I/O: SDIO (Safety Digital IO)

4.3.6 Schneider Electric - Triconex

Řada: Tricon, Tricon CX

4.3.7 Emerson Process Management

Řada: DeltaV SIS

4.3.8 ABB

Řada: ABB System 800xA High Integrity

4.4 Rozsah dodávky

Kontraktor musí dodat DCS/ESD v takovém rozsahu, aby byl plně funkční a splňoval veškeré technické, provozní a bezpečnostní požadavky. Jak při tvorbě nabídky tak při projektování musí kontraktor dodržet požadavky na DCS/ESD uvedené ve všech následujících odstavcích kapitoly 4.

4.5 Hardware

4.5.1 Kontroléry

1. Kontroléry musí být redundantní s automatickým přepnutím při poruše jednoho z páru bez vlivu na řízenou technologii.
2. Za běžného i abnormálního stavu (výpadek výrobny, najetí a sjetí výrobny apod.) musí být vytížení kontroléru maximálně 70% hodnoty maximálního vytížení doporučeného výrobcem.
3. Celkový počet kontrolérů musí být optimalizován z hlediska požadovaného výkonu a vhodného rozdělení řízení jednotlivých částí technologie mezi kontroléry.
4. Peer-to-peer komunikace mezi jednotlivými kontroléry musí být minimalizována na nezbytně nutný počet případů, které nelze vyřešit jiným způsobem (redesignem architektury systému, přerozdělením položek mezi kontroléry apod.).
5. Proto všechny signály jedné řízené technologické části či smyčky musí být zavedeny do stejného kontroléru, pokud to samozřejmě není v rozporu s jinými požadavky vyšší priority (rozdělení kvůli redundanci či bezpečnost apod.).
6. Pro komunikaci mezi DCS a ESD musí být vyhrazený kontrolér nebo kontroléry s ohledem na počet přenášených údajů a odpovídající rezervu.

4.5.2 I/O moduly

Počty jednotlivých typů vstupů/výstupů budou navrženy s 20% rezervou zapojených I/O, rovnoměrně rozloženou přes všechny kontroléry.

Vstupy i výstupy jedné měřící smyčky musí být ve stejném kontroléru a pokud možno na stejném I/O modulu.

Modul analogových vstupů (AI) musí splňovat alespoň následující požadavky:

- minimálně 12bitový A/D převodník
- self-diagnostika
- detekce rozpojené a zkratované smyčky
- možnost galvanického oddělení jednotlivých kanálů
- podpora HART protokolu, „pass-through“ funkcionality
- možnost redundance

Modul digitálních vstupů (DI) musí splňovat alespoň následující požadavky:

- indikace stavu každého jednotlivého kanálu přímo na kartě
- self-diagnostika
- možnost galvanického oddělení jednotlivých kanálů

Modul analogových výstupů (AO) musí splňovat alespoň následující požadavky:

- detekce otevřené smyčky

- ochrana výstupu proti zkratované smyčce
- podpora HART protokolu, „pass-through“ funkcionality
- self-diagnostika

Modul digitálních výstupů (DO) musí splňovat alespoň následující požadavky:

- možnost galvanického oddělení jednotlivých kanálů
- indikace stavu každého jednotlivého kanálu přímo na kartě
- self-diagnostika

4.5.3 Aktivní síťové prvky

DCS bude vybaven firewallem, který bude jediným propojovacím místem s podnikovou IT sítí.

Veškeré switche, routery a ostatní aktivní prvky musí být managovatelné a musí umožňovat vzdálenou diagnostiku po lokální síti DCS. Pokud DCS nabízí takovou možnost, musí být tyto prvky zavedeny přímo do systému a jejich poruchy alarmované (systémový alarm).

Součástí dodávky musí být také SW pro správu a monitoring dodávaných aktivních síťových prvků.

Specifikace firewallu:

- redundantní provedení (High availability), pokud nebude specifikováno jinak
- zdvojené napájení
- vendor i typ firewallu bude upřesněn při konkrétní akci

4.5.4 Rozvaděče

Kromě periferií operátorských stanic, umístěných na velínu, musí být všechny prvky DCS/ESD – zejména kontroléry, I/O moduly, komunikační moduly, servery, operátorské stanice, aktivní síťové prvky, napájecí prvky – umístěny ve vyhrazených průmyslových rozvaděčových skříních splňujících následující požadavky:

- odmontovatelné střešní desky a boky kabinetů
- pro IT rack nebo serverové kabinety skleněné přední dveře, pokud nebude uvedeno jinak
- měření teploty uvnitř rozvaděče alarmované a historizované v DCS
- osvětlení, které se rozsvítí po otevření dveří pole
- čidlo otevření dveří alarmované v DCS/ESD
- vybavení detekčním a/nebo hasicím systémem dle strategie určené společností nebo dle výsledků HAZOP studie konkrétní výrobny
- vybavené PDU pro napájení všech instalovaných komponent ze dvou nezávislých zálohovaných zdrojů
- vybavené systémem kabelového managementu

Veškeré rozvaděče DCS/ESD musí být umístěné v oddělené místnosti (rozvodna, serverovna) s omezeným přístupem osob splňující veškeré požadavky na teplotu, čistotu, vlhkost a další podmínky vyžadované umístěným zařízením.

Pokud se buduje nová rozvodna či serverovna, musí se počítat s prostorovou rezervou pro instalaci dalších rozvaděčů při rozšiřování systémů v budoucnu. Tato rezerva musí být 30%, minimálně však pro dva rozvaděče od každého druhu (kontroléry, I/O, IT rack).

4.5.5 Optické a metalické sítě

- veškeré kritické komunikační sítě DCS/ESD musí být redundantní
- jedná se zejména o síť propojující I/O moduly a kontroléry a síť propojující kontroléry, servery a operátorské stanice
- v případě redundantní optické či metalické sítě musí být každá větev z páru vedena jinou trasou
- DCS bude vybaven doplňkovou sítí, do které budou připojeny servery, operátorské stanice a další počítače. Účelem této sítě je odlehčit provoz na hlavní řídicí síti tím, že bude provozovat služby jako např. zálohování, update antivirů a MS Windows, kopírování dat, vzdálený přístup pomocí RDP apod. Počítače tedy musí být vybaveny ethernet portem speciálně pro tuto síť. Tato síť nemusí být redundantní.
- IP adresy v sítích DCS/ESD přidělí ASŘTP
- optické i metalické kabely budou dimenzované s dostatečnou délkovou rezervou pro případné budoucí přesuny rozváděčů

Požadavky na optické sítě:

- venkovní optické kabely budou uloženy po celé trase v chráničkách, každý kabel ve vlastní chráničce
- chráničky budou žluté barvy v provedení odolávající povětrnostním vlivům včetně UV záření
- všechny optické kabely, resp. chráničky, budou označeny
- na výstupu/vstupu z objektu nebo požárního úseku
- na křížení a rozdělení kabelové trasy
- po každých 50 metrech, pokud nebylo aplikováno nějaké z výše uvedených pravidel
- všechny typy kabelů a chráničky budou na obou koncích označeny tak, aby bylo zřejmé odkud a kam kabel vede (budova, patro, rozvaděč, zařízení atd. ..)
- štítky ke kabelům budou připevněny pomocí nerezových vázacích pásků a budou v provedení odolávajícím povětrnostním vlivům včetně UV záření
- všechny nově instalované kabely/vlákna/konektory budou řádně proměřeny a o tomto bude dodán protokol

4.5.6 Fieldbus

Foundation Fieldbus nebo Profibus může být použit pro komunikační spojení mezi instrumentací v poli a DCS a také pro komunikaci s MCC.

Prostřednictvím běžných vodičů a signálů 4 -20 mA a digitálních ON/OFF signálů (tzv. hardwired) musí však být přivedeny:

- veškeré signály ESD
- ovládací a kritické či jinak důležité signály DCS

Fieldbus musí být konstrukčně bezpečný při selhání. Ztráta komunikace nebo napájení musí způsobit, že ventily se dostanou do svých bezpečných poloh.

Použitá průmyslová sběrnice včetně napájecích zdrojů a karet musí být plně redundantní; žádná jednotlivá porucha nesmí vést ke ztrátě více než jedné řídící smyčky nebo k neschopnosti operátora přistupovat k zařízení nebo k části zařízení.

4.5.7 PC pro operátorské stanice a servery

- alarmové klávesnice musí být součástí DCS, umožňuje-li jejich použití
- veškerá PC musí být v provedení do racku s montáží včetně vysouvacích lyžin s přístupem zpředu i zezadu
- veškerá PC budou s pětiletou podporou Next Business Day Onsite Service
- všechna PC musí být umístěná v kabinetech, žádné PC nesmí být umístěno v prostoru velínu, kromě výjimky uvedené v kapitole 4.6.2. (v případě tenkých klientů umístěných v operátorských pracovištích musí být přístup k portům zajištěn v kombinaci SW nebo HW opatřeních)

4.5.8 PC pro PI kolektor – připojení do podnikového MES

Součástí DCS musí být PC „PI kolektor“. Ze síťového hlediska je toto PC umístěno v DMZ, čte data z OPC serveru DCS a posílá je do podnikového PI serveru.

DCS bude vybaveno veškerým HW i SW pro přenos minimálně všech analogových měření, kalkulovaných veličin, žádaných hodnot, výstupů a vybraných digitálních signálů do podnikové LAN využitím OPC technologie se zachováním maximální bezpečnosti propojení.

Minimální specifikace počítače pro PI kolektor:

- PowerEdge Rxxx s procesorem Intel Core i3/3.6GHz s anglickým OS Windows Server Standard, 32GB RAM, disky s kapacitou nejméně 2TB v konfiguraci RAID1, iDrac, redundantní napájení
- ProSupport and Next Business Day Onsite Service Initial, 12 měsíců
- ProSupport and Next Business Day Onsite Service Extension, 24 měsíců

Finální konfigurace musí být konzultována s ASŘTP a jím schválena.

4.5.9 Napájení, UPS

Veškeré kritické části DCS/ESD (kontroléry, I/O moduly, servery, operátorské stanice, síťové prvky) budou napájeny ze dvou nezávislých nepřerušitelných zdrojů. Napájení z těchto dvou zdrojů musí být distribuováno mezi jednotlivá (i nekritická) zařízení tak, aby výpadek jednoho zdroje neomezil schopnost DCS/ESD řídit technologii.

Do kabinetů DCS/ESD bude také přivedeno nezálohované napětí 230V pro osvětlení, servisní zásuvky apod.

Veškeré poruchy napájení musí být signalizovány a alarmovány v příslušném DCS/ESD, jističe budou vybaveny pomocnými kontakty pro zavedení signalizace do DCS/ESD.

Napájení musí být dimenzováno tak, aby umožňovalo bezpečné sjetí řízené technologie v případě rozsáhlého výpadku napájení.

4.5.10 KVM extendery, Thin Clients

Vzhledem k umístění operátorských pracovišť na velínu a PC operátorských stanic v oddělené místnosti, musí být použit vhodný a spolehlivý systém KVM extenderů, switchů či tenkých klientů pro vzdálené připojení klávesnic, displejů a polohovacích zařízení (myší, TrackBall apod.). To se týká i veškerých serverů a jiných počítačů, ke kterým musí být zajištěn přístup z velínu nebo inženýrské místnosti ASŘTP.

Rackové skříně, kde jsou instalovány počítače, budou vybaveny vysouvacím KVM switchem s LCD pro místní přístup k počítačům.

4.5.11 Datové úložiště

Součástí dodávky musí být zařízení typu NAS s úložištěm RAID s dostatečnou kapacitou pro ukládání všech záloh a udržování minimálně 3 starších verzí těchto záloh.

Minimální konfigurace NAS serveru:

- NAS server Synology RSxxx RackStation
- posuvné lyžiny do racku pro NAS server
- tři hard disky + jeden záložní (hot spare) typu Western Digital Red (popř. jiný typ podobných či lepších parametrů) s kapacitou podle potřeb konkrétní aplikace, nejméně však 10TB v konfiguraci RAID 10, RAID 01 nebo RAID 5

Finální konfigurace musí být konzultována s ASŘTP a jím schválena.

4.5.12 Klimatizace

Rozvodna či místnost s rozváděči DCS/ESD bude klimatizovaná přesným redundantním klimatizačním systémem CRAC (Computer Room Air Conditioning) se spodním výstupem studeného vzduchu s přetlakem do dvojité podlahy. Odtud bude vzduch veden perforovanými ventilačními podlahovými deskami zpátky do prostoru před rozváděče a tím bude zajištěn cílený přívod studeného vzduchu na tu stranu rozváděče, na které ventilátory serverů nasávají. Nad opačnou stranou rozváděčů, tam kde ventilátory serverů vyfukují ohřátý vzduch, bude instalováno nasávání tohoto vzduchu a jeho vedení zpět do CRAC jednotky. Všechny rozváděče i podlaha musí být vhodné pro tento typ chlazení.

Teplota v rozvodně či místnosti s rozváděči DCS/ESD bude zavedena do DCS a alarmována. Stejně tak bude do DCS zavedena informace o stavu klimatizační jednotky a případná porucha vyvolá alarm.

4.5.13 Tiskárny

Součástí DCS/ESD bude síťová laserová tiskárna sloužící operátorům pro tisk trendů, alarmových výpisů apod. a pro tisk dokumentace DCS/ESD.

4.5.14 Update server

Součástí dodávky musí být update server, umístěný v DMZ. Tento server musí být vybaven takovým softwarem, aby bylo možné distribuovat updaty antivirových databází/enginů a updatů Microsoft Windows na všechny ostatní počítače DCS systému.

Update server nebude připojen k internetu a požadované dodavatelem DCS schválené aktualizace se na něj budou nahrávat ručně.

4.5.15 Virtualizace

Kromě hlavních serverů a operátorských stanic mohou být počítače DCS provozovány jako virtuální stroje. Jedná se např. o doménové kontroléry, OPC servery, PI kolektory, update servery apod.

Při navrhování a implementaci DCS/ESD dáváme přednost virtualizovaným IT řešením všude tam, kde je to vhodné a přináší to výhody. Tento přístup umožňuje efektivnější využití hardwaru, lepší škálovatelnost a flexibilitu při správě systémů.

4.5.16 Synchronizace reálného času

Reálný čas DCS/ESD bude synchronizován z NTP serveru Unipetrolu (služba Windows Time) připojeného v DMZ.

PLC nebudou připojena přímo na síti DCS. V případě, že PLC server (počítač konfigurační stanice) bude propojen se sítí DCS přes firewall, bude se čas PLC serveru (počítače) synchronizovat dle inženýrské stanice DCS a samotný PLC si pak svůj čas synchronizuje s jeho serverem. V ostatních případech bude synchronizace času PLC zajištěna v rámci komunikace s DCS např. jednorázovým zápisem hodiny/minuty/sekundy v dohodnutém intervalu.

4.6 Řídící centrum, operátorská pracoviště a inženýrské pracoviště

4.6.1 Řídicí centrum

Veškeré řízení technologie prostřednictvím DCS probíhá v řídicím centru (velín). V řídicím centru jsou umístěna operátorská pracoviště. Pokud není v jiné místnosti (místnost ASŘTP), je v řídicím centru také umístěná inženýrská stanice, ze které se provádí změny aplikačního software a konfigurace DCS/ESD. V řídicím centru jsou také umístěny operátorské stanice či grafické panely dalších případných řídicích systémů PLC či balených jednotek apod.

Řídicí centrum musí umožňovat bezpečné, ergonomické a komfortní řízení technologie jak v normálních stavech, tak i v kritických situacích, v režimu 24/7. Tomu musí být přizpůsobena dispozice místnosti, rozmístění operátorských pracovišť, nábytek, řízení prostředí z hlediska teploty, osvětlení, ventilace.

Řídicí centrum musí splňovat platné požadavky na hygienu a ergonomii pracovního prostředí operátorů.

Řídicí centrum musí být vybaveno minimálně následujícím:

- automatický nastavitelný systém HVAC celého prostoru – topení, ventilace, klimatizace
- možnost efektivního zastínění oken
- osvětlení vhodné pro řídicí centra
  - bez odrazů na operátorských monitorech a ostatních površích
  - bez vnímatelného blikání
  - nastavitelné z hlediska intenzity osvětlení, vhodné pro 24-hodinový provoz
- inženýrské pracoviště pro inženýra ASŘTP, pokud není umístěno v jiné místnosti, např. v kanceláři ASŘTP dané výrobny
- telefony, vysílačky
- dostatečný počet zásuvek 230V pro další zařízení
- systém pro kontrolu přístupu do řídicího centra včetně logování přístupů a kamerového záznamu vstupních bodů

4.6.2 Operátorská a inženýrská pracoviště

Operátorská a inženýrská pracoviště budou vhodně rozmístěná z hlediska ergonomie a pohybu osob v řídicím centru.

Operátorské a inženýrské pracoviště musí splňovat minimálně následující obecné požadavky:

- profesionální stůl určený pro operátorské pracoviště s nepřetržitým provozem
- vybavení elektrickým systémem pro nastavení výšky celého pracoviště a tím možnost pracovat jak v sedě, tak ve stoje
- vybavení kombinací malých (min. 24“) a velkých (min. 50“) LCD monitorů, které umožňují zobrazení operátorských grafik; počet i velikosti monitorů bude upřesněn při konkrétní akci, závisí na náročnosti řízené technologie
- inženýrské pracoviště bude vybaveno stejným počtem monitorů jako operátorská pracoviště, minimálně však třemi
- monitory budou určeny pro trvalý provoz 24/7 a tento parametr bude výslovně uveden v jejich dokumentaci
- vybavení systémem alarmového ozvučení a osvětlení
- vybavení profesionálním operátorským křeslem, které splňuje veškeré ergonomické požadavky, s dostatečnou nosností a možnostmi nastavení polohy a výšky sedáku, opěradla i područek
- vybavení integrovaným systémem kabelového managementu
- podpora redundance napájení
- v případě DCS Honeywell musí být použito řešení „Honeywell Experion Orion Console“
- v případě DCS ABB musí být použito řešení „ABB EOW Extended Operator Workplace“
- v případě DCS Emerson musí být použito řešení „Emerson iOps Workspace Solution“
- pokud je standardním řešením dodavatele DCS umístění operátorských PC nebo PC typu tenký klient přímo v operátorském pracovišti, uděluje se pro tato PC výjimka z kapitoly 4.5.7 „PC pro operátorské stanice a servery“ - bod 4 této normy týkající se umístění PC operátorských stanic a serverů. Pro umístění těchto PC musí být pracoviště vybavená úschovnými boxy s integrovaným systémem pro možnost jejich napájení.

Konkrétní typ, počet a konfigurace operátorských pracovišť bude blíže určena zástupci provozu v rámci zadání konkrétní akce. Z důvodu redundance a zastupitelnosti musí být operátorská pracoviště nejméně dvě.

4.7 Software

4.7.1 Historizační HW a SW

- Historizační stanice musí mít pro ukládání historizačních dat diskovou kapacitu minimálně 2TB
- Historizační HW a SW musí umožňovat historizaci všech analogových měření, kalkulovaných veličin, žádaných hodnot a výstupů v sekundových frekvencích ukládání s online přístupem pro uživatele včetně operátorů minimálně po dobu minimálně 5 let s možností další archivace dat.
- Historizační HW a SW musí také umožňovat historizaci veškerých operátorských zásahů a dalších událostí („events“)

- Historizační SW musí umožňovat export zdrojových i agregovaných (průměry, minima za interval apod.) historických dat do Microsoft Excel.

4.7.2 Vývojový software

- Součástí dodávky musí být SW umožňující konfiguraci jednotlivých částí ASW (minimálně řídící databáze) offline na uživatelských PC mimo DCS/ESD i na PC v rámci DCS/ESD.
- Součástí dodávky musí být instalace SW včetně potřebných licencí umožňující simulaci kontrolérů a dalších zařízení pro účely testování aplikační logiky.

4.7.3 Zálohovací software

DCS/ESD musí být vybaven SW pro zálohování všech počítačů. Tento SW bude nainstalován na všech počítačích a bude centrálně spravovaný z jednoho serveru. Bude umožňovat mimo jiné on-line zálohování celých disků (formou image) a procesních dat na určené úložiště.

DCS/ESD musí být vybaven SW pro on-line zálohování a obnovu všech částí aplikačního SW (řídicí databáze, grafické a trendové displeje, konfigurace historické databáze, atd.).

V případě virtualizovaného řešení bude zálohování probíhat na úrovni virtualizační platformy, tzn. zálohování celých virtuálních strojů.

4.7.4 Alarmový systém a Alarm management software

- DCS musí být vybaven speciálním SW pro statistiku, analýzu a optimalizaci alarmového systému podle standardů EEMUA 191, ISA 18.2 a IEC 62682:2014, včetně funkce „Alarm Shelving“.
- DCS musí umožňovat funkci tzv. „Page Acknowledge“ – jedním kliknutím potvrdit všechny alarmy týkající se objektů na právě zobrazeném operátorském displeji.
- Jednou z funkcí alarmového systému musí být přímý odkaz z konkrétního alarmu v seznamu alarmů, vedoucí na příslušný operátorský displej. Operátor musí mít možnost z kteréhokoli alarmu v seznamu alarmů se rychle dostat k detailnímu displeji zařízení či části technologie, které se alarm týká. Pokud uvedenou funkci neumožňuje software, musí být zajištěna dostatečným počtem hardwarových alarmových klávesnic na každém operátorském pracovišti.

4.7.5 Management Of Change – software pro řízení změn a dokumentaci

- Součástí ESD musí být software pro řízení/audit změn. Tento software musí ukládat veškeré změny provedené v aplikačním software, včetně detailní informace o tom, jaká změna byla provedena, kdo změnu provedl, kdy a kde byla provedena. Tento software musí umožňovat zpětný audit provedených změn a návrat k předchozím verzím aplikačního software.
- Součástí DCS/ESD musí být funkce pro dokumentaci aplikačního software včetně křížových odkazů mezi položkami řídící databáze, historické databáze a operátorským prostředím včetně grafických displejů. Pořízení takovéto dokumentace musí být možné přímo z DCS/ESD formou tisku a/nebo exportu minimálně do PDF.

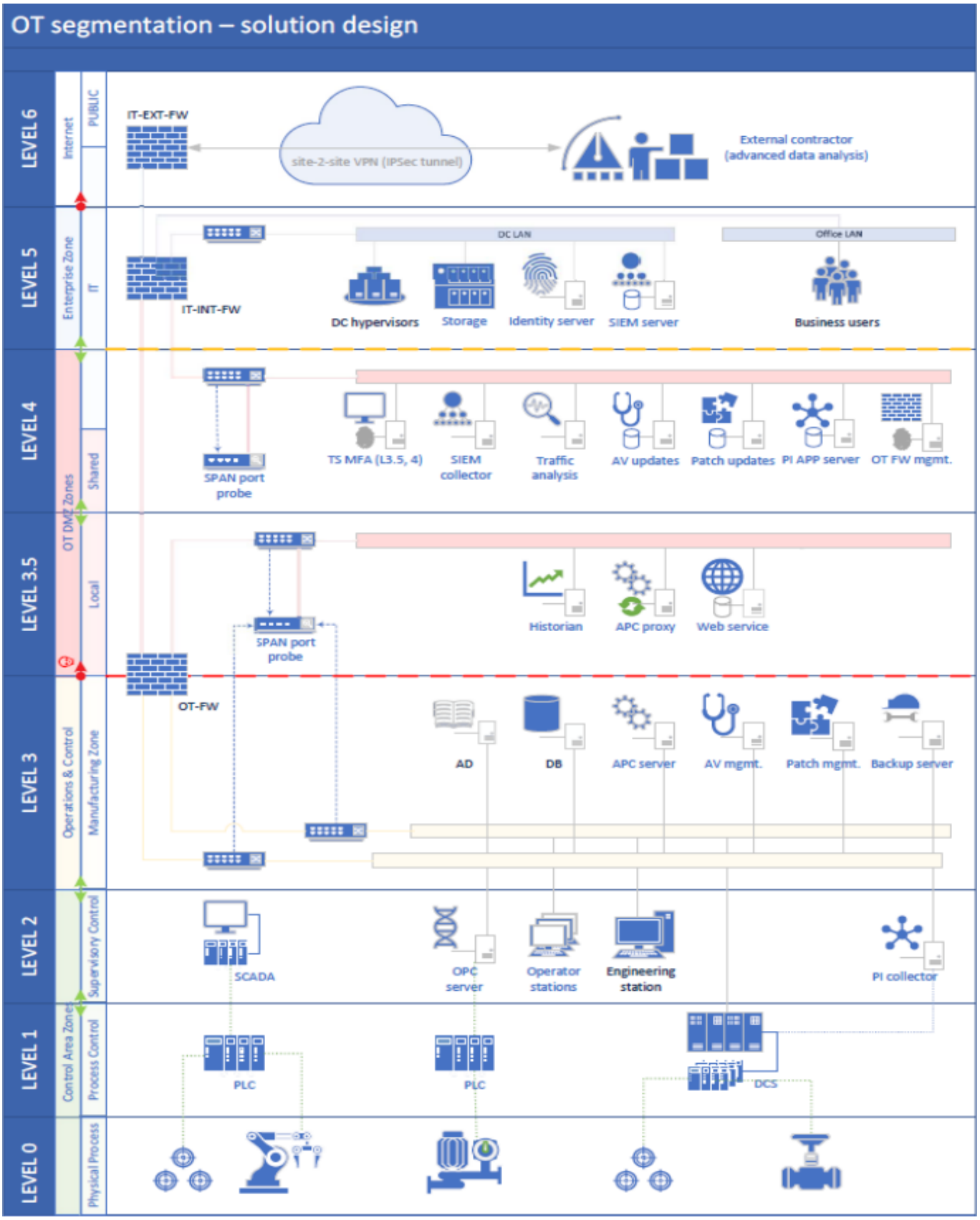
4.7.6 Antivirový a antimalware software

- Každý počítač DCS/ESD musí být vybaven antivirovým SW.
- Antivirový SW bude aktualizovat své virové databáze z jednoho společného serveru.
- Licence antivirového SW bude platná po dobu minimálně pět let včetně aktualizací virových databází i SW samotného.

4.7.7 Kybernetická bezpečnost

Kybernetická bezpečnost DCS/ESD musí být řešena kombinací všech následujících nástrojů:

- Bezpečná architektura DCS/ESD a jeho počítačové sítě dle aktuálních pravidel Společnosti – musí být odsouhlaseno útvarem ASŘTP v rámci schvalování FDS.
- Softwarový nástroj pro sledování a management sítě a síťových prvků s automatickou grafickou reprezentací topologie sítě DCS/ESD. Takový nástroj musí být součástí dodávky.
- Antivirový SW.
- Zálohovací SW.
- Systém řízení přístupu uživatelů.
- Logování veškerých událostí týkajících se bezpečnosti.
- Řízení vzdáleného přístupu z podnikové IT sítě.
- V případě požadavku na Kybernetickou bezpečnost musí být dodrženy požadavky na segmentaci a síťovou komunikaci v oblasti OT zón. Celkové řešení musí být odsouhlaseno oddělením IT Security naší Společnosti.
- Základní požadovanou OT segmentaci ukazuje následující schéma:


OT segmentation – solution design
LEVEL 6
Internet
PUBLIC
IT-EXT-FW
site-2-site VPN (IPSec tunnel)
External contractor
(advanced data analysis)
LEVEL 5
Enterprise Zone
IT
IT-INT-FW
DC LAN
Office LAN
DC hypervisors
Storage
Identity server
SIEM server
Business users
LEVEL 4
OT DMZ Zones
Shared
SPAN port probe
TS MFA (L3.5, 4)
SIEM collector
Traffic analysis
AV updates
Patch updates
PI APP server
OT FW mgmt.
LEVEL 3.5
Local
SPAN port probe
Historian
APC proxy
Web service
OT-FW
LEVEL 3
Operations & Control
Manufacturing Zone
AD
DB
APC server
AV mgmt.
Patch mgmt.
Backup server
LEVEL 2
Supervisory Control
SCADA
OPC server
Operator stations
Engineering station
PI collector
LEVEL 1
Control Area Zones
Process Control
PLC
PLC
DCS
LEVEL 0
Physical Process

4.7.8 Ostatní software

- Vybrané operátorské a inženýrská stanice musí být vybaveny Microsoft Office – minimálně Excel a Word, na inženýrské stanici i MS Access.
- Každá operátorská a inženýrská stanice musí být vybavena SW pro prohlížení PDF souborů.
- Součástí dodávky musí být příslušný počet OPC serverů pro komunikaci s jinými systémy a pro posílání dat do MES systému Společnosti. Veškeré OPC komunikace musí být vybaveny OPC Tunnellery.

4.8 Licence

Všechny části DCS/ESD, pro které se licence dimenzují na počet tagů nebo podobným způsobem, musí být dodány s rezervou 20%. To se týká zejména následujících licencí:

- samotný DSC/ESD systémový SW
- veškeré licence vázané na počty I/O
- OPC, MODBUS či jiná komunikace
- historizační SW
- zálohovací SW
- antivirový a antimalware SW
- Alarm Management SW
- licence Microsoft CAL pro vzdálený přístup
- licence standardního řešení výrobce DCS pro vzdálený přístup do DCS/ESD z podnikové IT sítě – např. ABB Smart Client, Honeywell eServer apod.

4.9 Dokumentace

4.9.1 Obecné požadavky na dokumentaci

Dokumentace musí být dodaná v PDF i v editovatelném formátu MS Excel, MS Word, DWG apod. Dokumentace musí být dodaná také v tištěné formě.

Tabulky, databáze apod. musí být v takovém formátu, který kromě editace umožňuje i vyhledávání, řazení a filtrování, tedy MS Excel, MS Access, INtools/SPI apod.

Pokud je k tvorbě dokumentace použit databázový dokumentační software jako např. Comos, Aveva, PDMS či jakýkoliv jiný podobný software, veškerá dokumentace bude předávána také v nativním formátu softwaru, v němž byla vytvořena, se všemi potřebnými daty nutnými pro zobrazení v prohlížečích kompatibilních s původní aplikací nebo přímo v ní, tj. včetně databází použitých technických dat a s uvedením plných názvů použitých SW aplikací včetně jejich verzí.

4.9.2 Požadované dokumenty

Součástí dodávky DCS/ESD musí být alespoň následující dokumenty:

4.9.2.1 Protokoly

- protokoly FAT/SAT DCS/ESD
- protokoly z testů napájecích zdrojů DCS/ESD
- protokoly z testů smyček (loopcheck), testů interlocků, sekvencí, ARC a dalších řídicích struktur
- kopie protokolů ze školení uživatelů DCS jimi podepsané; přílohou musí být agenda školení

4.9.2.2 Dokumentace DCS/ESD

- detailní schéma topologie celého DCS/ESD včetně napájení jednotlivých komponent a propojení s dalším zařízením (PLC, MCC, analyzátory apod.) – topologické schéma musí být vertikálně rozvrstveno podle principu segmentování sítí z hlediska počítačové bezpečnosti OT systémů
- I/O list
- výkresy smyček; Na Jednotkách Rafinérie Litvínov a Kralupy jednotlivé tagy musí být založeny do databáze INtools/SPI, výkresy v papírové podobě musí být vytištěny z této databáze
- Control and Safeguarding Narratives s relevantními výstupy z HAZOP či SIL studie (výsledky SIL klasifikace budou zapracovány do on-line SIFpro databáze)
- dokumentace pro komunikaci s ostatními systémy (PLC, analyzátory, jiná DCS apod.) – paměťové mapy, seznamy tagů, konfigurace komunikačních protokolů atd.
- standardní dokumentace výrobce DCS/ESD pro HW a SW
- seznam všech dodaných licencí včetně informací o jejich platnosti
- originální instalační média a uživatelské manuály veškerého instalovaného SW
- dokumentace skutečného stavu DCS/ESD
- obecná operátorská příručka pro práci s DCS a ESD (práce s trendy, alarmy, diagnostikou, popis faceplatů apod.) v českém jazyce

- seznam I/O obsahující:

  Analogové smyčky
  - název, popis
  - charakteristika signálu (např. 4-20 mA, odmocněný, neodmocněný,…)
  - rozsah a jednotky měření odpovídající SI soustavě měřených jednotek
  - veškeré hodnoty alarmových limit a parametrů
  - typ a směr regulace vztažný k fyzické pozici ventilu
  - charakteristika a rozsah výstupu
  - pozice ventilu při výpadku energie
  - pozice ventilu při 4 mA
  - inicializační hodnoty
  - umístění položky v P&I schématech
  - přesné určení pozice vstupů a výstupů do/z DCS/ESD (periférie)
  - odkaz na logickou případně další řídicí strukturu

  Digitální smyčky
  - název, popis
  - charakteristika signálu (trvalý, momentový,…)
  - význam jednotlivých stavů
  - určení alarmových stavů (případně určení alarmových stavů kombinací signálů) - alarmovým stavem a bezpečným stavem zařízení bude logická 0, koncová poloha ventilu i chod motoru budou indikovány logickou 1

- inicializační hodnoty
- přesné určení pozice vstupů a výstupů do/z DCS/ESD (periférie)
- odkaz na logickou případně další řídicí strukturu

4.9.2.3 Dokumentace k administraci a údržbě DCS/ESD

- návod na instalaci operátorských a inženýrských stanic a serverů
- návod na bezpečné sjetí/najetí jednotlivých komponent DCS/ESD
- návod na vytvoření záloh systémového a aplikačního SW
- návod na obnovení systémového a aplikačního SW ze záloh
- tři kompletní sady záloh ASW vytvořené před najetím výrobny, řádně popsané (obsah, typ a počet zálohovacích médií)

4.9.2.4 FDS

Velmi důležitým dokumentem je FDS – Functional Design Specification. Tento dokument musí být odsouhlasen ASŘTP před započetím dalších projektových činností.
FDS musí být vytvořen spoluprací dodavatele Detail Engineeringu (Kontraktora), dodavatele (výrobce) DCS/ESD, ASŘTP (tvůrce aplikačního software) a zástupců provozu (budoucí uživatel).

FDS je základní dokument, který popisuje DCS/ESD z hlediska systémového hardwaru, systémového softwaru a funkčnosti jednotlivých komponent aplikačního software, jako je logika, HMI atd.

Typické řídicí a grafické struktury aplikačního SW musí vycházet ze struktur již používaných na DCS/ESD ve Společnosti.

Zásadním požadavkem na projektovou dokumentaci pro tvorbu aplikačního software je maximální využití vlastností a možností konkrétního dodávaného systému. Cílem tohoto požadavku je vyhnout se neefektivnímu programování podle obecných vzorů připravených pro jakýkoli DCS/ESD systém. Během přípravy FDS je nutné se tímto zabývat a navrhnout ve spolupráci s ASŘTP typické struktury logiky i grafiky tak, aby byly s výhodou využity všechny možnosti konkrétního systému.

Musí obsahovat jak detailní popis systému jako takového včetně topologického schématu, tak i popis funkcionality všech standardních komponent aplikačního software, zejména:

- PID kontrolér
- ventil, motor
- požadavky na operátorské displeje a navigaci
- filosofii alarmového systému
- trendy
- bezpečnost

FDS musí obsahovat také detailní specifikaci pro zejména:

- veškeré řízení
- sekvence
- interlocky
- Control and Safeguarding Narratives
- rozhraní

- rozsahy přístrojů
- nastavení hodnot alarmů a tripů
- filosofii náhradních dílů a možností rozšíření DCS/ESD

Některé uvedené funkcionality nebo specifikace mohou být součástí projektové dokumentace.

V případě, že DCS/ESD bude komunikovat s balenými jednotkami (např. extrudery) s vlastním řídicím systémem, musí jejich dodavatel spolupracovat při vytváření FDS.

4.10 Testování a uvádění do provozu

Kontraktor musí provést testy ASW DCS/ESD za účelem ověření jeho shody s FDS.

Kontraktor musí provést ve vhodných fázích realizace testy FAT a SAT týkající se DCS/ESD na základě předem odsouhlasených procedur a protokolů dodavatele systému.

Tyto testy je možné provádět postupně v několika fázích:

- Testy typických funkčních bloků (Typicals test) – zahrnují generické softwarové komponenty a filosofie. Měly by být provedeny před hromadným použitím těchto komponent.
- Hardware a standardní komponenty – tento test zahrnuje veškerý systémový hardware, I/O testy, rozhraní k dalším systémům a veškeré jednoduché řízení, indikace a displeje. Veškerá rozhraní do DCS/ESD musí být otestována. Po dokončení tohoto testu je možné hlavní komponenty DCS/ESD dopravit na místo stavby, pokud se další testy obejdou bez nich.
- Složitější řízení – tento test zahrnuje všechny interlocky, logiku složitějšího řízení a regulací, sekvence a příslušné displeje. Tento test většinou vyžaduje ke svému provedení jednoduché simulace.

Pokud řízení balených jednotek je složitějšího rázu, měl by být přítomen i jejich dodavatel.

Kontraktor je zodpovědný za celkovou konzistenci všech testovaných systémů a za splnění veškerých požadavků na řízení technologie.

Před uvedením výrobny do provozu budou mimo jiné provedeny následující zkoušky:

- FAT – není akceptována on-line forma; procedura musí být provedena za fyzické přítomnosti zástupců Společnosti
- SAT
- Loopcheck – správnost zapojení obvodů a konfigurace v DCS/ESD musí být otestována kompletními zkouškami obvodů z pole přes všechny sdružovací skříňky a ranžírovací rozvaděče, případné jiskrové bariéry, I/O moduly, případnou komunikaci mezi ESD a DCS až na operátorské obrazovky DCS. Musí být provedeny a zaznamenány minimálně následující kontroly:
  - kontrola nastavení inženýrských rozsahů
  - kontrola pozice ventilů (100% = otevřeno, 0% = zavřeno)
  - kontrola stavových signálů
  - kontrola regulačních prvků
  - kontrola alarmových/spínacích/blokovacích limit (včetně prezentace alarmů na obrazovkách DCS)

- kontrola přítomnosti a správnosti jednotlivých signálů na technologických displejích v DCS
- kontrola správnosti komunikace jednotlivých signálů mezi DCS a ESD
- kontrola správnosti digitálních a analogových výstupů přímo na zařízení v poli nebo měřením na svorkách přímo v poli.

Po najetí nového nebo rozšířeného systému musí výrobce provést jeho audit z hlediska výkonnostního, síťového, komunikačního a bezpečnostního. Cílem tohoto opatření je znalost výchozího stavu, ve kterém se systém nachází po commissioningu a všech změnách spojených s najetím.

4.11 Školení

Součástí dodávky musí být školení u výrobce DCS/ESD podle následujících podmínek:

1. rozsah školení
   - DCS – minimálně čtyři týdny pro dva SW inženýry
   - ESD – minimálně čtyři týdny pro dva SW inženýry
   - rozsah školení musí pokrývat zejména administraci systému, konfiguraci a správu řídící databáze, historie, tvorbu grafiky, alarm management a jiné doplňkové konfigurátory a aplikace třetích stran
2. typ školení
   - standardní certifikované školení předem vybrané z katalogu výrobce DCS/ESD, které proběhne v oficiálním školicím středisku výrobce DCS/ESD
3. termín
   - školení musí proběhnout před připomínkováním první verze FDS ze strany Společnosti

4.12 Další obecné požadavky na DCS/ESD

1. Maximum technologických prvků musí být řízeno DCS. Počet ostatních řídicích systémů typu PLC musí být minimalizován. Případná PLC budou propojena digitální komunikací s DCS pro zadávání či monitorování údajů a všech položek v PLC. Pokud je to technicky možné, komunikace bude typu MODBUS RTU či MODBUS TCP - na Jednotkách Rafinérie Litvínov a Kralupy bude typu jen MODBUS TCP. Řídící a blokovací signály musí být samostatně prodrátované.

2. V ESD musí být realizovány výhradně bezpečnostní a blokovací funkce. Alarmové a blokovací limity ESD budou obsluze výrobny dostupné na obrazovkách DCS. Vykonání bezpečnostních a blokovacích funkcí musí být zcela nezávislé na stavu DCS.

3. Náhradní díly a podpora pro veškeré hardwarové části DCS/ESD musí být dostupné minimálně po dobu 15 let od najetí DCS/ESD.

4. V okamžiku předání DCS/ESD do provozu (po ukončení investiční akce, stavby apod.) musí veškerý software být plně podporovaný od výrobce ještě nejméně tři roky. Cílem tohoto a

předchozího bodu je vyhnout se situaci, kdy nově předaný systém potřebuje okamžitě upgrade, protože skončila podpora některých jeho HW nebo SW částí.

5. DCS/ESD bude navržen ve všech částech HW a SW tak, aby byl za běžného i abnormálního stavu (výpadek výrobny, najetí a sjetí výrobny apod.) vytížen v každé své části (včetně všech komunikací, řídících procesorů, operátorských stanic apod.) maximálně na 70% hodnoty maximálního vytížení doporučeného výrobcem.

6. Před započetím práce na projektové dokumentaci musí proběhnout revize návrhu DCS/ESD včetně přidružených PLC systémů. Cílem revize je nutnost minimalizace celkového počtu řídicích systémů typu DCS/ESD/PLC a optimalizace rozdělení řízení technologických celků mezi jednotlivými řídicími systémy, ať už DCS/ESD či PLC. Důvodem k této optimalizaci je mimo jiné snaha o maximální zefektivnění budoucí údržby všech dodávaných systémů.

7. Časovače v DCS delší než jedna minuta musí mít zobrazen zbývající nebo uběhlý čas na operátorské grafice.

5 Požadavky na systémy PLC

5.1 Úvod

Tato kapitola obsahuje základní požadavky na PLC dodávané do Společnosti. Při výběru pro konkrétní aplikaci je možné dohodnout dílčí specifika odlišná od této normy. Veškeré takové změny musí být konzultovány s ASŘTP a jím schváleny.

Ačkoli jsou požadavky v tomto dokumentu obecné, tedy nejsou určené pro žádný konkrétní PLC systém, kontraktor je musí považovat za specifikaci pro konkrétní nabízený či dodávaný PLC systém.

Dodaný PLC systém musí splňovat veškeré platné technické normy v oblasti napájení, barevného značení, jiskrové bezpečnosti apod.

5.2 Role útvaru ASŘTP

ASŘTP v rámci Společnosti určuje dlouhodobou strategii pořizování a údržby PLC systémů, které má ve své správě. Podílí se na všech investičních akcích či akcích údržby, kde je součástí dodávky PLC systém nebo úpravy ve stávajícím.

ASŘTP je při výběrových řízeních na dodávku PLC a její následné realizaci jediným odborným útvarem, který rozhoduje o technických specifikacích a požadavcích a o tom, zda je nabízený či dodávaný systém splňuje.

5.3 Vendor list

PLC	Siemens řady Simatic S7-1500 včetně I/O modulů
panely	Siemens řady Comfort
zdroje	Siemens, Weidmüller, Phoenix Contact, Axima
UPS	Siemens, APC
PC	Siemens, DELL – vždy v provedení do racku

5.4 Hardware

5.4.1 Kontroléry

- Musí být dodány kontroléry dle vendor listu vhodného typu z hlediska výkonu a spolehlivosti pro danou aplikaci.
- Za běžného i abnormálního stavu (výpadek, najetí a sjetí technologie apod.) musí být vytížení kontrolérů maximálně 80% hodnoty maximálního vytížení doporučeného výrobcem.
- Peer-to-peer komunikace mezi jednotlivými kontroléry musí být minimalizována. Proto všechny signály jedné řízené technologické části či smyčky musí být zavedeny do stejného kontroléru, pokud to samozřejmě není v rozporu s jinými požadavky vyšší priority (rozdělení kvůli redundanci či bezpečnost apod.).

5.4.2 I/O moduly

Použité I/O moduly musí být řady Siemens Simatic S7-1500.

Počty jednotlivých typů vstupů/výstupů budou navrženy s 20% rezervou zapojených I/O, rovnoměrně rozloženou přes všechny kontroléry.

V PLC systému musí být nakonfigurována diagnostická obrazovka s přehledem stavu všech I/O kanálů.

5.4.3 Rozvaděče

Kromě periferií operátorských stanic, umístěných na velínu, musí být všechny prvky PLC systému (zejména kontroléry, I/O moduly, komunikační moduly, servery, operátorské stanice, aktivní síťové prvky, napájecí prvky) umístěny ve vyhrazených průmyslových rozvaděčových skříních splňujících následující požadavky:

- měření teploty uvnitř rozvaděče alarmované a historizované v PLC
- osvětlení, které se rozsvítí po otevření dveří pole
- čidlo otevření dveří alarmované v PLC
- popisky všech I/O signálů přímo na I/O modulech
- klimatizované buď individuálně, nebo v případě klimatizované místnosti vybavené vhodnou ventilací; požadujeme odmontovatelné střešní desky kabinetů
- pokud není stanoveno jinak, musí být umístěné v oddělené místnosti s omezeným přístupem osob splňující veškeré požadavky na teplotu, čistotu, vlhkost a další podmínky vyžadované umístěným zařízením
- v případě umístění rozvaděčů venku, musí být jak skříně, tak jejich vybavení, navrženy na celý rozsah teplot, kterým mohou být vystaveny; musí být také vybaveny vhodnou stříškou proti dešti a sněhu a ventilací, nikoliv však klimatizací

5.4.4 Počítače

- veškerá PC musí být v provedení do racku s montáží včetně vysouvacích lyžin
- všechna PC musí být umístěná v kabinetech, žádné PC nesmí být umístěno v prostoru velínu či dokonce v nábytku operátorských pracovišť (v případě tenkých klientů umístěných v operátorských pracovištích musí být přístup k portům zajištěn v kombinaci SW nebo HW opatřeních)

5.4.5 Operátorské panely

V případě použití operátorských panelů HMI ve venkovních rozvaděčích musí být skříně vybavené dvojitými dveřmi, přičemž panely musí být umístěné na vnitřních dveřích tak, aby nebyly vystaveny venkovním podmínkám.

5.4.6 Napájení, UPS

Veškeré kritické části PLC (kontroléry, I/O moduly, servery, operátorské stanice, síťové prvky) budou napájeny ze dvou nezávislých nepřerušitelných zdrojů. Napájení z těchto dvou zdrojů musí být distribuováno mezi jednotlivá (i nekritická) zařízení tak, aby výpadek jednoho zdroje neomezil schopnost PLC systému řídit technologii.

Napájení procesorů bude vybaveno napájecím buffer modulem (např. SITOP PSE201U obj. č. 6EP1961-3BA01) určeným pro překlenutí krátkodobých výpadků zdroje.

Veškeré poruchy napájení musí být signalizovány a alarmovány v příslušném PLC, jističe budou vybaveny pomocnými kontakty pro zavedení signalizace do PLC.

Napájení musí být dimenzováno tak, aby umožňovalo bezpečné sjetí řízené technologie v případě rozsáhlého výpadku napájení.

5.4.7 KVM extendery, Thin Clients

V případě umístění operátorských pracovišť na velínu a PC operátorských stanic v oddělené místnosti, musí být použit vhodný a spolehlivý systém pro vzdálené připojení klávesnic, displejů a polohovacích zařízení (myší, TrackBall apod.) – KVM extendery, tencí klienti apod.

5.4.8 Klimatizace

Jednotlivé rozvaděče PLC systému nebo celý prostor, kde jsou umístěny, musí být vybaveny vhodnou klimatizací a ventilací tak, aby byly splněny požadavky veškerého instalovaného zařízení na teplotu, vlhkost, čistotu a ostatní parametry prostředí. Klimatizace musí být dostatečně výkonná, aby se minimalizovalo riziko vystavení zařízení nevyhovujícím podmínkám, zejména vysoké teplotě.

Teplota v rozvodně či místnosti s rozváděči PLC bude zavedena do PLC a alarmována. Stejně tak bude do PLC zavedena informace o stavu klimatizační jednotky a případná porucha vyvolá alarm.

5.5 Software

5.5.1 Vývojový SW

Jak program v kontroléru, tak vizualizace na operátorském panelu či operátorském PC se musí konfigurovat v softwaru Siemens „TIA portal“. Konkrétní verze TIA portal bude dohodnuta pro konkrétní akci.

Pro vizualizace na platformě PC musí být použit software Siemens WinCC v rámci TIA portal.

Vývojové licence budou součástí dodávky dle potřeb konkrétní akce.

Podle potřeby bude součástí dodávky také simulační software.

5.5.2 Aplikační software

Aplikační software musí splňovat následující požadavky:

- zdrojový kód musí být čitelný, tzn. FC, FB, OB atd. bloky nesmí být uzamčené
- zdrojový kód musí být důsledně okomentovaný (komentáře bloků, symbolických jmen apod.)
- hlavní řídící funkce ASW musí být vytvořeny v jazyce FBD popř. Ladder Logic

5.5.3 Zálohovací software

Dodaný PLC systém musí být vybaven SW pro zálohování všech počítačů. Tento SW bude nainstalován na všech počítačích, a pokud je to možné, bude centrálně spravovaný z jednoho místa (serveru). Bude umožňovat mimo jiné zálohování celých disků (formou image) na určené úložiště.

5.5.4 Antivirový a antimalware software

- Každý počítač musí být vybaven antivirovým a antimalware SW.
- Antivirový a antimalware SW bude aktualizovat své virové databáze z jednoho společného serveru.
- Licence antivirového a antimalware SW bude platná po dobu nejméně pět let včetně aktualizací virových a malware databází i SW samotného.

5.6 Licence

Všechny části dodávaného PLC systému, pro které se licence dimenzují na počet tagů nebo podobným způsobem, musí být dodány s rezervou 20%.

To se týká zejména následujících licencí:

- samotný systémový SW
- vizualizace WinCC
- veškeré licence vázané na počty I/O
- historizační SW
- zálohovací SW
- antivirový a antimalware SW
- OPC, MODBUS či jiná komunikace

5.7 Dokumentace

5.7.1 Obecné požadavky na dokumentaci

Dokumentace musí být dodaná v PDF i v editovatelném formátu MS Excel, MS Word, DWG apod.

Tabulky, databáze apod. musí být v takovém formátu, který kromě editace umožňuje i vyhledávání, řazení a filtrování, tedy MS Excel, MS Access, INtools/SPI apod.

Pokud je k tvorbě dokumentace použit databázový dokumentační software jako např. Comos, Aveva, PDMS či jakýkoliv jiný podobný software, veškerá dokumentace bude předávána také v nativním formátu softwaru, v němž byla vytvořena, se všemi potřebnými daty nutnými pro zobrazení v prohlížečích kompatibilních s původní aplikací nebo přímo v ní, tj. včetně databází použitých technických dat a s uvedením plných názvů použitých SW aplikací včetně jejich verzí.

5.7.2 Požadované dokumenty

Součástí dodávky PLC systému musí být alespoň následující dokumenty:

5.7.2.1 Protokoly

- protokoly FAT/SAT
- protokoly z testů napájecích zdrojů
- protokoly z testů smyček (loopcheck), testů interlocků, sekvencí, ARC a dalších řídicích struktur

5.7.2.2 Dokumentace PLC

- detailní schéma topologie celého včetně napájení jednotlivých komponent a propojení s dalším zařízením (PLC, MCC, analyzátory apod.)
- I/O list
- výkresy smyček; Na Jednotkách Rafinérie Litvínov a Kralupy jednotlivé tagy musí být založeny do databáze INtools/SPI, výkresy v papírové podobě musí být vytištěny z této databáze
- Control and Safeguarding Narratives s relevantními výstupy z HAZOP či SIL studie (výsledky SIL klasifikace budou zapracovány do on-line SIF pro databáze)
- dokumentace pro komunikaci s ostatními systémy (PLC, analyzátory, jiná DCS apod.) – paměťové mapy, seznamy tagů, konfigurace komunikačních protokolů atd.

- standardní dokumentace výrobce PLC pro HW and SW
- manuál pro operátory
- popis ovládání systémových částí vizualizace – alarmy, historie, trendy apod.
- popis ovládání samotné aplikace pro řízení technologie
- seznam všech dodaných licencí včetně informací o jejich platnosti
- originální instalační média a uživatelské manuály veškerého instalovaného SW
- dokumentace skutečného stavu

- seznam I/O obsahující:

  Analogové smyčky
  - název, popis
  - charakteristika signálu (např. 4-20 mA, odmocněný, neodmocněný,…)
  - rozsah a jednotky měření odpovídající SI soustavě měřených jednotek
  - veškeré hodnoty alarmových limit a parametrů
  - typ a směr regulace vztažný k fyzické pozici ventilu
  - charakteristika a rozsah výstupu
  - pozice ventilu při výpadku energie
  - pozice ventilu při 4 mA
  - inicializační hodnoty
  - umístění položky v P&I schématech
  - přesné určení pozice vstupů a výstupů do/z PLC (periférie)
  - odkaz na logickou případně další řídicí strukturu

  Digitální smyčky
  - název, popis
  - charakteristika signálu (trvalý, momentový,…)
  - význam jednotlivých stavů
  - určení alarmových stavů (případně určení alarmových stavů kombinací signálů) - alarmovým stavem a bezpečným stavem zařízení bude logická 0, koncová poloha ventilů bude indikována logickou 1
  - inicializační hodnoty
  - přesné určení pozice vstupů a výstupů do/z PLC (periférie)
  - odkaz na logickou případně další řídicí strukturu

5.7.2.3 Dokumentace aplikačního software
- regulační obvodová schémata
- schéma rozvodu napájení
- soupis použitého HW PLC
- provozní předpis pro údržbu HW a SW PLC
- popis funkce SW (popis funkce celého programu)
- struktura programu (struktura programu a volání jednotlivých bloků)

- výpis programu (výpis celého programu s popisem jednotlivých segmentů a signálů)
- popis adres SW (kompletní popis všech signálů)
- popisy datablоků a proměnných (kompletní popis všech datawordů včetně jejich hodnot)
- křížové reference SW (návaznosti mezi jednotlivými signály)
- použité bity (kompletní seznam všech bitů použitých v programu)

5.7.2.4 FDS (Functional Design Specification)

FDS musí být vytvořen spoluprací dodavatele Detail Engineeringu a dodavatele PLC systému. Musí obsahovat popis funkcionality všech standardních komponent, zejména:

- PID kontrolér
- ventil, motor
- filozofii operátorských displejů a navigace
- filosofii alarmového systému
- trendy
- bezpečnost

FDS musí obsahovat také detailní specifikaci pro zejména:

- veškeré řízení
- sekvence
- interlocky
- Control and Safeguarding Narratives
- rozhraní
- rozsahy přístrojů
- nastavení hodnot alarmů a tripů
- filosofii náhradních dílů a možností rozšíření PLC

Některé uvedené funkcionality nebo specifikace mohou být součástí projektové dokumentace. Relevantní výstupy z HAZOP či SIL studií musí být v FDS zahrnuty.

5.8 Testování a uvádění do provozu

Kontraktor musí provést testy aplikačního software za účelem ověření jeho shody s FDS.

Kontraktor musí provést ve vhodných fázích realizace testy FAT a SAT týkající se PLC na základě předem odsouhlasených procedur a protokolů dodavatele systému.

Před uvedením výrobny do provozu budou mimo jiné provedeny následující zkoušky:

- FAT – není akceptována on-line forma; procedura musí být provedena za fyzické přítomnosti zástupců Společnosti
- SAT
- Loopcheck – správnost zapojení obvodů a konfigurace v PLC musí být otestována kompletními zkouškami obvodů z pole přes všechny sdružovací skříňky a ranžírovací rozvaděče, případné jiskrové bariéry, I/O moduly, případnou komunikaci mezi PLC a DCS až na operátorské obrazovky DCS. Musí být provedeny a zaznamenány minimálně následující kontroly:
  - kontrola nastavení inženýrských rozsahů

- kontrola pozice ventilů (100% = otevřeno, 0% = zavřeno)
- kontrola stavových signálů
- kontrola alarmových/spínacích/blokovacích limit (včetně prezentace alarmů na obrazovkách DCS)
- kontrola přítomnosti a správnosti jednotlivých signálů na technologických displejích v DCS
- kontrola správnosti komunikace jednotlivých signálů mezi DCS a ESD
- kontrola správnosti digitálních a analogových výstupů přímo na zařízení v poli nebo měřením na svorkách přímo v poli.

6 Obecné požadavky

6.1 Značení položek

Je snaha o sjednocení značení položek měřených obvodů. Značení vychází z norem ČSN ISO 3511-1 až 4. Nutno podotknout, že uvedená norma řeší pouze pojmenování obecných typů položek. Pokud se jedná o obvody se speciálními funkcemi, je nutno jejich značení před implementací v projektu konzultovat s ASŘTP.

Při implementaci systémů DCS/ESD/PLC je stanovena ve Společnosti konvence pro úpravy značení jednotlivých položek. V případě nových aplikací nebo rekonstrukcí je lze zapracovat již do projektu.

Úpravy vycházejí z těchto zásad:

1. respektování všeobecných standardů při značení jednotlivých typů měření
2. eliminace nadbytečných znaků v názvu položek při respektování identity položky
3. jednoznačnost jmen položek pro celou Společnost
4. sdružování položek, kdy se racionalizuje jejich užití a zpřehledňuje jejich funkce

Jelikož se systém tvorby jmen položek (Tagnaming systém) mírně liší na jednotlivých výrobnách, bude součástí zadání každé jednotlivé akce dokument (tagnaming manuál), který tuto problematiku detailně popisuje. Konkrétní řešení musí být vždy konzultováno s oddělením ASŘTP. Na Jednotkách Rafinérie Litvínov a Kralupy se pojmenování tagů a pravidla práce s databází INtools/SPI řídí normou N 00 502.

Pokud si PLC s DCS vyměňují data, pak značení DCS položek pocházejících z PLC musí odpovídat tagnaming zásadám DCS a PLC položky musí mít tagname takový, aby bylo na první pohled jasné, že se jedná o PLC položku, např. jiné číslo AREA, jiný číselný rozsah apod. (např. všechny položky dané výrobny z PLC mají číselný rozsah 800 - 999).

7 Související normy a předpisy

7.1 Obecné

Všechny normy a předpisy platí se všemi dodatky a rozšířeními.

ČSN 33 3051	Ochrany elektrických strojů a rozvodných zařízení
ČSN 33 2000-5-51 ed.3	Elektrické instalace nízkého napětí - Část 5-51: Výběr a stavba elektrických zařízení - Všeobecné předpisy
ČSN IEC/TR 61439-0	Rozváděče nízkého napětí - Část 0: Návod na specifikaci rozváděčů
ČSN 73 0875	Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení
ČSN ISO 3511-1 až 4	Měření, řízení a přístrojové vybavení technologických procesů - Schematické zobrazování
Směrnice EU 2009/125/ES	o stanovení rámce pro určení požadavků na ekodesign energetických spotřebičů
Vyhláška č. 246/2001	o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)
Zákon č. 258/2000 Sb.	o ochraně veřejného zdraví a o změně některých souvisejících zákonů
Nařízení vlády č. 272/2011 Sb.	o ochraně zdraví před nepříznivými účinky hluku a vibrací
Zákon č. 73/2012 Sb.	o látkách, které poškozují ozonovou vrstvu a o fluorovaných skleníkových plynech
Zákon č. 201/2012 Sb.	o ochraně ovzduší
Předpis č. 87/2014 Sb.	kterým se mění zákon č. 201/2012 Sb. o ochraně ovzduší (novelizace)
Zákon č. 360/1992 Sb.,	o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě
Zákon č. 458/2000 Sb.	Energetický zákon
Zákon č. 250/2021 Sb. a NV 194/2022 Sb.	o bezpečnosti práce v souvislosti s provozem vyhrazených technických zařízení, Nařízení vlády o požadavcích na odbornou způsobilost k výkonu činnosti na elektrických zařízeních a na odbornou způsobilost v elektrotechnice
ČSN EN 60079-0 ed.5	Výbušné atmosféry – Část 0: Zařízení – Obecné požadavky
NV č. 101/2005 Sb.	Nařízení vlády o podrobnějších požadavcích na pracoviště a pracovní prostředí
Vyhláška č. 48/1982 Sb.	Vyhláška Českého úřadu bezpečnosti práce, kterou se stanoví základní požadavky k zajištění bezpečnosti práce a technických zařízení

Zákon č. 90/2016 Sb.	Zákon o posuzování shody stanovených výrobků při jejich dodávání na trh
Zákon č. 22/1997 Sb.	Zákon o technických požadavcích na výrobky a o změně a doplnění některých zákonů
NV č. 116/2016 Sb.	Nařízení vlády o posuzování shody zařízení a ochranných systémů určených k použití v prostředí s nebezpečím výbuchu při jejich dodávání na trh
NV č. 117/2016 Sb.	Nařízení vlády o posuzování shody výrobků z hlediska elektromagnetické kompatibility při jejich dodávání
NV č. 118/2016 Sb.	Nařízení vlády o posuzování shody elektrických zařízení určených pro používání v určitých mezích napětí při jejich dodávání na trh

7.2 Vnitropodnikové normy

S 027	Řízení investičních projektů
S 350	Technická dokumentace
S 350/1	Požadavky na výkresovou dokumentaci izometrií potrubních rozvodů
S 350/2	Požadavky na zhotovení schémat toků procesu (PFS) a schémat P&ID
S 350/3	Seznam a struktura hodnot DCC kódu
N 00 502	Zásady pro práci s databází SI
N 11 003	Provoz elektrických strojů
N 11 017	Norma pro provádění zpětných kontrol obvodů Loop check
N 11 006	Pravidla elektrických zařízení
N 11 012	Standardy elektro pro Unipetrol
N 11 022	Standardy zařízení MaR pro UNIPETROL RPA, s.r.o.
N 11 984	Norma pro dodávání technické dokumentace k novým strojům a zařízení

7.3 Mezinárodní standardy

IEC 61131	Standard IEC pro programovatelné kontrolery PLC

IEC 61511	Standard IEC „Functional safety - Safety instrumented systems for the process industry sector“