ZÁKLADNÍ TERMINOLOGIE PRŮMYSLOVÝCH ŘÍDICÍCH SYSTÉMŮ

NÚKIB

Okruhy a témata

On-line kurz má 9 okruhů, které se zaměřují na základní informace z oblasti průmyslových řídicích systémů.

Úvodní informace

Okruh poskytuje úvodní informace ke kurzu, představí jeho obsahové zaměření a seznámí s tím, pro koho je kurz určen a jak s ním pracovat.

Okruhy

Vítejte v našem on-line kurzu!

Kurz, do kterého jste vstoupili, je určen pro IT bezpečnostní pracovníky, kteří se chtějí seznámit se základní terminologií průmyslových řídicích systémů a specifikami kybernetické bezpečnosti těchto systémů.

V kurzu si osvojíte následující schopnosti a znalosti:

- Umět vysvětlit, co je to kritická infrastruktura
- Definovat průmyslový řídicí systém
- Znát nejrozšířenější typy průmyslových řídicích systémů
- Popsat architekturu SCADA a DCS
- Znát rozdíl mezi PLC a HMI
- Vyjmenovat programovací jazyky používané pro PLC
- Znát nejrozšířenější zařízení používané z průmyslových řídicích systémech
- Uvědomovat si rozdíly v IT systémech a průmyslových řídicích systémech
- Seznámit se s problémy aktualizací průmyslových řídicích systémů
- Vyjmenovat nejběžnější metody útoků na průmyslové systémy

Jak pracovat s kurzem?

Kurz Základní terminologie průmyslových řídících systémů poskytuje úvodní vhled do problematiky průmyslových řídících systémů a jejich zabezpečení. Čeká na vás 9 okruhů z nichž každý představuje jeden konkrétní systém.

Celý kurz Vám nezabere více než hodinu. Nemusíte jej absolvovat jednorázově, můžete jím procházet postupně, kdykoliv budete mít čas. **Na absolvování kurzu máte 30 dní od data zápisu.**

Protož se v kurzu budete setkávat s velkým množstvím zkratek, je jeho součástí také výkladový slovník použitých zkratek. Můžete do něj kdykoliv vstoupit.

V případě dotazů nás kontaktujte na vzdelavani@nukib.gov.cz.

Kritická infrastruktura

Kritická infrastruktura (KI) je infrastruktura, která je klíčová pro chod společnosti a ekonomiky. Její ochrana je důležitá, aby nenastala krizová situace, která by mohla mít za následek velké finanční ztráty nebo dokonce ztráty na životech.

KI je součástí Evropské kritické infrastruktury (EKI). Její narušení by mělo závažný dopad na chod států celé Evropské Unie. V České republice je kritická infrastruktura definována podle zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů.

Pro potřeby našeho kurzu je nutné si uvědomit, že kromě KI a EKI existuje ještě také Kritická informační infrastruktura (KII), která je definována v zákoně č. 264/2025 Sb., o kybernetické bezpečnosti. Její narušení by mohlo mít opět za následek velké finanční nebo materiální ztráty či dokonce ztráty na životech.

Průmyslové řídicí systémy

Průmyslové řídicí systémy (Industrial Control Systems = ICS) jsou programovatelné systémy sloužící k ovládání průmyslového technologického procesu v reálném čase. Zahrnují prostředky pro řízení v reálném čase, diagnostiku, služby a další funkce nezbytné pro efektivní a bezpečný provoz automatizačního systému.

Řídicí systém se skládá ze softwaru, který využívá různé hardwarové prostředky jako jsou senzory, manipulační prostředky, síťové prvky, výpočetní technika a dalších zařízení, která jsou navzájem propojená a vzájemně komunikují.

V závislosti na průmyslové oblasti, kde je systém nasazený, má každý průmyslový řídicí systém svá specifika a odlišnosti. Systém může být umístěn na jednom místě (např. řízení výrobního procesu závodu nebo procesu smíchávání směsí v chemické továrně) případně může zabírat velkou geografickou oblast (např. řízení distribuce elektřiny do domácností nebo koordinace vlaků na železničním koridoru).

Průmyslové řídicí systémy a kybernetická bezpečnost

Většina průmyslových řídicích systémů je nasazena v prostředích, kde vysoká dostupnost je naprosto zásadním parametrem. Dříve po dlouhou dobu nebyla kybernetická bezpečnost vnímána jako problém, protože jednotlivé průmyslové řídicí systémy nebyly navzájem propojeny a nacházeli se v bezpečném chráněném prostředí (fyzická bezpečnost dokázala zajistit i bezpečnost kybernetickou). Postupně však do průmyslových řídicích systému začali pronikat IT technologie jako např. vzdálený přístup a síťové technologie. Současně s tím se začali objevovat i zranitelnosti, na které bylo potřeba reagovat. Odstranit tyto zranitelnosti v průmyslovém prostředí je velkou výzvou.

Pokud se vzdáme fyzické bezpečnosti výměnou za vyšší výkon a pohodlí a vyžadujeme-li zachování dostupnosti jako priority, je aplikace standardních opatření vyvinutých pro tradiční IT systémy velmi náročná až nemožná. Je proto potřeba hledat jiné cesty a možnosti.

V informačních systémech je na prvním místě typická snaha o ochranu dat (zajištění jejich důvěrnosti), těsně následovaná integritou a dostupností těchto dat. V angličtině se hovoří o **C-I-A modelu (Confidentiality-Integrity-Availability = Důvěrnost-Integrita-Dostupnost)**. Sice i v některých tradičních IT odvětvích existují případy, kdy jsou rozhodující i integrita a dostupnost (např. převod financí v reálném čase), tak ve většině organizací je nejdůležitější ochrana proti vyzrazení informací.

Jedním z požadavků na KI je vysoká dostupnost služeb této infrastruktury. Mnohdy je vyžadována až pěti devítková dostupnost (99,999 %), protože je třeba, aby služba byla funkční 24 hodin denně, 7 dní v týdnu, 365 dní v roce.

Některé systémy řízení navíc vyžadují výměnu informací v řádu milisekund nebo i méně. Je proto zřejmé proč se oblast řídicích systémů orientuje především na dostupnost a až následně na integritu a důvěrnost **(v angličtině někdy označeno jako model A-I-C)**. Přestože důvěrnost má také význam pro ochranu kritických řídicích systémů, dostupnost a integrita řídícího systému a dat je rozhodující pro fungování průmyslového řídicího systému.

Typy průmyslových systémů

V tomto kurzu budeme pracovat s následujícími druhy průmyslových systémů. Zde je na úvod jejich přehled:

SCADA – Supervisory Control And Data Acquisition – rozsáhlý distribuovaný systém zahrnující měření a regulaci. Často se používá pro přenos a distribuci ropy, plynu, vody a elektřiny. Podrobněji je systém popsán v další kapitole kurzu.

DCS – Distributed Control System – Při řízení se využívají data distribuovaná v reálném čase po celém systému, bez centrálního uzlu. DCS se používají při výrobě energie, rafinaci ropy, čištění odpadních vod a zpracování v chemickém průmyslu. Podrobněji je systém popsán dále v kurzu.

PCS – Process Control System – obecný výraz může zahrnovat různé typy řídících systémů, včetně SCADA a DCS nebo menší řídicí systémy s PLC. Např. ve farmacii, úpravě vody, chemickém a výrobním průmyslu.

EMS – Energy management system – Je systém založený na počítačem podporovaných nástrojích používaných k řízení elektrické rozvodné sítě (monitoring, řízení a optimalizace výkonu výrobního nebo přenosového systému).

AS – Automatizační Systém – Jedná se o systém pro automatizaci (samočinné řízení) technologických zařízení a procesů.

SIS – Safety Instrumented System – Sada hardware a softwarových ovládacích prvků v bezpečnostních systémech kritických systémů. Účelem systému je při chybě bezpečné odstavení zařízení, tak aby se zabránilo jeho poškození nebo zničení. Samotné odstavení se může skládat ze složité sekvence úkonů, které musí být nezbytně dodrženy, aby nedošlo k poškození technického vybavení.

BAS – Building Automation System – Systém Automatizace Budov – Systém pro automatické centralizované řízení HVAC, elektrického osvětlení, stínící techniky, přístupu do místností, bezpečnostních systémů a pod.

HVAC – Heating, Ventilation and Air Conditioning – Systémy topení, ventilace

a klimatizace, které zajišťují kvalitu vzduchu v moderních budovách.

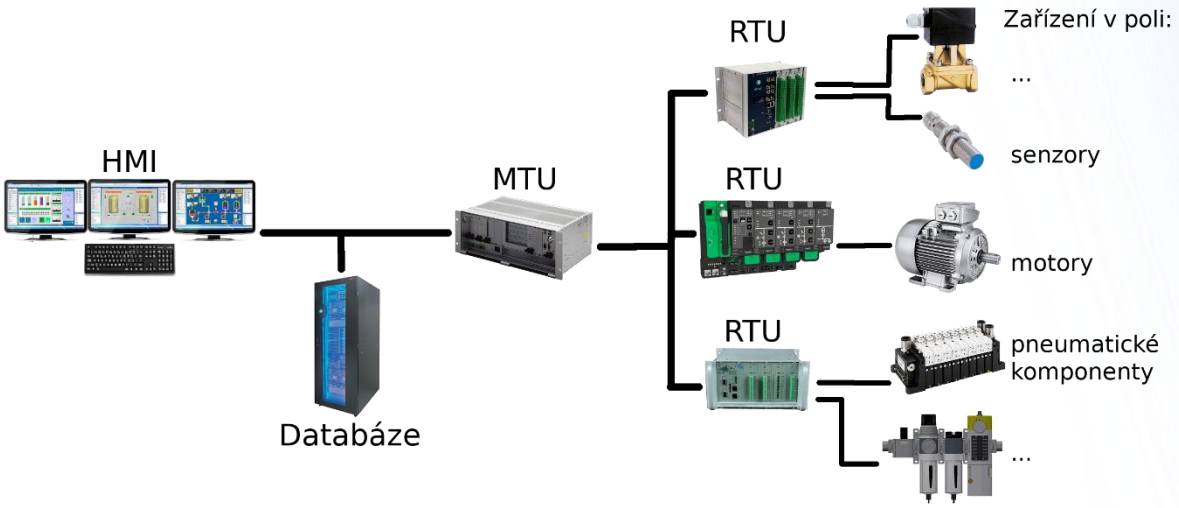
SCADA

Supervisory Control And Data Acquisition

„Dispečerské řízení a sběr dat“ je systém navržený kolem ústřední řídicí jednotky (Master Terminal Unit nebo Central Terminal Unit), která získává data z různých zdrojů (zařízení v poli).

Zdroje dat jsou připojeny do **RTU (Remote Terminal Unit)**. **RTU** přeposílá data od zdrojů do **MTU (Master Terminal Unit)**, které ke své činnosti většinou využívá databázový sever pro uchování všech dat z jednotlivých **RTU**. Data z databáze jsou obsluze (operátorovi) zpřístupňována pomocí **HMI (Human-Machine Interface)**. **HMI** zobrazuje všechny aktuální stavy, které umožňují operátorovi řídit proces.

SCADA je průmyslový systém řízený událostmi – čeká se až událost s nastavenými parametry procesu spustí předepsanou akci. Součástí systému jsou databáze uchovávající hodnoty parametrů. Při výpadku nějaké hodnoty je použita poslední známá hodnota.



Na obrázku výše je znázorněno, jak mohou být jednotlivé komponenty (zdroje dat - např. zařízení v poli, senzory, motory, pneumatické komponenty, aj.) napojeny přes jednotlivé řídící jednotky (RTU) do nadřízené řídící jednotky (MTU). Odsud se data ukládají do databáze a operátorovi jsou přístupná prostřednictvím HMI s grafickým rozhraním.

DCS

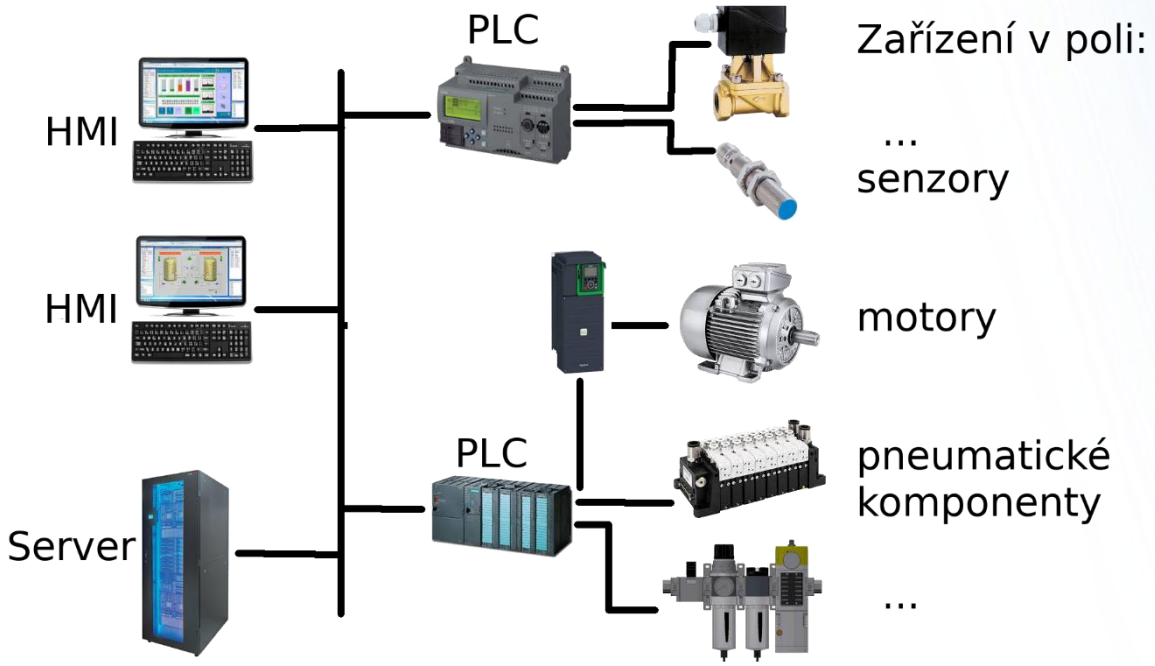
Distributed Control System

Oproti centralizované architektuře **SCADA** jsou řídicí jednotky **DCS** systému rozprostřeny v infrastruktuře.

Každá část infrastruktury má vlastní řídicí jednotky **(RTU)**. Tyto **RTU**, **PLC** a ostatní zařízení jsou řízený pomocí lokálních **HMI**. Stálá komunikace je zajišťována rychlými komunikačními sítěmi nebo sběrnicemi.

DCS pomáhají řídit geograficky rozprostřené a komplexní systémy.

DCS je procesně řízený systém. To znamená, že neustále skenuje proces a výsledky zobrazuje operátorovi (je možný i režim „na vyžádání“). Systém neuchovává data v databázi, operátor je neustále v přímém spojení se zdrojem dat.



PLC

Programmable Logic Controller

PLC mívají modulární koncepci. Skládající se z centrální procesorové jednotky, napájecí jednotky, modulu vstupů, výstupů a komunikačních rozhraní. Například vstupy můžeme rozlišovat na digitální, analogové, enkodérové, pomalé a rychlé atd. Velká variabilita jednotlivých modulů činí **PLC** vysoce přizpůsobitelnými prostředí a úkolu, který mají plnit. Koncová zařízení jsou připojena na vstupy a výstupy **PLC**.

PLC jsou jedny z nejvíce používaných komponent v průmyslové automatizaci na světě.

První **PLC** bylo vytvořeno firmou Modicon (dnes součást Schneider Electric) v roce 1968 pro firmu General Motors. Do té doby bylo řízení prováděno pomocí elektromechanických relé. Logická funkce byla dána vzájemným zapojením relé.

PLC nahradilo rozměrné panely s relé a umožnily inženýrům jednoduše a rychle měnit konfiguraci a časování sekvencí logických akcí. Vznikla tím možnost měnit konfiguraci během několika minut, namísto dnů a týdnů.

PAC – PROGRAMMABLE AUTOMATION CONTROLLER

Jedná se o nová zařízení, která plní obdobné funkce jako PLC, ale mají více paměti, jsou rychlejší a snadněji rozšiřitelné než PLC. Jsou ještě více orientovaná na modulárnost. Na tyto zařízení se lze dívat jako na pokročilá PLC. Rozdíl mezi PLC a PAC není pevně definován. Některá PAC mohou být programována v jazyce C a C++.

PROGRAMOVACÍ JAZYKY PLC

Mezinárodní standard IEC 61131-3 uvádí následující programovací jazyky. Jazyky jsou voleny tak, aby respektovali historický vývoj a zohledňovali různé aplikace využití PLC. Stejně tak mají umožnit programovat PLC i technikům, kteří neznají vyšší programovací jazyky používané ve výpočetní technice.

LD – LADDER DIAGRAM (LAD)

FBD – FUNCTION BLOCK DIAGRAM

ST – STRUCTURED TEXT

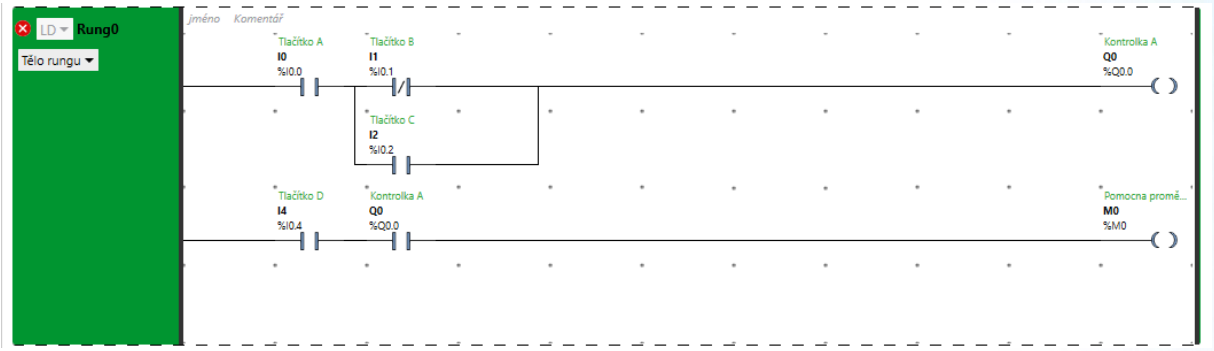
IL – INSTRUCTION LIST

SFC – SEQUENTIAL FUNCTION CHART

Více informací je třeba možno získat na například na [plc-automatizace.cz]

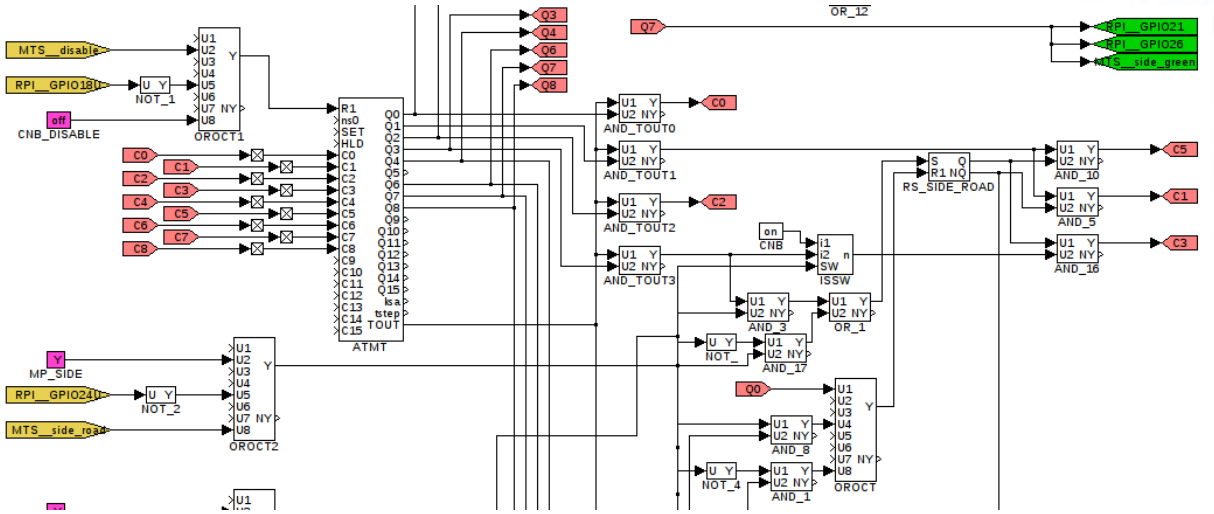
LD – LADDER DIAGRAM

Grafický způsob zápisu vycházející ze struktury schémat zapojení reléových logických obvodů v liniovém provedení (vyskytují se, zde například spínací a zapínací kontakty). Logika čtení signálu je zleva doprava shora dolů.



FBD – FUNCTION BLOCK DIAGRAM

Grafický zápis vycházející ze struktury kreslení schémat zapojení digitálních logických obvodů (integrovaných obvodů). Logika čtení signálu je zleva doprava.



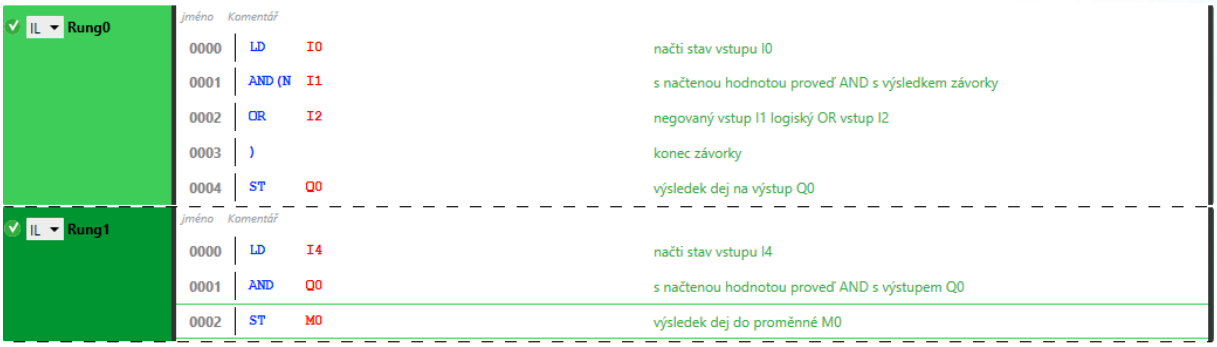
ST – STRUCTURED TEXT

Vyšší programovací jazyk s textovým zápisem. Programování je podobné jako ve strukturovaném programovacím jazyce Pascal.

```
PROGRAM Prepni_vystupy          // podprogram

    VAR_EXTERNAL
        Vstup_0      : BOOL;
        Vstup_1      : BOOL;
        Vystup_0     : BOOL;
        Vystup_1     : BOOL;
    END_VAR
    VAR                 // lokalni pomocne promenne
        Pomocna_0    : BOOL;
    END_VAR

    // zacatek logiky programu
    Pomocna_0 := Vstup_0 AND Vstup_1; // nastavení pomocné proměnné dle hodnot vstupů
    Vystup_1 := Vystup_2 AND NOT Pomocna_0;
    Vystup_2 := (Vystup_1 AND Pomocna_0) OR (Vstup_0 AND NOT Pomocna_0);

END_PROGRAM
```

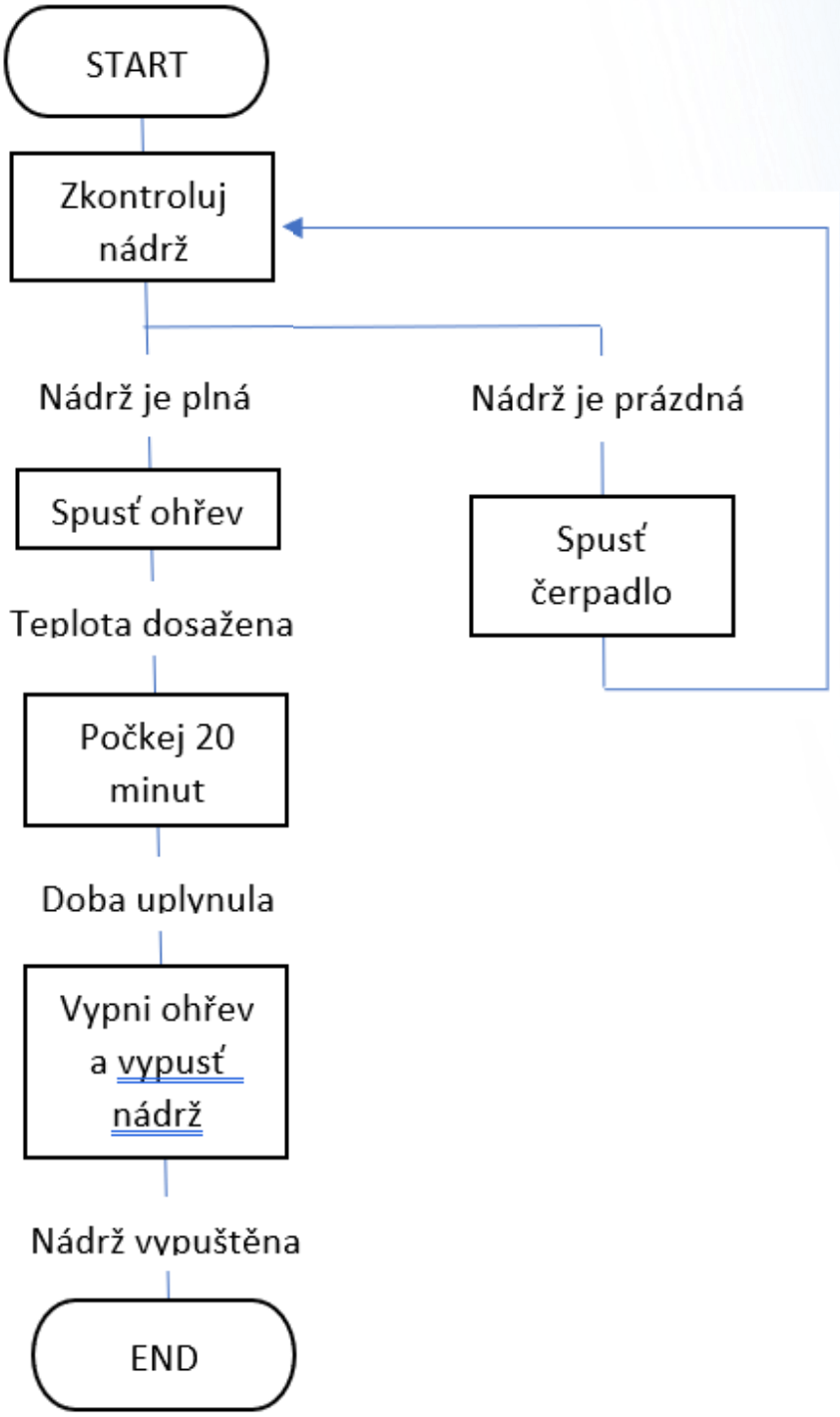
IL – INSTRUCTION LIST

Někdy též STL (Statement list) jedná se o textový zápis programování obdobný jako je zápis programu v JSA (Assembler). Je však univerzální pro všechny procesory používané v PLC různých výrobců nejedná se tedy přímo o kód pro procesor a je nutné ho kompilovat.



SFC – SEQUENTIAL FUNCTION CHART

Grafický zápis – obdoba vývojových diagramů používaných při vývoji software. Vychází z Petriho sítí (Grafcet). Využívá se pro tvorbu složitých sekvenčních programů. Jednotlivé bloky se se skládají z kódů, které mohou být vytvořeny některým z předchozích PLC programovacích jazyků. Umožňuje paralelní zpracování operací.


START
Zkontroluj nádrž
Nádrž je plná
Nádrž je prázdná
Spusť ohřev
Spusť čerpadlo
Teplota dosažena
Počkej 20 minut
Doba uplynula
Vypni ohřev a vypusť nádrž
Nádrž vypuštěna
END

HMI

Human-Machine Interface

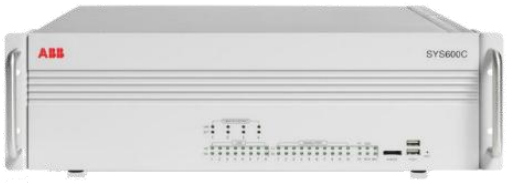
HMI – Rozhraní mezi člověkem a strojem (systémem nebo zařízením), které informuje operátora (obsluhu) o stavu systému nebo procesu a také umožňuje ovládat stav systému nebo procesu. Dříve se jednalo o soustavu kontrolek a tlačítek, která jsou postupně vytlačována počítačovými monitory, klávesnicemi, polohovacími zařízeními a dotykovými displeji. **HMI** samo nic neřídí jen zobrazuje informace z řídicí jednotky anebo naopak informuje řídicí jednotku o akci operátora **(stisku tlačítka)**.

Místo **HMI** se lze setkat i s označeními **Man-Machine Interface (MMI)**, **Operator Interface Terminal (OIT)**, **Local Operator Interface (LOI)** anebo **Operator Terminal (OT)**. Je dobrá nezaměňovat **GUI (Graphical User Interface)** a **HMI**. **HMI** může využívat pro vizualizaci dat **GUI**, ale stejně tak může být rozhraní tvořeno kontrolkami či ručičkovými přístroji bez využití **GUI**.

MTU

Master Terminal Unit

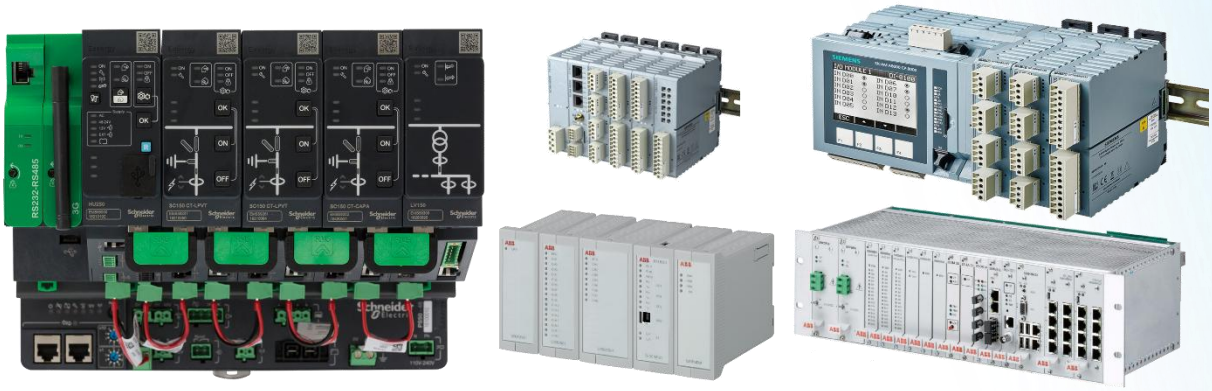
Jednotka obsahující software pro komunikaci s podřízenými jednotkami **(RTU, PLC)** po průmyslové síti. Ve **SCADA systému** může být také nazývána jako **SCADA server**. Aktivně získává informace z podřízených zařízení, navazuje s nimi komunikaci.



RTU

Remote Terminal Unit / Remote Telemetry Unit

Zařízení pro sběr a vyhodnocování dat ze zařízení v poli. Tyto data dále na vyžádání poskytuje nadřazené jednotce. Má síťové, bezdrátové nebo jiné komunikační rozhraní pro komunikaci s nadřazenou jednotkou. Může se jednat i o **PLC** využité jako vzdálená jednotka v poli.



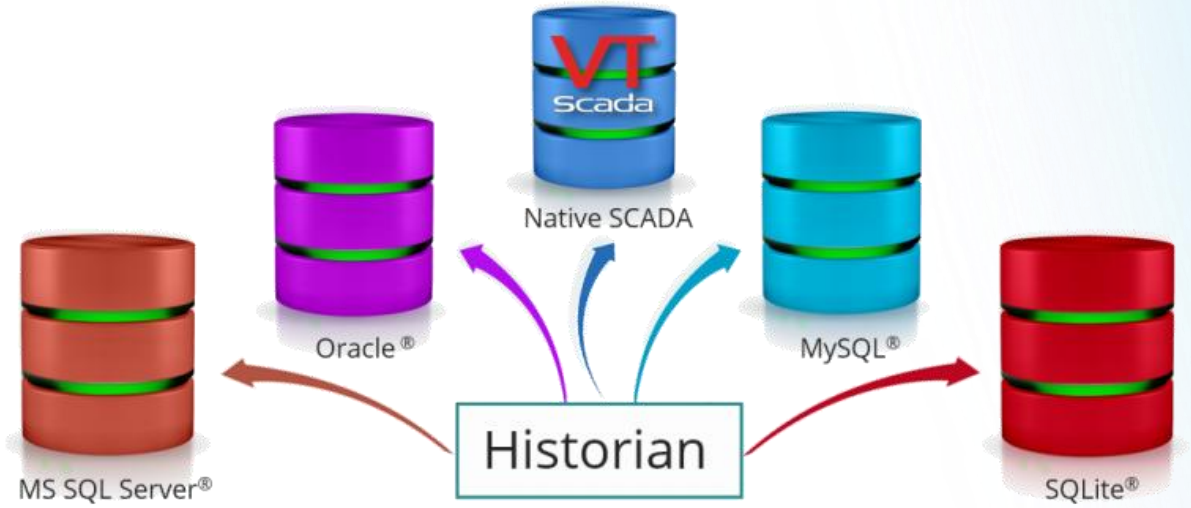
IED

Intelligent Electronic Device

Obecné označení pro zařízení, které je schopné data přijímat z nějakého zdroje nebo odesílat data do jiného zařízení. V praxi to mohou být měřicí jednotky, ochrany pole, digitální relé apod.

Historian

Jedná se **zařízení pro časový záznam stavů systému, stavových proměnných a ostatních významných hodnot řízeného procesu. V současnosti je nejčastěji řešen databázovým serverem.**



Shrnutí & doporučení

Největší rozdíly v IT a průmyslových řídicích systémech

	Informační technologie	Průmyslové řídicí systémy
Délka životního cyklu	do cca 5 let	10 až 30 let
Zařízení	Soudobé technologie s vícevrstvou redundancí	Kombinace historických a nových systémů s omezenou redundancí
Největší problém	Ztráta dat	Ohrožení života, poškození životního prostředí
Poruchovost	Většinou obnova po restartu, restart může vyvolat uživatel	Musí být odolné poruchám, restart může trvat i dny nebo týdny
Aktualizace	Update pravidelné, víceméně bez problémů	Nutno provést odstávku, něco může být nemožné updatovat, technologicky náročné
Změny konfigurace	Možné upravovat, dle aktuálních potřeb	Závislé na dodavateli technologie
Komunikační rozhraní	Sítě TCP/IP	Sériové linky, průmyslové sběrnice, zákaznická řešení, TCP/IP
Nároky na datovou propustnost	Vysoká datová propustnost	Nízká datová propustnost
Nároky na zpoždění komunikace	Zpoždění většinou nevadí	Nezbytné minimální zpoždění – reálný čas
Zranitelnosti	Rozsáhlé databáze signatur a identifikace zranitelností	Omezené množství informací, velké množství zero-day zranitelností na koncových zařízeních

Priority:

Informační technologie	Průmyslové řídicí systémy
1. Utajení dat	1. Bezpečnost obsluhy a technologického procesu
2. Integrita dat	2. Dostupnost dat nutných pro řízení
3. Dostupnost dat	3. Integrita dat
	4. Utajení dat

Doporučení pro průmyslové sítě

1. **Identifikace kritických procesů –** určete co je nejdůležitější, identifikujte kritické procesy jejichž selhání ohrozí společnost nejvíce. Nejprve se věnujte zabezpečení těmto systémům.
2. **Zmapujte celou svou síť –** je nezbytné vědět, co je třeba chránit a jak je to, co chráníme zapojené a navzájem propojené. Shromáždit informace o všech zařízeních průmyslových řídicích systémů (model, typ, verzi firmware, verzi operačního systému), způsob zapojení do sítě, jakým způsobem se informace v síti pohybují a jak se do této sítě připojují interní i externí uživatelé a zařízení. Je nezbytné zmapovat a monitorovat vzdálená připojení dodavatelů technologií.
3. **Identifikujte pravděpodobné cesty útoku –** penetrační testování a modelování hrozeb může pomoci zjistit jakým způsobem se útočníci budou pokoušet dostat do vaší sítě a napadat vaše zařízení.
4. **Zajistěte dobrou „kybernetickou hygienu“ –** minimalizujte množství propojení do Internetu, využívejte dvou-faktorovou autentizaci, kde jen to je možné, neukládejte hesla to prostého textu, pravidelně instalujte opravy a nepovolujte neautorizované externí zařízení v síti průmyslových řídicích systémů.
5. **Vytvořte si zvládnutelný plán upgradů systémů –** aktualizace průmyslových systémů je většinou obtížná, ale i tak je důležitá. Dochází jimi k uzavření široké škály možných útoků. Je třeba naplánovat zodpovědně tak, aby byl plán zvládnutelný. Oddělte a pečlivě monitorujte každý systém, který není možné aktualizovat nebo nahradit novější verzí.
6. **Odstraňte separaci mezi IT a průmyslovými řídicími systémy –** integrujte pracovníky pracovních technologií do SOC a zajistěte, aby IT bezpečnostní týmy spolupracovali s odděleními spravujícími průmyslové systémy na výměně znalostí a vzájemně si pomáhali lépe porozumět požadavkům na zabezpečení systému.

Aktualizace v prostředí SCADA

Co je třeba si uvědomit o aktualizacích v prostředí průmyslových sítí

Aby bylo možné určit jaký vliv mají nově objevené zranitelnosti na váš řídicí průmyslový systém, je třeba mít pečlivě zaznamenaný veškerý používaný software včetně verze produktu a nainstalovaných záplat. U hardware je třeba evidovat typ, model, verze firmware atd. Ideální je dosažení co největší automatizace, kdy systém zprávy aktiv automaticky informuje o všech nových zranitelnostech, které byly objeveny pro váš systém.

O zranitelnostech se můžete dozvědět od výrobce, **ICS-CERTu**, médií nebo upozornění na významné zranitelnosti bývá i na stránkách **NÚKIB**.

Obvykle bývá problém identifikovat, zda se objevená zranitelnost týká i vašeho systému – identifikovat verzi vašeho firmware, které funkce jsou používané a které ne – příklad, pokud se zranitelnost týká webového rozhraní, které máte vypnuté.

Na rozdíl od IT není možné používat automatické aktualizace. Není možné jen tak resetovat průmyslová řídicí systém. **Většina důležitých systémů běží 24 hodin denně, 7 dní v týdnu a není možné přerušit výrobu kvůli instalaci bezpečnostní aktualizace nebo nové verzi firmware.**

Každá oprava nebo aktualizace firmware musí být zkontrolována na kompatibilitu s nainstalovanými aplikacemi a knihovnami. Instalace záplaty nebo aktualizace může vyvolat nechtěný vedlejší efekt jehož důsledkem může být i přerušení výroby. V mnoha provozech aktualizace odpovídá procesu řízení změn (což je dobře) a je třeba, aby byla schválena.

Neexistuje standardizovaný formát publikování aktualizací a záplat. Někteří výrobci je zveřejňují na svých webových stránkách, někteří o nich informují pomocí e-mailu a lze se setkat i s přístupem, kdy instalace záplaty způsobí zánik záruky.

Je žádoucí mít vytvořený proces pro stanovení významu aktualizace, její kompatibility a určení času, který bude zavedení aktualizace vyžadovat. Stejně tak je nezbytné mít definováno postupy pro testování aktualizací, jejich nasazování, případný návrat k předchozí verzi a kontrolu systémů po provedení aktualizací. Ideální je mít na testování aktualizací vyčleněný zvláštní testovací systém, bohužel to není ve většině případů možné pro příliš vysoké náklady na vybudování tohoto systému. Při tvorbě plánů aktualizačních procesů je možné se inspirovat například **normou IEC 62443-2-3** nebo starším **doporučením Recommended Practice for Patch Management of Control Systems (DHS)**.

Aktualizace patří k nejvíce nákladným opatřením kybernetické bezpečnosti v průmyslových řídicích systémech, protože většinou vlastní technické oddělení nemá dostatek prostředků a znalostí pro provedení aktualizací je třeba využít dodavatele. Bohužel se jedná také o opakující se nikdy nekončicí činnost. Nové zranitelnosti se objevují každý týden. Mnoho provozovatelů proto aktualizace důsledně plánuje a provádí je jednou nebo dvakrát ročně, protože častěji to pro ně není možné zrealizovat.

Pokud uvažujeme dobu života průmyslových zařízení kolem 15 let je třeba si uvědomit postupné zastarávání použitých prostředků, zejména IT. 15 let je například pro operační systém velmi dlouhá doba a mnoho těchto systémů, přestane postupně být podporováno. Přeinstalace operačního systému sebou nese spoustu problémů. Je nezbytné ověřit, zda všechny používané softwarové prostředky jsou na novém operačním systému podporovány, zda jejich aktualizace jsou zdarma, zda nebudou vyžadovat

silnější hardware a zda jsou konfigurační soubory nových verzí software navzájem kompatibilní, proto je údržba průmyslových systémů v aktualizovaném stavu opravdovou výzvou.

Také je třeba si uvědomit, že samotné aktualizace nezajistí bezpečnost vašeho průmyslového řídicího systému. Je třeba i uvědomit, že spousta průmyslových komunikačních protokolů nebyla navržena s ohledem na kybernetickou bezpečnost a neumožňuje spolehlivou autentizaci účastníků komunikace. Pokud tedy získá útočník přístup k síťovým prostředkům nebude mu nic bránit v jeho činnosti. Problémem velkého množství zejména starších zařízení je náchylnost na přetížení svého komunikačního rozhraní. Většinou pro útok typu **DoS** stačí obyčejný **NMAP**. Velkým problémem bývají webové servery umístěné na **PLC**, které otevírají další možností útoků jako je například **cross-site scripting**.

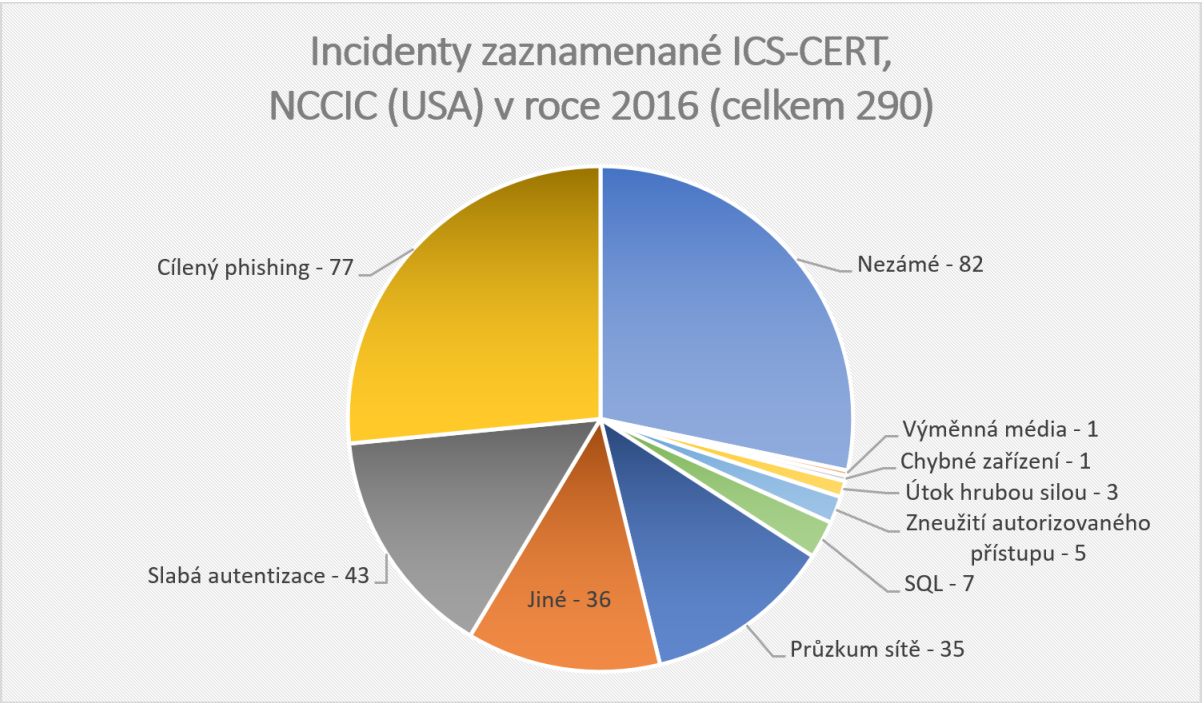
Situaci nelze zjednodušit na prohlášení, že aktualizace se nevyplatí pro špatný poměr cena/výkon, ale je třeba postupovat systematicky a zaměřit se na nejdůležitější části systému a snažit se modernizovat zařízení využívající zastaralé mechanizmy. Je vhodné upřednostnit aktualizace nejvíce exponovaných systémů jako jsou systémy umístěné v **DMZ**, **JUMP servery a firewally.** Jelikož jsou toto především IT systémy lze očekávat, že jejich aktualizace nebudou mít tak drastické nároky na testování a tedy i čas.

Je vhodné vytvořit si standardizované konfigurace a referenční architektury a snažit se je využívat, všude, kde je to možné. Například využijte stejnou konfiguraci pro inženýrské stanice, **HMI** a operátorské stanice. Rozšířením těchto standardizovaných stanic dojde k usnadnění následného testování aktualizací a záplat, nebude již třeba testovat tolik různých variant systémů.

Blokujte nepotřebné programy a funkce – proveďte hardening. Je výhodnější blokovat nebo odinstalovat nepotřebnou službu než ji muset udržovat neustále aktuální.

Všude, kde je to možné, využívejte whitelisting, tím sice nedojde k odstranění zranitelností systému, ale výrazně se omezí možnosti útočníka, zmenší se mu škála použitelných nástrojů.

Incidenty v ICS



Z grafu je patrné, že e-mailový phishing je velmi populární pro získání přístupu do průmyslových systémů a je nutné být velmi obezřetný při mailové komunikaci. Stejně tak je třeba nepodceňovat sílu autentizace osob přistupujících k průmyslovým systémům.

Slovník použitých zkratek a pojmů

AS
Automatizační systém – systém pro automatizaci (samočinné řízení) technologických zařízení a procesů.

BAS
Building Automation System – systém automatizace budov. Systém pro automatické centralizované řízení HVAC, elektrického osvětlení, stínicí techniky, přístupu do místností, bezpečnostních systémů apod.

DCS
Distributed Control System – při řízení se využívají data distribuovaná v reálném čase po celém systému, bez centrálního uzlu. Používá se při výrobě energie, rafinaci ropy, čištění odpadních vod a v chemickém průmyslu.

EMS
Energy Management System – systém založený na počítačem podporovaných nástrojích používaných k řízení elektrické rozvodné sítě (monitoring, řízení a optimalizace výkonu výrobního nebo přenosového systému).

FBD
Function Block Diagram – grafický způsob programování, založený na funkčních blocích a jejich vzájemném propojení.

Historian
Zařízení nebo systém pro časový záznam stavů systému, stavových proměnných a dalších významných hodnot řízeného procesu. Nejčastěji realizován jako databázový server.

HMI
Human-Machine Interface – rozhraní mezi člověkem a strojem (systémem nebo zařízením), které informuje operátora o stavu systému nebo procesu a umožňuje ovládání.

HVAC
Heating, Ventilation and Air Conditioning – systémy topení, ventilace a klimatizace, které zajišťují kvalitu vzduchu v moderních budovách.

IED
Intelligent Electronic Device – inteligentní elektronické zařízení schopné přijímat data ze zdroje nebo odesílat data do jiného zařízení (např. měřicí jednotky, ochrany pole, digitální relé).

IL
Instruction List – textový programovací jazyk pro PLC podobný assembleru.

KI
Kritická infrastruktura – infrastruktura klíčová pro chod společnosti a ekonomiky; její narušení může mít závažné dopady včetně finančních ztrát a ohrožení života.

KII
Kritická informační infrastruktura – informační systémy a sítě, jejichž narušení může způsobit velké finanční či materiální škody nebo ohrožení života.

LD
Ladder Diagram – jazyk pro programování PLC inspirovaný reléovými schématy, grafický zápis logických obvodů.

MTU
Master Terminal Unit – nadřazená řídicí jednotka obsahující software pro komunikaci s podřízenými jednotkami (RTU, PLC) po průmyslové síti. V SCADA systému často plní roli SCADA serveru.

PAC
Programmable Automation Controller – programovatelný automatizační kontrolér. Pokročilejší zařízení než PLC, s větší pamětí, vyšší rychlostí a lepší rozšiřitelností.

PCS
Process Control System – procesní řídicí systém. Obecný výraz, který může zahrnovat různé typy řídicích systémů, včetně SCADA, DCS a menších systémů s PLC (např. ve farmacii, úpravě vody, chemickém a výrobním průmyslu).

PLC
Programmable Logic Controller – programovatelný logický automat používaný pro řízení technologických procesů, často s modulární koncepcí (CPU, vstupy, výstupy, komunikace).

RTU
Remote Terminal Unit / Remote Telemetry Unit – vzdálená jednotka pro sběr a vyhodnocování dat ze zařízení v poli, která tato data poskytuje nadřazené jednotce.

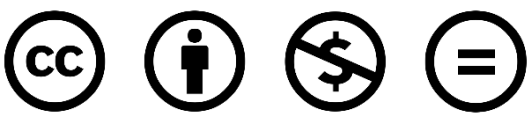
SCADA
Supervisory Control And Data Acquisition – rozsáhlý distribuovaný systém zahrnující měření a regulaci. Často se používá pro přenos a distribuci ropy, plynu, vody a elektřiny.

SFC
Sequential Function Chart – sekvenční funkční diagram. Grafický jazyk pro popis sekvenčních procesů, inspirovaný vývojovými diagramy a Petriho sítěmi.

Licence, autorství, kontakt

Obsahovým garantem těchto webových stránek je vládní CERT.

Obsah je publikován s licencí CC:



V případě dotazů nás kontaktujte na vzdelavani@nukib.gov.cz.