Průmyslová bezpečnost OT

Přemysl Šrámek[1]

Anotace

Předmětem článku je nastínění základů průmyslové bezpečnosti OT vč. legislativního ukotvení a uvedení vybraných metodik. Článek dále konkretizuje jednotlivé typy OT zařízení a používaných protokolů.

Abstract

The aim of this article is to find the base of industrial OT security, including legislative anchoring and introduction of selected methodologies. The article further specifies the different types of OT devices and protocols used.

Klíčová slova

Kybernetická bezpečnost, OT (operational technology), primární referenční architektura, průmyslová bezpečnost.

Keywords

Cyber security, OT (operational technology), PERA (Purdue Enterprise Reference Architecture), industrial security.

Úvod

Jedním ze základních pilířů provozování dráhy a drážní dopravy je bezpečnost systému provozování dráhy a drážní dopravy jako celku. Jednotlivé aspekty tohoto celku jsou velmi často komplexními procesy, které vyžadují multikriteriální způsob hodnocení. Jedním z těchto aspektů je i kybernetická bezpečnost, která v drážním prostředí velmi úzce souvisí s průmyslovou bezpečností, resp. zabezpečením tzv. OT (operational technology).

1. Legislativa

Mezi hlavní poznávací znaky OT prvků patří, že řídí, resp. jsou zapojeny do řídícího procesu spojeného s fyzickým světem (např. senzory v kolejišti). Takto mohou být řízeny všechny typy procesů, tedy procesy kontinuální, diskrétní, dávkové, ale i jejich kombinace představující procesy hybridní. Základní legislativou pro kybernetickou bezpečnost OT prvků v ČR je vyhláška č.82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), konkrétně její § 28 Průmyslové, řídicí a obdobné specifické systémy, která požaduje po povinné osobě následující:

a) použití technických a programových prostředků, které jsou určeny do specifického prostředí,

[1] Ing. Přemysl Šrámek, Ph.D., CISA, odbor interního auditu, Správa železnic, státní organizace

b) omezení fyzického přístupu k zařízením těchto systémů a ke komunikační síti,
c) vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury,
d) omezení a řízení vzdáleného přístupu k těmto systémům,
e) ochranu jednotlivých technických aktiv těchto systémů před využitím známých zranitelností a
f) obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu (1).

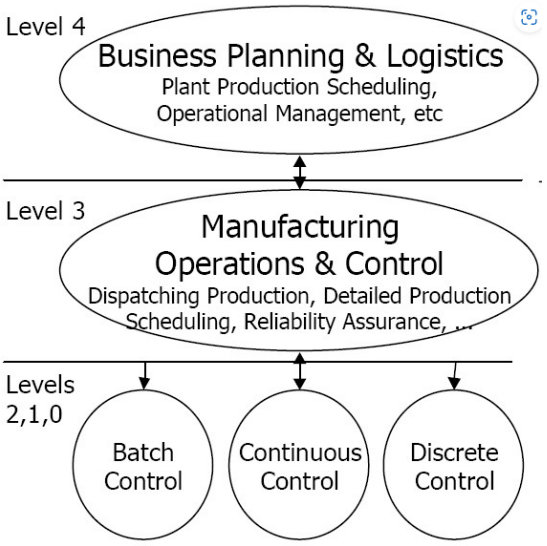
Pro implementaci výše uvedených ustanovení je dále vhodné blíže stanovit, resp. konkretizovat tzv. primární referenční architekturu.

2. Primární referenční architektura

Primární referenční architektura používaná pro OT systémy je např. Purdue Enterprise Reference Architecture (PERA). Tato architektura rozděluje systémy a prvky do celkem 5 vrstev – viz Tabulka 1 (1) a Obr. 2. Větší detail k problematice PERA rozvádějí standardy uvedené v rámci PERA Enterprise Integration Web Site (2).

Tabulka 1 – Jednotlivé vrstvy PERA architektury (1)

Vrstva	Přiřazené systémy / prvky
L4	IT síť organizace
L3	OT síť, systémy celkového dohledu a řízení
L2	Ovládací a dohledové systémy pro dílčí procesy
L1	Řídící systémy dílčích procesů
L0	Akční prvky a senzory dílčích procesů



Obr. 1: Purdue Enterprise Reference Architecture (3)

V tabulce 2 jsou dále uvedeny vybrané OT systémy a jejich prvky s jejich obvyklým umístěním v rámci PERA (OT je obecně zařazeno do vrstev L0-L3 PERA). Některé

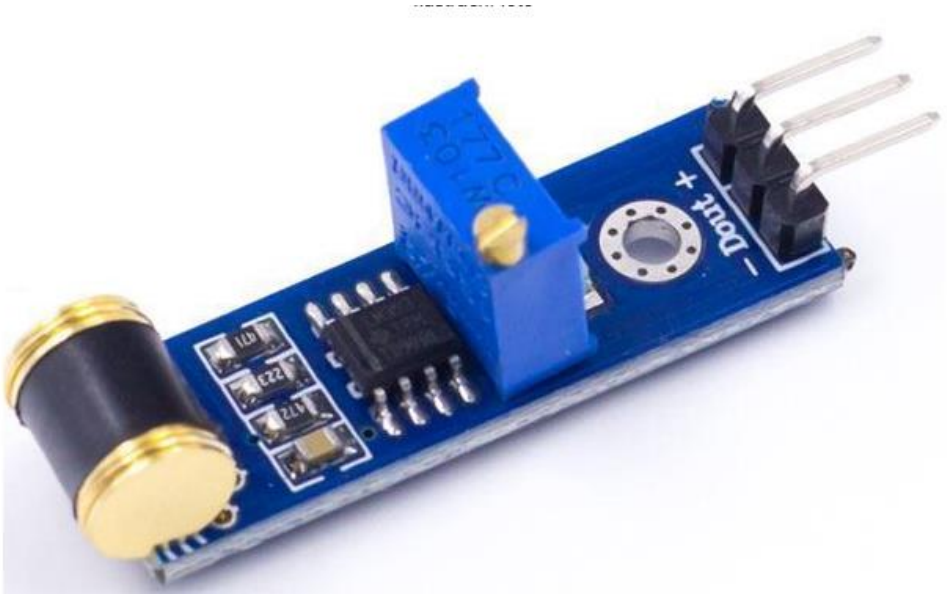
z prvků mohou být zařazeny i do více vrstev této architektury (mohou v konkrétních případech sloužit lehce k rozdílným účelům). (1)

Tabulka 2 – Vybrané OT systémy a jejich umístění v rámci PERA (1)

Vrstva	OT systém
L3	SCADA, Data historiany, Operátorské a inženýrské stanice
L2	DCS, HMI, Operátorské a inženýrské stanice
L1	Chytré akční prvky a senzory, DCS, PLC, RTU, SIS
L0	Akční prvky a senzory (vč. chytrých)

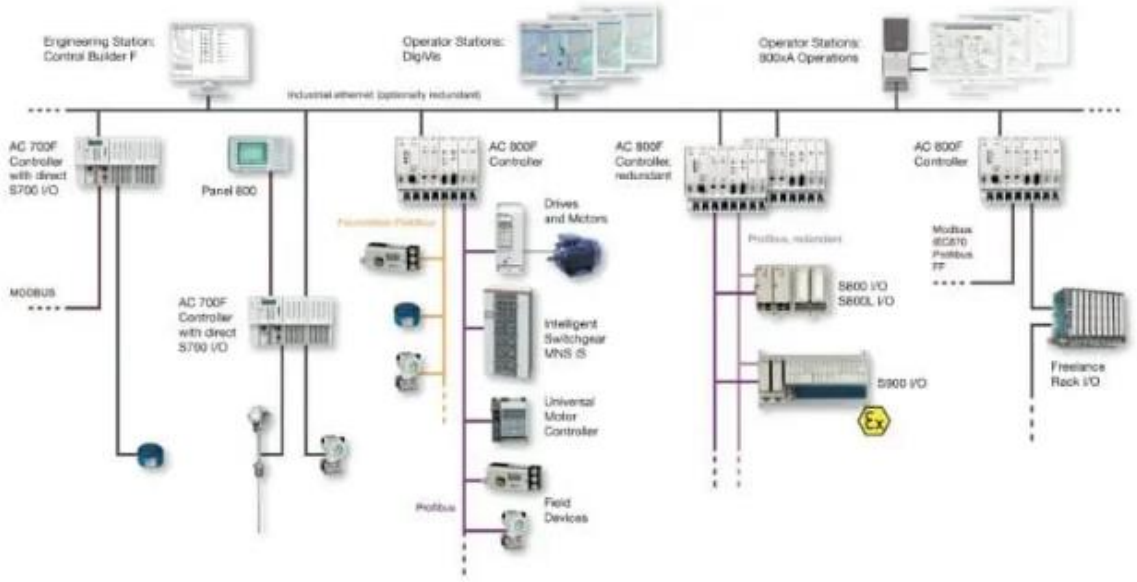
Jednotlivé OT systémy z tabulky 2 jsou dále stručně popsány níže (1), a to vč. vyobrazení:

- PLC – programovatelný logický kontrolér – programovatelný čip, řídící průmyslové a specifické procesy, komunikující prostřednictvím specifických (průmyslových) protokolů,



Obr. 2: PLC – snímač vibrací / otřesů (4)

- DCS (Distributed Control System) – průmyslový řídící systém s distribuovanou architekturou, integrovaným řízením a monitoringem, určený pro kompletní řízení kontinuálních procesů prostřednictvím proprietárních komunikačních protokolů. Je orientován na řízení procesů (rozdíl oproti SCADA, který je orientován především datově – sběr a řízení dat),

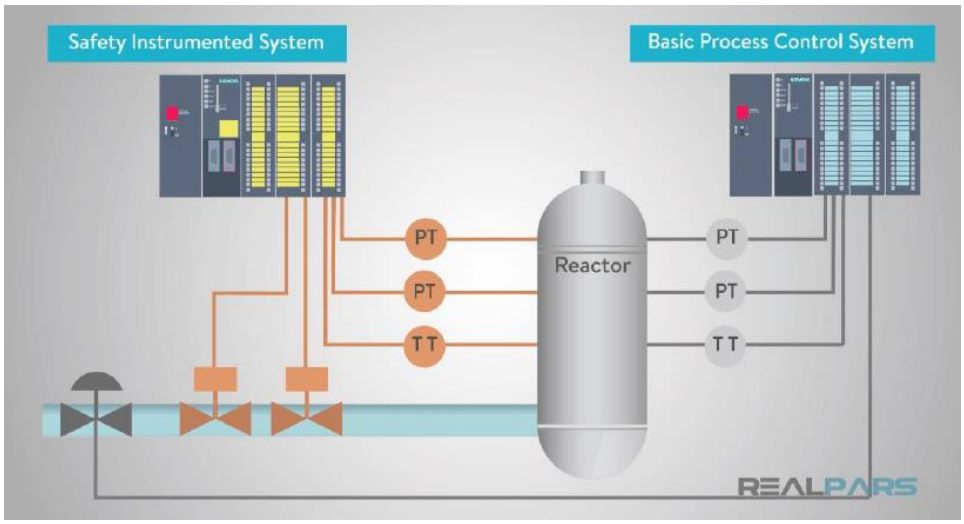


Obr. 3: DCS (5)

- RTU (Remote Terminal Unit) – průmyslový PC, instalovaný v geograficky oddělených lokalitách (od centrálního řídícího systému) za účelem monitoringu a ovládání lokálních akčních prvků a senzorů, komunikující prostřednictvím specifických (průmyslových) protokolů, připojený vzdáleně (optickým či metalickým vedením, rádiovým signálem),

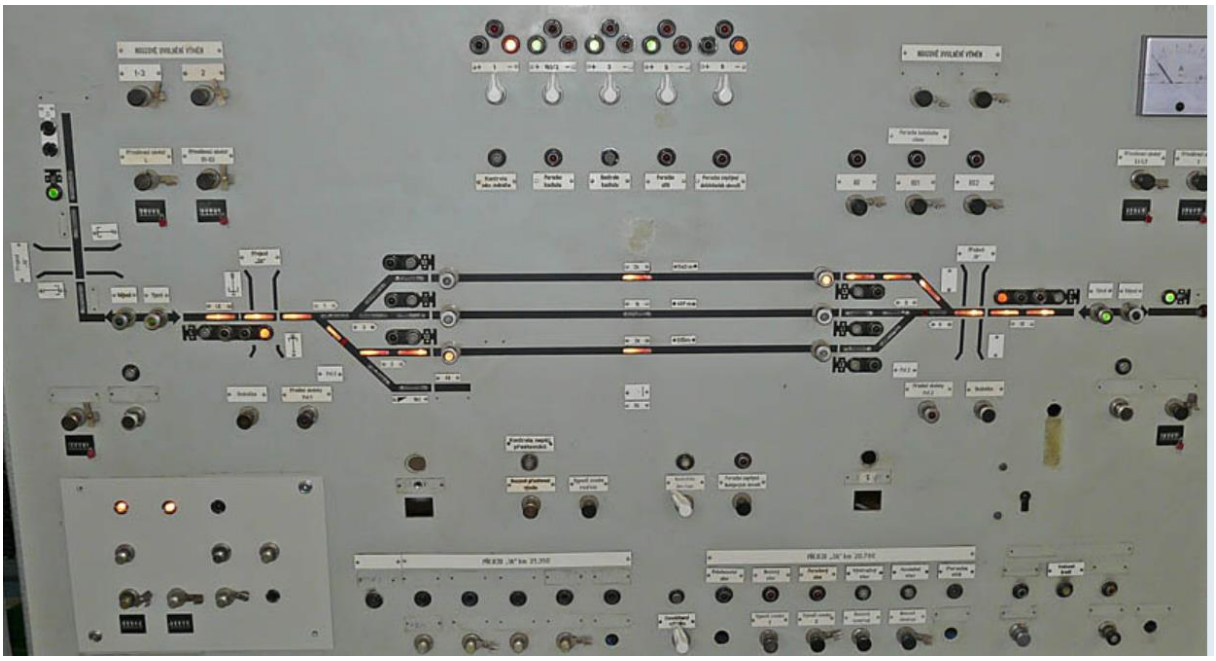
Obr. 4: RTU (6)

- SIS (Safety Instrumented System) – nezávislý bezpečnostní systém specifických (průmyslových) prostředí, chránící vysoce kritické procesy prostřednictvím jejich dodatečné kontroly s možností automatického zastavení při výskytu nebezpečných stavů (např. systém pro měření lomu kolejí, systém kontrolující postavení vlakové cesty a stav výhybkových přestavníků),



Obr. 5: SIS (1)

- HMI (Human Machine Interface) – interakční rozhraní pro ovládání a monitoring jednotlivých dílčích procesů (např. ovládací pulty zabezpečovacího zařízení, přenosný tablet pro diagnostiku tratě),



Obr. 6: HMI (7)

- SCADA (Supervisory Control And Data Acquisition) – systém sběru a vyhodnocování dat vč. grafického interakčního rozhraní pro ovládání a monitoring komplexních lokálních i geograficky distribuovaných procesů (např. sběr meteorologických jevů od meteostanic, servery, které zpracovávají data a linky a přenosové části, měření otřesů náprav a celkový systém pro vyhodnocení – technické zařízení i SW),

Obr. 7: SCADA (8)

- Data Historian – centralizovaný log management nástroj (sběr, uchovávání a práce s daty specifických (průmyslových) systémů),

Obr. 8: Data historian (9)

- Operátorské a inženýrské stanice – pro řízení a monitoring procesů (operátorské), pro konfiguraci a správu (inženýrské) – především inženýrské stanice jsou z pohledu zabezpečení extrémně citlivé (1).

Obr. 9: Operátorská (inženýrská) stanice (9)

OT systémy a prvky, uvedené v kapitole výše, mezi sebou komunikují prostřednictvím velmi specifických (průmyslových) protokolů – ty nejčastěji využívané jsou uvedeny níže:

- MODBUS (bez bezpečnostních mechanismů, možnost rozšíření MODBUS/TCP Security),
- OPC DA (nativně suboptimální úroveň bezpečnosti díky DCOM, problematický z pohledu nutnosti konfigurací ACL na FW),
- OPC UA (nativně využívá autentizovaná a šifrovaná spojení),
- IEC 60870-5_104 (IEC 104) – bez bezpečnostních mechanismů, možnost bezpečnostního rozšíření dle standardu IEC 62351,
- EIBnet/IP, KNXnet/IP (bezpečnostní rozšíření EIBsec),
- Lantronix Discovery Protocol (defaultně slabý, ale s podporou bezpečnostních mechanismů),
- S7comm (protokol firmy Siemens pro PLC),
- BACnet/IP (bezpečnostní rozšíření BACnet/SC),
- DNP3 (bezpečnostní mechanismy a rozšíření různého rozsahu dle standardu IEC 62351). (1)

3. Zabezpečení specifických (průmyslových) systémů

Specifická (průmyslová) prostředí se často potýkají s následujícími problémy:

- dlouhé životní cykly použitých zařízení a technologií s omezenou možností skenování zranitelností a omezeným patchováním,
- proprietární uzamčení od dodavatele příslušných systémů (vendor lock-in), vedoucí k nehospodárnosti jejich provozování,
- zastaralé operační systémy i na přilehlých IT prvcích (z důvodu zajištění kompatibility),
- velmi omezená možnost zásahu do stávající OT infrastruktury (nutnost přezkoušení, akceptačních testů),
- komunikace na bázi specifických protokolů (často bez bezpečnostních mechanismů, proprietární protokoly či sériové protokoly přenášené přes Ethernet/TCP IP).

Pro zajištění průmyslové bezpečnosti a určitou mitigaci problémů, uvedených výše, lze využít např. následující přístupy:

- CIA triáda – jedná se o klasické zajišťování důvěrnosti (C), integrity (I) a dostupnosti (A), pro zabezpečení OT není ale dostačující,
- Parkerovská hexáda – jedná se o rozšíření CIA přístupu o možnost kontroly, autenticitu systému a jeho „užitečnost“ (utility),
- RAMS – jedná se o kombinaci spolehlivosti (R), dostupnosti (A), udržovatelnosti (M) a bezpečnosti (S – zde ale Safety). Je možná např. i kombinace s CIA triádou výše,
- IEC 62443 – obsahuje nad rámec CIA triády 7 základních požadavků – řízení identifikace a autentizace, kontrolu používání, systémovou a datovou integritu, důvěrnost dat, omezení toku dat, včasnou odpověď na událost, dostupnost zdrojů.

Současně je možné pro zajištění průmyslové bezpečnosti v OT definovat 5 esenciálních bezpečnostních oblastí:

- obranyschopná architektura – podporuje viditelnost v síti, identifikaci jednotlivých zařízení, sběr logů a segmentaci vč. využívání demilitarizovaných zón,
- zvládání bezpečnostních incidentů – na základě jednotlivých operací a procesů vytvořený plán zvládání incidentů vč. plánů obnovy (a pravidelných cvičení),
- monitoring sítí – kontinuální bezpečnostní monitoring (vč. monitoringu viditelnosti sítě),
- zabezpečený vzdálený přístup – využití maximální použitelné míry zabezpečení (vícefaktorové autentizace, jump servery apod.),
- řízení zranitelností na bázi rizik – nastavení odpovídajících kontrol zabezpečení vč. procesu patchování a mitigace případného dopadu zranitelnosti (10).

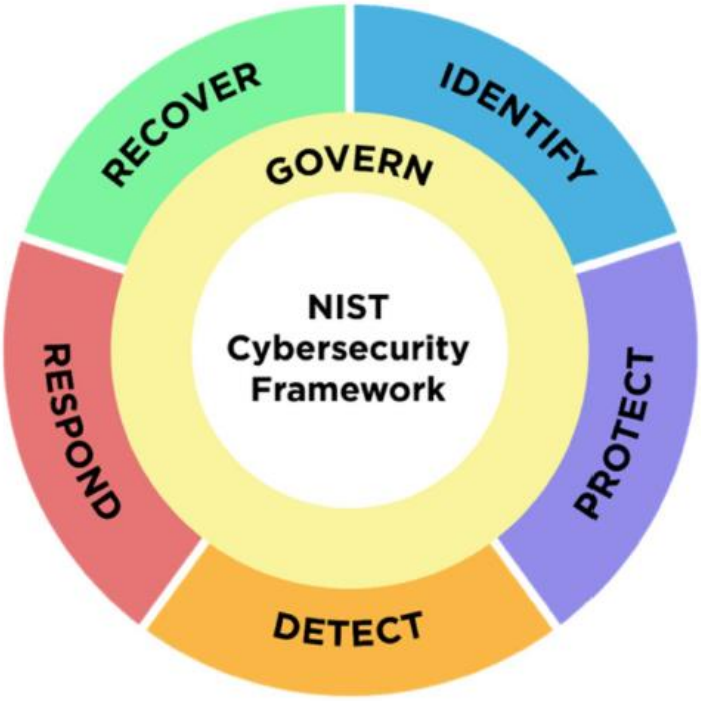
Výše uvedené bezpečnostní oblasti technického charakteru je dále vhodné doplnit organizačními opatřeními vč. zvyšování bezpečnostního povědomí zaměstnanců.

4. Řízení kybernetické bezpečnosti v OT

Řídit kybernetickou bezpečnost, a to nejen v OT, je nezbytné vždy systematicky, a to na základě dokumentu, který schválilo a vzalo za své vrcholové vedení organizace. Tímto dokumentem může být např. strategie kybernetické bezpečnosti organizace či koncepce zabezpečení OT prostředí. Tyto dokumenty mohou být sepsány na základě různých bezpečnostních metodik, vždy by měly ale obsahovat obdobná elementární ustanovení, resp. harmonogram jednotlivých procesů. Níže jsou uvedeny jednotlivé prvky programu kybernetické bezpečnosti dle rámce NIST, konkrétně NIST SP 800-82 (11) – program kybernetické bezpečnosti OT by měl zahrnovat:

- stanovení governance pro kybernetickou bezpečnost OT,
- ustanovení a vycvičení (školení a potřebná praxe) multioborového týmu pro implementaci kybernetické bezpečnosti OT,
- definici strategie / koncepce kybernetické bezpečnosti OT,
- definici specifických politik a procedur pro kybernetickou bezpečnost OT,
- zvyšování bezpečnostního povědomí jednotlivých bezpečnostních rolí vč. uživatelů v oblasti zabezpečení OT (opakovaná aktualizovaná školení),
- implementaci rámce řízení rizik specifického pro OT (vč. hrozeb a zranitelností),
- vytvoření kontinuální schopnosti organizace kontrolovat údržbu a provozování OT, reagovat adekvátně na bezpečnostní incidenty vč. schopnosti zajištění obnovy.

Dalším ze základních předpokladů řízení kybernetické bezpečnosti OT je nutnost kontinuálního zlepšování, pro které je nejčastěji používán Demingův (PDCA) cyklus – jedna z jeho modifikací je na Obr. 10.



Obr.: 10: Bezpečnostní rámec a kontinuální zlepšování (1)

Pro zabezpečení OT prostředí platí také pravidlo security vs. safety, kdy ochrana zdraví a života osob (safety) má vždy přednost před kybernetickou bezpečností (security). V rámci implementace zabezpečení OT to např. znamená aplikaci kompenzačních bezpečnostních opatření pro procesy, u kterých z objektivních důvodů nebylo možné použít předepsané bezpečnostní opatření (vždy ale musí být zdokumentováno). Pro vytvoření obranyschopné architektury OT a zmenšení případného rizikového interakčního povrchu platí také (stejně jako pro kybernetickou bezpečnost obecně) nutnost k nastaveným procesům a technickým opatřením vždy disponovat proškoleným, kompetentním a loajálním personálem (1).

Závěr

Průmyslová bezpečnost OT je jedním ze základních prvků kybernetické bezpečnosti, umožňujícím manažerovi železniční infrastruktury bezpečné provozování dráhy. Specifická prostředí a systémy je více než kdy dříve potřeba systematicky bránit a chránit, neboť útočníci vyvíjejí stále větší snahu tato prostředí kompromitovat. Především v případě útočníků podporovaných státem je cílem kompromitace OT prostředí ochromení běžného života občanů napadeného státu.
Zabezpečení OT prostředí jako takové je velmi komplexní disciplínou, na které musí mít zájem celá organizace vč. jejího vrcholového vedení. Náklady na zabezpečení OT se mohou sice jevit jako vysoké, ale odůvodnitelné, protože vedou k ochraně základních procesů provozovatele dráhy.

Literatura

[1] Nettles Consulting. Bezpečnost průmyslových a specifických systémů a prostředí. Školení pro Správu železnic, 06/2024.
[2] PERA Enterprise Integration Web Site [online]. 2024 [cit. 2024-10-08]. Dostupné z: https://www.pera.net/
[3] PERA Decision-making and control hierarchy [online]. 2024 [cit. 2024-08-28]. Dostupné z: https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture#/media/File:PERA_Decision-making_and_control_hierarchy.jpg
[4] Snímač vibrací / otřesů – modul 801S [online]. 2024 [cit. 2024-10-08]. Dostupné z: https://www.hadex.cz/m478a-snimac-vibraciotresu---modul-801s/
[5] What is distributed control system? [online]. 2024 [cit. 2024-10-08]. Dostupné z: https://www.electricaltechnology.org/2016/08/distributed-control-system-dcs.html
[6] RTU: Řešení WAGO v energetické automatizaci [online]. 2024 [cit. 2024-10-08]. Dostupné z: https://elektrika.cz/data/clanky/rtu-reseni-wago-v-energeticke-automatizaci
[7] Ovládací pult [online]. 2024 [cit. 2024-10-08]. Dostupné z: http://diskuze.modely.biz/viewtopic.php?t=10411&p=207513
[8] CDP Přerov řídí dopravu již 17 let [online]. 2024 [cit. 2024-10-08]. Dostupné z: https://sirdo.eu/cdp-prerov-ridi-dopravu-jiz-17-let/
[9] MS Copilot v Bingu na základě promptů autora [online]. 2024 [cit. 2024-08-28]. Dostupné z: https://www.bing.com/chat?form=NTPCHB

[10] The Five ICS Cybersecurity Critical Controls (sans.org) [online]. 2022 [cit. 2024-08-24]. Dostupné z: *https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/*
[11] SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC (nist.gov) [online]. 2023 [cit. 2024-08-24]. Dostupné z: *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

Lektorovali:
Ing. Radek Kánský, CIA – České dráhy, a.s.

Pavel Kříž – ČD Informační Systémy, a.s.