Implementace MITTRE ATT&CK pro průmyslové řídící a kontrolní systémy v kontextu objektů SEVESO III: Nové výzvy pro kritickou infrastrukturu

Podtitul: Analýza vektorů útoku na průmyslové řídící a kontrolní systémy v kontextu objektů SEVESO III

Ing. Pavel Dobeš, Ph.D.[a)], Ing. Barbora Martiníková, Ph.D. [b)], Ing. Luboš Kotek, Ph.D.[c)]

a) Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav ochrany obyvatelstva. Studentské náměstí 1532, 686 01 Uherské Hradiště. pdobes@utb.cz
b) Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství. Katedra bezpečnosti práce a procesů. barbora.martinikova@vsb.cz
c) Vysoké učení technické Brno, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. kotek.l@fme.vutbr.cz

Souhrn

S nástupem nové evropské a národní legislativy dochází k významnému rozšíření okruhu subjektů kritické infrastruktury (KI), do kterého nově spadají i vybrané průmyslové areály podléhající směrnici SEVESO III. Pro tyto subjekty, nakládající s nebezpečnými chemickými látkami, představuje kybernetický útok na provozní technologie jedno z možných rizik nejen pro kontinuitu výroby, ale primárně pro životy a zdraví zaměstnanců a případně i obyvatelstva v přilehlém okolí. Tento příspěvek se zaměřuje na popularizaci a praktické využití mezinárodního rámce MITRE ATT&CK pro průmyslové řídicí a kontrolní systémy (Industrial Control Systems, zkráceně ICS), jako nástroje pro modelování hrozeb a zvyšování situačního povědomí v průmyslovém prostředí. V rámci článku jsou analyzovány vybrané specifické techniky a taktiky útočníků zaměřené na narušení výrobních procesů, které mohou vést k haváriím s environmentálními dopady.

Klíčová slova: *Mittre Att&ck, průmysl, provoz, systém, řízení, kontrola, analýza, kybernetický útok, vektor, riziko, havárie, bezpečnost, SEVESO, chemické látky, ICS.*

1. Úvod

Kybernetické útoky na průmyslové řídicí systémy (ICS) představují v současnosti jednu z vážných hrozeb pro objekty nakládající s nebezpečnými chemickými látkami. Incidenty, ke kterým již došlo, kdy útočníci cíleně napadli bezpečnostní systémy chemického závodu se záměrem způsobit fyzickou havárii s potenciálními obětmi na životech, demonstrují, že útočníci jsou schopni a ochotni využít slabiny v systémech ICS a eskalovat nebezpečnou situaci. Zkušenosti s tím firmy a instituce mají dle ohlasů nejen v zemích s probíhajícím válečným konfliktem, ale také v rámci Evropy.

V oblasti kyberbezpečnosti je v současnosti na útok vůči zranitelnému systému pohlíženo jako na cestu (vektor), směrovanou z bodu A (průnik do systému) do bodu B (dosažení dílčího cíle / překonání určité vrstvy zabezpečení a způsobení incidentu). Celý scénář útoku může být realizován dosažením několika postupných bodů (cílů), a to jak sérií postupných kroků za sebou nebo laterálně (různými dalšími možnostmi).

V matematice a fyzice má vektor dva klíčové parametry: velikost a směr. V kyberbezpečnosti tento koncept přenášíme do analýzy útoků následovně:

- Sledování trajektorie: Útok není izolovaný incident, ale řetězec kroků, který má svůj směr (například z podnikové sítě IT hlouběji do technologické sítě OT).
- Identifikace vektorů útoku: Matice pomáhá definovat konkrétní cesty, kterými se útočník pohybuje. Každá technika v matici představuje jeden segment tohoto vektoru.

- Kvantifikace a analýza: Rozdělením útoku na technické kroky můžeme „měřit“ efektivitu obrany v každém bodě této trajektorie.

Vektorové metody, jako například Cyber Kill Chain (Lockheed Martin), Diamond model, matice MITRE ATT&CK, stromy útoků (Attack Trees), STRIDE (Microsoft) či PASTA, nám při analýze a ošetřování kybernetických rizik pomáhají tyto scénáře kybernetických útoků rozdělit na konkrétní technické kroky útočníka a navrhovat účinná opatření pro minimalizaci rizik.

2. Příklady kybernetických útoků na průmyslové řídící a kontrolní systémy

Historie kybernetických útoků na ICS/SCADA systémy poskytuje cenné poznatky o metodách, motivacích a důsledcích takových incidentů. Pro objekty SEVESO III jsou zvláště relevantní útoky, které vedly nebo mohly vést k fyzickým haváriím s únikem nebezpečných látek.

Stuxnet (2010) představuje kybernetický útok speciálně navržený k poškození průmyslového zařízení. Cílem bylo íránské zařízení na obohacování uranu v Natanzu, kde malware manipuloval s programovatelnými automaty Siemens S7-315 a S7-417, řídícími centrifugy. Útok využíval čtyři dosud neznámé zranitelnosti (zero-day) a šířil se prostřednictvím infikovaných USB disků, čímž překonával vzduchovou mezeru (air-gap) oddělující technologickou síť od internetu. Manipulací frekvence otáčení centrifug mezi 1410 Hz (přetáčení) a 2 Hz (praktické zastavení) způsobil mechanické namáhání vedoucí ke zničení přibližně 1000 centrifug. Pro SEVESO objekty tento útok demonstroval, že i fyzicky izolované systémy mohou být kompromitovány a že manipulace s procesními parametry může způsobit destrukci zařízení. (Kushner, 2013).

BlackEnergy (2015) a **Industroyer/CrashOverride (2016)** cílily na ukrajinskou energetickou infrastrukturu. BlackEnergy zasáhl tři distribuční společnosti pomocí spear-phishingu, následného pohybu laterálně sítí a přímé manipulace s HMI rozhraními metodou „phantom mouse" – vzdáleného ovládání kurzoru operátora. Útok způsobil výpadek elektřiny pro 230 000 odběratelů a využil destruktivní komponentu KillDisk pro ztížení obnovy. Industroyer o rok později prokázal hluboké znalosti průmyslových protokolů IEC 60870-5-101/104, IEC 61850 a OPC DA, které útočníci využili k přímé komunikaci s rozvodnou infrastrukturou bez nutnosti exploitovat konkrétní zranitelnosti – legitimní příkazy protokolů postačovaly k manipulaci s vypínači. (Štefko, 2025).

TRITON/TRISIS (2017) představuje dosud nejzávažnější útok z hlediska bezpečnosti procesů. Útok cílil na bezpečnostní instrumentované systémy (SIS) Schneider Electric Triconex v saudskoarabském petrochemickém závodě. Na rozdíl od předchozích útoků měl TRITON za cíl vyřadit poslední vrstvu ochrany bránící fyzické havárii. Malware využíval proprietární protokol TriStation, který útočníci museli reverzně analyzovat, a zero-day zranitelnost ve firmware řadičů Tricon pro získání privilegovaného přístupu. Útok byl odhalen pouze díky chybě v kódu, která způsobila aktivaci bezpečnostního mechanismu TMR (Triple Modular Redundancy) a nouzové odstavení závodu. Výzkumníci potvrdili, že prostředky potřebné k vytvoření podobného útoku nevyžadují nutně státní podporu – zařízení je dostupné na sekundárním trhu za 5-10 tisíc dolarů. Pro SEVESO objekty TRITON prokázal, že bezpečnostní systémy navržené dle IEC 61511 mohou být cílem sofistikovaných útoků se záměrem způsobit ztráty na životech. (Abraham, 2025).

Mezi další relevantní incidenty patří útok na úpravnu vody v Oldsmar, Florida (2021), kde útočník prostřednictvím vzdáleného přístupu TeamViewer zvýšil dávkování hydroxidu sodného ze 100 ppm na 11 100 ppm, a ransomwarový útok na Colonial Pipeline (2021), který vedl k šestidennímu odstavení klíčové palivové infrastruktury zásobující 45 % východního pobřeží USA. (Jeffries, 2022).

3. Související legislativní požadavky a možné pokuty

Směrnice NIS2 (2022/2555) vytváří přímý legislativní základ pro kybernetickou bezpečnost kritické infrastruktury. Chemický průmysl spadá pod Přílohu II jako důležitý subjekt (výroba, produkce a distribuce chemických látek), přičemž velké podniky v sektoru mohou být klasifikovány jako základní subjekty. Článek 21 směrnice vyžaduje implementaci technických, provozních a organizačních opatření pro řízení kybernetických rizik včetně politik analýzy rizik, zvládání incidentů, kontinuity činností a bezpečnosti dodavatelského řetězce. Směrnice

stanovuje povinné hlášení incidentů ve třech fázích: časné varování do 24 hodin, oznámení do 72 hodin a závěrečná zpráva do jednoho měsíce. Maximální sankce dosahují 10 milionů EUR nebo 2 % celosvětového obratu pro základní subjekty.

Český zákon o kybernetické bezpečnosti (č. 264/2025 Sb.) transponující NIS2 nabyl účinnosti 1. listopadu 2025. Zákon zavádí dvouúrovňový režim: režim vyšších povinností pro subjekty strategického významu a režim nižších povinností pro důležité subjekty. Česká implementace jde nad rámec minimálních požadavků NIS2 tím, že vyžaduje hlášení všech kybernetických incidentů, nikoli pouze významných. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) působí jako národní kompetentní orgán s pravomocí ukládat pokuty až do výše 250 milionů Kč, včetně realizace opatření vůči statutárním orgánům firem a organizací při opakovaných nebo závažných porušeních.

Pro objekty SEVESO III (zejména zařazené do skupiny B), které současně spadají (nebo budou spadat) pod NIS2, vzniká povinnost integrace požadavků a vyžaduje zahrnutí kybernetických hrozeb do bezpečnostních zpráv prevence závažných havárií (BZ PZH) jako potenciálních iniciačních událostí, rozšíření systému řízení bezpečnosti o kybernetická opatření, koordinaci hlášení incidentů na MŽP a NÚKIB, a rovněž začlenění kybernetických scénářů rizik do vnitřních a vnějších havarijních plánů.

4. Výběr metody pro teoretickou analýzu vektorů kybernetických útoků na ICS

Pro vstupní teoretickou analýzu možných vektorů kybernetických útoků na ICS, jako možných kořenových či přispívajících příčin průmyslových havárií (včetně závažných) si autorský tým zvolil rámec, respektive metodu MITRE ATT&CK. A to jak z důvodů dílčí znalosti metody, tak kvůli dostupnosti grafického a neustále rozvíjeného rámce on-line (https://attack.mitre.org/) a v neposlední řadě podrobného blokového členění popsaných technik útočníků na různé ICT systémy a platformy (enterprise, mobile, ICS). K výběru této metody přispěla i skutečnost, že je využívána k analýze a následnému popisu chování testovaného malware v rámci volně dostupných profesionálních on-line sandboxů, jako je https://www.virustotal.com nebo https://any.run/.

MITRE ATT&CK je primárně metoda klasifikace a popisu chování útočníků. Konkrétně se zaměřuje na:

- Taktiky, techniky a postupy útočníků (tactics, techniques, procedures, TTPs). Poskytuje v podstatě taxonomický slovník v dané oblasti. Místo vágního „hackli nás“ díky matici lze říci a popsat: „Útočník použil taktiku získání počátečního přístupu (initial access) skrze techniku vnějších vzdálených služeb (external remote services, s kódovým označením T0822).“
- Modelování hrozeb (threat modeling). Metoda pomáhá simulovat, jak by reálný útok na vybranou infrastrukturu mohl vypadat.
- Analýza mezer (gap analysis). Zároveň je to metoda vhodná pro zjištění, které technické kroky útočníka dokáže obránce (provozovatel a jeho správci informačních systémů) spíše detekovat, a které jsou pro něj pravděpodobně spíše „neviditelné“.

5. Aplikace vektorové metody MITRE ATT&CK pro zjištění možných kořenových či přispívajících příčin vybraných scénářů průmyslových havárií, při útocích na ICS

V této části článku se autorský tým zaměřil na rozbor pěti vybraných scénářů kybernetických útoků na řídicí a kontrolní systémy, které mohou vyústit ve vrcholovou havarijní událost typu „runaway reaction“, „loss of containment“, „loss of integrity“ a „loss of function“, používanou analytiky rizik zároveň ve stromech poruchových stavů (FTA) a stromech událostí (ETA). Tyto scénáře vycházejí z reálných útočných vzorců, například těch použitých při útocích jako Stuxnet nebo Industroyer (viz výše část 2. článku), které jsou dále analyzovány optikou MITRE ATT&CK, k detekci anomálií v ICS provozu.

Tento přístup je validní a umožňuje teoreticky analyzovat potenciální dopady kybernetických útoků na fyzické procesy v zařízeních SEVESO III, aniž by bylo nutné provádět náročné a potenciálně nebezpečné simulace. Zaměření na matici MITRE ATT&CK pro ICS navíc poskytuje strukturovaný rámec pro tuto analýzu.

Scénář I.: Nekontrolovaná (exotermická) reakce, samovolně se zrychlující (runaway reaction)
Tento scénář simuluje útok na reaktor, kde je kritické chlazení a míchání.

- Cíl: Vyvolat neřízený nárůst teploty a tlaku v reaktoru.
- Využité techniky MITRE (uvedeny anglicky, dle originálu matice MITRE on-line):
  - Impair process control (T0827): Útočník manipuluje s logikou PLC, aby uzavřel ventily chladicího média.
  - Modify parameter (T0836): Změna žádané hodnoty (setpoint) pro dávkování katalyzátoru na maximum.
  - Inhibit response function (T0824): Zablokování alarmů, aby operátor včas nezasáhl.
- Vrcholová událost: nekontrolovaná reakce, následovaná explozí nádoby (zdroje rizika, reaktoru, destilační kolony, …) v důsledku překročení konstrukčního tlaku.

Scénář II.: Ztráta obsahu (loss of containment, únik nebezpečných látek)
Zaměřeno na skladovací terminály (např. zkapalněné plyny pod tlakem).

- Cíl: Přetečení nádrže nebo mechanické porušení potrubí.
- Využité techniky MITRE:
  - Spoof reporting message (T0856): Falešné hlášení hladinoměru (stále ukazuje "bezpečno"), zatímco čerpadla běží.
  - Unauthorized command message (T0834): Vzdálené otevření vypouštěcích ventilů do nechráněných, nezajištěných prostor.
  - Loss of view (T0829): Odpojení obrazovek na dispečinku (HMI), aby operátor zčásti nebo úplně ztratil přehled o stavu provozu.
- Vrcholová událost: Ztráta obsahu – toxický mrak nebo únik hořlavé kapaliny do okolí zdroje rizika.

Scénář III.: Ztráta integrity (loss of integrity, destrukce zařízení manipulací s tlakem)
Útok na kompresorové stanice nebo vysokotlaká potrubí.

- Cíl: Vyvolat únavu materiálu nebo rázovou vlnu vedoucí k roztržení systému.
- Využité techniky MITRE:
  - Manipulation of control (T0831): Cyklické otevírání a zavírání uzavíracích armatur (vytvoření vodního/tlakového rázu).
  - Block reporting message (T0804): Zamezení přenosu dat o kritickém nárůstu tlaku do systému SCADA.
- Vrcholová událost: Ztráta integrity – fyzická destrukce technologie a následný požár.

Scénář IV.: Ztráta zabezpečení (Loss of safety function, ochrnutí bezpečnostních systémů)
Tento scénář je rovněž nebezpečný, protože míří přímo na systémy SIS (Safety Instrumented Systems).

- Cíl: Vyřadit poslední linii obrany a bezpečnostní systémy před vznikem, případně rozvojem havárie.
- Využité techniky MITRE:
  - Loss of safety (T0880): Přepsání logiky bezpečnostního PLC (např. TRICONEX), aby ignorovalo mezní stavy.
  - Program download (T0843): Nahrání modifikovaného projektu do bezpečnostního kontroléru, který deaktivuje nouzové odstavení (ESD).
- Vrcholová událost: Samotná technika nevyvolá havárii okamžitě, ale připraví podmínky pro to, aby běžná provozní porucha (např. výpadek čerpadla) přerostla v katastrofální havárii, protože bezpečnostní systém nezareaguje.

Scénář V.: Ztráta funkce a domino efekt (Loss off function & cascade failure)
Útok na pomocné provozy (utility), jako je chlazení, elektrická energie nebo inertizace dusíkem.

- Cíl: Vyvolat selhání v jedné části závodu, které způsobí řetězovou reakci v ostatních (tzv. domino efekt dle směrnice SEVESO III).
- Využité techniky MITRE:

    - Denial of service (T0814): Zahlcení komunikační sběrnice, vedoucí k pádu všech řídicích jednotek do "chybového stavu".
    - Brute force (T0806): Průnik do správy energetické sítě areálu a vypnutí přívodu elektřiny pro kritické systémy podpory života.
- Vrcholová událost: Ztráta funkce a domino efekt – totální ztráta kontroly nad areálem, vedoucí k souběhu více havárií (požáry, úniky) v důsledku ztráty podpůrných médií.

Výše nastíněné scénáře, jejichž výčet ani příčiny nejsou vyčerpávající, i přesto demonstrují, že kybernetický útok na technologiích tzv. SEVESO objektů není jen o "ukradených datech", ale zejména o fyzikálních dopadech. Propojení matice MITRE s vhodnými metodami analýzy rizik (například FTA, ETA, HAZOP, FMEA) by mělo umožnit analytikům a manažerům bezpečnosti přesněji identifikovat místa, kde je (a bude) potřeba posílit detekci.

6. Diskuse

Implementace rámce MITRE ATT&CK pro ICS v kontextu zařízení SEVESO III představuje pro manažery bezpečnosti několik možných překážek. Tyto překážky vyplývají ze specifické povahy průmyslových řídicích systémů (ICS), odlišností mezi IT a OT prostředími a zvýšenými riziky spojenými s nebezpečnými látkami.

Mezi hlavní praktické překážky mohou patřit:

- Složitost a různorodost prostředí ICS: Průmyslové řídicí systémy jsou komplexní díky široké škále technologií a protokolů, které využívají (Toker, 2021)
- Zařízení SEVESO III, která často zahrnují heterogenní systémy, od starších proprietárních technologií po moderní síťově propojené systémy, představují významnou výzvu pro sjednocené modelování hrozeb pomocí MITRE ATT&CK.
- Rozdílné požadavky IT a OT bezpečnosti: provozní technologie (operational technologies, OT), která tvoří provozní strukturu ICS, má odlišné požadavky na výkon a bezpečnost ve srovnání se standardní IT infrastrukturou (Toker, 2021)
- Bezpečnostní manažeři musí překlenout propast mezi světem IT, kde je rámec MITRE ATT&CK široce zaveden, a světem OT, kde je potřeba zohlednit specifické provozní priority, jako je dostupnost a integrita před důvěrností (Georgiadou, 2021).
- Nedostatek integrovaných datových sad a testovacích prostředí: Pro efektivní monitorování, analýzu a validaci bezpečnostních opatření založených na MITRE ATT&CK pro ICS (možná) stále chybí komplexní datové sady a testovací prostředí (byť jsou průběžně doplňovány), která by zahrnovala jak síťovou, tak fyzickou úroveň (Choi, 2020)
- To omezuje možnosti testování, validace a tréninku pro integrované monitorovací systémy, což ztěžuje bezpečnostním manažerům ověřování účinnosti jejich obrany.
- Mapování zranitelností na specifické průmyslové komponenty: Ačkoliv MITRE ATT&CK pro ICS poskytuje metodologický přístup k identifikaci zranitelností (Afenu, 2024), praktické mapování zranitelností specifických průmyslových komponent (jako jsou PLC, HMI, SIS) v rámci komplexního zařízení SEVESO III na techniky útočníků může být časově náročné a vyžaduje hlubší odborné znalosti.
- Vysoké nároky na systémy detekce hrozeb: Prostředí ICS generuje vysokorychlostní a objemný síťový provoz, což představuje jedinečnou výzvu pro systémy detekce narušení (IDS). Tyto systémy musí monitorovat velké a různorodé objemy dat, přičemž si zachovávají nízkou latenci a vysokou přesnost, což je pro bezpečnostní manažery obtížné zajistit v reálném provozu (Joy, 2024)
- Integrovaný přístup k bezpečnosti: Potřeba integrovat organizační a individuální kulturní faktory s chováním útočníků, jak je popsáno v MITRE ATT&CK, vyžaduje holistický pohled na bezpečnost (Georgiadou, 2021).
- Bezpečnostní manažeři v zařízeních SEVESO III musí navíc koordinovat kybernetickou bezpečnost s fyzickou bezpečností a krizovým řízením.

Dříve byl svět OT od IT více izolovaný (jejich sítě byly ovykle odděleny). Systémy IT byly určeny primárně pro zpracování, ukládání a přenos informací, šlo o e-maily, databáze, systémy plánování podnikových zdrojů, webové servery, apod.). Systémy provozních technologií (OT) představují zejména hardware a software, detekující či způsobující změnu prostřednictvím přímého monitoringu a řízení fyzických zařízení. V OT jde například o programovatelné logické automaty (PLC), robotická ramena, snímače tlaku či ventily.

Dnes se tyto světy stále více propojují (Průmysl 4.0, IIoT) a projevuje se fenomén jejich konvergence. IT chce data z výroby, aby mohlo optimalizovat byznys. OT se začíná podobat IT (používá Windows, Linux, Wi-Fi). Když do OT světa pronikne malware z IT (třeba přes infikovaný e-mail účetní), tradiční IT ochrana (např. agresivní skenování sítě) může paradoxně OT systémy shodit, protože jsou velmi citlivé na latenci a neobvyklý síťový provoz.

Tabulka: Shrnutí klíčových rozdílů mezi systémy IT a OT

Vlastnost	**IT (informační technologie)**	**OT (provozní technologie)**
Priorita **(triáda)**	Hlavním cílem je důvěrnost (aby data nikdo nepřečetl). **C-I-A** (confidentiality - integrity - availability)	Hlavním cílem je dostupnost a bezpečnost (aby stroj běžel a nikoho nezabil). **A-I-C** (availability - integrity - confidentiality)
Životní cyklus	Krátký (3–5 let, rychlá obměna)	Dlouhý (15–30 let, stroje z 90. let nejsou v průmyslu velkou výjimkou)
Dostupnost	Výpadky jsou nepříjemné (restart je běžný)	Výpadek je kritický (restart může trvat dny nebo zničit stroj)
Patchování (aktualizace)	Časté a automatizované	Vzácné, vyžaduje odstávku a testování bezpečnosti
Prostředí	Klimatizované kanceláře, čisté servery	Prašné haly, vibrace, extrémní teploty
Protokoly	Standardní (HTTP, TCP/IP, SMTP, …)	Specifické (Modbus, Profibus, DNP3, EtherCAT, …)

Dále je potřeba si přiznat, že čistě teoretický přístup k analýze scénářů zneužití zranitelností v ICS zařízeních SEVESO III, bez jakýchkoliv simulací či praktického testování, má několik významných omezení a nevýhod, které by bylo vhodné zvážit:

- Chybějící validace v reálném prostředí a omezený pohled na fyzikální dopady: Teoretická analýza, i když je založena na rámcích jako MITRE ATT&CK pro ICS, nemusí plně zachytit složitou dynamiku a interakce v reálném průmyslovém řídicím systému (Khan, 2022).
- ICS se vyznačují jedinečnými charakteristikami, které je činí zranitelnými, a simulace jsou nezbytné pro pochopení chování a dynamiky komponent ICS v reálných podmínkách (Alves, 2016).
- Bez praktické validace je obtížné plně porozumět tomu, jak se kybernetický útok projeví ve fyzickém světě a jaké budou jeho skutečné dopady na provoz zařízení SEVESO III.
- Podcenění nebo přecenění rizika: Bez ověření v simulovaném nebo reálném prostředí existuje riziko, že teoreticky navržené scénáře budou buď podceňovat skutečnou zranitelnost systému, nebo naopak přeceňovat pravděpodobnost či závažnost některých útoků. Virtuální „testbeds“ sice nabízejí cenově efektivní řešení, ale mohou poskytovat omezený pohled na provozované výrobní systémy ICS, což může zhoršit vývoj přesných detekčních a preventivních mechanismů (Shamsuzzaman, 2024).
- Nedostatečné porozumění dynamickým interakcím: Mnoho kybernetických útoků na ICS zahrnuje složité sekvence kroků a interakcí mezi kybernetickými a fyzikálními komponenty. Teoretická analýza může mít potíže s přesným modelováním těchto dynamických jevů a kaskádových efektů, které mohou vést k havárii (Khan, 2022).
- Zkoumání kybernetických hrozeb v ICS prostředích vyžaduje emulaci scénářů kybernetických útoků z reálného světa, aby bylo možné překlenout propast mezi teoretickými znalostmi a praktickou aplikací. (Ekisa, 2024)
- Omezená schopnost dolaďování obranných mechanismů: Návrh účinných preventivních a mitigačních opatření (v souladu s principy "Security by Design") vyžaduje iterativní proces testování a ladění. Bez možnosti simulace a testování

různých obranných strategií je obtížné zjistit, které přístupy budou v praxi nejefektivnější a zda nebudou mít nežádoucí vedlejší účinky na provozní stabilitu.
- Obtížnost kvantifikace dopadů: Ačkoli lze teoreticky popsat, jak útok může vést k havárii, je bez simulací extrémně obtížné kvantifikovat konkrétní parametry, jako je čas do selhání, rozsah poškození nebo rychlost šíření nebezpečných látek. Tyto kvantitativní údaje jsou klíčové pro krizové řízení a ochranu obyvatelstva.
- Snížená přesvědčivost pro stakeholdery (zainteresované strany): Pro manažery bezpečnosti a vedoucí pracovníky v průmyslových podnicích, kteří jsou zodpovědní za investice do kybernetické bezpečnosti, mohou být výsledky čistě teoretické analýzy méně přesvědčivé než poznatky získané ze simulací, které demonstrují hrozby v "reálnějším" kontextu (Domínguez, 2022).
- Překlenutí mezery mezi experty na informační bezpečnost a specialisty na fyzickou bezpečnost a krizové řízení je cílem, ale bez praktických ukázek je to náročnější.
- Limitovaná viditelnost a nedostatek hloubkových informací: ICS často trpí omezenou viditelností do svých systémů a nedostatkem účinných informací o hrozbách, což představuje významnou překážku pro včasnou detekci a predikci útoků (Gazzan, 2023). Teoretická analýza sama o sobě tuto viditelnost nezlepší. I přes tyto nevýhody je teoretická analýza založená na MITRE ATT&CK pro ICS neocenitelným prvním krokem. Poskytuje strukturovaný rámec pro identifikaci potenciálních hrozeb a zranitelností. (Ekisa, 2024).

7. Závěr

Příspěvek poskytuje zejména v částech 4. až 6. praktický návod s příklady pro analytiky rizik a manažery bezpečnosti, jak pomocí matice MITRE ATT&CK pro ICS (nebo jiné podobné vektorové metody) mapovat zranitelnosti specifických průmyslových komponent (PLC, HMI, SIS). Tento přístup umožňuje proaktivní zjišťování možných hrozeb a může pomoci včasné detekci kybernetických hrozeb proti ICS zařízením (Jadidi, 2021).

Na teorerickou analýzu vektorů možných útoků nejen na ICS systémy by dále mělo v bezpečnostní praxi navazovat testování odolnosti kritických ICS, s využitím metody fyzických či digitálních dvojčat v izolovaném prostředí. Souběžně by měly být v rámci prevence a mitigace navrhovány opatření pro posílení odolnosti kritické infrastruktury, v souladu s principy "Security by Design". To zahrnuje adaptaci nástrojů pro hodnocení rizik a kybernetických bezpečnostních kontrol, jako jsou ty odvozené z NIST CSF (Progoulakis, 2021).

Dílčím cílem článku i snahou autorů bylo přispět k překlenutí mezery mezi experty na informační bezpečnost a specialisty na posuzování průmyslových rizik, fyzickou bezpečnost a krizové řízení. Na závěr je potřeba zdůraznit nezbytnost integrovaného přístupu k ochraně subjektů kritické infrastruktury v digitálním věku, při reálných rozdílech v požadavcích na výkon a bezpečnost výrovních systémů ve srovnání s požadavky na výkon a zabezpečení standardní IT infrastruktury (Ekisa, 2024), (Toker, 2021).Tato integrace vyžaduje zohlednění jak IT, tak OT sítí a jejich vzájemných interakcí (Georgiadou, 2021).

8. Reference

Abraham, D., D'Souza, A., Kappiarukudil, K., Rai, S. "Cyber-Attacks on Energy Infrastructure—A Literature Review." *Appl. Sci.* 2025, *15*, 9233.

Alexander, O D et al. (2020). MITRE ATT\&CK® for Industrial Control Systems: Design and Philosophy. https://www.semanticscholar.org/paper/51a2b3210d8d24944500c182c7224f8c1c21e729

Ekisa, C et al. (2024). Leveraging the MITRE ATT\&CK Framework for Threat Identification and Evaluation in Industrial Control System Simulations. 2024 35th Irish Signals and Systems Conference (ISSC), 1-6. https://doi.org/10.1109/ISSC61953.2024.10602968

Georgiadou, A et al. (2021). Assessing MITRE ATT\&CK Risk Using a Cyber-Security Culture Framework. Sensors (Basel, Switzerland), 21. https://doi.org/10.3390/s21093267

Choi, W et al. (2024). Detecting Cybersecurity Threats for Industrial Control Systems Using Machine Learning. IEEE Access, 12, 153550-153563. https://doi.org/10.1109/ACCESS.2024.3478830

Jadidi, Z, Lu, Y (2021). A Threat Hunting Framework for Industrial Control Systems. IEEE Access, 9, 164118-164130. https://doi.org/10.1109/access.2021.3133260

Jeffries, B., Saravia, S., Carter, C., Ankuda, Z. Cyber Risk to Mission Case Study. Mitre Corporation, 2022.
Joy, A et al. (2024). An Investigative Evaluation of Open Source Intrusion Detection Systems for Operational Technology Networks Using MITRE ICS Attack Simulation on a Thermal Power Plant Test Bed. 2024 IEEE 21st India Council International Conference (INDICON), 1-6. https://doi.org/10.1109/INDICON63790.2024.10958514
Kushner, D. "The real story of stuxnet." in *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013, doi: 10.1109/MSPEC.2013.6471059.
Progoulakis, I et al. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering. https://doi.org/10.3390/jmse9121384
Štefko, R., Eliáš, K., Glajc, K., Hyseni, Margita, Šimčák, J. "Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations." 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025.
Toker, F., S., et al. (2021). MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System. 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 1-6. https://doi.org/10.1109/ISDFS52919.2021.9486331