Univerzita Tomáše Bati
Fakulta aplikované informatiky

Konsolidovaný a standardizovaný implementační model bezpečnosti IT/OT pro SMR

Ing. Aleš Navrátil
doc. RNDr. Vojtěch Křesálek, CSc.

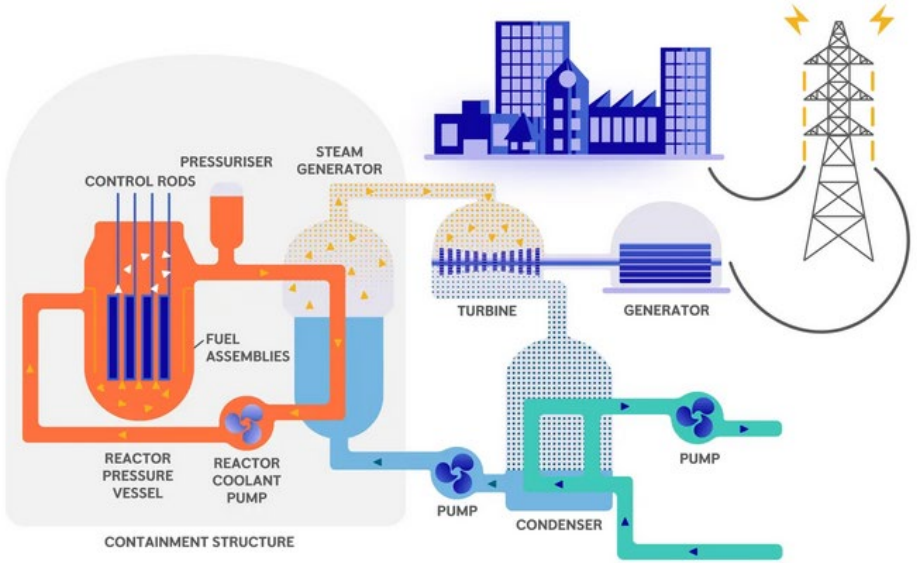
MODULÁRNÍ JADERNÉ REAKTORY

Konference APROCHEM
22. - 23. 4. 2026

Fakulta aplikované informatiky UTB
Ústav elektroniky a měření

OSNOVA:

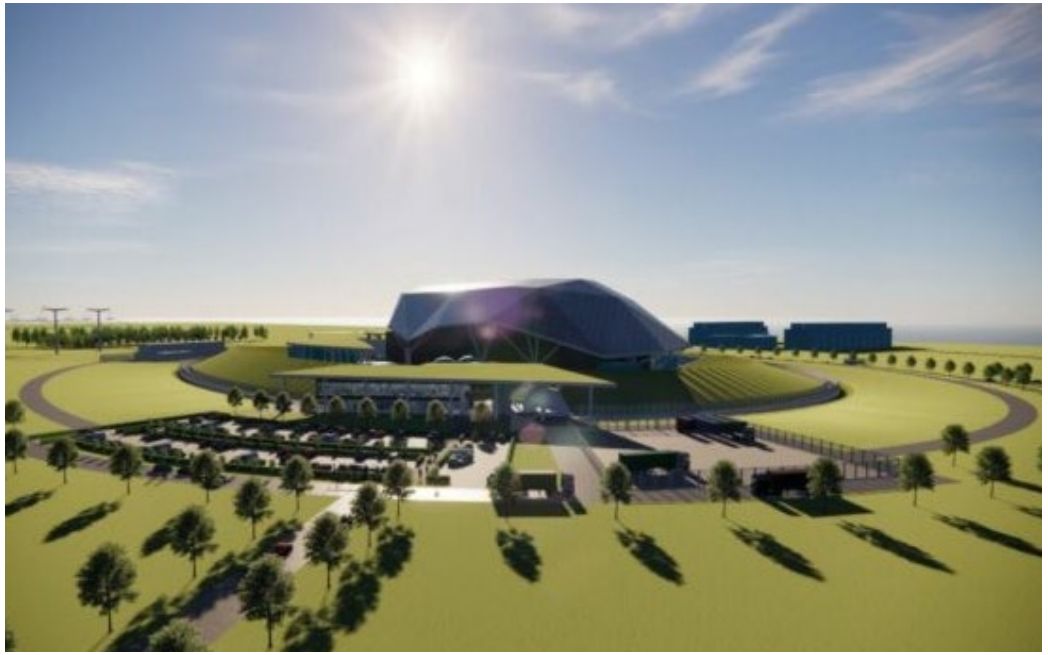
- **DIGITALIZACE SYSTÉMŮ SMR**
- **DOPADY DIGITALIZACE NA BEZPEČNOST**
- **INTEGRACE IT A OT SYSTÉMŮ**
- **KONSOLIDOVANÝ IMPLEMENTAČNÍ MODEL BEZPEČNOSTI IT/OT V SMR**
  - **Strategická vrstva (Governance)**
  - **Procesní vrstva (Safety Management Processes)**
  - **Technologická vrstva (Technical Implementation)**



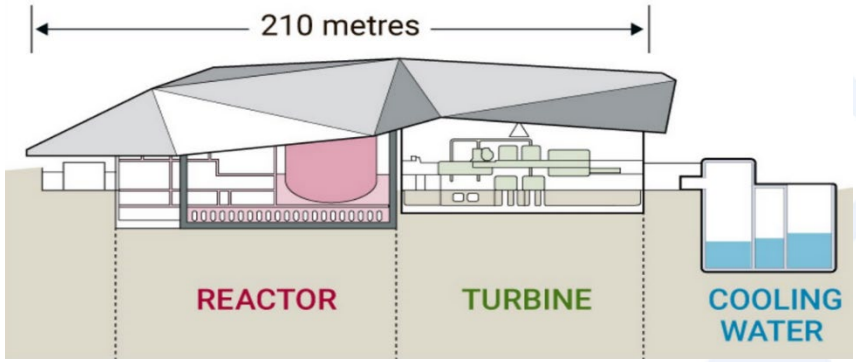
Univerzita Tomáše Bati
Fakulta aplikované informatiky

DIGITALIZACE SYSTÉMŮ SMR

Digitalizace představuje jeden z klíčových trendů moderní energetiky [1]. Moderní I&C budou využívat rozsáhlé sítě senzorů, řídicích jednotek a analytických nástrojů, které budou umožňovat kontinuální monitoring provozních parametrů [2; 3].



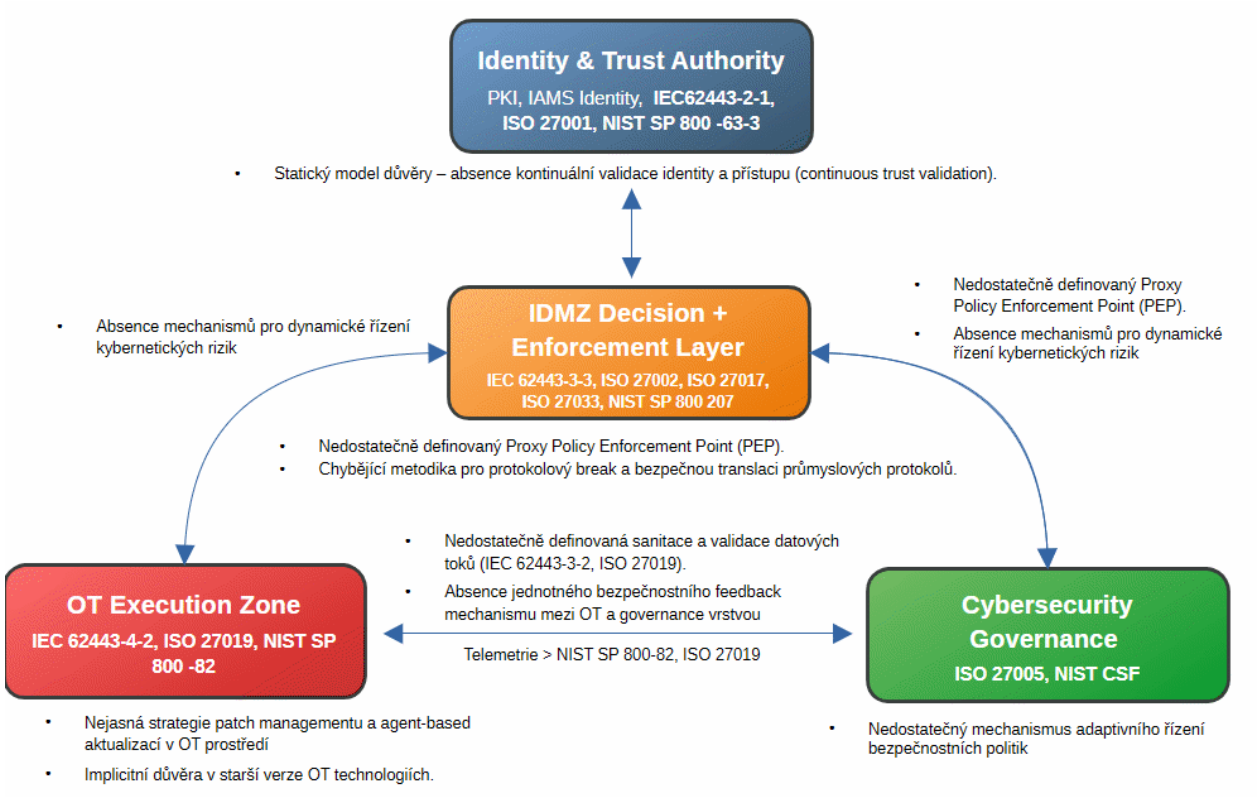
Obrázek 1. Návrhu jaderné elektrárny SMR společnosti Rolls-Royce [2].



Obrázek 2. Návrhu jaderné elektrárny SMR společnosti Rolls-Royce [4].

DOPADY DIGITALIZACE NA BEZPEČNOST

Digitalizace průmyslových systémů přináší řadu výhod, současně však vede ke zvýšení složitosti bezpečnostního prostředí [5; 6]. Integrace digitálních systémů vytváří nové komunikační kanály, které mohou být potenciálně zneužity útočníky [6].

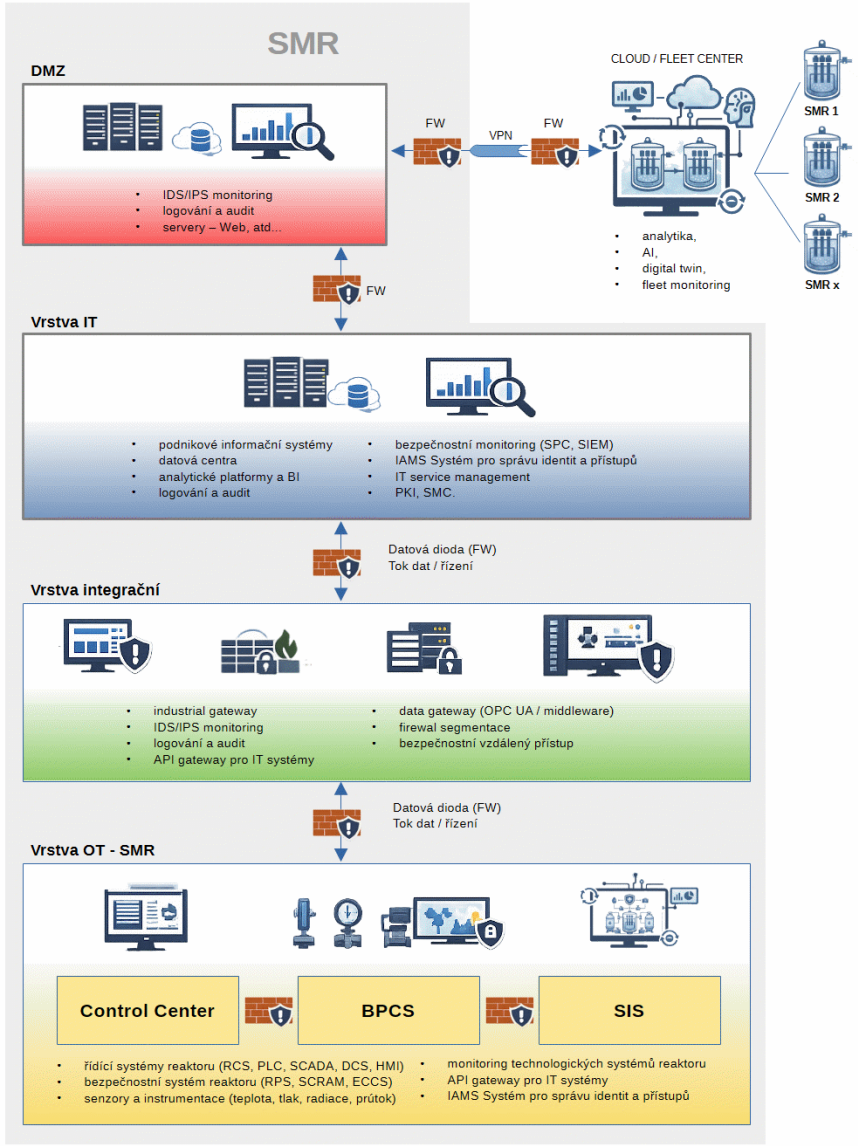


Obrázek 3. Příklad kritické analýzy současných bezpečnostních standardů pro IT/OT v kontextu SMR (vlastní zpracování na základě [7–28]).

INTEGRACE IT A OT SYSTÉMŮ

Integrace IT a OT se bude stávat strategickým faktorem ovlivňujícím bezpečnost, ekonomiku a regulatorní přijatelnost projektů SMR [20; 21].

Současně však bude kladen větší důraz na kybernetickou bezpečnost mezi jednotlivými technologickými vrstvami [22].



Obrázek 4. Architektura IT/OT pro SMR (vlastní zpracování na základě [7; 25; 26; 29]).

INTEGRACE IT A OT SYSTÉMŮ

Propojení IT a OT:

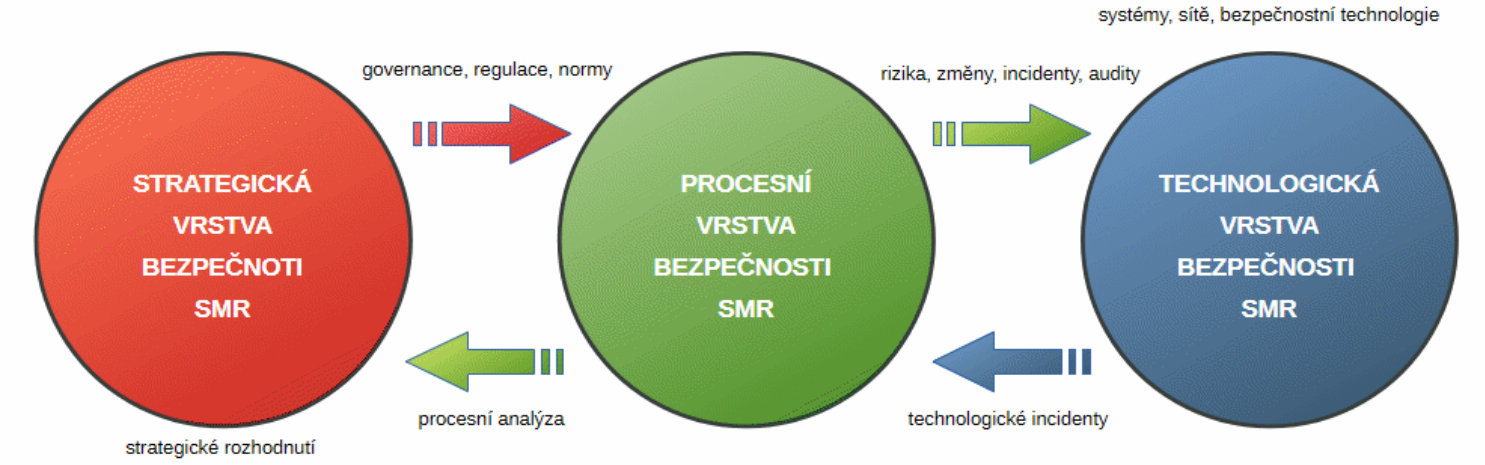
- architekturu založenou na segmentaci sítí a definovaných bezpečnostních zónách [22; 31],
- propojení mezi zónami musí být realizováno pouze prostřednictvím řízených rozhraní „Controlled Interfaces“[31],
- řízení a monitorování datových toků mezi zónami [31],
- aplikaci principu „Defence in Depth“ [7; 29; 31],
- provedení hodnocení rizik před zavedením nebo změnou konektivity mezi IT a OT [7; 22],
- použití demilitarizované zóny mezi podnikovou a provozní sítí,
- ochranu systémů důležitých pro jadernou bezpečnost a ochranu před kybernetickými hrozbami vyplývajícími z propojení s méně chráněnými sítěmi [7; 20; 29].

KONSOLIDOVANÝ IMPLEMENTAČNÍ MODEL BEZPEČNOSTI IT/OT V SMR

Model musí definovat propojení IT a OT se sjednoceným bezpečnostním dohledem, společnou „Governance“ strukturou, tiketovým systémem o hrozbách a koordinovaným incident managementem [12; 16].

Základní vrstvy [9; 18; 29]:

- strategická vrstva „Governance“,
- procesní vrstva „Safety Management Processes“,
- technologická vrstva „Technical Implementation“.



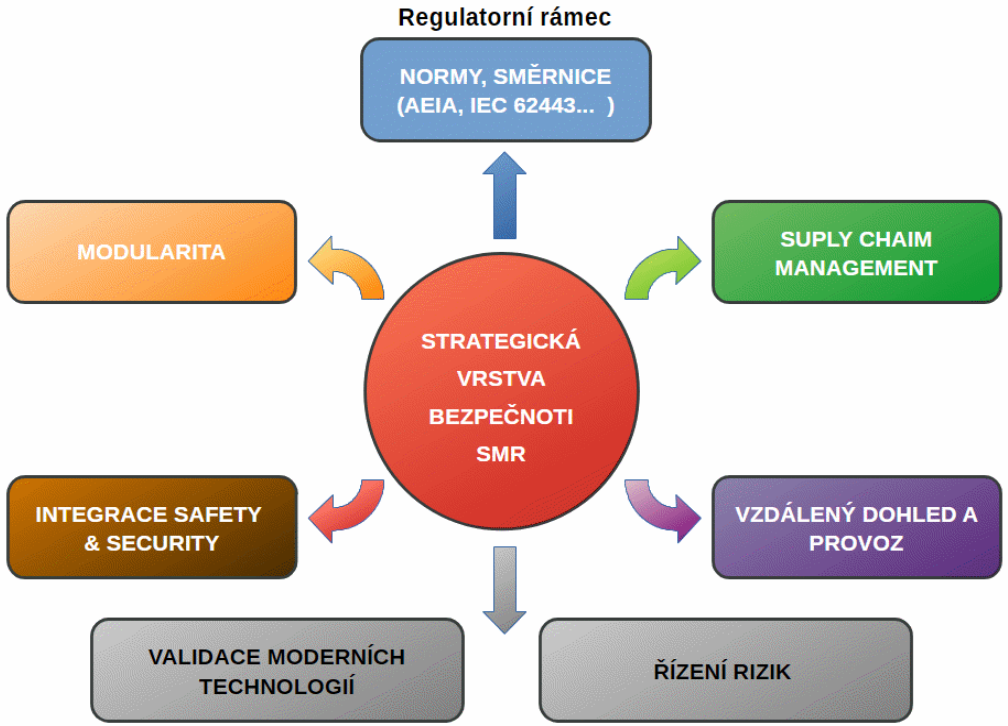
Obrázek 5. Základní rozdělení (vlastní zpracování na základě [9; 18; 29; 30]).

KONSOLIDOVANÝ IMPLEMENTAČNÍ MODEL BEZPEČNOSTI IT/OT V SMR

Strategická vrstva (Governance)

Strategická vrstva představuje nejvyšší úroveň řízení bezpečnosti v prostředí SMR a určuje směr a principy ochrany IT/OT systémů.

Bezpečnost není jen technickým opatřením, ale systematicky řízenou oblastí, integrovanou do rozhodovacích procesů organizace [24; 31; 32].

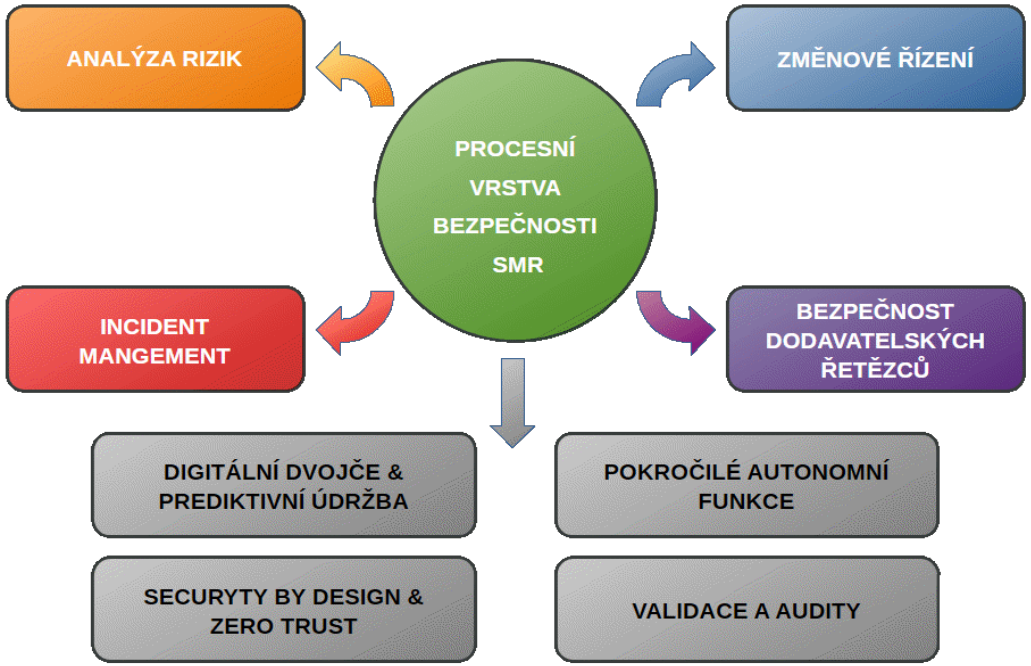


Obrázek 6. Strategická vrstva bezpečnosti rizik (vlastní zpracování na základě [9; 24; 33; 34]).

KONSOLIDOVANÝ IMPLEMENTAČNÍ MODEL BEZPEČNOSTI IT/OT V SMR

Procesní vrstva (Safety Management Processes)

Procesní vrstva musí být spojená s odpovídající procesní koncepcí [31]. Zásadní roli musí sehrát analýza rizik, která musí zahrnovat analýzu dopadů s dopadem na inovativní koncept bezpečnosti SMR [31; 35]. Neméně důležitá je oblast incident managementu, kde musí být jasně definovány scénáře zahrnující kybernetické útoky na zařízení I&C.



Obrázek 7. Procesní vrstva bezpečnosti rizik (vlastní zpracování na základě [13; 14; 20; 22; 27; 36; 37; 38]).

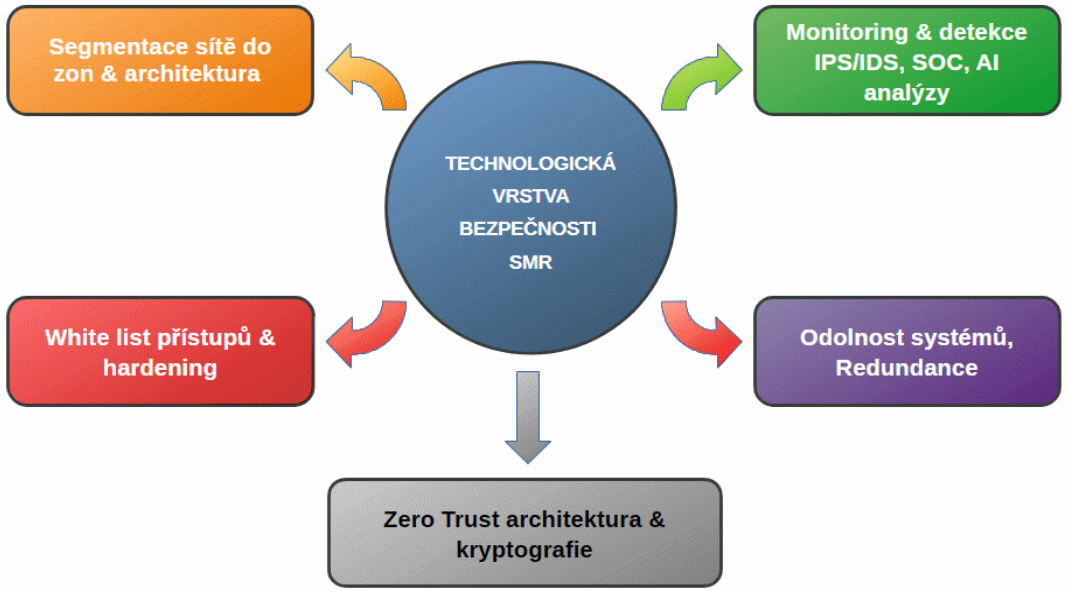
KONSOLIDOVANÝ IMPLEMENTAČNÍ MODEL BEZPEČNOSTI IT/OT V SMR

Technologická vrstva (Technical Implementation)

Technologická vrstva zahrnuje implementaci specifikovaných bezpečnostních nástrojů a architektonických principů pro ochranu kritických zařízení [31].

Důležité prvky [36]:

- segmentace systémů do zón,
- řídicí (I&C) a IT systémy,
- air-gap,
- datové diody.



Obrázek 8. Technická vrstva bezpečnosti rizik (vlastní zpracování na základě [8; 13; 15; 21; 23; 26; 27; 29; 37; 39].

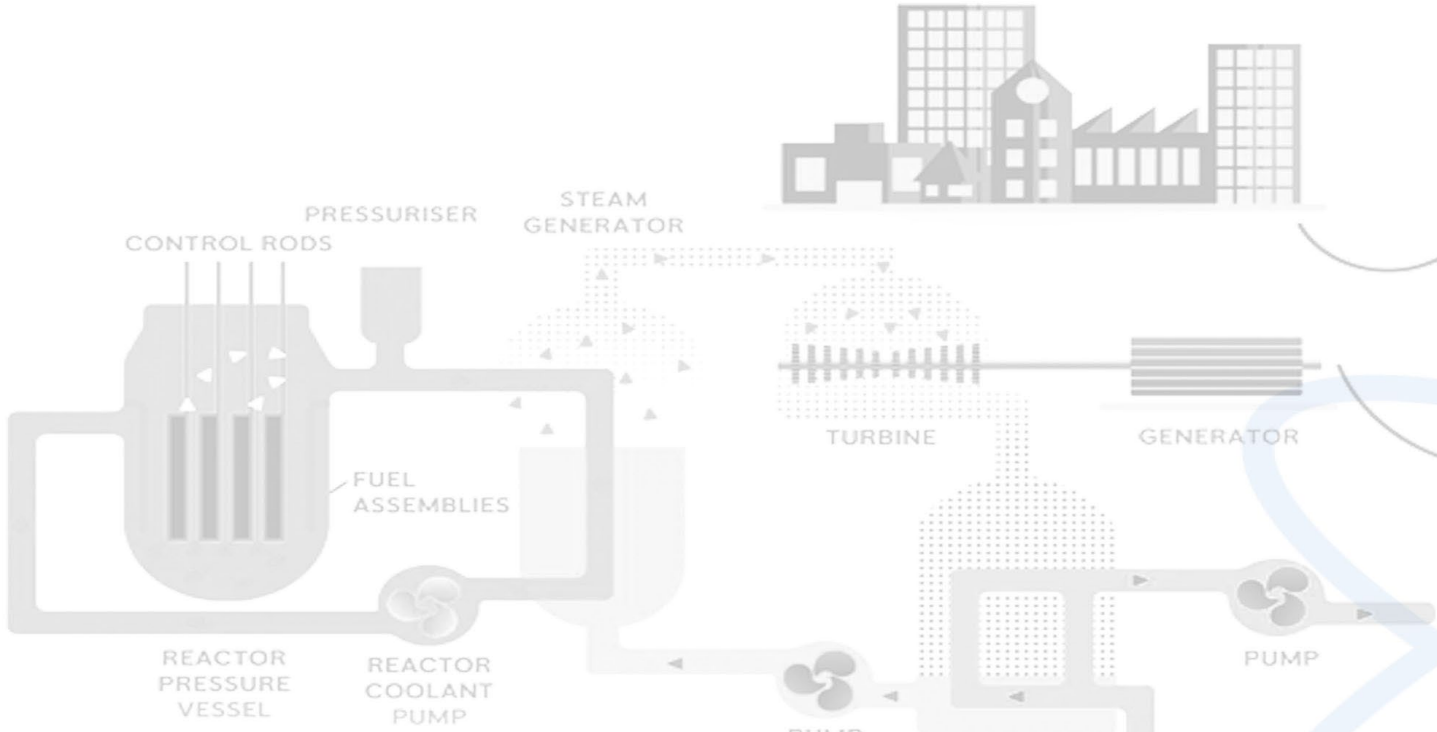
Univerzita Tomáše Bati
Fakulta aplikované informatiky

Závěr

Digitalizace SMR představuje zásadní technologický trend, který přináší nové možnosti optimalizace provozu, ale současně vytváří nové bezpečnostní výzvy. Navržený konsolidovaný implementační model bezpečnosti IT/OT musí poskytnout systematický rámec pro řízení těchto rizik v prostředí SMR.

Integrace mezinárodních standardů, regulatorních požadavků a technologických opatření musí vytvořit robustní bezpečnostní architekturu podporující bezpečný a spolehlivý provoz.

Nedílnou součástí tohoto procesu je rovněž systematická příprava nové generace odborníků, neboť implementace a provoz SMR technologií vyžadují interdisciplinární přístup propojující dosud oddělené technické i netechnické obory.



Děkuji za pozornost

POUŽITÁ LITERATURA:

[1] *Small Modular Reactors: Advances in SMR Developments 2024.* Online. 2024. Dostupné z: https://doi.org/10.61092/iaea.3o4h-svum. [cit. 2026-03-14].

[2] KHARCHENKO, Vyacheslav; SHCHEHLOV, Vladyslav; IVASIUK, Oleksandr a MOROZOVA, Olga. *Digital Twin-Based Lifecycle Methodology for Ensuring Safety of NPP/SMR I.* Online. Technologies. 2026, roč. 14, č. 1, s. 46. ISSN 2227-7080. Dostupné z: https://doi.org/10.3390/technologies14010046. [cit. 2026-03-14].

[3] *IAEA Nuclear Energy Series No. NP-T-3.19*. Online. IAEA. 2017. Dostupné z: https://www.iaea.org/publications. [cit. 2026-03-14].

[4] SMALL MODULAR REACTORS (SMR). Online. Foreningen Atom-kraft Ja Tak. 2025. Dostupné z: https://rpmanetworks.com/atomkraftclonesite-english/docs/small-modular-reactors-smr/. [cit. 2025-01-26].

[5] BHAMARE, Deval; ZOLANVARI, Maede; ERBAD, Aiman; JAIN, Raj; KHAN, Khaled et al. Cybersecurity for industrial control systems: A survey. Online. *Computers*. 2020, roč. 89, s. 101677. ISSN 0167-4048. Dostupné z: https://doi.org/10.1016/j.cose.2019.101677. [cit. 2026-03-16].

[6] HUMAYUN, Mamoona; NIAZI, Mahmood; JHANJHI, NZ; ALSHAYEB, Mohammad a MAHMOOD, Sajjad. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Online. *Arabian Journal for Science and Engineering*. 2020, roč. 45, č. 4, s. 3171-3189. ISSN 2193567X. Dostupné z: https://doi.org/10.1007/s13369-019-04319-2. [cit. 2026-03-16].

[7] *Computer Security at Nuclear Facilities*. Online. IAEA. 2011. Dostupné z: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities. [cit. 2026-03-15].

[8] Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants [CP-08]. Online. NEA – NUCLEAR ENERGY AGENCY. 2022. Dostupné z: https://www.oecd-nea.org/jcms/pl_75241/consensus-position-on-the-impact-of-cyber-security-features-on-digital-instrumentation-and-control-systems-important-to-safety-at-nuclear-power-plants-cp-08?details=true. [cit. 2026-03-18].

POUŽITÁ LITERATURA:

[9] STOUFFER, Keith; PILLITTERI, Victoria; LIGHTMAN, Suzanne; ABRAMS, Marshall a HAHN, Adam. Guide to Industrial Control Systems (ICS) Security. Online. 2015. Dostupné z: https://doi.org/10.6028/nist.sp.800-82r2. [cit. 2026-03-22].

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 62443 – Industrial communication networks – Network and system security*. Geneva: IEC, 2007. 1. vydání. ISBN [cit. 2026-03-22].

[11] DANIELL, James; KOBAYASHI, Kazuma; ALAJO, Ayodeji a ALAM, Syed Bahauddin. Digital twin-centered hybrid data-driven multi-stage deep learning framework for enhanced nuclear reactor power prediction. Online. *Energy and AI*. 2025, roč. 19, s. 100450. ISSN 2666-5468. Dostupné z: https://doi.org/10.1016/j.egyai.2024.100450. [cit. 2026-03-22].

[12] *New CRP: Enhancing Computer Security of Small Modular Reactors and Microreactors*. Online. AEIA. 2024. Dostupné z: https://www.iaea.org/newscenter/news/new-crp-enhancing-computer-security-of-small-modular-reactors-and-microreactors?utm_source=chatgpt.com. [cit. 2026-03-18].

[13] MONDAL, Kunal; MARTINEZ, Oscar a JAIN, Prashant. Advanced manufacturing and digital twin technology for nuclear energy*. Online. *Frontiers in Energy Research*. 2024, roč. 12. ISSN 2296598X. Dostupné z: https://doi.org/10.3389/fenrg.2024.1339836. [cit. 2026-03-22].

[14] ČESKÁ AGENTURA PRO STANDARTIZACI. *Bezpečnost systémů pro průmyslovou automatizaci a řízení – Část 2-1: Požadavky na program bezpečnosti pro vlastníky aktiv IACS: ČSN EN IEC 62443-2-1*. Aktuální vydání. 2025. [cit. 2026-03-28].

[15] ČESKÁ AGENTURA PRO STANDARTIZACI. *Bezpečnost pro systémy průmyslové automatizaci a řízení – Část 4-2: Požadavky technické bezpečnosti pro součásti IACS: ČSN EN IEC 62443-4-2*. Aktuální vydání. 2019. [cit. 2026-03-28].

[16] *Managing Cybersecurity in Small Modular Reactors: Strategies for Addressing Modularity, Cloud, and Remote Operation Risks*. Online. OSTI.GOV - U.S. Department of Energy Office of Scientific and Technical Information. 2025. Dostupné z: https://www.osti.gov/servlets/purl/2588291?utm_source=chatgpt.com. [cit. 2026-03-18].

POUŽITÁ LITERATURA:

[17] YU, Hongcheng. A digital twin-based system for full-lifecycle safety management and dynamic risk assessment in nuclear power plants. Online. *Discover Artificial Intelligence*. 2025, roč. 5, č. 1. ISSN 2731-0809. Dostupné z: https://doi.org/10.1007/s44163-025-00618-w. [cit. 2026-03-23].

[18] *Digital transformation: Opportunities and challenges for the nuclear sector*. Online. NEA. 2021. Dostupné z: https://www.oecd-nea.org/jcms/pl_59100/digital-transformation-opportunities-and-challenges-for-the-nuclear-sector?utm_source=chatgpt.com. [cit. 2026-03-22].

[19] HUANG, Qingyu; ZENG, Wei; LIU, Jia; ZHANG, Zhuo; DENG, Jian et al. Shaping the future of nuclear reactors with digital twins: Current developments and perspectives. Online. *Applied Energy*. 2025, roč. 402, s. 126922. ISSN 0306-2619. Dostupné z: https://doi.org/10.1016/j.apenergy.2025.126922. [cit. 2026-03-23].

[20] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení: ČSN EN ISO/IEC 27004*. Aktuální vydání. 2018. [cit. 2026-03-28].

[21] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační technologie – Bezpečnostní technologie – Bezpečnostní postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002: ČSN EN ISO/IEC 27017*. Aktuální vydání. 2017. [cit. 2026-03-28].

[22] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti: ČSN EN ISO/IEC 27005*. Aktuální vydání. 2023. [cit. 2026-03-28].

[23] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační technologie – Bezpečnostní techniky – Opatření bezpečnosti informací pro energetický průmysl: ČSN EN ISO/IEC 27019*. Aktuální vydání. 2020. [cit. 2026-03-28].

[24] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu bezpečnosti informací – Požadavky: ČSN ISO/IEC 27001*. Aktuální vydání. 2023. [cit. 2026-03-28].

[25] ČESKÁ AGENTURA PRO STANDARTIZACI. *Bezpečnost systémů pro průmyslovou automatizaci a řízení – Část 3-2: Posouzení bezpečnostních rizik pro návrh systému: ČSN EN IEC 62443-3-2*. Aktuální vydání. 2021. [cit. 2026-03-28].

POUŽITÁ LITERATURA:

[26] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační technologie – Bezpečnostní technologie – Bezpečnost sítě – Část1: Přehled a pojmy: ČSN EN ISO/IEC 27033-1*. Aktuální vydání. 2016. [cit. 2026-03-28].

[27] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti: ČSN EN ISO/IEC 27002*. Aktuální vydání. 2023. [cit. 2026-03-28].

[28] GRASSI, Paul A; GARCIA, Michael E a FENTON, James L. Digital identity guidelines: revision 3. Online. 2017. Dostupné z: https://doi.org/10.6028/nist.sp.800-63-3. [cit. 2026-03-28].

[29] LOCATELLI, Giorgio; BINGHAM, Chris a MANCINI, Mauro. Small modular reactors: A comprehensive overview of their economics and strategic aspects. Online. *Progress in Nuclear Energy*. 2014, roč. 73, s. 75-85. ISSN 0149-1970. Dostupné z: https://doi.org/10.1016/j.pnucene.2014.01.010. [cit. 2026-03-15].

[30] The NIST Cybersecurity Framework (CSF) 2.0. Online. 2024. Dostupné z: https://doi.org/10.6028/nist.cswp.29. [cit. 2026-03-28].

[31] *Computer Security Techniques for Nuclear Facilities*. Online. IAEA. 2021. Dostupné z: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities. [cit. 2026-03-15].

[32] STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria et al. Guide to Operational Technology (OT) security. Online. 2023. Dostupné z: https://doi.org/10.6028/nist.sp.800-82r3. [cit. 2026-03-28].

[33] ROSE, Scott; BORCHERT, Oliver; MITCHELL, Stu a CONNELLY, Sean. Zero Trust Architecture. Online. 2020. Dostupné z: https://doi.org/10.6028/nist.sp.800-207. [cit. 2026-03-28].

[34] *Advances in Small Modular Reactor Technology Developments*. Online. IAEA. 2020. Dostupné z: https://aris.iaea.org/Publications/SMR_Book_2020.pdf. [cit. 2026-03-15].

[35] *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*. Online. IAEA. 2018. Dostupné z: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf. [cit. 2026-03-16].

POUŽITÁ LITERATURA:

[36] ČESKÁ AGENTURA PRO STANDARTIZACI. *Průmyslové komunikační sítě – Bezpečnost sítě a systému 3-3: Požadavky na bezpečnost systému a bezpečnostní úrovně: ČSN EN IEC 62443-3-3*. Aktuální vydání. 2019. [cit. 2026-03-28].

[37] Considerations for Deploying Artificial Intelligence Applications in the Nuclear Power Industry. Online. *IAEA Nuclear Energy Series*. 2025. ISBN 9789201155252. ISSN 1995-7807. Dostupné z: https://doi.org/10.61092/iaea.s6uy-wjt8. [cit. 2026-03-28].

[38] ČESKÁ AGENTURA PRO STANDARTIZACI. *Informační technologie – Management incidentů – informační bezpečnosti: Část1: Principy a proces: ČSN EN ISO/IEC 27035-1*. Aktuální vydání. 2024. [cit. 2026-03-28].

[39] KAPOOR, Sarthak; KUMAR, Sumit a VARDHAN, Harsh. *Cyber security of OT networks: A tutorial and overview*. Online. Cornell Univerzity. 2025. Dostupné z: https://arxiv.org/abs/2502.14017. [cit. 2026-03-18].