# Konsolidovaný a standardizovaný implementační model bezpečnosti IT/OT pro SMR

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

***Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,***

***Ústav elektroniky a měření***

***email: a1_navratil@utb.cz***

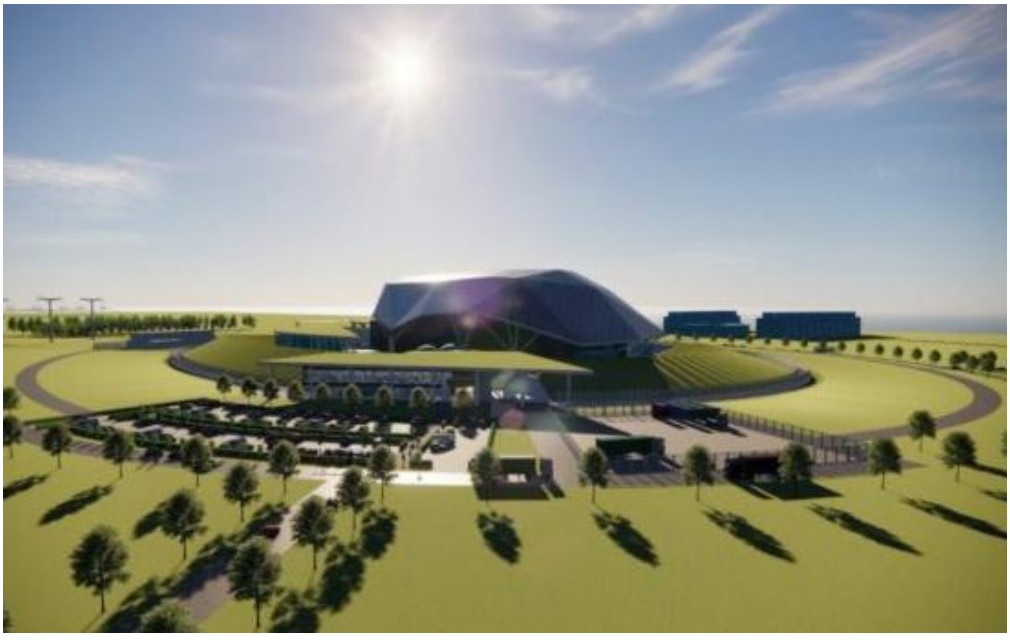
***Souhrn***

*Malé modulární reaktory (dále jen „SMR“) představují novou generaci jaderných reaktorů, které budou navrhovány s důrazem na modulární konstrukci, vysokou úroveň bezpečnosti a flexibilitu implementace. Na rozdíl od tradičních velkých jaderných elektráren jsou SMR koncipovány tak, aby mohly být vyráběny sériově a instalovány postupně podle potřeb energetického systému. Moderní návrhy SMR předpokládají rozsáhlé využití digitálních technologií, zejména v oblasti systémů instrumentace a řízení (dále jen „I&C“). Tyto systémy budou umožňovat automatizované řízení provozu, pokročilé monitorování provozních parametrů a implementaci analytických nástrojů pro optimalizaci výkonu a údržby. V některých částech této práce jsou záměrně ponechány anglické výrazy převzaté z anglicky psaných norem, protože v českém jazyce pro ně neexistují zcela přesné ekvivalenty.*

***Klíčová slova:*** *malé modulární reaktory, informační technologie, provozní technologie.*

## Digitalizace systémů SMR

Digitalizace představuje jeden z klíčových trendů moderní energetiky [1]. V případě SMR se předpokládá výrazné zlepšení provozní efektivity, bezpečnosti a spolehlivosti při implementaci digitálních řídicích systémů [2; 3]. Moderní I&C budou využívat rozsáhlé sítě senzorů, řídicích jednotek a analytických nástrojů, které budou umožňovat kontinuální monitoring provozních parametrů. Tato data mohou být využívána pro prediktivní údržbu, optimalizaci provozu a podporu rozhodování operátorů [2; 4].

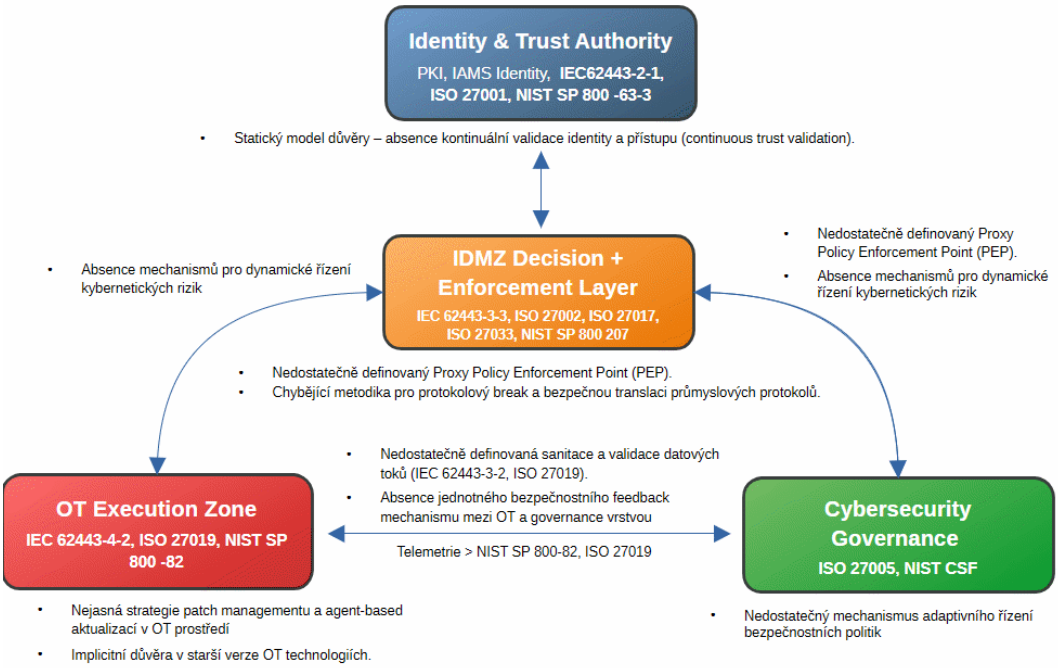


***Obrázek 1. Návrh jaderné elektrárny SMR společnosti Rolls-Royce [2].***

V prostředí SMR bude digitalizace ještě významnější, protože modulární architektura reaktorů bude umožňovat standardizaci digitálních řídicích systémů a jejich integraci do centralizovaných monitorovacích platforem [1; 2]. Při zvyšování míry digitalizace bude docházet ke komplexitě technologické infrastruktury a tím se budou vytvářet nové bezpečnostní hrozby. Půjde zejména o hrozby v oblasti kybernetických útoků. Je tedy nutné zavedení jednotného bezpečnostního konceptu v rámci všech systémů SMR [5; 6].

## Digitalizace systémů SMR

Digitalizace průmyslových systémů přináší řadu výhod, současně však vede ke zvýšení složitosti bezpečnostního prostředí [7; 8]. Jedním z hlavních problémů je dynamika a komplexita při detekci vektorů kybernetických útoků [7]. Integrace digitálních systémů vytváří nové komunikační kanály, které mohou být potenciálně zneužity útočníky [8]. Dalším problémem je složitost správy bezpečnostních opatření. Moderní energetické systémy budou zahrnovat velké množství zařízení a softwarových komponent, které musí být správně nakonfigurovány a pravidelně aktualizovány [9]. Z tohoto důvodu je nutné sladit, popřípadě upravit legislativní a normativní rámec. Dále musí dojít k jednoznačnosti při koncepci kybernetické bezpečnosti, založené na vícevrstvém přístupu, který integruje strategické řízení bezpečnosti, procesní řízení a technologická opatření [9; 10]. V rámci SMR je stále nutné dodržovat zásady, které nařizují nezávislost bezpečnostních systémů na externích sítích. Dále samotné systémy reaktorů musí být řízeny lokálně a izolovaně. V rámci cloudových technologií musí být využity pouze podpůrné funkce. Celkově lze říct, že systémy SMR musí nadále fungovat i při úplném výpadku internetového připojení nebo výpadku celkové externí komunikace [11; 12; 13].



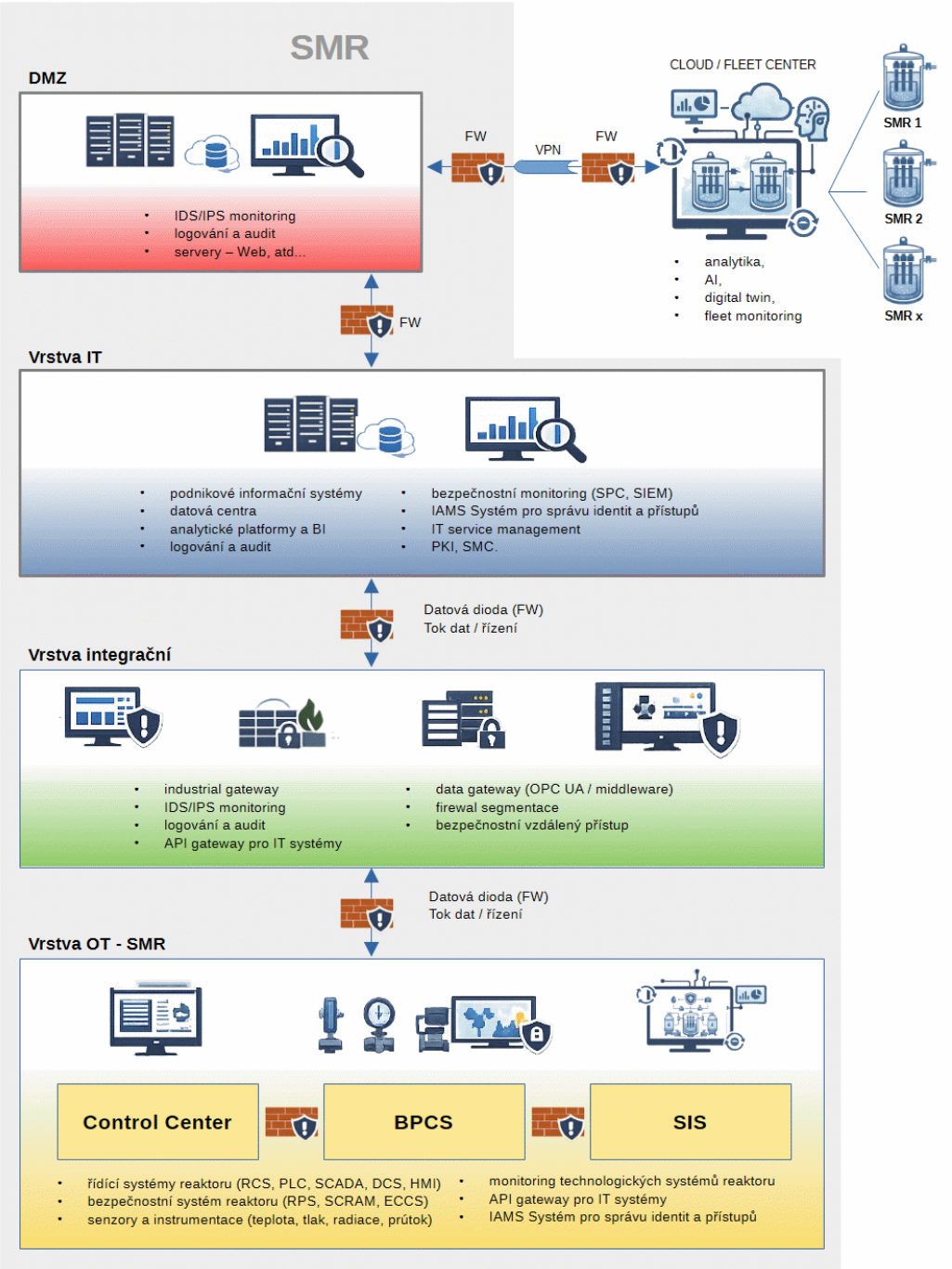

***Obrázek 2: Příklad kritické analýzy současných bezpečnostních standardů pro IT/OT v kontextu SMR (vlastní zpracování na základě [12–33]).***

## Integrace IT a OT systémů

Integrace IT a OT se bude stávat strategickým faktorem ovlivňujícím bezpečnost, ekonomiku a regulatorní přijatelnost projektů SMR [25; 26]. Integrace těchto dvou technologických domén bude umožňovat efektivnější provoz a lepší analytické schopnosti [2]. Současně však bude kladen větší důraz na kybernetickou bezpečnost mezi jednotlivými technologickými vrstvami [27].

V oblasti propojení IT a OT je nutná jednotná bezpečností architektura, která v sobě bude zahrnovat: architekturu založenou na segmentaci sítí a definovaných bezpečnostních zónách [10; 27], propojení mezi zónami musí být realizováno pouze prostřednictvím řízených rozhraní „Controlled Interfaces“,

řízení a monitorování datových toků mezi zónami [10], aplikaci principu „Defence in Depth“ [10; 11; 12], provedení hodnocení rizik před zavedením nebo změnou konektivity mezi IT a OT [12; 27], použití demilitarizované zóny (dále jen „DMZ“) mezi podnikovou a provozní sítí, ochranu systémů důležitých pro jadernou bezpečnost a ochranu před kybernetickými hrozbami vyplývajícími z propojení s méně chráněnými sítěmi [11; 12; 25].



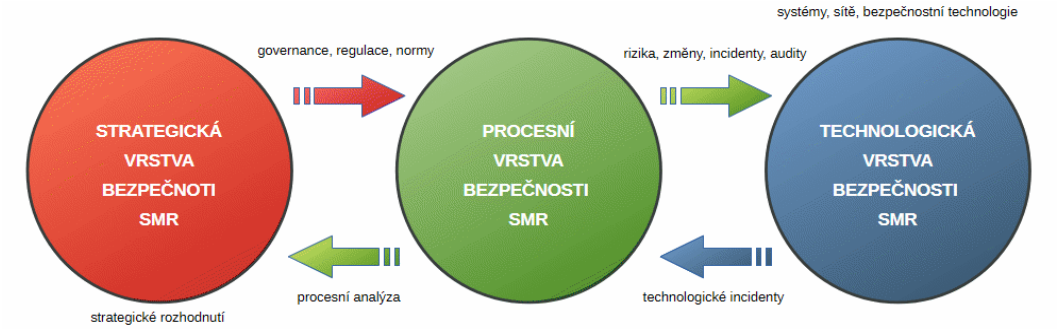

***Obrázek 3: Architektura IT/OT pro SMR (vlastní zpracování na základě [11; 12; 30; 31]).***

## 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 [17; 21]. Navrhovaný bezpečnostní model musí integrovat základní technologická opatření, procesní řízení a strategické řízení bezpečnosti [17; 37]. Další vrstvy pak budou: fyzická bezpečnost, lidský faktor, integrace „Safety a Security“ [17; 24; 28].

Základní vrstvy [11; 14; 23]:

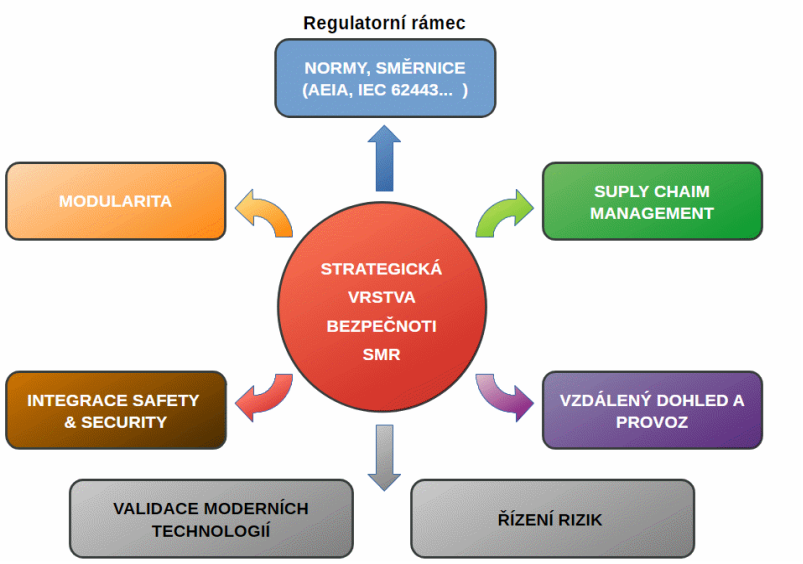
- strategická vrstva „Governance“,
- procesní vrstva „Safety Management Processes“,
- technologická vrstva „Technical Implementation“.




***Obrázek 4: Základní rozdělení (vlastní zpracování na základě [11; 14; 23; 34]).***

## 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 [10; 29; 35]. Současné normy, například normy řady IEC 62443 nebo doporučení International Atomic Energy Agency (dále jen „IAEA“), poskytují základní rámec, ale nejsou plně přizpůsobeny specifikům SMR. Ty přinášejí vysokou modularitu, digitalizaci a možnost vzdáleného provozu, což vyžaduje doplnění procesů pro řízení jednotlivých vrstev, jejich propojení a bezpečnost dodavatelského řetězce [9; 12; 27]. Dalším klíčovým bodem je integrace „Safety a Security“. Standardy se tradičně řeší odděleně, ale v SMR mohou kybernetické incidenty ovlivnit například fyzickou bezpečnost. Strategická vrstva proto stanovuje jednotný rámec pro řešení konfliktů mezi bezpečností provozu a kybernetickou ochranou a zahrnuje procesy pro validaci moderních automatizačních technologií, včetně AI [2; 12; 16]. Celkově musí strategická vrstva zajišťovat komplexní, systematické a dlouhodobé řízení bezpečnosti, doplněné o procesy reflektující specifika SMR. Jedná se například o modularitu, „Supply Chain“, integraci „Safety a Security“ a vzdálený dohled a provoz [9; 12; 14; 29].

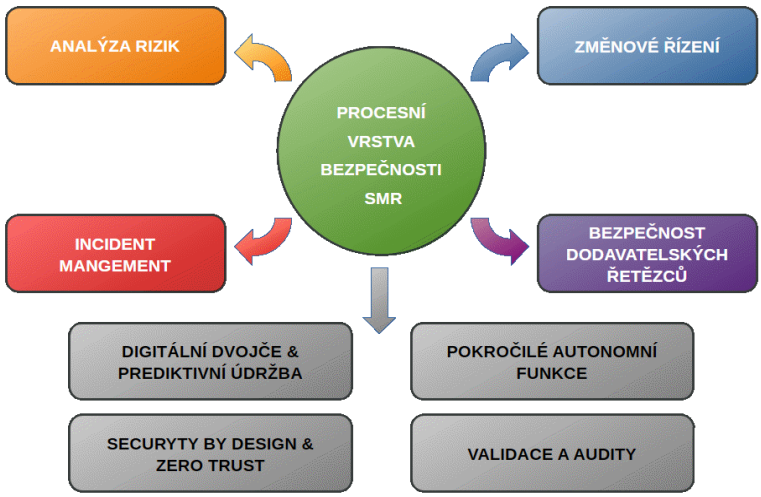



***Obrázek 5: Strategická vrstva bezpečnosti rizik (vlastní zpracování na základě [14; 29; 36; 38]).***

### Procesní vrstva (Safety Management Processes)

Procesní vrstva musí být spojená s odpovídající procesní koncepcí [10]. Zásadní roli musí sehrát analýza rizik, která musí zahrnovat analýzu dopadů s dopadem na inovativní koncept bezpečnosti SMR [9; 10]. Neméně důležitá je oblast incident managementu, kde musí být jasně definovány scénáře zahrnující kybernetické útoky na zařízení I&C. Příkladem může být například narušení komunikace mezi systémy. Zde by měly být efektivní incident managment v rámci koordinace mezi IT bezpečností, provozním personálem a krizovým řízením [9; 14]. V prostředí SMR musí být rovněž nezbytné zavedení změnového řízení, které zahrnuje důkladnou validaci každé změny v izolovaném nebo testovacím prostředí. Je to z důvodů minimalizace rizika narušení bezpečnosti a provozní stability [14; 15]. Významnou součástí procesní vrstvy by měla být koncepce pro bezpečnost dodavatelského řetězce. Zde musí být definována důsledná kontrola dodavatelů pro SMR [1; 15].

V kontextu moderních SMR se však musí procesní vrstva dále rozšiřuje o inovativní přístupy založené na digitalizaci a automatizaci. Významným trendem je využití digitálních dvojčat, která umožní prediktivní údržbu, simulaci poruchových stavů a optimalizaci provozu v reálném čase [1; 16; 18]. Další inovací by měla být implementace pokročilých autonomních bezpečnostních funkcí s prvky hlubokého učení a neuronových sítí. Tyto pokročilé technologie musí vytvářet podporu včasné detekci anomálií a rozhodování operátorů, samozřejmě při zachování principu „Human in the Loop“ [14; 16; 18]. Dále musí být prosazován koncept „Security by Design“, zahrnující „Zero Trust Architekturu“, segmentaci sítí a integraci bezpečnosti již ve fázi návrhu [14; 15; 23]. Inovace se musí také týkat dodavatelských řetězců, kde se musí využívat pokročilé metody sledování komponent a kontinuální verifikace například softwaru [15; 23]. Tyto přístupy musí být jasně definovány, aby tak mohli reflektovat oblast výstavby SMR. Je nutné si uvědomit, že dojde k evoluci od izolovaných k integrovaným bezpečnostním opatřením, datově řízenému a adaptivnímu systému řízení bezpečnosti [1; 16; 18].

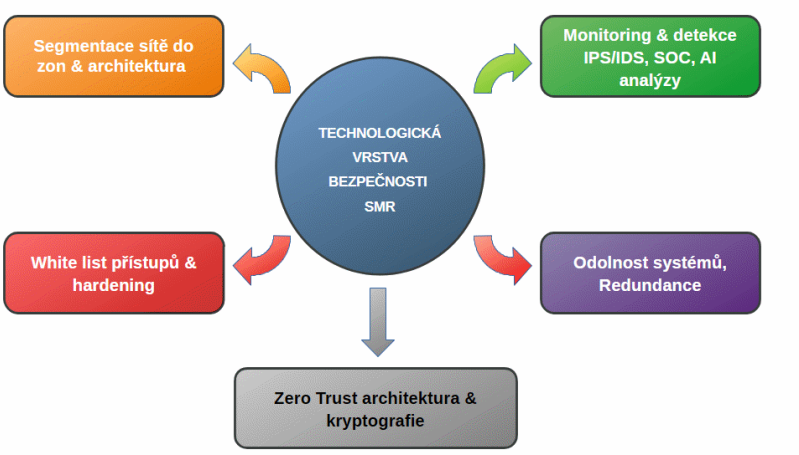



***Obrázek 6: Procesní vrstva bezpečnosti rizik (vlastní zpracování na základě [18; 19; 25; 27; 32; 39; 40; 44]).***

### Technologická vrstva (Technical Implementation)

Technologická vrstva zahrnuje implementaci specifikovaných bezpečnostních nástrojů a architektonických principů pro ochranu kritických zařízení [10]. Důležitým prvkem musí být segmentace systémů do zón, které musí oddělovat bezpečnostní, řídicí (I&C) a IT systémy, přičemž mezi nimi mohou být využity mechanismy jako air-gap nebo datové diody v souladu s modelem „Zones and Conduits“ dle standardu International Electrotechnical Commission (dále jen „IEC“) 62443 [39]. Ochrana kritických systémů zahrnuje „Whitelist“ přístupů, „Hardening“ zařízení (PLC, DCS, SCADA), omezení vzdáleného přístupu a vhodně implementovanou kryptografii [10; 30; 37]. Monitoring a detekce musí být zajištěny pomocí IPS a IDS sond, analýzy anomálií s využitím centrálního bezpečnostního dohledu (dále jen

„SOC“) [10; 13; 18]. Důležitá je také odolnost systémů, zahrnující redundanci, „Fail Safe“ režimy a schopnost bezpečného odstavení nejen reaktoru. Může se jednat například o výpadek serverových nebo diskových zařízení [10].




***Obrázek 7: Technická vrstva bezpečnosti rizik (vlastní zpracování na základě [11; 13; 18; 20; 26; 28; 31; 32; 40; 41]).***

## 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 SMR.

Budoucí výzkum a vývoj by se měl systematicky zaměřit na ověření navrženého modelu prostřednictvím pilotních projektů v oblasti SMR, které umožní posoudit jeho funkčnost, spolehlivost a praktickou aplikovatelnost v reálných podmínkách. Současně je nezbytné pokračovat v jeho dalším rozvoji s ohledem na dynamicky se vyvíjející technologické a regulatorní požadavky, přičemž získané poznatky mohou být přenositelné i do dalších systémů kritické infrastruktury. 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.

## Seznam použité literatury


[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] *Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors*. Online. IAEA. 2022. Dostupné z: https://www.iaea.org/events/evt2100684?utm_source=chatgpt.com. [cit. 2026-03-14].

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

[5] EGGERS, Shannon a ANDERSON, Robert. Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control. Online. *Nuclear Reactors - Spacecraft Propulsion, Research Reactors, and Reactor Analysis Topics*. 2022. ISBN 9781839699399. Dostupné z: https://doi.org/10.5772/intechopen.101807. [cit. 2026-03-14].

[6] AYODEJI, Abiodun; MOHAMED, Mokhtar; LI, Li; DI BUONO, Antonio; PIERCE, Iestyn et al. Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. Online. *Progress in Nuclear Energy*. 2023, roč. 161, s. 104738. ISSN 0149-1970. Dostupné z: https://doi.org/10.1016/j.pnucene.2023.104738. [cit. 2026-03-14].

[7] 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].

[8] 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].

[9] *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].

[10] *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].

[11] 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].

[12] *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].

[13] *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].

[14] 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].

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

[16] 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].

[17] *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].

[18] 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].

[19] 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].

[20] 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].

[21] *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].

[22] 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].

[23] *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].

[24] 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].

[25] 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].

[26] 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].

[27] 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].

[28] 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].

[29] 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].

[30] 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].

[31] 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].

[32] 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].

[33] 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].

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

[35] 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].

[36] 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].

[37] *Critical Infrastructure Cybersecurity: Key Concepts Explained*. Online. SSH Academy. 2025. Dostupné z: https://www.ssh.com/academy/operational-technology/critical-infrastructure-cybersecurity-key-concepts-explained?utm_source=chatgpt.com. [cit. 2026-03-18].

[38] *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].

[39] 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].

[40] 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].

[41] 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].

[42] *Guide to Industrial Control Systems (ICS) Security*. Online. NIST Technical Series Publications. 2015. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. [cit. 2026-03-18].

[43] ČESKÁ AGENTURA PRO STANDARTIZACI. *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Správa a řízení bezpečnosti informací: ČSN EN ISO/IEC 27014*. Aktuální vydání. 2021. [cit. 2026-03-28].

[44] 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].

## Seznam použitých symbolů a zkratek

| | |
|---|---|
| AEIA | International Atomic Energy Agency |
| AI | Artificial Intelligence |
| BI | Business Intelligence |
| BPCS | Basic Process Control System |
| DCS | Distributed Control System |
| DMZ | Demilitarized Zone |
| FW | Firewall |
| HIM | Human Machine Interface |
| I&C | Instrumentation and Control |
| IAMS | Identity and Access Management System |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| OPC UA | Open Platform Communications Unified Architecture |

| | |
|---|---|
| OT | Operational Technology |
| PEP | Policy Enforcement Point |
| PKI | Public Key Infrastructure |
| PLC | Programmable Logic Controller |
| RCS | Reactor Coolant System |
| RPS | Reactor Protection System |
| SCADA | Supervisory Control and Data Acquisition |
| SCRAM | Salted Challenge Response Authention Mechanism |
| SIS | Safety Instrumented System |
| SMC | Security Management Center |
| SMR | Small Modular Reactor |
| SOC | Security Operations Center |