Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2024 Proceedings | Mediterranean Conference on Information Systems (MCIS)

10-3-2024

Governance of IT/OT Convergence: A Review of Academic and Practitioner Literature

Carolin Hantsch
4C Group AG, carolin.hantsch@4cgroup.com

Markus Westner
OTH Regensburg, markus.westner@oth-regensburg.de

Follow this and additional works at: https://aisel.aisnet.org/mcis2024

Recommended Citation

Hantsch, Carolin and Westner, Markus, "Governance of IT/OT Convergence: A Review of Academic and Practitioner Literature" (2024). *MCIS 2024 Proceedings*. 7.
https://aisel.aisnet.org/mcis2024/7

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2024 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

GOVERNANCE OF IT/OT CONVERGENCE: A REVIEW OF ACADEMIC AND PRACTITIONER LITERATURE

Research full-length paper

Hantsch, Carolin, 4C Group AG, Munich, Germany, carolin.hantsch@4cgroup.com

Westner, Markus, OTH Regensburg, Regensburg, Germany, markus.westner@oth-regensburg.de

Abstract

The convergence, i.e., integration, of Information Technology (IT) and Operational Technology (OT) is a critical aspect of digital transformation in industries, driving efficiency, innovation, and competitive advantage. However, this integration also introduces significant challenges, particularly in governance. This paper presents a comprehensive literature review of IT/OT convergence, focusing on the governance challenges and strategies drawn from both academic and practitioner literature. The findings reveal that effective governance is crucial for successful IT/OT convergence, requiring clear definitions of roles and responsibilities, cross-functional collaboration, and a unified approach to mitigate risks and align organizational goals. Key IT/OT convergence governance strategies include establishing a Center of Excellence, adopting a risk-based approach, and fostering a culture of change. The paper highlights the need for further research to develop comprehensive governance frameworks and empirically examine the impact of governance on IT/OT convergence success. This paper provides valuable insights for both researchers and practitioners navigating the complexities of IT/OT convergence and governance in the era of Industry 4.0.

Keywords: IT/OT convergence, governance, digital transformation, Industry 4.0.

1 Introduction

Information Technology (IT)/Operational Technology (OT) convergence, i.e., integration, is a critical aspect of Industry 4.0, driving the digital transformation of industrial operations (Ehie and Chilton, 2020). However, the integration of IT and OT poses significant challenges, particularly in the area of governance (Gharpure et al., 2022).

The existing literature on IT/OT convergence focuses primarily on the technical aspects, such as cybersecurity, architecture and infrastructure (Corradi et al., 2022; Dutta et al., 2021). While these aspects are undoubtedly important, there is a lack of comprehensive research on the governance challenges associated with IT/OT convergence (Kiener et al., 2021; Sivasubramaniyan, 2021).

To address this gap, this paper aims to answer the following research question:

RQ: What is the current state of research on IT/OT convergence, with a particular focus on governance, as identified in the academic and practitioner literature?

To answer this question, we conducted a comprehensive literature review, encompassing both academic and practitioner perspectives, to explore the governance challenges posed by IT/OT convergence and to propose strategies for addressing them effectively. The review includes a systematic analysis of academic articles, industry reports, case studies and best practice guidelines related to IT/OT convergence and its governance.

The findings of our paper show that effective governance is critical to managing the complexities and risks associated with IT/OT convergence. Key governance challenges include defining roles and responsibilities, establishing policies and procedures, and ensuring compliance with industry standards and regulations (Ehie and Chilton, 2020; Verhaeghe et al., 2021). Our paper also identifies best practices and strategies to address these challenges, such as establishing an IT/OT convergence Centre of Excellence (CoE), adopting a risk-based approach, and fostering a culture of change (AWS, 2022; Bronson, 2022; Hayes, 2020).

By providing a comprehensive overview of governance challenges and strategies in IT/OT convergence, our paper extends existing knowledge in the field and offers valuable insights for practitioners seeking to navigate the complexities of digital transformation in the industrial sector. The findings contribute to the development of more effective governance frameworks and practices that can support successful IT/OT convergence initiatives.

The remainder of this paper is structured as follows: Section 2 provides background information on key concepts related to IT/OT convergence and governance. Section 3 describes the research methodology employed in this paper. Sections 4 presents the findings from the academic and practitioner literature, respectively. Section 5 discusses the implications of these findings and identifies gaps for future research. Finally, Section 6 concludes the paper by summarizing the main contributions and limitations of our paper.

2 Background

2.1 IT vs. OT

IT encompasses all information processing technologies and related services, including hardware, software, networks, and databases (Reynolds, 2016). IT applications manage and protect data involved in various organizational processes like Enterprise Resource Planning and Customer Relationship Management (Shilenge and Telukdarie, 2022).

OT – sometimes known as Operations Technology – refers to hardware and software that directly monitor and control physical devices and industrial processes. OT is commonly used in systems like Industrial Control Systems (ICS), Distributed Control Systems, Programmable Logic Controllers, or

Supervisory Control and Data Acquisition (SCADA) systems, which are integral to managing industrial equipment (Cisco, 2022; Garimella, 2018).

2.2 IT/OT convergence and related terms

IT/OT convergence involves linking OT with IT systems to integrate directly into organizational processes. This convergence aims to merge, i.e., integrate, IT and OT systems and functionalities (Ehie and Chilton, 2020). IT/OT alignment refers to the process adjustments during IT/OT convergence, whereas IT/OT integration defines the final state of a fully integrated IT and OT environment (Gartner, 2023a, 2023b).

2.3 IT governance

IT governance involves measures, procedures, and principles ensuring that IT supports the organization's goals effectively and responsibly (Meyer et al., 2003). It is focused on aligning IT development with business strategies and objectives and establishes the critical link between IT and business strategies, primarily overseen by the board of directors (Haes and van Grembergen, 2005).

3 Methodology

To provide a comprehensive overview of IT/OT convergence and its relation to governance, both a semi-structured database search for academic literature and a web search for practitioner literature were conducted.

3.1 Database search for academic literature

The literature search utilized the databases AISeLibrary, Google Scholar, IEEEXplore, and Scopus focusing on literature published between January 2018 and beginning of 2023. The search targeted publications related to IT/OT convergence and governance with the query:

(("IT OT" OR "OT IT" OR ("Information Technology" AND "Operational Technology") OR ("Operational Technology" AND "Information Technology")) AND ("Convergence" OR "Governance")).

In IEEEXplore and Scopus, the query was limited to the title, abstract, and keywords, while AISeLibrary searched in all fields since a limitation on title, abstract, and keywords is not supported. Google Scholar's search was limited to titles only to manage the scope of results.

This process yielded 131 contributions. After excluding non-English or non-German articles, inaccessible texts, and duplicates, and removing irrelevant or tangentially related papers, 37 publications remained, with four specifically addressing governance. The majority of these were journal articles, with significant contributions in 2021 as displayed in Figure 1.

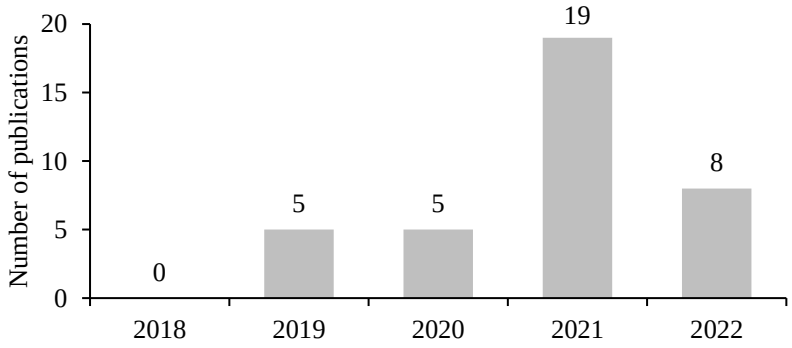

Figure 1. Year of publication – academic literature

3.2 Web search for practitioner literature

The exploratory web search aimed to capture the practitioner's perspective on IT/OT convergence, particularly from consultancies. No date restrictions were applied. Titles and content were initially scanned to assess relevance, resulting in 16 articles that addressed IT/OT convergence and often included discussions of governance.

Most articles were sourced from prominent consulting firms like Accenture, Deloitte, and McKinsey & Company. Publications from this search primarily appeared in 2021 as displayed in Figure 2, with notable contributions also coming from renowned companies such as Amazon Web Services (AWS) and Cisco.

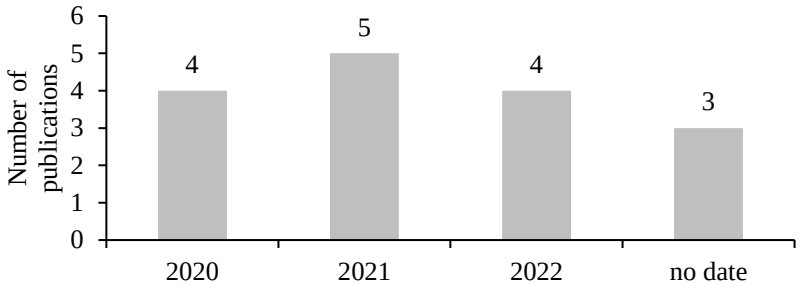

Figure 2. Year of publication – practitioner literature

Both the academic and practitioner findings will be synthesized to illuminate current trends and issues in IT/OT convergence and governance.

4 Findings

4.1 Academic literature

A review of the academic literature shows a predominant focus on security, technology, infrastructure and architecture approaches to IT/OT convergence, with only a fraction addressing governance in different contexts. Our paper focuses primarily on governance, while briefly touching on other aspects. Publications are categorised into security, technology and infrastructure, architecture and governance, with some covering more than one topic. Each sub-chapter is introduced by a brief summary of the findings.

4.1.1 Characterization of IT/OT convergence

The existing literature on IT/OT convergence outlines the requirements, benefits, challenges, and key enablers of this phenomenon. It emphasises the importance of consistent alignment, communication, and adaptability between IT and OT departments to overcome organisational, infrastructural, and security challenges and achieve sustainable convergence.

Khan et al. (2022) outline IT/OT convergence requirements including extensive asset distribution, standards for data exchange, significant data processing needs, centralized data delivery, and system monitoring and maintenance.

The benefits of convergence include enhanced monitoring, data accuracy, real-time system availability, transparency, efficient asset management, improved decision-making, and energy savings (Garimella, 2018; Zahran et al., 2021). These lead to improved collaboration, more precise key performance indicators (KPIs), automated workflows, better utilization of machinery, and lower maintenance costs (Corradi et al., 2022; Dhlamini and Mawela, 2022).

However, challenges persist, primarily the siloed nature of IT and OT departments, which foster disparate practices, priorities, and governance structures (Dhlamini and Mawela, 2022; Garimella, 2018). This separation contributes to security vulnerabilities and integration issues, alongside resistance to change from employees fearing job loss (Dhlamini and Mawela, 2022).

Gharpure et al. (2022) categorize convergence challenges into organizational, infrastructural, and security domains. Organizational issues stem from communication gaps and diverse KPIs, while infrastructure challenges relate to outdated systems struggling to keep pace with technological advancements and high update costs. These factors make OT systems especially prone to cyber-attacks, heightening security risks (Dhlamini and Mawela, 2022; Gharpure et al., 2022).

Key enablers for overcoming these challenges include integrating IT operations into core business processes, cross-functional employee training, organizational restructuring, and a metrics-driven strategy (Corradi et al., 2022; Dhlamini and Mawela, 2022). Garimella (2018) highlights the benefits of data quality management solutions, such as standardized OT protocols and enhanced cybersecurity measures, for smoother IT/OT integration. Consistent alignment, communication, and adaptability between IT and OT departments are crucial for sustainable convergence (Gharpure et al., 2022).

4.1.2 Security

The existing literature highlights the increasing security concerns associated with IT/OT convergence, particularly in Cyber Physical Systems (CPS) across various sectors. Researchers are actively developing risk assessment tools, secure infrastructures, and advanced detection systems to address these challenges and ensure robust cybersecurity strategies in Industry 4.0 and critical infrastructure environments.

Progoulakis et al. (2021) highlight CPS security in the maritime sector, while Chattha et al. (2021) discuss real-time safety testing using CPS. Hollerer et al. (2021) explore the merging of IT and OT's impacts on safety and security within Austrian industry, emphasizing risk management and secure infrastructures.

Zahran et al. (2021) and Kanamaru (2021) present systems for Industrial Internet of Things (IIoT) risk assessment, addressing security concerns in industrial automation. Mubarak et al. (2021) have developed technologies for real-time ICS cyber-attack detection, reflecting the increasing threats due to IT/OT convergence.

Trifonov et al. (2021) discuss the adaptability of IT security systems for industrial use, integrating artificial intelligence for enhanced security measures. Mantravadi et al. (2020) and Shah (2019) focus on designing secure infrastructures for Industry 4.0 and critical infrastructures, respectively, underscoring the need for robust cybersecurity strategies.

Furthermore, Rosa et al. (2021) review anomaly detection frameworks for SCADA systems, demonstrating advances in intrusion detection. Muguira et al. (2020) and Azarmipour et al. (2020) explore secure data transmission technologies, emphasising the importance of secure gateways and cryptography in maintaining secure IT/OT interactions.

4.1.3 Technology and infrastructure

The literature demonstrates that researchers are developing various tools, frameworks, and models to address the challenges and opportunities associated with IT/OT convergence. These include enhancing communication, data management, and system maintenance in Industry 4.0 and IIoT environments.

Pokhrel and Garg (2021) explore wireless communication in Industry 4.0, developing a deep Q-network to enhance multipath communication for smart manufacturing. Garimella (2018) presents a case study on the implementation of IT/OT convergence in an electrical utility context, outlining the associated benefits and challenges. Scheffer et al. (2021) subsequently investigate the use of augmented reality for maintaining IT/OT systems, with a particular focus on digital trains, and demonstrate how this can

enhance failure resolution. The and Kuusk (2021) analyse digital transformation in Industry 4.0, extending the ISA95 framework to include data management under the RAMI 4.0 model.

Corradi et al. (2022) developed a software prototype to support reliable data management for small to medium-sized enterprises in manufacturing, facilitating internal and external data exchange. Saurav et al. (2021) developed SCADA WebView, a distributed web-based enterprise transmission engine, with the objective of enhancing IT/OT data interactions.

Koorapati et al. (2022) concentrated on the creation of a unified ontology for Internet of Things (IoT) ecosystems within enterprises, with the intention of addressing IT/OT convergence challenges. Khan et al. (2022) propose a digital twin model for the IIoT with the objective of centralising and analysing data, thereby streamlining the processes of IT/OT convergence.

4.1.4 Architecture

The literature indicates that researchers are engaged in the active exploration and development of architectures, middleware solutions, and frameworks with the objective of facilitating and optimising the convergence of IT and OT. This is being addressed through the identification and resolution of challenges such as security, real-time performance, and the management of centralised data.

Åkerberg et al. (2021) discuss future scenarios for process automation and the evolving architecture of factories. Patera et al. (2021) propose a two-layered middleware architecture tailored for IT and OT integration, accompanied by software solutions that support these functions. Foschini et al. (2021) introduce a software-defined network architecture that enhances IT/OT convergence and assess its resilience against denial-of-service attacks. Pop et al. (2021) present a fog computing platform designed for IIoT applications that facilitates IT/OT convergence. Kourtis et al. (2022) develop a prototype architecture for Industry 4.0 and 5G systems that integrates various OT devices on the factory floor. Shilenge and Telukdarie (2022) propose an optimised IT/OT integration architecture based on the RAMI 4.0 framework, with a particular focus on the management of centralised data and the real-time performance of the system. Lara et al. (2019) extend the enterprise architecture modelling language ArchiMate 3.0 to include OT, thereby enhancing the capabilities of enterprise modelling.

4.1.5 Governance

Relationship of IT governance to IT/OT convergence and IoT

Ehie and Chilton (2020) examine the influence of IT governance, IT/OT infrastructure, and interoperability, in conjunction with staff collaboration, on the convergence of IT and OT and the adoption of IoT. They define interoperability as the capability of distributed systems to communicate. The survey involved 239 U.S. manufacturing firms, with respondents including Chief Executive Officers, Chief Information Officers (CIOs), IT directors, and senior IT specialists. The key findings indicate that IT governance, infrastructure, and system interoperability are crucial for IT/OT convergence, with a positive effect on it. In contrast, staff collaboration did not directly correlate with convergence, but was significant when linked with IT governance, suggesting a major influence through joint development. Ehie and Chilton (2020) also indicate a strong connection between IT/OT convergence and IoT adoption, highlighting a significant mediation effect of convergence.

Implementation model for IT/OT convergence

Gharpure et al. (2022) outline a multi-dimensional implementation model for IT/OT convergence tailored to organizational maturity levels. The model encompasses five phases:

(1) Baseline and Awareness: Evaluate systems, establish a company-specific baseline, and define the integration team, ensuring transparent communication to all stakeholders.

(2) Trust Building and Buy-In: Address major organizational changes, build consensus on the need for convergence, and introduce collaborative management processes to handle ownership issues and enhance competitiveness.

(3) Process and Governance Model: Develop KPIs and standardized plans, including software governance, lifecycle management, and cybersecurity strategies. Introduce a governance hierarchy to mitigate security risks.

(4) Convergence: Achieve data flow and visibility between IT and OT, enhancing transparency along the supply chain and real-time decision-making.

(5) Standardization and Optimization: Following convergence, integrate all components, including resources and stakeholders, into a networked structure to streamline processes, reduce personnel needs, and incorporate stakeholder feedback into continuous improvement.

The implementation emphasizes culturally sensitive leadership and the establishment of a clear governance structure during phases two and three to support effective IT/OT convergence.

Critical success factors for IT/OT convergence in the energy sector

Dhlamini and Mawela (2022) emphasise the significance of IT/OT convergence, particularly for smart grid implementations in the energy sector where seamless data exchange between IT and OT is crucial. The study included an online survey of 30 participants from both IT and OT departments and two semi-structured interviews with department managers. However, it should be noted that all participants were from the same organisation.

The findings indicated a disparity in the understanding and vision of IT/OT convergence. Two-thirds of participants understood the concept, but fewer than half had a clear vision for it. Nevertheless, over half of the respondents acknowledged the existence of clearly defined roles for collaboration. The presence of information silos, identified through poor communication and differing skills among teams, highlights the necessity for cross-functional training.

Dhlamini and Mawela (2022) identified four critical success factors for IT/OT convergence: (1) Clearly defined and possibly revised roles for IT and OT; (2) A unified reporting structure under a single head or a merged department; (3) Consolidated support groups for IT and OT reporting directly to a CIO or Chief Technology Officer; and (4) Cross-functional, multi-skilled team members.

These factors underscore the central role of effective governance in ensuring successful IT/OT convergence, as proper role definition and unified reporting structures are pivotal.

Technology, organization, and people as governance dimensions

In their study, Kuusk and Gao (2021) present a framework that facilitates data-driven decision-making through the integration of IT, OT, and IoT. This framework targets improvements in time and cost efficiencies during digital transformation in engineering asset management organisations. It is observed that there has been a historical separation of IT and OT, which have developed distinct characteristics in information and operational technology, organisational processes, and personnel aspects.

The research, which is based on seven case studies and a comprehensive Delphi survey involving technology and engineering experts, identifies critical factors across three governance dimensions: technology, organisation, and people. The key factors include:

(1) Technology: Interoperability, IT architecture, data modeling, technology security.

(2) Organization: Resource management, project and risk management, information quality, strategic alignment.

(3) People: Training, skills and knowledge, roles.

These dimensions and factors serve to illustrate the diverse challenges and necessities in the integration of IT and OT. This, in turn, suggests that governance in digital integration must encompass comprehensive organisational and human resource strategies. Despite focusing on data integration, Kuusk and Gao

(2021) emphasise the broader governance implications of IT/OT convergence, particularly in operational management, where the existing literature is limited.

4.2 Practitioner literature

As we could identify few academic papers on IT/OT convergence, we also conducted an exploratory search for relevant high quality practitioner literature. The analysis of the practitioner literature showed that most of the articles can be divided into the categories of benefits, challenges and key success factors. Some articles also addressed the issue of governance. The results are therefore structured according to these categories and supplemented by an overview of the characterisation of IT/OT convergence in the practitioner literature. Each sub-chapter is introduced by a brief summary of the findings.

Characterization of IT/OT convergence

The practitioner literature characterizes IT/OT convergence as a critical strategic initiative that requires a comprehensive approach involving organizational, technical, and operational aspects to bridge the historical silos between IT and OT, and highlights the importance of leadership, collaboration, and governance in achieving successful integration.

Bronson (2022) highlights IT/OT convergence as critical for competitive advantage, especially in sectors like manufacturing and energy. Bigelow and Lutkevich (2024) extend its importance to other industries, including utilities, transportation, retail, and more, emphasizing the need for a comprehensive strategy involving organizational, technical, and operational phases to bridge IT and OT.

Hayes (2020) also underscores IT/OT integration as pivotal for enhancing profitability, efficiency, and reliability. Key phases include increasing collaboration between IT and OT teams, converging security and management architectures, and updating infrastructures and technologies to support ongoing development.

Historically, IT and OT have operated independently, creating silos and fragmented systems due to minimal cooperation (Wennmann, 2021; Yokogawa, 2021). These silos pose significant challenges to digital transformation and convergence (BCG Platinion, 2021).

Approaches to IT/OT integration vary, including separate networks, segregated networks, or fully integrated environments (Bigelow and Lutkevich, 2024). Yokogawa (2021) discusses several structuring models such as IT/OT interfaces, combined departments, cross-functional teams, and integrated manufacturing IT teams, which often involve a CTO or similar leadership roles to bridge gaps between IT and OT.

Significant differences in security priorities exist between IT and OT. IT prioritizes data confidentiality, while OT focuses on operational availability and data integrity (Bigelow and Lutkevich, 2024; Coombs, 2022). Additionally, their roles in the organization diverge, with IT supporting communication and business operations and OT focusing on operational processes and outcomes.

Stakeholders in IT/OT convergence include business leaders, top management, IT departments, and operational personnel (Wennmann, 2021). For successful integration, leadership should be well-informed about the benefits, challenges, and risks associated with convergence (Bronson, 2022).

Verhaeghe et al. (2021) stress the importance of not only addressing technological changes but also redesigning processes and landscapes to enhance collaboration and governance for successful IT/OT convergence.

Benefits of IT/OT convergence

The practitioner literature highlights numerous benefits of IT/OT convergence, including increased efficiency, reduced costs, enhanced transparency, improved decision-making, and optimized performance across various industries, achieved through the integration of data, processes, and systems.

IT/OT convergence is widely recognized for enhancing efficiency and reducing costs across multiple industries (AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Cisco, 2022; Hayes, 2020; Yokogawa, 2021). Key advantages include breaking down IT and OT silos, increasing transparency and awareness of assets and operational processes, and improving the application landscape (Bigelow and Lutkevich, 2024; Bronson, 2022; Cisco, 2022; Hayes, 2020; Verhaeghe et al., 2021).

Enhanced data exchange along the supply chain fosters easier data analysis, more comprehensive monitoring, predictive maintenance, and subsequently, more effective and real-time decision-making and reporting (AWS, 2022; Bigelow and Lutkevich, 2024; Cisco, 2022; Verhaeghe et al., 2021).

Additional benefits include better compliance, more efficient asset management, enhanced support, reduced unplanned downtimes, and improved automation which collectively boost overall performance and productivity (Bigelow and Lutkevich, 2024; Bronson, 2022; Cisco, 2022; Yokogawa, 2021).

Table 1 summarizes the most frequently mentioned benefits associated with IT/OT convergence.

Nr.	Benefits	Publication outlets
1	Reduction of costs	AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Cisco, 2022; Hayes, 2020; Yokogawa, 2021
2	Better performance and productivity	Bronson, 2022; Cisco, 2022; Hayes, 2020; Verhaeghe et al., 2021; Yokogawa, 2021
3	More transparency/visibility	Bigelow and Lutkevich, 2024; Bronson, 2022; Cisco, 2022; Hayes, 2020; Verhaeghe et al., 2021
4	More predictive maintenance	Cisco, 2022; Bigelow and Lutkevich, 2024; Verhaeghe et al., 2021
5	Less siloed departments/breaking down IT/OT silos	Bigelow and Lutkevich, 2024; Bronson, 2022
6	Fast and more direct decision making	AWS, 2022; Verhaeghe et al., 2021
7	More complete monitoring	Bigelow and Lutkevich, 2024; Cisco, 2022

Table 1. Benefits of IT/OT convergence from practitioner literature

Challenges of IT/OT convergence

The practitioner literature highlights that IT/OT convergence faces significant challenges due to organizational and technical silos, conflicting priorities and cultures, and cybersecurity risks arising from the integration of legacy OT systems with IT, necessitating robust security measures and a shared vision for collaboration to overcome these hurdles.

While IT/OT convergence offers significant benefits, it also presents substantial challenges including engineering, management, and cybersecurity issues (Mahajan et al., 2022). Organizational and technical silos lead to independent department structures, isolated processes, and communication barriers, along with divergent protocols and standards (Bigelow and Lutkevich, 2024; Bronson, 2022; Yokogawa, 2021).

The segregated IT and OT teams often have conflicting priorities, perspectives, cultures, and strategies. Additionally, differing skill sets and limited cross-departmental insight create knowledge islands and hinder effective integration (AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Verhaeghe et al., 2021; Yokogawa, 2021). A lack of a shared vision for collaboration, or an overly ambitious one, further complicates convergence efforts (Verhaeghe et al., 2021).

Operational divides result in sporadic data exchange and integration challenges, with difficulties in device communication and system integration, especially when merging old systems with new (Bigelow and Lutkevich, 2024; Chang et al., 2022; Verhaeghe et al., 2021; Yokogawa, 2021). The slower evolution of OT compared to IT, alongside legacy systems that are often outdated and poorly maintained,

poses significant cybersecurity risks. These risks are exacerbated by the increased connectivity required for IT/OT convergence, elevating the potential for industrial espionage and sabotage (AWS, 2022; Bigelow and Lutkevich, 2024; Mahajan et al., 2022; Verhaeghe et al., 2021; Yokogawa, 2021). Thus, ensuring robust cybersecurity and information security measures becomes paramount (Wennmann, 2021).

Table 2 summarizes the most frequently mentioned challenges associated with IT/OT convergence.

Nr.	Challenges	Publication outlets
1	Security challenges – cybersecurity and information security	AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Kiener et al., 2021; Mahajan et al., 2022; Verhaeghe et al., 2021; Wennmann, 2021; Yokogawa, 2021, 2022
2	Different skillset/competencies	AWS, 2022; BCG Platinion, 2021; Coombs, 2022; Yokogawa, 2021, 2022
3	Organizational and technical silos	Bigelow and Lutkevich, 2024; Chang et al., 2022; Yokogawa, 2021, 2022
4	Lack of collaboration between IT and OT teams/segregated IT and OT teams	AWS, 2022; Bigelow and Lutkevich, 2024; Verhaeghe et al., 2021; Yokogawa, 2021
5	Different priorities and perspectives	AWS, 2022; Bigelow and Lutkevich, 2024; BCG Platinion, 2021
6	OT legacy systems/different asset and software lifespan	Bigelow and Lutkevich, 2024; Yokogawa, 2021; Cisco, 2022
7	Conflicting cultures	Yokogawa, 2022; Hayes, 2020

Table 2. Challenges of IT/OT convergence from practitioner literature

Governance in the context of IT/OT convergence

The practitioner literature emphasizes the crucial role of governance and cultural change in IT/OT convergence, highlighting the need for a comprehensive governance framework, clear definition of roles and responsibilities, and centralized management under IT leadership or a CoE to effectively address the challenges of integration.

Governance and cultural change are crucial for IT/OT convergence (Sivasubramaniyan, 2021). Kiener et al. (2021) note the primary challenge lies not in technology but in adapting responsibilities and organizational cultures. Governance must be initiated and maintained at management levels to mitigate non-technical weaknesses (Kiener et al., 2021).

The role of IT managers, particularly CIOs, is becoming more strategic, heavily influenced by IT/OT convergence (Naef, 2020a). Traditionally, CIOs handle enterprise IT while Chief Operating Officers or Chief Technology Officers manage operational technology. This separation is diminishing as integration progresses (Naef, 2020b; Chang et al., 2022).

Currently, most organizations lack a comprehensive governance framework that unifies IT and OT strategies (Chang et al., 2022). Effective governance involves defining roles, responsibilities, and security measures for critical processes (Hayes, 2020). Industrial cybersecurity, a governance issue, requires enhanced coordination and a pragmatic focus on people and processes (Hayes, 2020).

Centralized data and communications management under overarching IT governance can harmonize technology across enterprises, leveraging synergies and minimizing data silos (Wennmann, 2021). Mahajan et al. (2022) emphasize the importance of establishing clear governance structures to define cross-functional roles and responsibilities, especially in OT security.

While joint governance is generally supported, there is debate over its implementation and leadership. Some advocate for IT, particularly the CIO, to lead, ensuring innovations in OT; others suggest

leadership should be more collaborative or even outsourced to leverage external expertise (Chang et al., 2022; Naef, 2020b; Yokogawa, 2021). Coombs (2022) describes a centralized IT/OT model via a CoE that combines local IT and OT staff to provide standardized solutions across the organization.

Key success factors for IT/OT convergence

The practitioner literature highlights that the key success factors for IT/OT convergence include the formation of multidisciplinary teams, clearly defined roles and responsibilities, the establishment of a CoE to govern integration, and the implementation of organizational and cultural changes to promote a unified approach, all while considering the unique context of each organization.

Successful IT/OT convergence varies by organization, depending on factors like location, size, and digital maturity (Wennmann, 2021; Yokogawa, 2021). Critical to success is the integration of IT and OT into multidisciplinary teams to facilitate joint projects and skill sharing, enhancing mutual understanding and capabilities (AWS, 2022; BCG Platinion, 2021; Hayes, 2020; Sivasubramaniyan, 2021).

Clearly defined roles and responsibilities help maintain focus on collaboration benefits and ensure consistent implementation across the organization (AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Chang et al., 2022). Establishing a CoE is recommended to govern integration, manage risks, and optimize value through shared goals and open communication (AWS, 2022; Chang et al., 2022; Verhaeghe et al., 2021).

The CoE also plays a pivotal role in educating employees, driving innovation, and disseminating best practices across business and manufacturing sectors (AWS, 2022; Sivasubramaniyan, 2021). Organizational and cultural adjustments are necessary to redefine interfaces between IT and OT, promoting a unified approach to achieving common goals and enhancing cross-functional interactions (Coombs, 2022; Kiener et al., 2021; Verhaeghe et al., 2021).

Finally, defining and measuring common KPIs across IT and OT is crucial to track success, productivity, and performance, supported by tools that improve visibility and control over assets (AWS, 2022; Chang et al., 2022).

Table 3 summarizes the most frequently cited recommendations.

Nr.	Key Success Factor	Publication outlets
1	Defined roles and responsibilities	AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Chang et al., 2022; Wennmann, 2021; Hayes, 2020; Mahajan et al., 2022
2	Provide training/skill transformation	AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022; Chang et al., 2022; Cisco, 2022; Kiener et al., 2021
3	Establish common governance	AWS, 2022; Chang et al., 2022; Wennmann, 2021; Hayes, 2020; Mahajan et al., 2022; Kiener et al., 2021
4	Build multi-discipline IT/OT teams	AWS, 2022; Wennmann, 2021; Hayes, 2020; BCG Platinion, 2021; Sivasubramaniyan, 2021
5	Establish CoE	AWS, 2022; Chang et al., 2022; Verhaeghe et al., 2021
6	Perform organizational change	Wennmann, 2021; Coombs, 2022; Kiener et al., 2021; Verhaeghe et al., 2021
7	Perform cultural change	Wennmann, 2021; Hayes, 2020; Verhaeghe et al., 2021
8	Establish common KPIs/monitoring	AWS, 2022; Chang et al., 2022; Wennmann, 2021
9	Use (the right) tools	AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022
10	Establish risk management	AWS, 2022; Wennmann, 2021; Kiener et al., 2021

Table 3. Key success factors for IT/OT convergence from practitioner literature

5 Discussion

The findings from the academic and practitioner literature provide insights into the complex nature of IT/OT convergence and its associated governance challenges. The academic literature predominantly addresses security, technology, infrastructure, and architectural approaches to IT/OT convergence, whereas the practitioner literature emphasises the benefits, challenges, and key success factors.

One of the key themes that emerges from both the academic and practitioner literature is the importance of effective governance in achieving successful IT/OT convergence. The academic literature highlights the crucial role of IT governance, infrastructure, and system interoperability in positively affecting IT/OT convergence (Ehie and Chilton, 2020). Gharpure et al. (2022) propose a multi-dimensional implementation model that emphasises the establishment of a clear governance structure during the trust-building and process development phases. Similarly, Dhlamini and Mawela (2022) identify critical success factors such as clearly defined roles, unified reporting structures, consolidated support groups reporting directly to executive management, and cross-functional teams, underscoring the central role of effective governance.

The practitioner literature stresses the significance of governance and cultural change for successful IT/OT convergence even more (Sivasubramaniyan, 2021). Kiener et al. (2021) posit that the primary challenge lies in adapting responsibilities and organisational cultures, rather than technology itself. The importance of defining roles, responsibilities, and security measures for critical processes is emphasised (Hayes, 2020). Centralised data and communications management under overarching IT governance is seen as a way to harmonise technology across enterprises (Wennmann, 2021).

However, there is a lack of consensus regarding the implementation and leadership of joint governance. Some argue that the CIO should head this initiative, while others propose a more collaborative approach or even outsourcing to leverage external expertise (Chang et al., 2022; Coombs, 2022; Naef, 2020b; Yokogawa, 2021). This underscores the necessity for organisations to meticulously assess their distinctive circumstances and requirements when establishing governance frameworks for IT/OT convergence.

Another key theme that emerges from the literature is the importance of addressing organisational and cultural challenges. The academic literature identifies the siloed nature of IT and OT departments as a major challenge, leading to different practices, priorities and governance structures (Dhlamini and Mawela, 2022; Garimella, 2018). The practitioner literature also highlights organisational and technical silos, separate IT and OT teams, and conflicting priorities and perspectives as major challenges (AWS, 2022; Bigelow and Lutkevich, 2024; Bronson, 2022).

To overcome these challenges, the literature emphasises the importance of integrating IT and OT into multidisciplinary teams, clearly defining roles and responsibilities, and establishing a CoE to govern integration and manage risk (AWS, 2022; BCG Platinion, 2021; Hayes, 2020; Sivasubramaniyan, 2021). Organisational and cultural adjustments are seen as necessary to redefine the interfaces between IT and OT and promote a unified approach to achieving common goals (Coombs, 2022; Kiener et al., 2021; Verhaeghe et al., 2021).

The literature also highlights the increasing security concerns associated with IT/OT convergence, particularly in CPS across different sectors. The academic literature emphasises the development of risk assessment tools, secure infrastructures and advanced detection systems to address these challenges (Progoulakis et al., 2021; Zahran et al., 2021; Mubarak et al., 2021). The practitioner literature also identifies security challenges as a major concern, with the slower evolution of OT compared to IT and legacy systems posing significant cybersecurity risks (AWS, 2022; Bigelow and Lutkevich, 2024; Mahajan et al., 2022).

To address these security challenges, the practitioner literature suggests establishing clear governance structures to define cross-functional roles and responsibilities, especially in OT security (Mahajan et al., 2022). Centralised data and communication management under overarching IT governance is also seen as a way to minimise data silos and improve security (Wennmann, 2021).

In terms of technology and infrastructure, the academic literature shows the development of various tools, frameworks and models to address the challenges and opportunities associated with IT/OT convergence (Pokhrel and Garg, 2021; Corradi et al., 2022; Koorapati et al., 2022). The practitioner literature also highlights the importance of using the right tools and establishing common KPIs and monitoring to track success, productivity and performance (AWS, 2022; Chang et al., 2022).

Overall, the findings from the academic and practitioner literature provide a comprehensive understanding of the complex nature of IT/OT convergence and the associated governance challenges. The literature highlights the importance of effective governance, addressing organisational and cultural challenges, ensuring robust cybersecurity measures, and deploying appropriate technology and infrastructure to achieve successful IT/OT convergence.

However, there are some gaps and limitations in the current literature. The academic literature focuses primarily on security, technology, infrastructure and architectural approaches, with limited attention to governance aspects. The practitioner literature, while providing valuable insights into the benefits, challenges and key success factors, lacks the depth and rigour of academic research.

6 Conclusion

This paper explores IT/OT convergence with a focus on governance. Security and architectural approaches are prevalent in academic literature, where governance is less emphasized. Conversely, governance gains significant attention in practitioner literature, often recommending the establishment of a CoE to implement common governance strategies.

Despite limited commonality between academic and practitioner perspectives on governance, both recognize its importance for successful IT/OT convergence. Our paper also discusses the key benefits, challenges, and governance approaches for IT/OT convergence, noting the limited common findings but highlighting their significance.

Our literature review faces limitations such as potential omissions despite extensive database searches and potential subjective biases during the selection process. This suggests opportunities for future research, particularly in filling the documented gaps about governance in academic literature and examining the practical implementation of IT/OT convergence by German CIOs and IT/OT leaders.

Future research could investigate the role of IT leadership in governing IT/OT convergence, considering the common assumption of IT leaders' involvement in directing cross-functional teams and governance structures. This area's exploration might clarify why IT leaders are frequently chosen to lead these initiatives. Furthermore, future research could focus on developing comprehensive governance frameworks that address the specific challenges and requirements of IT/OT convergence. Case studies and empirical research could provide valuable insights into the practical implementation of governance structures and their impact on the success of IT/OT convergence initiatives.

Disclaimer

Artificial intelligence (AI) tools, namely ChatGPT, Claude, and DeepL Write, were employed in the preparation of this paper. These AI assistants were primarily used to enhance the language, grammar, and overall readability of the manuscript. While the content, ideas, and research presented in this paper are the original work of the authors, it is important to acknowledge the use of these AI tools as a support in the writing process. However, the authors have carefully reviewed and edited the AI-generated content to ensure the accuracy, integrity, and quality of the final paper. The use of AI tools was intended to improve the clarity and presentation of the research and does not diminish the academic contribution or originality of the work. The authors take full responsibility for the content and conclusions presented in this paper.

References

Åkerberg, J., J. Furunäs Åkesson, J. Gade, M. Vahabi, M. Björkman, M. Lavassani, R. Nandkumar Gore, T. Lindh and X. Jiang (2021). "Future industrial networks in process automation. Goals, challenges, and future directions" *Applied Sciences* 11 (8), 3345.

AWS (2022). *Managing Organizational Transformation For Successful OT/IT Convergence*. URL: https://aws.amazon.com/de/blogs/iot/managing-organizational-transformation-for-successful-ot-it-convergence/.

Azarmipour, M., C. von Trotha, C. Gries, T. Kleinert and U. Epple (2020). "A secure gateway for the cooperation of information technologies and industrial automation systems". In: *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*: IEEE, pp. 53–58.

BCG Platinion (2021). *IT/OT Integration. The Journey Toward A Hybrid Network Architecture In Manufacturing*. URL: https://bcgplatinion.com/insights/it-ot-integration/.

Bigelow, S. J. and B. Lutkevich (2024). *What Is IT/OT Convergence? Everything You Need To Know*. URL: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.

Bronson, B. (2022). *Connecting IT And Operations. The Best Practices To Get It Right, And The Risks To Avoid*. URL: https://www.forbes.com/sites/forbestechcouncil/2022/04/27/connecting-it-and-operations-the-best-practices-to-get-it-right-and-the-risks-to-avoid/.

Chang, M., B. Koerber and M. Soganci (2022). *Converge IT And OT To Turbocharge Business Operations' Scaling Power*. URL: https://www.mckinsey.com/capabilities/operations/our-insights/converge-it-and-ot-to-turbocharge-business-operations-scaling-power.

Chattha, H. A., M. M. U. Rehman, G. Mustafa, A. Q. Khan, M. Abid and E. U. Haq (2021). "Implementation of cyber-physical systems with modbus communication for security studies". In: *2021 International Conference on Cyber Warfare and Security (ICCWS)*: IEEE, pp. 45–50.

Cisco (2022). *How Is OT Different From IT? OT vs. IT*. URL: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html.

Coombs, S. (2022). *The 7 Best Practices for IT-OT Convergence*. URL: https://www.accenture.com/us-en/blogs/industry-digitization/the-7-best-practices-for-it-ot-convergence.

Corradi, A., G. Di Modica, L. Foschini, L. Patera and M. Solimando (2022). "SIRDAM4.0. A support infrastructure for reliable data acquisition and management in industry 4.0" *IEEE Transactions on Emerging Topics in Computing* 10 (3), 1605–1620.

Dhlamini, T. and T. Mawela (2022). "Critical success factors for information technology and operational technology convergence within the energy sector". In A. Abraham, A. M. Madureira, A. Kaklauskas, N. Gandhi, A. Bajaj, A. K. Muda, D. Kriksciuniene and J. C. Ferreira (eds.) *Innovations in Bio-Inspired Computing and Applications*, pp. 425–434. Cham: Springer.

Dutta, A. K., B. Mukhoty and S. K. Shukla (2021). "CatchAll. A robust multivariate intrusion detection system for cyber-physical systems using low rank matrix". In: *CPSIoTSec 2021 - Proceedings of the 2nd Workshop on CPS and IoT Security and Privacy, co-located with CCS 2021*, pp. 47–56.

Ehie, I. C. and M. A. Chilton (2020). "Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation" *Computers in Industry* 115, 1–11.

Foschini, L., V. Mignardi, R. Montanari and D. Scotece (2021). "An SDN-enabled architecture for IT/OT converged networks. A proposal and qualitative analysis under DDoS attacks" *Future Internet* 13 (258), 1–19.

Garimella, P. K. (2018). "IT-OT integration challenges in utilities". In: *3rd IEEE International Conference on Computing, Communication and Security, ICCCS 2018*, pp. 199–204. URL: http://ieeexplore.ieee.org/servlet/opac?punumber=8557205.

Gartner (2023a). *IT/OT Alignment*. URL: https://www.gartner.com/en/information-technology/glossary/it-ot-alignment.

Gartner (2023b). *IT/OT Integration*. URL: https://www.gartner.com/en/information-technology/glossary/it-ot-integration.

Gharpure, R., A. Kardekar and R. Vyas (2022). "Industry 4.0 digital transformation. Information technology (IT)–operations technology (OT) convergence model and its implementation in asset-heavy manufacturing industry" *International Journal of Mechanical Engineering* 7 (1), 1545–1554.

Haes, S. and W. van Grembergen (2005). "IT governance structures, processes and relational Mechanisms. Achieving IT/business alignment in a major belgian financial group". In: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*: IEEE, 237b-237b.

Hayes, R. (2020). *Managing The Successful Convergence Of IT And OT*. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-deloitte-managing-the-successful-convergence-of-it-and-ot.pdf.

Hollerer, S., W. Kastner and T. Sauter (2021). "Safety und Security – ein Spannungsfeld in der industriellen Praxis" *e & i Elektrotechnik und Informationstechnik* 138 (7), 449–453.

Kanamaru, H. (2021). "The extended risk assessment form for IT/OT convergence in IACS security". In: *2021 60th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, pp. 1365–1370.

Khan, R., N. Tsiga and K. Ghanem (2022). "Building a digital twin for industrial internet of things with interoperability". In: *2022 Moscow Workshop on Electronic and Networking Technologies (MWENT)*: IEEE, pp. 1–5.

Kiener, W., J. Zimmermann and P. Schmitz (2021). *OT-Sicherheit Durch Integriertes Governance-Model*. URL: https://www.security-insider.de/ot-sicherheit-durch-integriertes-governance-model-a-1000164/.

Koorapati, K., R. Pandu, P. K. Ramesh, S. Veeraswamy and U. Narasappa (2022). "Towards a unified ontology for IoT fabric with SDDC" *Journal of King Saud University - Computer and Information Sciences* 34 (8), 6077–6091.

Kourtis, M.-A., A. Oikonomakis, D. Santorinaios, T. Anagnostopoulos, G. Xilouris, A. Kourtis, I. Chochliouros and C. Zarakovitis (2022). "5G NPN performance evaluation for I4.0 environments" *Applied Sciences* 12 (15), 1–16.

Kuusk, A. and J. Gao (2021). "Automating data driven decisions for asset management. A how to framework for integrating OT/IT operational and information technology, procedures and staff". In A. Crespo Márquez, D. Komljenovic and J. Amadi-Echendu (eds.) *14th WCEAM Proceedings*, pp. 201–213. Cham: Springer.

Lara, P., M. Sánchez and J. Villalobos (2019). "OT modeling. The enterprise beyond IT" *Business & Information Systems Engineering* 61 (4), 399–411.

Mahajan, R., G. Shukla and S. Jinugu (2022). *Reimaging OT Cybersecurity Strategy*. Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-reimagining-OT-cybersecurity-strategy-noexp.pdf.

Mantravadi, S., R. Schnyder, C. Moller and T. D. Brunoe (2020). "Securing IT/OT links for low power IIoT devices. Design considerations for industry 4.0" *IEEE Access* 8, 200305–200321.

Meyer, M., R. Zarnekow and L. M. Kolbe (2003). "IT-governance. Begriffe, status quo und bedeutung" *Wirtschaftsinformatik* 45 (4), S. 445–448.

Mubarak, S., M. H. Habaebi, M. R. Islam and S. Khan (2021). "ICS cyber attack detection with ensemble machine learning and DPI using cyber-kit datasets". In: *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*: IEEE, pp. 349–354.

Muguira, L., J. Lazaro, S. Alonso, A. Astarloa and M. Rodriguez (2020). "Secure critical traffic of the electric sector over time-sensitive networking". In: *2020 XXXV Conference on Design of Circuits and Integrated Systems (DCIS)*: IEEE, pp. 1–6.

Naef, P. (2020a). "Mehrwert schaffen mit IT" *CIO*.

Naef, P. (2020b). "Produkt- und Prozesstechnik verschmelzen" *CIO*.

Patera, L., A. Garbugli, A. Bujari, D. Scotece and A. Corradi (2021). "A layered middleware for OT/IT convergence to empower industry 5.0 applications" *Sensors* 22 (1), 1–14.

Pokhrel, S. R. and S. Garg (2021). "Multipath communication with deep q-network for industry 4.0 automation and orchestration" *IEEE Transactions on Industrial Informatics* 17 (4), 2852–2859.

Pop, P., B. Zarrin, M. Barzegaran, S. Schulte, S. Punnekkat, J. Ruh and W. Steiner (2021). "The FORA fog computing platform for industrial IoT" *Information Systems* 98, 1–20.

Progoulakis, I., P. Rohmeyer and N. Nikitakos (2021). "Cyber physical systems security for maritime assets" *Journal of Marine Science and Engineering* 9 (12), 1–24.

Reynolds, G. W. (2016). *Information Technology For Managers.* Second edition. Australia: Cengage.

Rosa, L., T. Cruz, M. B. de Freitas, P. Quitério, J. Henriques, F. Caldeira, E. Monteiro and P. Simões (2021). "Intrusion and anomaly detection for the next-generation of industrial automation and control systems" *Future Generation Computer Systems* 119, 50–67.

Saurav, S. K., P. B. Sudhakar, K. J. Mohan, R. Senthil Kumar and S. Bindhumadhava Bapu (2021). "SCADA WebView. A state-of-the-art enterprise transmission SCADA engine". In: *2021 IEEE 18th India Council International Conference (INDICON)*: IEEE, pp. 1–7.

Scheffer, S., A. Martinetti, R. Damgrave and L. van Dongen (2021). "Augmented reality for IT/OT failures in maintenance operations of digitized trains: current status, research challenges and future directions" *Procedia CIRP* 100, 816–821.

Shah, R. (2019). *Protecting Critical National Infrastructure In An Era Of IT And OT Convergence.* Australian Strategic Policy Institute - International Cyber Policy Centre. URL: https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence.

Shilenge, M. C. and A. Telukdarie (2022). "Optimization of operational and information technology integration towards industry 4.0". In: *2022 IEEE 31st International Symposium on Industrial Electronics (ISIE)*: IEEE, pp. 1076–1081.

Sivasubramaniyan, K. (2021). *Five Considerations For A Successful IT/OT Convergence Program*. URL: https://www.hcltech.com/blogs/five-considerations-successful-itot-convergence-program.

The, Y.-L. and A. G. Kuusk (2021). "Aligning IIoT and ISA-95 to improve asset management in process industries". In A. Crespo Márquez, D. Komljenovic and J. Amadi-Echendu (eds.) *14th WCEAM Proceedings*, pp. 153–163. Cham: Springer.

Trifonov, R., S. Manolov, R. Yoshinov, G. Tsochev and G. Pavlova (2021). "Applying the experience of artificial intelligence methods for information systems cyber protection at industrial control systems". In: *25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*: IEEE, pp. 21–25.

Verhaeghe, X., J. Vincke, J. van der Straeten, B. Peeters, B. Vossen, S. Mertens and D. Catteceur (2021). *IT/OT Convergence As Basis For Digitisation In The Fast-Changing Industrial Environment.* PwC. URL: https://www.pwc.be/en/FY21/documents/Report-IT-OT-convergent-2021.pdf.

Wennmann, M. (2021). "Warum IT und OT in Unternehmen Verschmelzen Sollten" *EY*.

Yokogawa (2021). *IT/OT Convergence*. *Bringing Two Worlds Together*. URL: https://www.yokogawa.com/de/library/resources/white-papers/itot-convergence-bringing-two-worlds-together/.

Yokogawa (2022). *IT/OT Convergence*. *Integration Business and Manufactoring*. URL: https://www.yokogawa.com/eu/solutions/featured-topics/digital-infrastructure-wiki/general/itot-convergence/.

Zahran, B., A. Hussaini and A. Ali-Gombe (2021). "IIoT-ARAS. IIoT/ICS automated risk assessment system for prediction and prevention". In: *11th ACM Conference on Data and Application Security and Privacy, CODASPY 2021*, pp. 305–307.