

The Security of OT/IT Convergence: A survey on Research Trends, Standards and Regulations

Journal:	*Computing Surveys*
Manuscript ID	CSUR-2026-0728
Paper:	Long Survey Paper
Date Submitted by the Author:	03-May-2026
Complete List of Authors:	Masi, Massimiliano; Autostrade Per L'Italia, ITD Maccari, Leonardo; Ca' Foscari University of Venice, Dept. of Environmental Sciences Informatics and Statistics
Computing Classification Systems:	Software Security Engineering, Cyber-physical networks, Enterprise architecture frameworks, Reference models



The Security of OT/IT Convergence: A survey on Research Trends, Standards and Regulations

MASSIMILIANO MASI, Autostrade Per L'Italia, Italy
LEONARDO MACCARI, University of Venice, Italy

The convergence of Information Technology (IT) and Operational Technology (OT) has emerged as a key enabler for data-driven optimization, cloud integration, and advanced analytics in industrial and critical infrastructure environments. At the same time, regulatory pressure and cybersecurity standards increasingly constrain how such convergence can be realized, particularly in legacy OT systems characterized by long life cycles, strict certification processes, and stringent availability requirements. This paper analyzes the current state of OT/IT convergence by examining relevant industrial standards, existing academic and industrial research and the legislative landscape. Through a systematic literature review, we investigate proposed convergence architectures, the main concerns related to the integration, and the application domains in which they are deployed. Our analysis highlights a significant gap between academic research and industrial practice: while research often proposes modifications to protocols or novel risk frameworks, such approaches are rarely feasible in real-world OT environments. The most practical convergence initiatives should rely on established architectural models, notably the Purdue Enterprise Reference Architecture, with cybersecurity as a dominant design concern. We further examine two representative industrial implementations and discuss their strengths and limitations. These findings suggest the need for future research that better aligns with existing standards, operational constraints, and deployment realities.

CCS Concepts: • **Security and privacy → Software security engineering**; • **Networks → Cyber-physical networks**; • **Applied computing → Enterprise architecture frameworks**; **Reference models**.

Additional Key Words and Phrases: IT/OT Convergence, Cybersecurity, Purdue Model

ACM Reference Format:
Massimiliano Masi and Leonardo Maccari. 2018. The Security of OT/IT Convergence: A survey on Research Trends, Standards and Regulations. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX)*. ACM, New York, NY, USA, 35 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

The term Operational Technology (OT) refers to the hardware and software systems used to control and monitor industrial equipment that form the core of production lines in manufacturing and in critical infrastructures such as energy, transportation, and waste management. OT is at the base of o ICS, Industrial Automation and Control Systems (IACS), and has life cycles spanning several decades. The design philosophy of OT systems differs substantially from that of Information Technology (IT) systems as OT must guarantee extremely high reliability and availability at the expense of the flexibility commonly found in IT environments. In many cases, OT systems also undergo strict certification processes; once deployed, updates, patches, or configuration changes are highly discouraged or even

Authors' Contact Information: Massimiliano Masi, mmasi@autostrade.it, Autostrade Per L'Italia, Rome, Italy; Leonardo Maccari, leonardo.maccari@unive.it, University of Venice, Venezia, Italy.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.
Manuscript submitted to ACM

For Peer Review

prohibited because they would invalidate the certification – an approach that would be unacceptable from a security perspective in any IT infrastructure. Consequently, a long-standing assumption has been that IT and OT systems are strictly separated, "*air-gapped*" environments with no communication between them.[1]

Beginning in the early 2000s, however, data generated and processed by OT systems has become increasingly valuable at the organizational level. Such data enables AI model training, predictive maintenance, optimization of resource usage, and improvements in market competitiveness. As a result, consulting and technology providers began promoting the modernization of legacy OT environments through the integration of IT technologies into production systems. From elastic storage to scalable compute capabilities, OT infrastructures gradually began to *converge* toward cloud-based architectures. With this shift, even the illusion of physical separation faded, exposing OT systems to a broader class of cyber threats.

Despite these trends, practical OT/IT convergence remains in its infancy. OT systems are often highly specialized, tailored to their operational environment, and far from general-purpose computing platforms. OT-to-OT communication protocols are primarily designed for reliability and seldom provide features typical of modern IT protocols, such as authentication tokens or crypto-agility and TCP/IP-based networks cannot be assumed [95]. Even data formats are frequently proprietary and lack interoperability. Furthermore, introducing cybersecurity controls in operational environments is notoriously difficult, for example, deploying an Endpoint Detection and Response (EDR) system may be unacceptable if the risk exists that legitimate industrial traffic could be dropped as a false positive. Last but not least, skill gaps further complicate convergence: OT engineers often possess strong automation expertise but typically lack formal computer science or cybersecurity training, which is increasingly rare [66].

This scenario gives rise to new and compelling research challenges, which we structure and analyze in this paper. Our first goal is to conduct a systematic literature review of existing academic and industrial research in the context of OT/IT convergence. We survey major sources to address three research questions concerning (i) the architectures proposed for convergence, (ii) the concerns they aim to address, and (iii) the application domains in which convergence initiatives are most prevalent. During this process, we observe a clear divide between research and practice: academic proposals often introduce technically sophisticated solutions but rely on unrealistic assumptions about the modifiability of OT systems, whereas industrial approaches prioritize practical architectures aligned with real-world deployments but offer limited innovation. Our second goal is therefore to provide an overview of the industrial standards bound to normative frameworks available for OT/IT convergence. These architectures are the ones proposed by Standard Development Organisationss (SDOs), and often represent the non-negotiable constraints any solution aiming for real-world applicability should take into consideration. Of course, these architectures have their own limitations, that we also describe to outline possible room for improvement.

We organize our contributions as follows:

- Section 2 Presents the repeatable methodology we used for our survey, based on the best scientific practices. We also place our contribution in the current literature about OT/IT convergence and show the need for a new survey;
- Section 3 provides a primer on OT;
- Section 4 briefly summarises the results of our survey;
- Section 5 and section 6 present the detailed analysis of the academic and commercial sources respectively;
- Section section 7 provides an overview of the standards shaping the OT landscape;

[1] An assumption that has always been questionable, see, e.g., https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap, Last Accessed October 26, 2025

For Peer Review

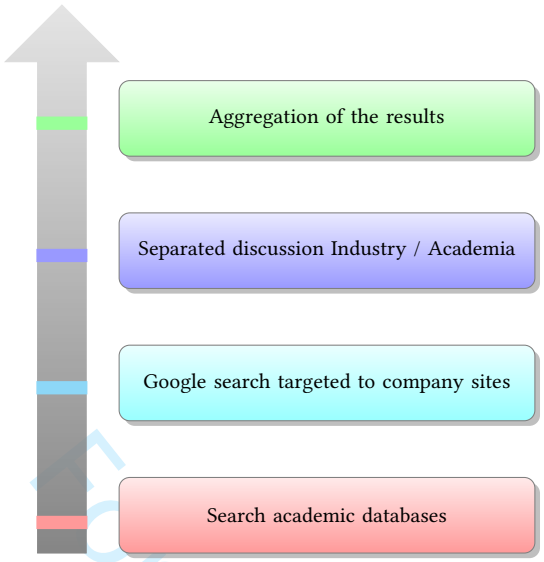


Fig. 1. Review protocol

For Peer Review

- Section section 8 analyzes two market implementations of this model, highlighting both their strengths and limitations;
- Section section 9 reviews the legislative landscape relevant to convergence.
- Finally, Section section 10 summarizes our findings and outlines directions for future work.

2 Literature Review: Methodology and Research Gap

In this section we present the review methodology that we used to analyze the literature describing OT/IT convergence approaches. Our study, performed during September-December 2025, analyzes and interprets the available evidence related to three main research questions described below. The review has been also conducted to be unbiased and repeatable, using a well known review methodology proposed by Kitchenham et al [57]. Since the theme spans across the two domains, we consider academic sources but also industrial resources to compare both results. The review steps are shown in fig. 1, while section 2.1 briefly describes the protocol and the research questions, together with a summary of the sources. Section 2.2 reports on the threats to validity that we have considered when conducting the review.

2.1 Review protocol

The systematic review is driven by the following research questions:

Q1 What are the common reference architectures and protocols used in OT/IT convergence projects?
Q2 What are the concerns evaluated during the planning phase of OT/IT convergence projects?
Q3 What are the application domains (e.g., energy, manufacturing, maritime, etc.) that are the target of OT/IT convergence projects?

Every question is structured following the *Population/Intervention/Outcomes* concepts. As described by [57], in software engineering experiments, the *populations* might be, e.g., a specific software engineering role, or an application

area, while the *interventions* is e.g., the tool, technology, or procedure that address a specific issue. Finally, the *Outcome* is the result of the intervention on the population, e.g., reduced production costs or time to market. In Q1, the population of interest is composed by IT reference architectures, as is intended in relevant standards. For instance, ISO 42010:2011 defines a reference architectures as: "*fundamentals concepts or properties of a system in its environment embodied in its elements, relationships, and the principles of its design and evolution*" [53]. In practical terms, an architecture describes the system building blocks, their interconnections and allows to have a common ground to plan the integration. As the term OT is applied to a wide number of different fields, it is fundamental to understand if both academia and industry converge to a set of common architectures when integrating IT and OT.

This is not only an academic curiosity, OT technologies are already in place, and convergence must be planned based on their current state. Researchers should avoid a clean sheet approach and take into consideration the architectures already in use in the industry in order to provide useful contributions. The study of architectures is a key contribution of our paper, and common architectures will be further discussed in section 7.3.

Q2 has the "concern" population, like, e.g., cybersecurity, operational risks, financial costs, that are all considered when planning a convergence project. The goal of Q2 it to discover if a common set of concerns emerges from the literature. Finally, Q3, aims at creating clusters of domains where OT/IT convergence projects are mostly performed. For all the questions, the intervention is the OT/IT convergence project, so in a nutshell the *Population/Intervention/Outcomes* approach starts from the possible architectures/concerns/applications and analyses the literature dealing with OT/IT convergence providing as an outcome a synthesis of the most successful architectures, considered concerns and frequent application domains. Studies are selected using the following inclusion criteria:

- Engineering-oriented publishers search engines (Springer Nature, IEEE, Scopus, and Pubmed) for academic, peer-reviewed papers;
- Consultancy firms that had a prominent role in raising initial interest in OT/IT convergence. We include Google searches targeted to non-peer-reviewed gray literature containing designs, strategies, and patterns, typically used to create awareness to C-level managers. The query string has been appended with the following parameters:
  - Gartner, +site:https://www.gartner.com;
  - McKinsey & Company, +site:https://www.mckinsey.com;
  - Boston Consulting Group, +site:https://www.bcg.com;
  - Deloitte, +site:https://www.deloitte.com/.
- Google searches targeted to cloud providers (AWS, Azure) and device manufacturer (Siemens, Cisco, Fortinet), for available technologies. Notably, for each site, the same google search constraint "(`+site:`)" has been added to the respective landing pages.

The search strings used in conducting the survey are: `"OT" OR "Operational Technology" OR "Convergence" OR "IT/OT"`.

The exclusion criteria are as follows.

- Articles published before 2017 or gray-literature technical reports before 2010;
- Non-English articles;
- Technical reports available upon payment (e.g., paywalls);
- Duplicate or similar entries. This phenomenon is mostly seen in gray literature, as many companies duplicate the same content on different parts of their respective websites;

For Peer Review

- Product manuals;
- Article lacking methodological, architectural, or algorithmic contribution;
- Articles focused on Large Language Model.

Notably, the reason of the date discrepancy in the protocol when considering the publication date, is due to the fact that OT/IT convergence concepts were firstly introduced in late 2010 from consultancy firms, and then applied by industry. The first academic papers arrived in 2017, years after the inception of such convergence concepts. Subsequently, around 2024, industry began to consider the importance of Converging OT/IT Data to train AI models. We excluded Large Language Models because they are not yet considered by international standards and because they are mostly considered as a technology that is applied to the effects of OT/IT convergence and not in the process of convergence itself.

For each resource, either academic paper or article in a website, the following information is extracted: *Architecture used, Concern, Application Domain* plus *Keywords*. Keywords provide a short summary of the resource that we don't use in the protocol but help navigating the lists of resources reported in tables 4 and 5 in A.

The search criteria applied returned 260 papers in the academic area. After applying the exclusion criteria, only 58 articles have been evaluated. In the gray literature area, 38 resources have been selected. The total number of results returned is irrelevant in the case of Google searches. Table 1 reports all the publications we analysed, together with their provenience.

Search Engines	Number of papers	After excl. criteria
IEEEXplore	40	22
Springer Nature	100	23
Scopus	118	13
Pubmed	2	0
Total	260	58

Table 1. Academic search engines results

Not all the sources are relevant for all research questions, i.e. some of them do not use a specific architecture or address any specific application domain, table 2 reports a breakdown of the papers that we used to answer each question.

Sources	Architecture	Concern	Domain
Academic	22	30	18
Commercial	17	30	6
Total	39	60	24

Table 2. Sources divided per relevance for each research question

The discussion of the results is performed in a two-stage process in which first we analyse the academic literature and then the commercial one.

2.2 Threats to Validity

Before diving into the technical topics, let us briefly review the limits of our systematic literature review. Being carried out over both academic search engines and Google, the results may not be guaranteed for their repeatability, although

For Peer Review

care has been put to limit the research scope, using the `+site:` keyword. In the Google searches, the exclusion of documents behind paywalls may limit the specialization of some concepts. In fact, some websites deliver publicly only partial content, leaving the details to papers available upon subscription or paywalls. Other search keywords have been initially excluded, however, while carrying out the review, it has been observed that in some papers, the word "integration" and "convergence", is equivalent, and "digital twins" are also a method for analyzing some aspects of OT/IT convergence. Thus, as a future extension to the current review these keywords might be included.

2.3 Related Work

The topic of literature review of OT/IT convergence has been tackled before by other papers, but with a different focus. In [87], authors conducted a survey on data acquisition and analytics in manufacturing. The survey has been performed on works in the interval of 2019-2023, and considers OT/IT convergence, covering 7 unique industries (coating, automotive, aerospace, sheet metal, steel, energy, tools & fixtures), concentrating on how to move data from OT to IT. Differently from them, we consider a broader scope of OT/IT convergence projects and we do not concentrate on a singular concern (data extraction). Similarly, works such as [2] and [1] consider vertical concerns such as communication protocols in manufacturing and Industry 4.0. Industry 4.0 is also at the base of [99], in which authors performed a literature review on IT, Industrial IoT, and OT technologies, considering also standard architectures (such as RAMI 4.0). The survey results concentrates in some concerns that are also shared by our work, such as cybersecurity. However, Industry 4.0 is a completely new approach, it treats all the components as "flat" because it does not assume to respect a legacy, and proposes new technologies and protocols. Our work concentrates on pure OT environments, e.g., static legacy systems that do not embrace Industry 4.0 and can not be nodified.

Hence, to the best of our knowledge, our paper is unique in its scope (OT/IT convergence projects), it outlines a gap between academic and industrial literature, and provides also the description of two *solution architectures* that should be the building blocks of future research. Furthermore, we give an overview of the normative framework that guide the adoption of the standards. Last but not least, our survey is the only one that adopts a sound, repeatable methodology which can be repeated in the years to come.

3 OT Primer

In this section we provide an introduction to OT and Industrial Control Systems (ICS)[2]. An OT System is a broad class of automation systems used to provide control and monitoring functionality in various domains, such as manufacturing, energy (the *smart grid*), or transport (motorway/railway tunnels, aircraft, or vessels). An OT System is the aggregate of a variety of systems including control systems, Safety Instrumented System (SIS), and Supervisory Control and Data Acquisition (SCADA). Figure 2 provides a simplified representation of an OT System consisting of two sites (*Industrial Network 1*, and *2*) that can represent two different factories or production lines. Each site has a controller, the Programmable Logic Controller (PLC) connected to Industrial Devices (e.g., valves, gauges, motors) or field devices (e.g., other PLCs, or, recursively, other Industrial devices) that work in a tightly integrated manner to perform an automated task. Such task is controlled by an application or logic running inside the SCADA, visualised by an Human-Machine Interface (HMI) that provides a view on the process implemented by the controller and the devices. The *Historian* is a specialized software system that collects values, alarm events, and other information from industrial devices and systems and stores them in a purpose-built database.

[2]We will use the acronym ICS and IACS with the same meaning through the text.

For Peer Review

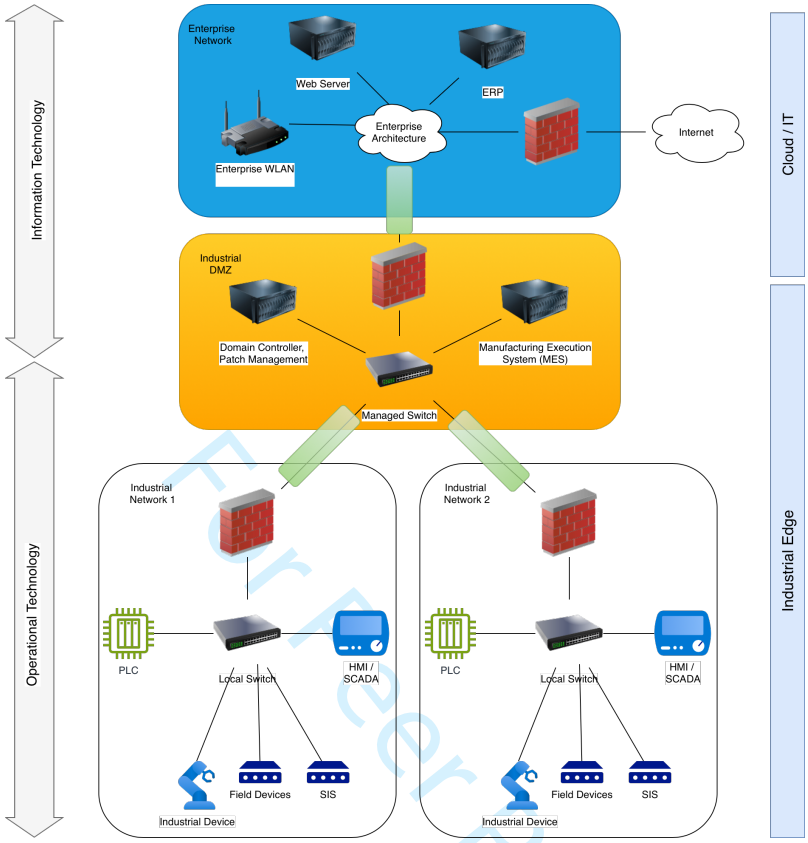


Fig. 2. Sample OT system

Most OT systems utilize specialized communication protocols that may be vendor-specific (e.g. Siemens S7), or non-proprietary such as OPC, MODBUS, PROFIBUS, PROFINET[3]. Many of these were originally designed for serial communications, and have later on been adapted to Ethernet, so they were not designed for use in broadly accessible or public networks. Hence they miss cybersecurity features such as authentication, payload signature, or confidentiality. For this reason, exposing OT networks to complex Internet-connected IT systems is considered dangerous and the Enterprise Network, which is made by modern IT solutions, is separated by a Demilitarized Zone (DMZ). The *Industrial DMZ* also contain common infrastructure services that must be completely autonomous and shall operate even when the Enterprise Network or the Internet connection fail. Typical services at this level are the Domain Controller, necessary for the user authentication, disseminating common technological policies, and the Manufacturing Execution System, the MES, which is a component typically used in manufacturing to control the various sites and production lines. Specifically critical components are the SIS, that enforce functional safety for humans working or using the OT environment. For instance, a device that automatically blocks a certain machine when it could injury a person is part of SIS and reside in the OT.

[3]OPC, https://opcfoundation.org, MODBUS, https://www.modbus.org, are typical OT protocols found in production. PROFIBUS is an industrial protocol defined by IEC 61158/IEC61784-1, and PROFINET, https://www.siemens.com/it-it/products/profinet/ is an implementation of PROFIBUS designed to operate over ethernet.

For Peer Review

Notably in some deployments, the Industrial Network or the DMZ are *air-gapped*, i.e., the networks do not have any physical connection to the IT. Even if no connections are possible, there are many business cases to exchange data or files among the networks. An adversary can take advantage of these ad-hoc channels by tricking staff or contractors into installing fake software updates and patches, or transferring files that will introduce malware into industrial networks via USB drives. This is exactly how the notorious Stuxnet malware operated. In order to avoid developing a false sense of cybresecurity, the air-gap has recently been considered a risk [14].

Above the industrial DMZ there is the already mentioned *Enterprise Network*, i.e., the zone where IT applications are deployed. Typical examples are the Enterprise Resource Planning (ERP), the company web servers, or the Enterprise WLAN where all the company's laptops and PCs are connected. This zone is connected to the Internet using a border firewall.

Drawing a hypothetical line between "what is IT" and "what is OT" is hard and context-dependent. The driving concept is that *OT processes shall work even if the company IT is disrupted* as *Availability* must be always guaranteed. In fig. 2, Operational Technology may have a boundary in the *managed switch*, assuming that the plants work continuously in parallel. Naive OT/IT convergence projects move the industrial logic from the OT to the IT and in some case, remotely hosted by cloud providers. Obviously, the industrial protocols are then exposed to all the IT threats without having any protection. A naive convergence puts the whole system at risk, for example it is not acceptable that human lives are endangered because a SIS stopped working due to the Internet connection in the IT zone being temporarily unavailable.

4 Summary of Results

The sectorial analyses we present in sections 5 and 6 clearly provide an answer to our original research questions, which we summarize here:

- R1 The common reference architectures defined for OT/IT convergence projects is the Purdue Enterprise Reference Architecture, the PERA model. While the academic sources show a large variability and many non-standard, ad-hoc architectures, the commercial sources mostly rely on PERA. Not surprisingly, PERA is the basis for the international standards (such as the ISA/IEC 62443 family) and it is supported by cloud providers such as AWS and Microsoft Azure. RAMI 4.0 is also considered for those projects which are related to Industry 4.0, specially in the manufacturing domain.
- R2 The main concern for planning OT/IT convergence is *cybersecurity*, for both industry and academia. Initiating a OT/IT convergence project without taking into account cybersecurity from the beginning will increase the costs and the chances of security incidents.
- R3 The domain that is the most studied in OT/IT convergence projects is manufacturing. However, there is a difference between works in the academic community that tend to be more specific compared to the works from the industry, that are purposely more generic in order to attract a wider range of customers.

On the basis of the results of R1 and R2 we devote sections 5.1 and 6.1 of the paper to standard architectures and section 7 to standards that address the cybersecurity of OT/IT converged systems. Industrial standards are notoriously complex and multi-faceted, with several SDOs producing relevant documents [35, 36]. Firms have several incentives to adhere to standards, due to product certifications and to the need to be compliant to international laws. Our goal is then to guide researchers in the academic and industrial context to propose solutions that are both innovative and realistically adoptable.

For Peer Review

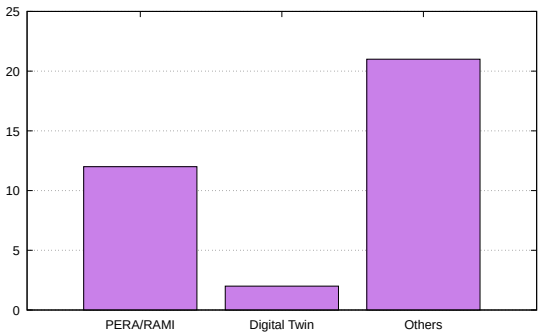


Fig. 3. Academic analysis: *Architecture used.*

5 Analysis of the Academic Sources

This section analyzes and comments the academic sources, categorized for Architecture used, Concern, and Application domain as in table 2. For each question, the results are eventually sub-divided in other concepts, if any, for instance, the cybersecurity *concern* has multiple facets, such as Risk Analysis, lack of awareness and skills, etc.

5.1 Architecture Used

As fig. 3 shows, the majority of the papers do not use a specific reference architecture, however, among those that use one, the choice favours PERA and RAMI 4.0. We then divide the discussion between papers adopting the PERA and RAMI 4.0 models and the others.

5.1.1 PERA and RAMI 4.0 -based solutions. In OT/IT convergence, many aspects have to be considered when defining a target architecture. In [29], authors discuss the complexity of converging IT and OT, and the common mistakes that can be done, such as exposing OT or IoT equipment to the public Internet where they can be found and attacked. Moreover, in [102] the complexity is extended to the OT protocols used to send and receive messages among OT components. The paper discusses that typical OT protocols have been designed with availability as the primary requirement. As an example, the MODBUS standard was designed in the early 1980s as a communication protocol over serial lines, and extended to TCP/IP communications in 2006. MODBUS provides the message syntax to obtain interoperability between two communicating devices, a server and a client, where all the messages are sent in a communication channel in clear, and do not enjoy neither encryption, integrity or non-repudiation. The same reasoning can be generalized to other protocols, except for the newer ones, such as OPC-UA which includes security considerations in its design [31]. The paper concludes that when designing a OT/IT convergence project, IT architects have to fully understand the peculiarities of the protocols and of their connected OT devices. The same applies to OT architects: they lack the knowledge of the peculiarities of modern IT protocols. This complexity can be tamed using reference models. The authors suggest to map the architecture to the PERA model.

The PERA model is analyzed also in [25] in which authors introduce a novel zoning architecture named MONDRIAN. In this architecture, the OT packets are encrypted and authenticated by a central security management system. MONDRIAN introduces a new layer which may break interoperability in older devices, furthermore, it changes parts of the system that are very unlikely to be modified. This approach differs from some of the standards in which the trend is to add a TLS 1.2 layer over the communication channels, hence not modifying the underlying protocols (as the

For Peer Review

secure version of MODBUS/TCP[4]). In [103], authors highlight that OT protocols are not properly analyzed in terms of cybersecurity, and, similarly to [102], lack of OT knowledge by IT architects is problematic. They focus on the fact that cybersecurity solutions available in current protocols are either based on TLS (e.g., REST API, MQTTs) or using proprietary solutions (OPC-UA). However, authors use the PERA model as a reference architecture to map their findings.

Authors of [84] note that most of the OT software has been coded by so-called "*baby boomers*" (people born in the range 1946-64) that are in the process of retirement, leaving managers the task to organize efficient knowledge transfer sessions with new professionals, that have more IT skills than OT. In order to base the convergence project on a solid foundation and avoid potential availability incidents, they suggest to use PERA. In this sense, standards are not only a way to implement communications between devices, but also to streamline knowledge transfer between professionals. Authors of [84] introduce the concept of Hybrid Cloud, where the typical OT equipment processing business-sensitive data remains on premises, while less business-sensitive systems are being deployed in a remote cloud. The authors also introduce modern technology in OT, such as Kubernetes.

PERA is also considered in [5] to avoid relying only on the talent of the system architect, while instead basing the convergence on a methodology using specific languages to automatically generate software artifacts to be enforced in a PERA architecture. Automatic and rigorous generation of software artifacts is seen as a way to prevent errors and to create architectures which may be evaluated by third parties.

The authors of [62] present RAMI 4.0, that is an innovative methodology that overcame legacy architectural approaches. RAMI 4.0 is a framework, i.e., a way to represent the system top-down starting from the business processes, the functionality that implements such processes, the communication protocols, down to the devices that are already deployed in OT/IT convergence projects or the need to be tailored before integration. We will dedicate section 7.2 to this standard that plays an important role in OT/IT convergence. The authors of [63] propose an extension to Archimate to draw architectures for OT/IT convergence projects. Archimate[5] is a standard language to express the *enterprise architecture* where the system to be analyzed is subdivided in layers (e.g., business, communication) and *views*, e.g., security. Archimate layers are similar to RAMI 4.0 layers, hence these two papers approach the same problem of representing a OT/IT convergence architecture from two similar perspectives.

An Archimate model can be further abstracted providing a metamodel, i.e. a language definition for models that are used in a specific domain. Authors in [64], highlight that a proper architectural metamodel is lacking in OT and that makes it hard to create sector-specific architectural descriptions. Thus, they provide an OT metamodel for Archimate, adding also domain-specific indicators to evaluate the architecture, hence making the results non-generalizable. With a complementary approach, authors of [104] introduce the need of a Data Governance system expressed by means of Enterprise Architecture approaches such as TOGAF[6]. In fact, both approaches complements each other: TOGAF's methodology requires the creation of reusable models, named *building blocks*, defining *what* are the tasks to be done to build an enterprise architecture, while Archimate *visualize* the architecture developed using TOGAF[7].

Other papers focusing on convergence architectures tackle different points. The authors of [35] describe how the standardization bodies cooperates to create frameworks and best practices, while [86] shows how those standards are relevant when applied to the security of naval ports using the PERA model. In [25] a similar approach is followed, by

[4]The Secure version of Modbus/TCP is an open standard from the Modbus organization which wraps the modbus payload in a TLS frame. Specifications are available at https://www.modbus.org/file/secure/modbussecurityprotocol.pdf
[5]See, e.g., https://www.opengroup.org/archimate-forum/archimate-overview, Last Access March 28, 2026
[6]See, e.g., https://www.opengroup.org/togaf, Last Access March 28, 2026
[7]See, e.g., https://help.opengroup.org/hc/en-us/articles/32115987894930-How-the-ArchiMate-Language-and-the-TOGAF-Standard-Complement-Each-Other, Last Access March 28, 2026

For Peer Review

eliciting threats to the railway sector and how to mitigate risk inducted by threats by means of a PERA representation.

5.1.2 Other Architectures. Even if standards are used in the academic literature, a majority of papers do not use a well-known architecture. In [90] a novel architecture for OT/IT convergence projects that concentrates data to a central location for streaming and process analysis is shown, while in [13] the adopted architecture is based on the OPC-UA protocol, that has the benefit of considering security in its design. Clearly, this pattern only applies to those components implementing OPC-UA.

A relevant approach derived from IT is the Zero Trust Architecture (ZTA), a security model in which no network communication is trusted by default and access to resources is granted only after authentication and authorization [37]. Some proposals introduce ZTA discussing how this solution may mitigate cybersecurity concerns as all communications are secured [38], [102]. However, ZTA is typically implemented through centralized components, such as an identity provider and a Policy Enforcement Point (PEP), which evaluates the identity, permissions, and so-called *security posture* of a requesting entity before allowing communication [82]. The application to OT is problematic because OT protocols do not natively support these mechanisms, and reliance on centralized authorization components may introduce single points of failure, negatively impacting system availability.

In [65] authors highlight the problem of converging IT and OT in terms of network protocols. In particular, authors concentrate on the time-sensitive property of OT networks (e.g., messages should arrive ordered and time bounded). To allow OT/IT convergence, they survey existing network protocols, such as Ethernet, and reason on their limitations. They also propose an Ethernet extension to maintain the time-sensitiveness property in backbone networks, which would guarantee seamless integration at network level between IT and OT.

Authors of [59] note that there are several issues hindering OT/IT convergence. In their work, they consider the OT/IT convergence architecture holistically, e.g., considering all the assets from the sensor up to the data center. The authors propose an ontology that considers Software-Defined Data Centers (SDDC) enabling reconfiguration of the systems based on the sensor deployments. SDDCs are data centers whose computing elements are virtual instances, e.g., virtual machines or computing images. Authors also consider cybersecurity as a concern, and include it within their ontological reasoning.

In [81] authors highlight the problem that OT protocols are not designed for convergence. Hence, they perform a survey of the available standards and protocols available in the Smart Grid Domain (a very typical case for convergence). Similarly, in [85], authors define an ontology to describe the data to plan OT/IT convergence projects, in a specific subset of manufacturing: motor winding. In [68], authors consider the manufacturing scenario highlighting the fact that despite the investments made in OT/IT convergence in manufacturing, companies are not ready to extract data from all their production equipment. Their main suggestion is that integration is successful only if it is followed by open standards and open APIs. Authors also show that although OT/IT convergence projects are designed to tackle supply chain disruption, the method to be followed is often unclear, as not many studies are available surveying real convergence projects.

The disruption of the supply chain is considered in [33]. Authors' approach is to instrument services in the Industrial DMZ with data obtained from OT sensors to give information to decision makers personnel to face supply chain disruptions. However, disturbances can happen in such distributed scenario. The ability to automatically reconfigure parts of the system is part of what is considered by [33] which introduces a definition of the OT/IT convergence system as a loosely-coupled Service Oriented Architecture, where each actor of the system is considered as a service (e.g., a Web Service, or a REST API endpoint). In the paper, authors provide a test instance of a manufacturing system to prove

For Peer Review

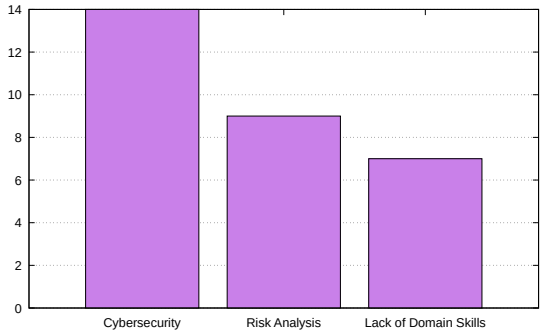


Fig. 4. Academic analysis: *Concerns*

For Peer Review

their findings.

In [67], authors compare between Industrial IoT and OT and outline the major differences. While IoT could include modern devices, usually OT is made of legacy systems which expose known vulnerabilities. Authors concentrate on a manufacturing use case, and propose a key exchange method which is inherently challenging to implement due to the heterogeneous nature of IT and OT devices.

Authors in [15] focus on the manufacturing sector introducing a new architecture paradigm, adding a *gateway* which, similarly to what happens in PERA, decouples IT with OT. The architecture proposed is technologically based on MQTT and OPC-UA, two protocols that add some security by design. Moreover, authors introduce the concept of Security Operation and Event Management (SOEM), as a platform for Critical Infrastructure Protection. However, adding the SOEM may have some impacts on how cybersecurity incidents are handled, as when reaching OT/IT convergence, threats may laterally move from IT. Hence, having cybersecurity-related events collected in two separate systems (SOEM and SIEM), it may create inefficiencies and difficulties for analysis to make correlations of nefarious IT/OT events (more will be discussed in section 5.2.1).

Finally, digital twins have attracted significant attention in the recent literature in several fields, however unexpectedly, they do not play a primary role when designing OT/IT convergence projects. In this context they can be used as an architectural component, because the digital twin constantly communicates with its physical counterpart, implying that the effect of a change on the digital twin results in an immediate exchange with the physical world, and vice versa [55]. Using this approach, data generated by the OT system is immediately available in its digital twin. Therefore, the digital twin can act as an intermediary (e.g., a proxy) between the IT/Cloud counterpart of the OT system, performing the integration. As an example, in [61], Digital Twins are added to the project to monitor the network of the OT environment, an aspect that has not been widely considered in other papers.

5.2 Concerns

The concerns extracted from the academic literature are summarised in fig. 4 and can be clustered by: cybersecurity, with special focus on risk analysis, and lack of specific domain skills. Although risk analysis is related to cybersecurity, we keep it separated because we want to stress its importance, which is confirmed by the presence of a dedicated standard in the family of standards ISA/IEC 62443 that we analyze later on.

5.2.1 Cybersecurity. Cybersecurity is seen as a major concern in OT/IT convergence projects, mostly due to the different expectations from the business. In the IT, threats as data loss, protection of intellectual property, confidentiality are paramount, while in OT availability and safety are more important. Simple measures as enforcing strong passwords, multi factor authentication, password rotation or avoiding group credentials are not implemented.

This misalignment is at the basis of several papers, in [69] authors state that there is a need to flow cybersecurity experience from IT to OT staff and viceversa, considering that such aspects are different in the two domains. Authors of [51] highlight the network threats when directly connecting IT to OT, and that if an attacker can do lateral movements from IT to OT, this will result in security consequences as described in [69]. As a consequence, OT Security Operation Centres (SOCs) need to learn OT processes in order to find threats to the availability of the OT system that they are monitoring. Some authors [102] remark that in addition to the fact that OT vulnerabilities are less known by the SOCs, OT protocols do not go under a strict security analysis, thus there are not common architectural patterns that are used to protect communications. For similar reasons, authors of [66] conclude that there is a need for a separated SOC dedicated to OT.

However, some proposals for structured cybersecurity methodologies that can reduce the risk are emerging. In [42] authors use the MITRE approach to systematically define cybersecurity concerns. The MITRE ATT&CK tool[8] gathers techniques and tactics which have been observed in previous attack campaigns and is routinely used in large enterprises in the IT context. For instance, the technique named *Exploit public-facing Application*, classified by MITRE with the ID `T0819`, has been used by threat actors to breach into OT systems via an exposed device. Hence, when architects design OT/IT convergence projects, they shall, at least, consider known attack techniques in the kill-chain, to avoid common mistakes.

The approach taken in [54] proposes a strategy for data analysis to detect cyber attacks. In fact, one of the most effective tools for the IT security is the Security Information Event Management (SIEM), that collects logs from different sources and correlates them to detect attacks. Most of the tools use the MITRE approach to classify the types of attack and have built-in correlations for common devices or systems, such as Active Directory. Clearly, IT systems have different methods to send log data, and they mostly have defined syntax and semantics. In OT logs are not available on every device, and they are in proprietary format. Hence, the authors' idea to define a strategy to analyze such OT-generated logs to create correlations is foundational for incident management.

5.2.2 Risk Analysis. Risk analysis is a structured process to identify, assess, and prioritize threats to an organization's objectives. It evaluates what could go wrong, how likely it is, and the potential impact. Risk analysis is particularly valuable when systems cannot be thoroughly tested before being put into operation, as is often the case in OT, where it is impractical or impossible to create test vessels or test railway tunnels. In such cases, risk-aware decisions must be made by reasoning over a model, and the use of a solid methodology is essential to minimize the likelihood of overlooking critical factors.

In [5], authors use Model Based System Engineering (MBSE) with SysML [83]. SysML is a modeling language for system engineering applications. Like other languages of the same kind, it enables to reason over the *model* of the architecture, before having a prototype. The paper delivers a SysML model of the OT system under consideration, used to perform the evaluation of system components, cybersecurity, and performance. Also the authors of [6] use SysML to create a model-based approach for the implementation of safety and security controls, satisfying the principle of security by design. Another approach to create architectural models is given in [9], where authors use techniques

[8] See, e.g., https://attack.mitre.org/matrices/ics/

For Peer Review

from the IEC 61499 standard as a modeling methodology that they claim to be a good fit for risk analysis of OT/IT convergence projects.

In [48], authors propose a combined approach, by defining a risk analysis framework integrated with IT and OT. This approach slightly differs from the others where OT-specific risks are treated differently from IT-specific ones.

Several papers analyze sector specific risks. In [86], the authors focus on safety and security risks specific to context of seaports, proposing an analysis based on Bowtie [52]. Bowtie is a well known methodology to create a visual representation of how threats and hazards interact to produce consequences, and the barriers and mitigations that could prevent an event or reduce its impact. Similarly, in [60] railway-specific threats are discussed. Here, risks are analyzed using the ISA 62443 family of standards we will analyze later.

Although devices are different, in the medical sector [100] the Internet of Medical Things (IoMT) suffers of similar cybersecurity risks than typical OT devices in other sectors. However, IoMT has specific regulations and standards. In Europe, the Medical Device Regulation (EU 2017/745) mandates the use of security measures to mitigate risks of unauthorized access, and all that is necessary to run the software as intended.

Two publications tackle risk analysis for the manufacturing domain. The authors of [47] introduce an architectural viewpoint of OT technology related to business objectives (similar concepts as RAMI 4.0), and highlight that the evaluation of risks is a priority when considering the integration between IT and OT, and an underestimation of risks can cause projects to fail, as the business goals can not be met by only investing in technology without proper risk evaluation. The authors of [97] focus on a typical manufacturing use case of Industry 4.0, a supply chain: the final product may be composed by a set of semi-finished parts manufactured in outsourcing. In the Industry 4.0 paradigm, the production line may be spawn among several companies, everyone with their security domain, internet connected. Here, cloud services orchestrate the production, eventually gathering and actuating OT messages. They observe that a compromise of the orchestrator may hinder the entire production, with financial losses to every partner of the supply chain. Authors of [22] acknowledge that a standard methodology for OT risk analysis exists: the ISA/IEC 62443-3-2 and propose a methodology that start by using a threat model which triggers the creation of compromising cyberattack scenarios, and then building a risk matrix. This methodology automatizes the ISA/IEC 62443-3-2 approach in order to reduce human error.

Summing up, Risk Analysis is considered very important in the literature. There are standard methodologies that provide an homogeneous approach to OT-specific risks, and the research on OT/IT convergence should be based on them. For this reason we will give an excerpt of ISA/IEC 62443-3-2 in Section section 7.3.4.

5.2.3 Lack of Specific Domain Skills. Besides the purely technical factors, the human factor is an equally important concern in OT/IT convergence. OT engineers have an automation background, while IT software engineers have a computer science background. In [66], authors notice that due to this fact, cybersecurity skills are lacking in OT engineers and IT vulnerabilities are poorly understood by OT engineers. As already mentioned, most of the OT development has been done by a generation of people close to retirement, and their skills are at risk of not being transferred if managers do not organize knowledge transfer properly. For instance, authors of [30] propose a strategy based on questionnaires to technicians and managers in order to streamline the knowledge transfer in a Smart Grid OT/IT convergence project while authors of [69] propose a hands-on workshop to share the cybersecurity knowledge between IT and OT staff. The workshop was tested by instrumenting a digital twin of a production system, allowing the staff to experience attacks and countermeasures. The questionnaire and interview-based approach is also used in [32] for the manufacturing sector. Here, authors interviewed manufacturing firms evaluating factors that can positively influence OT/IT convergence. The

For Peer Review

key identified factors are interoperability at all levels (e.g., technical, semantics, and architectural), a solid governance, and resilient IT infrastructure.

In [46] authors focus specifically on SIS, the already mentioned Safety Instrumented Systems, that enforce functional safety for humans working or using the OT environment. The paper explains that SIS technologies may go under a strict certification process and can not be modified in place. They are clear example of OT: legacy devices with long life cycles, unavailability of patches, and impossibility to reduce their availability. The authors focus on both human and technical factors when deploying SIS.

5.2.4 Other Concerns. Other concerns considered by academic papers are less relevant, and they are describing how OT/IT convergence enhance monitoring, the Return of Investment when performing OT/IT convergence projects, and how digital twins can help in many aspects, such as cybersecurity, monitoring, or maintenance.

Authors of [10], analyse the gaps and opportunities when performing OT/IT convergence projects, in terms of monitoring assets, such as gaining visibility, threat detection, and incident response capabilities. Monitoring is performed using a Digital Twin in [61], where the data is evaluated by connecting the digital representation of the system with the OT System, and all the data manipulation is performed in the DT, leaving the OT system untouched. In [90], authors present an architecture that concentrate in data-related cases, where the OT/IT convergence project is performed to gather data from the industrial control system to make it available to be further processed by Data Analysts. Similarly, in [71], authors concentrate on Data convergence from the industrial networks specifically for SMEs by proposing a data platform using an approach aligned with the PERA model. The use of standards is tackled by [8], which consider the IEC 61499 as a modeling methodology to attain OT/IT convergence projects. Notably, the use of IEC 61499 is relevant as its features allows the architectural description of industrial components and applications. Used together with Archimate (which complements it), it may enable a detailed reasoning of the OT/IT convergence: the industrial components are described using IEC 61499 while the other components (cybersecurity, proxies, etc) are modeled with Archimate. Data-related convergence is also tackled by [101] where authors shows the benefits of the Industry 4.0 OT/IT convergence projects, where IoT performs manufacturing processes and how good quality data is required to analyse and monitor the success of the project. Also governance is the topic of [49] which propose an "IT/OT Governance Framework" realised upon the analysis of the results of dozens of German-based OT/IT convergence projects. Authors provide recommendations on how to structure the team, the management, and roles and responsibilities for a successful OT/IT convergence initiative.

Opportunities are evaluated by [23] who covers the benefits of performing OT/IT convergence projects, yet highlighting the cybersecurity risks, and remarking the need of coordinated standards to avoid market solution fragmentation, who may bring practical maintenance problems, as lifecycle of OT systems is longer than the surrounding IT components that are wrapping it.

5.2.5 Application Domain. Among the ones that target a specific domain, manufacturing is the most addressed one followed by energy, other considered domains are the medical sector, oil and gas, maritime sector or railways. Notably, Small-Medium Enterprises (SMEs) have been considered as an application domain itself, for instance in both [21] and [71], authors tackle the SME research by proposing a data platform for the OT/IT convergence projects specific for SMEs.

Treating SMEs as a separate category makes sense, because the concerns we outlined so far are exacerbated when the firm has a small scale. On the one hand, a SME is more agile and can deploy ad-hoc innovative solutions more easily than a large firm, that provides an initial advantage. However, scaling is an issue because ad-hoc solutions are

For Peer Review

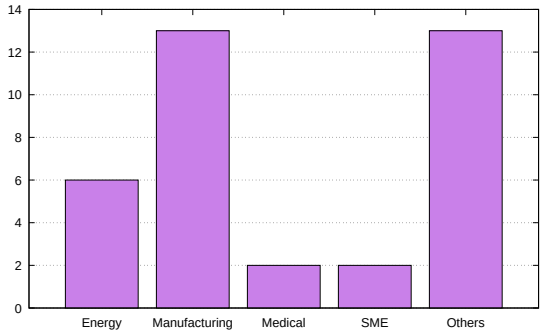


Fig. 5. Academic analysis: *Application Domain*

not imagined to scale, they must be made compliant with the norms, and it is easier to procure expertise from the market when adopting standard approaches. Not surprisingly, searching for architectural patterns that may help the usually unskilled personnel of the SMEs to mitigate risks is also an objective of the Digital Research Program of the EU commission[9] and research should support this trend.

Finally, the literature does not report details of sector-specific real-world, OT/IT convergence projects. This is a huge gap to be filled in the scientific literature, because cost/benefit analysis, lesson-learned, and shared best practices may dramatically help the architects to understand the implication of connecting OT systems to the cloud.

6 Analysis of Commercial Sources

This section analyzes and comments the commercial sources. Most sources use a standard architecture, which is a key difference compared to academic sources. The majority of the concerns are concentrated on *cybersecurity*, followed by *data integration*, and at the same level, *operational efficiency*. Notably, other aspects considered are *maintenance, skill increase, opportunities*, and *organizations*. Commercial sources try to stay general and do not target specific application domains.

6.1 Architecture Used

Unlike academic analysis, the trend presented in fig. 6 shows that industry tends to align to the mentioned PERA model. The PERA model is the basis for most of the implementations provided by technology providers [4, 79, 80] and bases the standards cited by the current legislation.

Some attention is dedicated to Zero trust Architectures [34]. An initial study [3] maps the concepts of ZTA to the requirements defined in the ISA 62443 family of standards, by e.g., reasoning over zone and conduits to limit the network traffic, or mandating user authentication on devices. In [7] a systematic literature analysis is made in the field of IoT. However, both studies do not fully consider a method to evaluate eventual availability risks introduced by transition from a legacy OT system to a ZTA, which we already referred to.

[9] See, e.g., https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en, Last Accessed, December 22, 2025.

For Peer Review

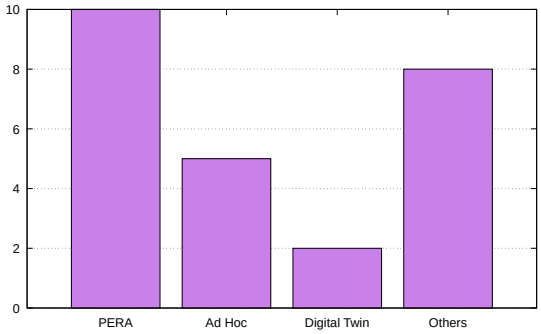


Fig. 6. Commercial Analysis: *Architecture Used*

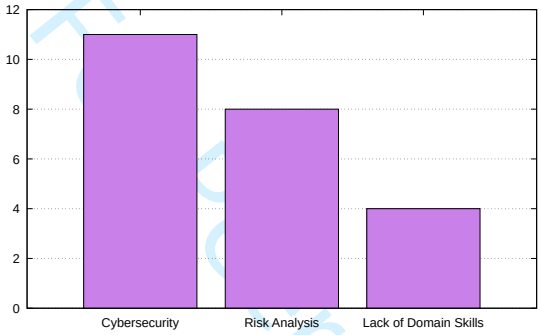


Fig. 7. Commercial analysis: grouping results by *Concern*

6.2 Concerns

The *concerns* have strict similarities with the academic literature, as cybersecurity is given topmost importance, although data usage is also considered.

6.2.1 Cybersecurity. The commercial analysis stresses that practical security measures shall be in place in OT/IT convergence process [18, 19, 26, 39, 40, 76, 91, 93], however, the proposed approaches do not always follow a unique guidance. This is eventually due to the fact that vendors tend to promote their solution (e.g., Cisco acting on networking, Fortinet on firewalls, while Mc Kinsey & Company, Boston Consulting Group, and others, on governance), and tailored cybersecurity measures are given for specific protocols, such as BACNet [94, 95], using IEC 61499 [88], or MQTT [44]. As an exception to the heterogeneity of the solutions, vendors give network segmentation a key importance [18, 19, 40, 74, 77] as the foundational measure when integrating IT and OT. This is relevant because network segmentation is also key in the standard architectures and solutions we describe in section 8. However vendors, in agreement with standards [39, 40, 98], outline that risks due to OT/IT convergence can't be mitigated only by network segmentation, and that physically separating networks is useless as malware may spread using other means.

A key insight provided by [93] is that we expect cybersecurity in OT to be performed using automated tools as much as possible in the future. Security Automation tools merge software deployment pipelines with continuous vulnerability scanning, known as Security Orchestration, Automation and Responses (SOAR) and are commonly used in the IT of

For Peer Review

large firms. Imagine instrumenting a pipeline in which software deployment is allowed only after the software went through internal security testing and automated scanning is continuously performed. Automation clearly increases the number of quality gates that software and firmware have to pass through its life cycle. However, not all OT software can be deployed using a pipeline as in a typical software company, as vendors may have their own proprietary installation method that can not be changed or automated. Similarly, continuous vulnerability scanning may not be practical due to the fact that it may add additional computing requirements to legacy devices, and this could impact their availability.

6.2.2 Data. A group of articles focus on converging information rather than infrastructure. The rationale is that OT systems eventually generate a huge amount of data that may be used by the companies to perform analysis, from predictive maintenance to market analysis. Predictive maintenance is a strategy that aims to predict when some equipment is likely to fail so maintenance can be performed, before a catastrophic breakdown occurs; i.e. analyzing the waste oils of industrial machinery suggests if some component needs to be replaced before its failure blocks the whole production. Predictive maintenance then improves *operational efficiency* which is another mentioned concern. It is easy to understand that, particularly in manufacturing, predictions can harness the power of AI [11, 28]. However, monitoring devices in production pipelines or IoT environmental sensors installed in the premises produce extremely large amounts of data, that could be better stored in the cloud exploiting Datalake or Data Lakehouse models [50]. Data convergence with the cloud can enable the use of dedicated hardware, including GPUs. Companies, specially SMEs, may not have the needed capacity locally, and see OT/IT convergence projects as a key to enable AI training, that would otherwise be impossible.

6.2.3 OT Skills lacking. As the scientific literature, the commercial sources outline the lack of skills as a major concern for OT/IT convergence projects. A particular case is raised by Fortinet [39] that highlights that SOCs on the market lack OT-specific skills. Typical SOC operators have IT cybersecurity skills and, in order to provide a service always available, they rotate over shifts, and operators may work on different customers. Gaining OT-specific skills for an operator may require on-site visits, understanding of the domain threats, and of the specific implementations. Eventually, if the system is not at least converged on data, the SOC may not have access to logfiles, requiring physical presence on the premises of the customers. Hence, research should be done in providing playbooks for the OT SOC operators to effectively act upon events on OT networks. For example, standardised log events would dramatically improve the correlation capabilities of the SIEM.

6.3 Application Domain

The breakdown of the application domains described in the commercial documents is presented in fig. 8.

Domains are generic, made to apply to a wide range of situations, without touching the OT domain specificity. The contents provided stay at a high level, and the solutions proposed need to be enforced by personnel that has specific OT skills per each domain. This is justified by the fact that commercial documents are written to interest potential customers, and thus, they try not to restrict their contents to some specific application.

7 Relevant Industrial Standards

Architectural Frameworks are layered ways to describe complex technical systems, helping engineers understand where functions, assets, and information belong without prescribing a specific implementation. Our literature analysis evidences that PERA is the prominent standard architecture guiding OT/IT convergence projects, with RAMI 4.0 being a more modern alternative, not always applicable to legacy systems. PERA was proposed in the 90s and offers the classic

For Peer Review

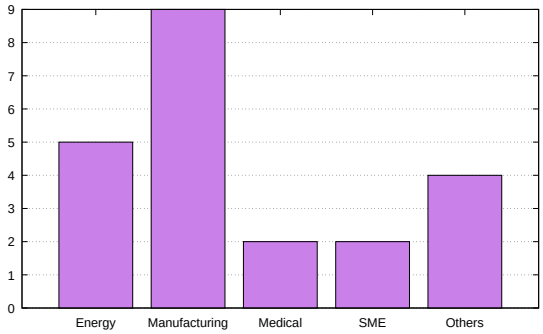


Fig. 8. *Application Domain* grouping

hierarchical view of IACS, from field devices at the lowest levels up to enterprise applications. RAMI 4.0, by contrast, was introduced in the 2010s, and provides a modern, multidimensional model that integrates lifecycle stages, digital asset representation, and interoperability for Industry 4.0 environments. In this section we will introduce both PERA and RAMI 4.0. We will also introduce the family of 62443 standards, that is the most relevant reference for cybersecurity in industrial settings, and it was significantly influenced by the PERA model. PERA's hierarchical layering naturally lent itself to the 62443 concepts of zones and conduits, which we will see align with the Purdue levels.

To draw a lose analogy with IT systems, PERA and RAMI 4.0 can be seen as the OSI or TCP/IP stacks in networks, and ISA/IEC 62443 can be seen as the ISO 27000 family of standards. Any IT professional can not propose a realistic solution ignoring these building blocks. Similarly, solutions for OT/IT convergence can not ignore PERA, RAMI 4.0 and and ISA/IEC 62443.

However, frameworks and standards provide a language, they don't dictate how systems must be built. Engineers and researchers must propose a solution, described using the correct terminology and respecting the security standards. In section 8 we describe two solutions adopted in real deployments. The first is the CISCO Converged Plantwide Ethernet (CPwE), a so-called *blueprint*, that is a detailed plan or design that guides the implementation of the OT/IT convergence. CPwE operationalizes the concepts found in PERA/RAMI and implements 62443 security principles in the network layer. The second is Gartner RA, that uses a different approach, and that we present as an alternative.

7.1 The Purdue Enterprise Reference Architecture Model - PERA

The PERA model is an architecture framework devised for computer integrated manufacturing[10]. It introduces the concept of *layers*, e.g., grouping of particular architecture *views*, from the point of view of different stakeholders. Table 3 shows the 5 PERA levels, together with their own responsibility and functions.

For each row of the table, we report an example of architectural asset that is considered to be part of the level. With respect to cybersecurity, PERA considers it as a *cross-cutting concern* meaning that it encompasses all the assets in every layer. This means that a cybersecurity program should consider the security of the Enterprise System (e.g., adding active intrusion detection systems in corporate PCs, adding Web Application Firewalls, Data Loss Prevention solutions, etc.), the security of the Plant (e.g., access control system for accessing the physical areas of the plant), the production area (e.g., defining specific cybersecurity trainings for the system operators on the countermeasures adopted to protect

[10] See, e.g., https://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.pdf

For Peer Review

PERA Layers			Description		
Level	**Hierarchy**	**Control**	**Responsibility**	**Basic Functions**	**Example**
5	Enterprise	Corporate Management	Achieving the mission of the enterprise and managing the corporate	Corporate Management, Finance, marketing, Research & Development.	Corporate management computer
4	Facility / Plant	Planning Production	Implementation of the enterprise functions, and planning and scheduling the production	Product Design & Production Engineering, Product Management, Procurement, Resource Management, Maintenance.	Plant management computer
3	Section / Area	Allocating and Supervising Materials and Resources	Coordinate the production, supporting the jobs and obtaining and allocating the resources to the jobs	Shipping, Waste Treatment.	SCADA, Supervisory Computer
2	Cell	Coordinate multiple machines and operations	Sequencing and supervising the job	Production at cell level.	Distributed Control System, RTU
1	Station	Command Machine Sequence and Motion	Directing and coordinating the activities	Production.	PLC
0	Equipment	Activate Sequence and Motion	Realization of the commands	Production.	Actuator, Sensor

Table 3. PERA Layers

the OT system), up to the cybersecurity of the Station components (e.g., defining hardware requirements for new procurement).

When PERA is used to define the architecture of OT/IT convergence projects, architects shall consider the convergent aspects (e.g., data, commands, services, and security) throughout the 5 layers. Usually, additional security countermeasures for protecting the corporate assets or services are considered within layer 5, which also includes Cloud services.

The division between layer 3 and layer 4 is considered the border between IT and OT environments. Note however that this border is conceptual, but not strictly technological. The OT devices at layer 0-1 must be controlled and supervised at level 3, and this happens remotely, not necessarily with one operator per device. This means that OT protocols are transported over IT protocols (Ethernet switches and Routers). However, the conceptual separation happens because the network used for the OT is ideally disconnected from the IT infrastructure of the company, and not Internet connected.

7.2 The Reference Architectural Model for Industry 4.0, RAMI 4.0

The RAMI 4.0 framework, depicted in Figure fig. 9, is structured along three axes. The first axis presents the six RAMI 4.0 architectural layers. From top down, the *business layer* addresses the economic and regulatory aspects, the *functional layer* describes the functionality implemented by the various architectural assets and their run-time environment. The *information layer* describes data and is used to support the semantic interoperability aspects. The *communication layer* describes the access to information and the functions of a connected asset (e.g., REST, SOAP, DSRC, 5G). The *integration layer* represents the transition from physical to information world (e.g., human-machine interfaces) and finally the *asset layer* represents the assets that exist in the physical world (sensors, actuators, SCADA). The second axis follows *Life cycle & Value stream* and distinguishes between the *instance* and the *type*: the type represents the concept, while the instance represents the physical object, or digital object in the system memory. The third axis, the *Hierarchy*, consists

For Peer Review

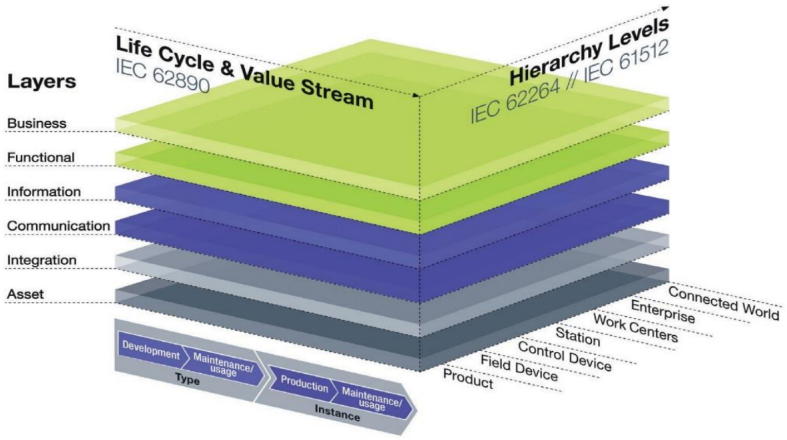


Fig. 9. The reference architectural model for Industrie 4.0 (source: [89])

of: *Product*, describing the unit produced by a system/machine; *Field Devices* and *Control Devices*, i.e. a physical unit coordinating other devices; *Stations* - systems grouped together into a *Work Center*; *Enterprise*, which is the organization and the *Connected World*, the interface with external systems.

7.3 ISA/IEC 62443 family of standards

The ISA 62443 is a family of standards providing both a methodological approach to OT cybersecurity as well as a practical guidance on how to create reliable infrastructures and products.

The ISA/IEC 62443 family is divided in 4 parts, as follows.

1 General topics, such as terminology, glossary, and use cases
2 Policy and Procedures, requirement definitions, implementation guidance, patch management, and maintenance requirements
3 System, security technology for the OT system, Security levels and risk analysis
4 Component, device security, product development requirements

Standards are named according to the above subdivision, e.g., the ISA/IEC 62443-1-1 is the first document of the first part, thus it contains general topics, while ISA/IEC 62443-3-2, is the second document of the third part, thus containing security technology and risk analysis.

The ISA/IEC family is shown in Figure fig. 10. Although each part is a stand-alone document, to secure an infrastructure ISA defines a *methodology* that goes across at least three steps and is represented in fig. 11:

(1) defining the cybersecurity management system and its security program (62443-2-1);
(2) defining the implementation requirements (62443-3-3);
(3) defining the product requirements for those devices which shall be inserted in the OT environment (62443-4-2)

Even if not strictly mandated by the methodology, *risk analysis* and *impact analysis* are essential to define a security level for each of the zone, and in cascade, the requirements of the devices. Therefore, the methodology must be complemented with a fourth element:

For Peer Review

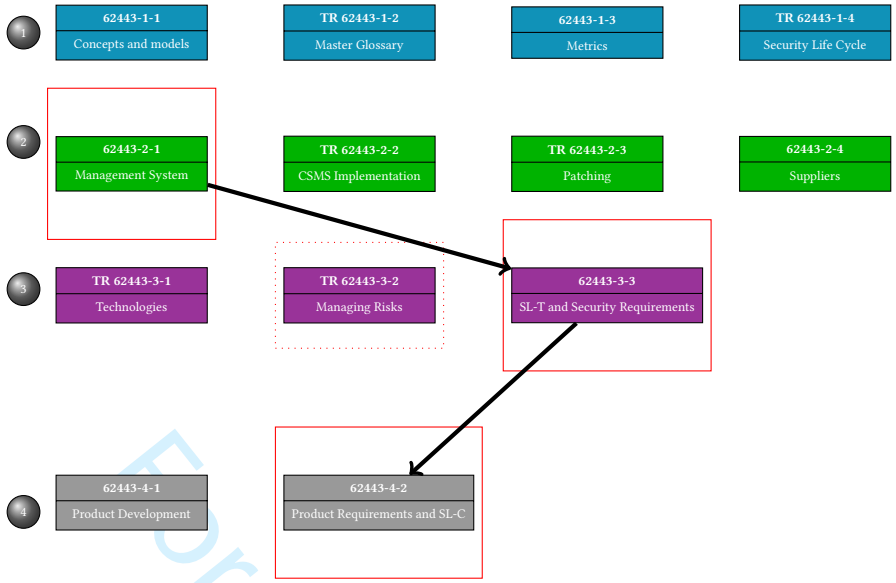


Fig. 10. The ISA/IEC 62443 family of standards. Red boxes indicate standards comprising the three steps of the ISA methodology, and the arrows indicate the order in which the standards are applied. The ISA/IEC 62443-3-2 is the optional risks management method.

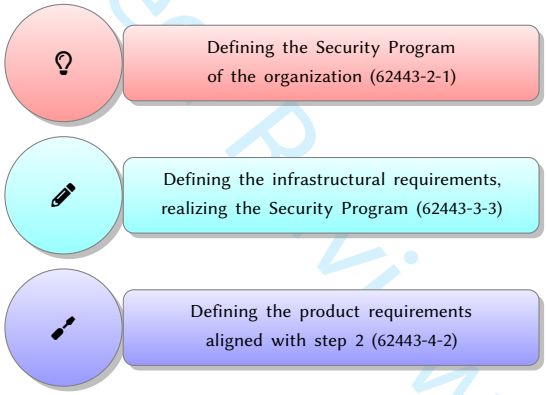


Fig. 11. The ISA/IEC 62443 methodology

(4) a structured, threat-based foundation for risk analysis (62443-3-2).

7.3.1 62443-2-1: Defining the Cybersecurity Management System. The security program defined in the part 2-1 is subdivided in 8 security program elements, varying from the definition of roles and responsibilities for the security operations, to the supply chain management. It mandates *what* policies and procedures shall be written by the company, but not *how*, left to the cybersecurity professionals. Foundational of the security program is the subdivision of the system under consideration in two entities: *Zones*, i.e., set of processes and devices sharing similar cybersecurity characteristics, and *Conduits*, i.e., zones where the data is only in transit and connect other zones. Zones are built upon geographical aspects, functional safety instrumented systems, or regulatory aspects; zones are then represented in the PERA model.

For each zone, the methodology requires risk analysis, i.e. identifying potential threats or failures and evaluating their likelihood and consequences. The risk analysis will establish the *Security Level Target (SL-T)*, a number from 1 (lowest) to 4 (higher)[11]. Higher is the potential impact of a risk, higher is the SL-T. As an example, zones that include the already mentioned SIS technologies potentially impact the life or operators or customers, and they are usually SL-T 3 or 4, while the zone for office tasks, may be SL-T 1. The SL-T also takes into consideration the attacker skills required to implement the threat, from lowest skill and less knowledge of the OT system, up to state-sponsored attackers, with high knowledge of the OT systems. SLs are evaluated using the standard procedure offered by 62443-3-2, so the evaluation is measurable and repeatable by external auditors.

At the end of this step, the typical outcome is the definition of a cybersecurity policy that requires, among other things, the IACS network to be functionally segmented. The policy defines the roles of the personnel, including people responsible for each segment. Furthermore, it mandates that risk assessments are performed and repeated on a regular basis to identify current and new threats to the OT network.

7.3.2 62443-3-3: Defining the System Security Requirements and Security Levels. Once the policies and procedures required for the security programs are available, and the OT system is divided into zones and conduit, 62443-3-3 is used to define *security requirements*. For each element in each zone, one or more security requirement is defined depending on the zone SL-T. At the end of this step, for instance, authentication requirements are set on a certain element. If the zone of the element has a low SL-T, then user authentication can be performed locally by the device using username and password, while if the SL-T is high, a Multi Factor Authentication scheme will be required.

7.3.3 62443-4-2: Defining the Product Requirements. Finally, ISA/IEC 62443-4-2 defines product requirements. Manufacturers design, build, and certify products with certain capabilities, named SL-Capability, SL-C. Capabilities have one-to-one mappings to SL-T, so that the system owner can procure products off-the-shelf which have the desired capabilities. In case a component can not be modified or replaced, and the original one does not respect the desired SL-C, the OT system owner must conduct a gap analysis and put compensating countermeasures in place.

7.3.4 The 62443-3-2: The Risk Analysis Method. We have seen that Risk Analysis is a fundamental component of the methodology, it has a prominent role also in our literature review, and it will become mandatory with the upcoming regulations (as we will describe in section 9). The methodology defined in ISA/IEC 62443-3-2 makes the process structured and repeatable, and paves the way for external consultants to be certified and to promote their services to both SMEs and Critical Infrastructures. It defines a two-stages approach, in the first one, a Business Impact Analysis is performed. Business Processes deemed relevant are analysed and a Maximum Tolerable Period of Disruption (MTPD) is defined. MTPD quantifies how much a failure in a certain zone would impact the business. The, when the assets are grouped in Zones, and a SL-T is defined, a detailed risk analysis is made, component per component, for the most relevant zones.

8 Two common *Solution* architectures

Given a reference architecture like PERA or RAMI 4.0, a *Solution Architecture* is an "instance" of a reference architecture, in the sense that it provides details of the concepts expressed in the template provided by the Reference Architecture.

This section presents two common solutions architectures: the Cisco Converged Plantwide Ethernet (CPWE) in Section section 8.1 and the Gartner Reference Architecture in Section section 8.2. The relevance of these two solution

[11] Notably, the SL-T can also be a vector, but here, for the sake of readability, we used its cardinal form

For Peer Review

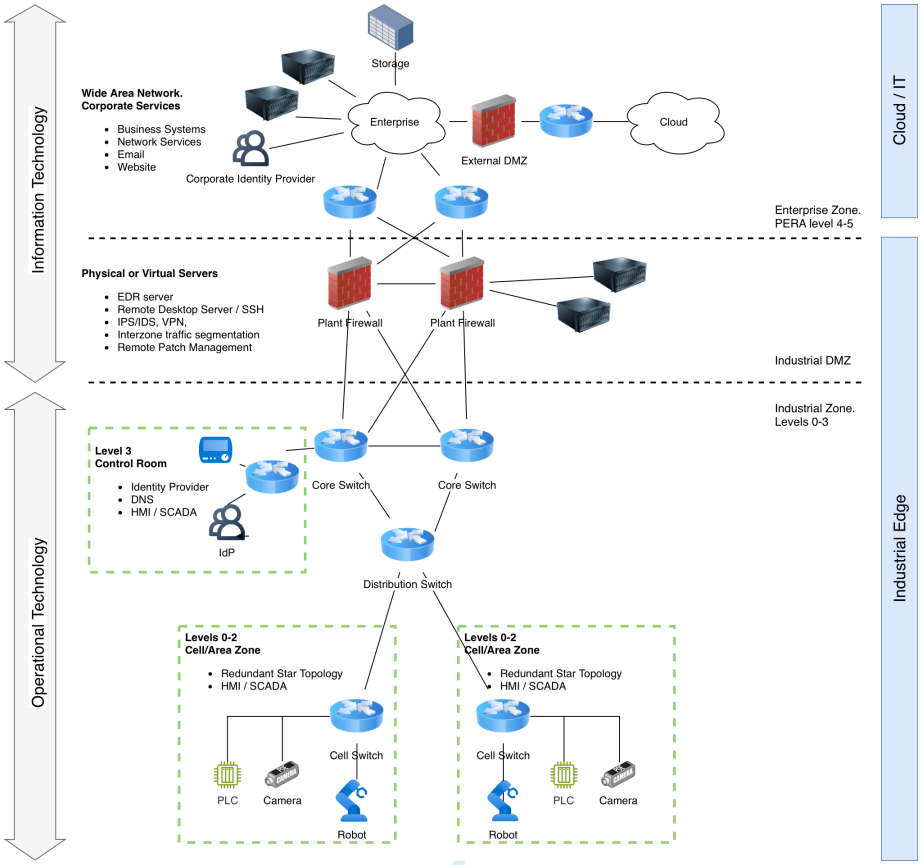


Fig. 12. An excerpt of the CISCO Converged Plantwide Ethernet (CPwE).

architectures is due to three main evidences. First, they are generic enough to apply to many domains as they do not constrain any domain-specific semantics, second, they are widely cited in the analyzed literature, third, they re-use many concepts we introduced when describing the standards.

8.1 The CISCO Converged Plantwide Ethernet (CPwE)

The CPwE [19] is a solution architecture based on PERA. It considers the PERA levels from 0 to 5, as defined in table 3. CPwE is depicted in fig. 12.

The architecture is described bottom up and, and following 62443 it is split into zones and conduits. The bottom part of the image contains the zones in which the OT technology resides. It is split into two industrial zones that contain assets which are necessary for the core business, like robotic arms or production lines, which shall work constantly and correspond to PERA levels 0-2. The two zones corresponds to two production plants, the cardinality depends on the complexity of the system, a shipment company may have one zone per ship, a motorway operator may consider to have one per Tunnel, etc. All the zones are connected using distribution and core switches to a particular zone (usually named *control room*) that implements the services (PERA level 3) which are common for the two lower zones, such as

user and identities in a Domain Controller, or the management system. Here, normally the MES resides, which is the entity that controls all the production lines.

Moving up, the CPwE implements segregation adding two firewalls to realize the industrial de-militarized zone (DMZ) that separates the IT from the OT. The DMZ contains the services which are needed in the Industrial Edge and need may connect to the cloud (e.g., downloading EDR updates, or Remote Desktop Gateway, in order to allow suppliers to connect to the equipment). The firewalls at this layer implement the *Intrusion Detection System* (IDS) and the *Intrusion Prevention System* (IPS), including VPNs.

At the top level we have the enterprise zone, where the cloud and the corporate network reside, that correspond to PERA levels 4 and 5.

The OT/IT convergence in the CPwE is realized in Industrial DMZ. In the case of data only integration, OT information flows from lower levels to the IT passing through firewalls and IDS/IPS, eventually using a VPN. When instead the integration is at monitoring or actuating levels this means that the control of OT devices happens in the cloud, so the MES is moved in the enterprise zone.

Let us note that this architectural decision has potential drawbacks, for instance, events taking place at the ISO/OSI layer 2 in the industrial zone, will not be detected by the IPS/IDS (e.g. ARP spoofing, MAC cloning etc.) Also, if a malware penetrates one plant (e.g. someone plugs a USB stick into a computer) and performs lateral movement among plants, this could go undetected. These risks should be addressed with the methodology provided by 62443-3-2 and mitigated if necessary. Recall that, as we already mentioned, the industrial zone contains all the OT technologies, but not only OT technology, routers and computers that are needed to pilot and interconnect the OT are present there too.

8.2 The Gartner RA

The Gartner Reference Architecture [44] is shown in fig. 13. The Gartner RA does not map to the PERA model directly, it conceives two layers, the *Industrial Edge* and *Cloud* but still uses the 62443 methodology, allowing concepts as *restricted data flow* and or separation of duties.

The Gartner RA is devised for OT/IT convergence, and considers Internet access to connect the two systems, both protected by firewalls. At the core of the RA, there is the use of the MQTT protocol, elected at both sides as the integration transport technology. The OT system considers the MQTT broker as a centralized platform to share data between the devices and the SCADA, including the Data Historian . The the MQTT broker implements OT/IT convergence as IT services are subscribed to the MQTT broker enables the flow to the cloud, and viceversa. The semantics is driven using *Sparkplug B*, a specification from the Eclipse foundation [96].

The use of the MQTT broker between the SCADA and the industrial device may limit the use of such industrial protocols as MODBUS, or Profinet, that are specifically devised for availability (e.g., not requiring a central broker). Similarly, most of the IPS/IDS detection tools are trained on standard protocols, hence introducing the risks that an attack to the data protocol may be undetected. Moreover, not being a consolidated standard, Sparkplug-b lack of technological sustainability.

9 Legislative Context for OT systems

This section briefly presents an overview of the legal context, with reference to the European Union (EU), including the NIS 2, RED and CSA Acts. Although non-EU norms exists (such as NIST SP 800-66 on healthcare, or NIST SP 800-82r3) they will not be discussed here, as they are not yet part of a legislative framework [70]. The legislation context indicated

For Peer Review

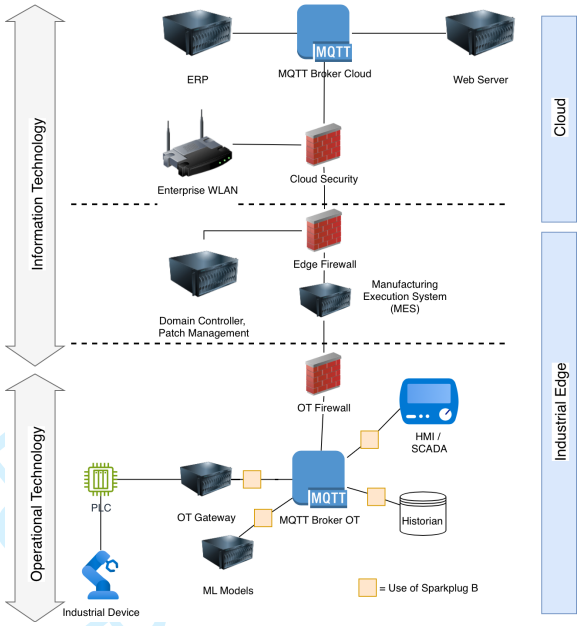


Fig. 13. An excerpt of the Gartner Reference Architecture

in this section is part of the European cybersecurity Strategy[12] and applies both to large companies and SMEs operating a critical infrastructure. The legislative scenario depicted in this section is relevant for OT/IT convergence scenarios for those companies that have OT devices. As an example, NIS 2 applies to, among others, Energy, Transport, Health, Space, Drinking and Waste water management, that have a strong OT component. Similarly, Machinery, RED, and the Cyber Resilience Act, focus on the security of components, including those used in OT environments.

9.1 The NIS 2 directive

The EU 2022/2555 Network and Information Security (referred to as NIS2, as the successor of a previous NIS directive) defines measures for a high common level of cybersecurity across the Union. Being a directive, member states are required to transpose it into their respective national law[13].

NIS 2's Annex A defines a list of critical sectors, many of which are subject to OT/IT convergence, that are subject to the cybersecurity measures laid down in Article 21. Those measures are, e.g., risk analysis policies, incident handling, definition of business continuity rules, cyber hygiene etc.. NIS 2 has a strong focus on standards, as some clauses explicitly encourage and promote the use of open standards.[14]

[12] See, e.g., https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, Last Accessed November 9, 2025. For an introduction on the security standards and regulations, see, e.g., OWASP at https://ot.owasp.org/v/2025/background-ot/related-standards/, Last Accessed November 9, 2025

[13] According with the European Cyber Security Organization (ECSO), onnly 15 out of 27 member states transposed the law in their national law, https://ecs-org.eu/activities/nis2-directive-transposition-tracker/, Last Accessed November 9, 2025

[14] Clause 52 states that "*open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders*", and that "*Member States should therefore be able to promote the use of open-source software and open standards*". Clause 59 insists saying that "*The Commission, ENISA* [the European Union Agency for cybersecurity], *and the Member State should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management*"

For Peer Review

9.2 The Machinery Regulation and the RED

The Machinery Regulation EU 2023/1230, that will enter into force in 2027, applies (Article 2) to any interchangeable, safety component that contains a firmware. The regulation states that manufacturers must adopt proportionate measures for the protection of the safety of the product on the market. This includes the use of cybersecurity best practices and standards, specially for those OT Components of the Shelf (COTS), like, e.g., PLC, or sensors and actuators. Typical equipment as devices that can be purchased from vendors and deployed in the premises of the OT system, will have, according with the regulation, basic protection on cybersecurity aspects.

The Radio Equipment Directive 2014/53/EU (RED), establishes a regulatory framework for placing radio equipment on the market. Articles 3(3)(d), (e) and (f) impose cybersecurity requirements on radio devices, such as protection of personal data, and safeguards from frauds. This directive is relevant for those OT technology using radio frequencies, such as OT devices using radio communications as WiFi, GPS, or GPRS.

9.3 The Cyber Security and Resilience Acts

The Cyber Security Act EU 2019/881 (CSA) aims to achieve a high level of cybersecurity, cyber resilience and trust in the European Union. Among other goals it establishes cybersecurity Certification Schemes for products. This goal is covered also by the Cyber Resilience Act, that will enter fully into force in 2027, and that defines a European Marking on products. The marking will be given upon a certification process based on cybersecurity testing. At the moment of writing the candidate standards are unknown, but they will be specified one year before the CRA enters into application[15] and are expected to rely on the known architectures described in Section section 7.3.

10 Conclusions

OT/IT convergence is no longer a theoretical trend but a practical necessity driven by organizational demand for data integration, operational visibility, and advanced analytics. However, our analysis shows that convergence is constrained by the fundamental characteristics of OT systems, including long life cycles, limited updatability, certification requirements, and strict availability guarantees. These constraints significantly shape which architectures and security mechanisms can be realistically adopted.

Our systematic review reveals that both academic and industrial efforts predominantly rely on established reference models, particularly the Purdue Enterprise Reference Architecture, and that cybersecurity is treated as a cross-cutting concern across all layers. Industrial solutions generally favor conservative, standards-aligned architectures that prioritize risk containment and operational continuity, whereas academic proposals often assume a degree of system modifiability that is rarely achievable in practice. Given that changes to deployed OT systems are often impractical or prohibited, future research should focus on methods that work within these constraints, such as architectural patterns, deployment strategies, and security controls that can be incrementally adopted without disrupting operations. Bridging the divide between research innovation and industrial feasibility is essential for enabling secure and sustainable OT/IT convergence in real-world environments.

[15] See, e.g., https://www.cencenelec.eu/news-events/news/2025/newsletter/ots-62-cra/, Last Accessed November 9, 2025

For Peer Review

11 Acknowledgments

This work is partially supported by project "SEcurity and RIghts In the CyberSpace - SERICS" (PE00000014 - CUP H73C2200089001) under the National Recovery and Resilience Plan (NRRP) funded by the European Union - NextGenerationEU. The methodologies and technologies reported in this work do not specifically refer to Autostrade Per L'Italia.

References

[1] Giuseppe Aceto, Valerio Persico, and Antonio Pescapé. 2019. A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges. *IEEE Communications Surveys and Tutorials* 21, 4 (2019), 3467–3501. doi:10.1109/COMST.2019.2938259

[2] Ahmadzai Ahmadi, Maisam Moradi, Chantal Cherifi, Vincent Cheutet, and Yacine Ouzrout. 2018. Wireless Connectivity of CPS for Smart Manufacturing: A Survey. In *2018 12th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. 1–8. doi:10.1109/SKIMA.2018.8631535

[3] ISA Global Cybersecurity Alliance. 2024. *Zero Trust Outcomes Using ISA/IEC 62443 Standards*. Technical Report. ISA GCA.

[4] Amazon Web Services. 2025. Guidance on using ISA/IEC 62443 for IIoT projects. https://aws.amazon.com/it/blogs/iot/guidance-on-using-isa-iec-62443-for-iiot-projects/. [Online; accessed 13-September-2025].

[5] Amirali Amiri, Gernot Steindl, Ian Gorton, Siegfried Hollerer, Wolfgang Kastner, and Thilo Sauter. 2024. Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Systems: A Graph-Based Approach. In *2024 IEEE International Conference on Software Services Engineering (SSE)*. 123–129. doi:10.1109/SSE62657.2024.00029

[6] Amirali Amiri, Gernot Steindl, and Siegfried Hollerer. 2024. Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Cyber-Physical Systems. In *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*. 1–2. doi:10.1109/ICPS59941.2024.10640023

[7] Muhammad Ajmal Azad, Sidrah Abdullah, Junaid Arshad, Harjinder Lallie, and Yussuf Hassan Ahmed. 2024. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things* 27 (2024), 101227. doi:10.1016/j.iot.2024.101227

[8] Zakaria Bencherki, Khaled Benfriha, Vincent Meyrueis, Laurent Cachot, and Philippe Soares. 2024. IEC 61499: A Key Enabler for Distributed Automation in Industry 4.0. In *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*. 1–6. doi:10.1109/ICECET61485.2024.10698592

[9] Zakaria Bencherki, Vincent Meyrueis, Khaled Benfriha, Laurent Cachot, and Philippe Soares. 2024. The IEC 61499 Standard in Industry 4.0. In *2024 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*. 24–29. doi:10.1109/I2CACIS61270.2024.10649815

[10] Mukund Bhole, Wolfgang Kastner, and Thilo Sauter. 2024. IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities. In *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*. 01–08. doi:10.1109/ETFA61755.2024.10710968

[11] Boston Consulting Group. 2025. Converging IT and OT Will Boost Value in Industrial Tech. https://www.bcg.com/publications/2024/converging-it-and-ot-will-boost-industrial-tech-value. [Online; accessed 13-September-2025].

[12] Boston Consulting Group. 2025. Our Critical Infrastructure Is More Vulnerable Than Ever—It Doesn't Have to Be That Way. https://www.bcg.com/publications/2017/engineered-products-critical-infrastructure-vulnerable-doesnt-have-to-be-that-way. [Online; accessed 13-September-2025].

[13] Wolfgang Bubeck, Florian Frick, Armin Lechler, and Alexander Verl. 2025. Enabling the Sensor-To-Cloud Vision Through IT/OT Convergence – Industrial Power Consumption Measurement Device as a Reference Use Case. In *Production at the Leading Edge of Technology*. Springer Nature Switzerland, Cham, 413–420.

[14] Eric Byres. 2013. The air gap: SCADA's enduring security myth. *Commun. ACM* 56, 8 (Aug. 2013), 29–31. doi:10.1145/2492007.2492018

[15] Roberto Caviglia, Daniyar Aliaskharov, Alessio Aceti, Mila Dalla Preda, Paola Girdinio, and Giovanni Battista Gaggero. 2025. A Security Operation and Event Management (SOEM) Platform for Critical Infrastructures Protection. *Computers, Materials and Continua* 85, 3 (2025), 5327–5340. doi:10.32604/cmc.2025.068509

[16] Cisco Systems. 2025. 4 Challenges IT Organisations in Manufacturing are Facing Today. https://www.cisco.com/c/m/en_uk/products/networking/cloud-management/manufacturing.html. [Online; accessed 13-September-2025].

[17] Cisco Systems. 2025. IT/OT Convergence in Critical Infrastructure and Industrials White Paper. https://www.cisco.com/c/en/us/solutions/collateral/industries/manufacturing/itot-convergence-wp.html. [Online; accessed 13-September-2025].

[18] Cisco Systems. 2025. IT/OT Whitepaper. https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide/m-introduction.pdf. [Online; accessed 13-September-2025].

[19] Cisco Systems. 2025. Network Security within a Converged Plantwide Ethernet Architecture. https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG/CPwE-5-1-NetworkSecurity-DIG1.html. [Online; accessed 13-September-2025].

[20] Cisco Systems. 2025. Where to Begin Your Journey to Digital Value in the Private Sector. https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/value-at-stake.pdf. [Online; accessed 13-September-2025].

[21] Antonio Corradi, Giuseppe Di Modica, Luca Foschini, Lorenzo Patera, and Michele Solimando. 2022. SIRDAM4.0: A Support Infrastructure

For Peer Review

for Reliable Data Acquisition and Management in Industry 4.0. *IEEE Transactions on Emerging Topics in Computing* 10, 3 (2022), 1605–1620. doi:10.1109/TETC.2021.3111974

[22] Mike Da Silva, Stéphane Mocanu, Maxime Puys, and Pierre-Henri Thevenon. 2025. Safety-security convergence: Automation of IEC 62443-3-2. *Computers and Security* 156 (2025), 104477. doi:10.1016/j.cose.2025.104477

[23] Jeff Daniels. 2023. Building the Factory of the Future With the Industrial Internet of Things. *Computer* 56, 8 (2023), 84–88. doi:10.1109/MC.2023.3260419

[24] Ralf Luis de Moura and Luciana de Landa Ceotto. 2024. Operational Technology: The New Role of Enterprise Architecture in the Context of IT & OT Convergence. In *2024 4th International Conference on Advanced Enterprise Information System (AEIS)*. 10–16. doi:10.1109/AEIS65978.2024.00010

[25] Piet De Vaere, Claude Hähni, Franco Monti, and Adrian Perrig. 2021. Tableau: Future-Proof Zoning for OT Networks. In *Critical Information Infrastructures Security*. Springer International Publishing, Cham, 207–227.

[26] Deloitte. 2025. Closing the IT-OT vulnerability gap. https://www.deloitte.com/an/en/Industries/mining-metals/perspectives/closing-the-it-ot-vulnerability-gap.html. [Online; accessed 13-September-2025].

[27] Deloitte. 2025. Managing the successful convergence of information and operational technology. https://www.deloitte.com/ch/en/services/risk-advisory/research/managing-the-successful-convergence-of-information-and-operational-technology.html. [Online; accessed 13-September-2025].

[28] Deloitte. 2025. Trends and Strategic Importance of IT/OT in Automotive Manufacturing. https://www.deloitte.com/cz-sk/en/Industries/automotive/blogs/trends-and-strategic-importance-of-it-ot-in-automotive-manufacturing.html. [Online; accessed 13-September-2025].

[29] Patrick Denzler and Wolfgang Kastner. 2023. *Reference Architectures for Closing the IT/OT Gap*. Springer Berlin Heidelberg, Berlin, Heidelberg, 95–123.

[30] Thabani Dhlamini and Tendani Mawela. 2022. Critical Success Factors for Information Technology and Operational Technology Convergence Within the Energy Sector. In *Innovations in Bio-Inspired Computing and Applications*. Springer International Publishing, Cham, 425–434.

[31] Jannik Dreier, Maxime Puys, Marie-Laure Potet, Pascal Lafourcade, and Jean-Louis Roch. 2019. Formally and practically verifying flow properties in industrial systems. *Computers & Security* 86 (2019), 453–470. doi:10.1016/j.cose.2018.09.018

[32] Ike C. Ehie and Michael 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 (2020), 103166. doi:10.1016/j.compind.2019.103166

[33] Maximilian Engelsberger and Thomas Greiner. 2018. Dynamic reconfiguration of service-oriented resources in cyber–physical production systems by a process-independent approach with multiple criteria and multiple resource management operations. *Future Generation Computer Systems* 88 (2018), 424–441. doi:10.1016/j.future.2018.06.002

[34] EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF MANAGEMENT AND BUDGET. 2022. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. [Online; accessed 21-September-2025].

[35] Max Felser, Markus Rentschler, and Oliver Kleineberg. 2019. Coexistence Standardization of Operation Technology and Information Technology. *Proc. IEEE* 107, 6 (2019), 962–976. doi:10.1109/JPROC.2019.2901314

[36] Max Felser, Markus Rentschler, and Oliver Kleineberg. 2019. Coexistence Standardization of Operation Technology and Information Technology. *Proc. IEEE* 107, 6 (2019), 962–976. doi:10.1109/JPROC.2019.2901314

[37] Eduardo B. Fernandez and Andrei Brazhuk. 2024. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces* 89 (2024), 103832. doi:10.1016/j.csi.2024.103832

[38] Mattia Fogli, Carlo Giannelli, Elena Mari, and Cesare Stefanelli. 2025. Zero Trust Architecture and Digital Twin to Improve the Cybersecurity Posture of Distributed Smart Factory Environments. In *2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. 01–08. doi:10.1109/DCOSS-IoT65416.2025.00115

[39] Fortinet. 2025. IT/OT Convergence Provides an Opportunity for Streamlining Operations. https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-streamline-noc-soc-operations.pdf. [Online; accessed 13-September-2025].

[40] Fortinet. 2025. A Solution Guide to Operational Technology Cybersecurity. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-solution-guide-to-ot-cybersecurity.pdf. [Online; accessed 13-September-2025].

[41] Fortinet. 2025. Tackling OT Security as Networks Converge. https://www.fortinet.com/blog/industry-trends/tackling-ot-security-as-networks-converge. [Online; accessed 13-September-2025].

[42] Phani Kumar Garimella. 2018. IT-OT Integration Challenges in Utilities. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*. 199–204. doi:10.1109/CCCS.2018.8586807

[43] Gartner. 2025. Gartner Identifies Top Five Smart Factory Implementation Risks for Supply Chain Leaders. https://www.gartner.com/en/newsroom/press-releases/2023-05-03-gartner-identifies-top-five-smart-factory-implementation-risks-for-supply-chain-leaders. [Online; accessed 13-September-2025].

[44] Gartner. 2025. Reference Architecture for Integrating OT and Modern IT. https://fonsecaadvisers.com/wp-content/uploads/2025/03/Gartner-reference-architecture-for-integrating-ot-and-modern-it.pdf. [Online; accessed 13-September-2025].

[45] Gartner. 2025. When IT and Operational Technology Converge. https://www.gartner.com/smarterwithgartner/when-it-and-operational-technology-converge. [Online; accessed 13-September-2025].

[46] Vahiny Gnanasekaran, Tor Olav Grøtan, Maria Bartnes, and Poul E. Heegaard. 2024. Rethinking Independence in Safety Systems. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Nature Singapore, Singapore, 153–166.

For Peer Review

[47] Adam Hahn. 2016. *Operational Technology and Information Technology in Industrial Control Systems.* Springer International Publishing, Cham, 51–68. https://doi.org/10.1007/978-3-319-32125-7_4

[48] Nourhan Halawi Ghoson, Khaled Benfriha, Vincent Meyrueis, Thomas Guiltat, and Chawki El Zant. 2025. ShieldFlow: a novel framework for OT cybersecurity in the context of industry 4.0. *International Journal of Information Security* 24, 4 (2025), 162. doi:10.1007/s10207-025-01083-3

[49] Carolin Hantsch, Markus Westner, and Markus Matschi. 2025. IT/OT-Konvergenz: Status-Quo und Umsetzungsempfehlungen. *HMD Praxis der Wirtschaftsinformatik* 62, 2 (2025), 402–418. doi:10.1365/s40702-024-01111-1

[50] Ahmed A. Harby and Farhana Zulkernine. 2025. Data Lakehouse: A survey and experimental study. *Information Systems* 127 (2025), 102460. doi:10.1016/j.is.2024.102460

[51] Ian Heritage. 2019. Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge. *Network Security* 2019, 10 (2019), 6–9. doi:10.1016/S1353-4858(19)30120-5

[52] ICAO. 2022. *Safety Risk Management Methodologies (SRM). Bowtie - guidelines.* Technical Report. ICAO.

[53] ISO/IEC/IEEE. 2022. *42010:2022.* Standard. International Organization for Standardization, Geneva, CH.

[54] Danial Jafarigiv, Keyhan Sheshyekani, and Marthe Kassouf. 2024. Tensor-Based Cybersecurity Analysis of Smart Grids Using IT/OT Convergence. *IEEE Access* 12 (2024), 191893–191906. doi:10.1109/ACCESS.2024.3515642

[55] David Jones, Chris Snider, Aydin Nassehi, Jason Yon, and Ben Hicks. 2020. Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology* 29 (2020), 36–52. doi:10.1016/j.cirpj.2020.02.002

[56] Hiroo Kanamaru. 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).* 1365–1370.

[57] Barbara Kitchenham and Stuart Charters. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Technical Report EBSE 2007-001. Keele University and Durham University Joint Report. http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf

[58] Arno Kok, Alberto Martinetti, and Jan Braaksma. 2024. The Impact of Integrating Information Technology With Operational Technology in Physical Assets: A Literature Review. *IEEE Access* 12 (2024), 111832–111845. doi:10.1109/ACCESS.2024.3442443

[59] Koundinya Koorapati, Rubini Pandu, Prem Kumar Ramesh, Sairam Veeraswamy, and Usha Narasappa. 2022. Towards a unified ontology for IoT fabric with SDDC. *Journal of King Saud University - Computer and Information Sciences* 34, 8, Part B (2022), 6077–6091. doi:10.1016/j.jksuci.2021.04.015

[60] Ravdeep Kour, Adithya Thaduri, and Ramin Karim. 2022. Operational Security in the Railway - The Challenge. In *International Congress and Workshop on Industrial AI 2021.* Springer International Publishing, Cham, 266–277.

[61] André Kummerow, Steffen Nicolai, Christoph Brosinsky, Dirk Westermann, André Naumann, and Marc Richter. 2020. Digital-Twin based Services for advanced Monitoring and Control of future power systems. In *2020 IEEE Power & Energy Society General Meeting (PESGM).* 1–5. doi:10.1109/PESGM41954.2020.9354468

[62] Sylvain Lacroix, Benoit Eynard, Julien Le Duigou, Xavier Godart, and Christophe Danjou. 2023. Distributed Approach for Integration in Industrial Systems. In *Product Lifecycle Management. PLM in Transition Times: The Place of Humans and Transformative Technologies.* Springer Nature Switzerland, Cham, 116–125.

[63] Paola Lara, Mario Sánchez, and Jorge Villalobos. 2019. OT Modeling: The Enterprise Beyond IT. *Business & Information Systems Engineering* 61, 4 (2019), 399–411. doi:10.1007/s12599-018-0543-3

[64] Paola Lara, Mario Sánchez, and Jorge Villalobos. 2020. Enterprise modeling and operational technologies (OT) application in the oil and gas industry. *Journal of Industrial Information Integration* 19 (2020), 100160. doi:10.1016/j.jii.2020.100160

[65] Wolfram Lautenschlaeger, Florian Frick, Konstantinos Christodoulopoulos, and Torben Henke. 2021. A scalable factory backbone for multiple independent time-sensitive networks. *Journal of Systems Architecture* 119 (2021), 102277. doi:10.1016/j.sysarc.2021.102277

[66] Yassine Maleh. 2021. IT/OT convergence and cyber security. *Computer Fraud & Security* 2021, 12 (2021), 13–16. doi:10.1016/S1361-3723(21)00129-9

[67] Soujanya Mantravadi, Reto Schnyder, Charles Møller, and Thomas Ditlev Brunoe. 2020. Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0. *IEEE Access* 8 (2020), 200305–200321. doi:10.1109/ACCESS.2020.3035963

[68] Soujanya Mantravadi, Jagjit Singh Srai, and Charles Møller. 2023. Application of MES/MOM for Industry 4.0 supply chains: A cross-case analysis. *Computers in Industry* 148 (2023), 103907. doi:10.1016/j.compind.2023.103907

[69] Matteo De Marchi, Marco Pomalo, Raphael Vallazza, Igor Falcomatà, Tanel Aruväli, and Erwin Rauch. 2025. Enhancing IT/OT Cybersecurity Knowledge Transfer Through Demonstrative Workshops in Cyber-Physical Production Systems. *Procedia Computer Science* 253 (2025), 2296–2305. doi:10.1016/j.procs.2025.01.290 6th International Conference on Industry 4.0 and Smart Manufacturing.

[70] Angelica Marotta and Stuart Madnick. 2025. Analyzing and Categorizing Emerging Cybersecurity Regulations. *ACM Computing Surveys, Volume 58, Issue 2* (2025).

[71] Mohammad Hasbullah Mazlan, Farihan Mohamad, Mohd Khairun Nizam Mohd Sarmin, Ahmad Farid Jamil, and Adee Zhafri Ismail. 2024. Review on Security Requirements for IT-OT Integration in Utility Internet-of-Things (IoT). In *2024 IEEE Sustainable Power and Energy Conference (iSPEC).* 473–478. doi:10.1109/iSPEC59716.2024.10892598

[72] Mc Kinsey & Company. 2025. Converge IT and OT to turbocharge business operations' scaling power. https://www.mckinsey.com/capabilities/operations/our-insights/converge-it-and-ot-to-turbocharge-business-operations-scaling-power. [Online; accessed 13-September-2025].

[73] Mc Kinsey & Company. 2025. Digital performance management: From the front line to the bottom line. https://www.mckinsey.com/capabilities/operations/our-insights/digital-performance-management-from-the-front-line-to-the-bottom-line. [Online; accessed 13-September-2025].

[74] Mc Kinsey & Company. 2025. How to enhance the cybersecurity of operational technology environments. https://www.mckinsey.com/capabilities/

For Peer Review

risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments. [Online; accessed 13-September-2025].

[75] Mc Kinsey & Company. 2025. It's the last IT/OT mile that matters in avoiding Industry 4.0's pilot purgatory. https://www.mckinsey.com/capabilities/operations/our-insights/operations-blog/its-the-last-it-ot-mile-that-matters-in-avoiding-industry-40s-pilot-purgatory. [Online; accessed 13-September-2025].

[76] Mc Kinsey & Company. 2025. Leveraging Industrial IoT and advanced technologies for digital transformation. [Online; accessed 13-September-2025].

[77] Mc Kinsey & Company. 2025. SBuilding cyber resilience in national critical infrastructure. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/building-cyber-resilience-in-national-critical-infrastructure. [Online; accessed 13-September-2025].

[78] Mc Kinsey & Company. 2025. A scalable IIoT tech stack starts with business-focused use cases. https://www.mckinsey.com/capabilities/operations/our-insights/operations-blog/a-scalable-iiot-tech-stack-starts-with-business-focused-use-cases. [Online; accessed 13-September-2025].

[79] Microsoft Azure. 2025. Achieving IT/OT Convergence with Azure Cloud. https://sdtslmn.blog/2024/07/14/achieving-it-ot-convergence-with-azure-cloud/. [Online; accessed 13-September-2025].

[80] Microsoft Azure. 2025. Extending Operational Technology to Azure. https://techcommunity.microsoft.com/blog/azureinfrastructureblog/extending-operational-technology-to-azure/3265466. [Online; accessed 13-September-2025].

[81] Mamdouh Muhammad, Abdullah S. Alshra'a, and Reinhard German. 2024. Survey of Cybersecurity in Smart Grids Protocols and Datasets. *Procedia Computer Science* 241 (2024), 365–372. doi:10.1016/j.procs.2024.08.049 19th International Conference on Future Networks and Communications/ 21th International Conference on Mobile Systems and Pervasive Computing/14th International Conference on Sustainable Energy Information Technology.

[82] National Institutes of Standards and Technology, NIST. 2025. Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207. [Online; accessed 21-September-2025].

[83] OMG. 2024. *OMG Systems Modeling Language.* Technical Report. OMG. https://sysml.org/.res/docs/specs/OMGSysML-v1.7-24-01-07.pdf

[84] Cyril Perducat, David C. Mazur, Wes Mukai, Scott N. Sandler, Michael J. Anthony, and Jon A. Mills. 2023. Evolution and Trends of Cloud on Industrial OT Networks. *IEEE Open Journal of Industry Applications* 4 (2023), 291–303. doi:10.1109/OJIA.2023.3309669

[85] K.S.K.U. Perera, Riku Ala-Laurinaho, and Petri Kuosmanen. 2026. Ontologies for the generic motor winding process. *Advanced Engineering Informatics* 69 (2026), 103937. doi:10.1016/j.aei.2025.103937

[86] Iosif Progoulakis, Nikitas Nikitakos, Dimitrios Dalaklis, Anastasia Christodoulou, Angelos Dalaklis, and Razali Yaacob. 2023. *Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure.* Springer International Publishing, Cham, 227–248. https://doi.org/10.1007/978-3-031-25296-9_12

[87] Andi Sama, Harco Leslie Hendric Spits Warnarsa, Harjanto Prabowo, Meyliana, and Achmad Nizar Hidayanto. 2023. Acquiring Automation and Control Data in The Manufacturing Industry: A Systematic Review. *Procedia Computer Science* 227 (2023), 214–222. doi:10.1016/j.procs.2023.10.519 8th International Conference on Computer Science and Computational Intelligence (ICCSCI 2023).

[88] Schneider. 2025. IEC 61499: The Industrial Automation Standard for Portability that Unleashes Industry 4.0. https://www.se.com/ww/en/download/document/998-21041914/. [Online; accessed 13-September-2025].

[89] Karsten Schweichhart. 2015. Reference Architectural Model Industrie 4.0 (RAMI 4.0). https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf

[90] M.C. Shilenge 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).* 1076–1081. doi:10.1109/ISIE51582.2022.9831605

[91] Siemens. 2025. Connect IT and OT networks optimally. https://www.siemens.com/global/en/products/automation/industrial-communication/industrial-network-solutions/ot-it-networks.html. [Online; accessed 13-September-2025].

[92] Siemens. 2025. The convergence of IT and OT. https://www.siemens.com/global/en/products/automation/topic-areas/it-ot-convergence.html. [Online; accessed 13-September-2025].

[93] Siemens. 2025. Cybersecurity for Industrial Control Systems. https://www.siemens.com/au/en/company/press-centre/blogs/cybersecurity-for-industrial-control-systems.html. [Online; accessed 13-September-2025].

[94] Siemens. 2025. Siemens Industrial IoT – Spark for the IT-OT fusion. https://www.siemens.com/global/en/products/automation/topic-areas/it-ot-convergence/siemens-iiot.html. [Online; accessed 13-September-2025].

[95] Siemens. 2025. What is IT/OT convergence in smart buildings? https://www.siemens.com/us/en/products/buildingtechnologies/trends-topics/building-technologies-blog-center/cybersecurity/it-ot-convergence.html. [Online; accessed 13-September-2025].

[96] Sparkplug Specification Project Team. 2015. The Sparkplug Specification. https://sparkplug.eclipse.org/specification/. [Online; accessed 21-September-2025].

[97] Lane Thames and Dirk Schaefer. 2017. *Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges.* Springer International Publishing, Cham, 1–33. https://doi.org/10.1007/978-3-319-50660-9_1

[98] The ISA Global Cybersecurity Alliance. 2025. The Air Gap: Myth and Reality. https://gca.isa.org/blog/the-air-gap-myth-and-reality. [Online; accessed 13-September-2025].

[99] Riccardo Venanzi, Giuseppe Di Modica, Luca Foschini, and Paolo Bellavista. 2026. Towards IT/OT integration in industry digitalization: A comprehensive survey. *Journal of Network and Computer Applications* 245 (2026), 104373. doi:10.1016/j.jnca.2025.104373

For Peer Review

[100] Sebastiaan Von Solms and Jaco du Toit. 2024. Cybersecurity Governance in the Medical Ecosystem: An Orientation Guide with Specific Reference to the Merging of IT and OT Devices. In *Intelligent Computing*. Springer Nature Switzerland, Cham, 402–417.

[101] Kirti Wanjale, A. V. Chitre, and Ruchi Doshi. 2023. *Opting for Industry 4.0: Challenge or Opportunity.* Springer International Publishing, Cham, 3–20. https://doi.org/10.1007/978-3-031-29713-7_1

[102] Bassam Zahran and Fuad Abu Zahra. 2023. IT/OT Convergence Protocols: DNP3, Ethernet/IP, and Modbus. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*. 1743–1748. doi:10.1109/CSCE60160.2023.00287

[103] Bassam Zahran and Fuad Abu Zahra. 2023. IT/OT Convergence Protocols: MQTT, OPC, and REST. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*. 1732–1737. doi:10.1109/CSCE60160.2023.00285

[104] Marta Zorrilla and Juan Yebenes. 2022. A reference framework for the implementation of data governance systems for industry 4.0. *Computer Standards and Interfaces* 81 (2022), 103595. doi:10.1016/j.csi.2021.103595

For Peer Review

A Detailed analysis of the studies

Table 4. Detailed analysis of the academic studies.

Academic Resources				
Application Domain	**Architecture used**	**Keywords**	**Scope**	**Ref**
n/a	n/a	Cybersecurity Skills lacking in OT; OT vulnerabilities are poorly understood; Cyber hygiene for OT; Separated SOC	Cybersecurity	[66]
n/a	Enterprise Architecture	Lack of Architecture Frameworks (*does not considers RAMI 4.0*); Convergence changes the way OT operates	Architecture	[24]
Energy, Manufacturing	PERA	OT Protocols are not analyzed in terms of cybersecurity; Lack of knowledge of IT in OT and viceversa	Cybersecurity	[102]
Manufacturing	PERA and 62443	Uses MBSE and SysML to define an approach for safety and security; automatic generation of artifacts	Cybersecurity	[5]
Manufacturing	Model-Driven	Uses SysML 2.0 to create a model-based approach to implemented safety and security in CPS	Architecture; Cybersecurity	[6]
Energy	Ad Hoc	Cybersecurity Skills lacking in OT;Cybersecurity is a problem, and exposes MITRE tactic. OT Convergence use case: monitoring.	Architecture	[42]
n/a	PERA	OT Protocols are not analyzed in terms of cybersecurity; Lack of knowledge of IT in OT and vice versa; REST, MQTTs, and OPC UA offers cybersecurity implementation, either with TLS or with proprietary encryption	Cybersecurity	[103]
n/a	n/a	Define a risk assessment methodology	Risk	[56]
Energy	n/a	Define a strategy for cybersecurity data analysis for attack detection	Cybersecurity	[54]
Manufacturing; Medical; Automotive; Logistics	PERA	Defines the PERA model. Shows the fact that as the baby boomers retire, more IT-skilled people are on board. Introduce the concept of Hybrid cloud, such that sensitive stays on premise, while less sensitive stays on cloud;	Cybersecurity	[84]
Manufacturing	n/a	Analyses gaps and opportunities in integrating IT with OT	Monitoring	[10]
n/a	Ad Hoc	Presentation of a novel architecture that brings data to a central location and streams for processing and analysis	Data	[90]
n/a	PERA	Shows how the various standardization bodies cooperates (ISO, ISA, IEC, OASIS)	Standardization	[35]
SME	Ad Hoc	Introduces cybersecurity as a concern also for the SME	Cybersecurity	[21]
SME	Ad Hoc	Propose a data platform for SME for the IT/OT Convergence; Pushes for a coordinated and homogeneous approach	Data	[71]
n/a	n/a	Survey on the convergence. Find three research domains: maintenance, cybersecurity, and configuration management	Cybersecurity	[58]
Manufacturing	Ad Hoc	Focuses on the Industrial IoT, which is not entirely OT; concentrates on manufacturing (the MES); we can't converge with confidence; proposes a key exchange method; potentially against the standards	Cybersecurity	[67]
n/a	61499	Introduces the use of 61499 as a modeling method for attaining convergence	Standardization	[8]
Manufacturing	ZTA	Defines guidelines to support a ZTNA approach	Architecture; Cybersecurity	[38]
n/a	61499	Introduces the use of 61499 as a modeling method for attaining convergence	Standardization	[9]
Energy	Digital Twin	Shows the usage of a Digital Twin for Monitoring; Data is pushed to the network	Digital Twin	[61]
n/a	n/a	Shows the benefits of using the convergence; highlights the cybersecurity risks, the need for data, and the need for standards	Opportunities	[23]
n/a	n/a	Proposes a framework for the governance of IT/OT Convergence; Based on interviews[16]	Governance	[49]
n/a	Enterprise Architecture	Says that the Convergence is complex; to cope with this complexity we should use Architecture Reference Models (ARM)	Architecture	[29]
Manufacturing	OPC-UA	Uses OPC-UA to connect to the cloud, against the common use of patterns	Architecture	[13]
n/a	n/a	Define Shieldflow, a framework for Risk Analysis;Risk integrated with IT and OT	Cybersecurity	[48]
Energy	n/a	Shows the benefits in productivity of the IT/OT Convergence in Smart Grids; Questionnaire to technicians and managers to see their perceptions. Cybersecurity as a risk	Risk	[30]
Medical	n/a	Introduces the risks of convergence in the medical sector; Introduces background on the IoMT	Risk	[100]
n/a	n/a	Focuses on safety systems risks when in an IT/OT convergence; Considers Human and Technical factors	Risk	[46]
Maritime	PERA	Focuses on port security; introduces standards and methodologies; shows that bow-tie analysis has value; considers incidents and recovery plans	Risk	[86]
n/a	Mondrian, PERA	Present a new zoning architecture, based on MONDRIAN; Introduce Tableau, as Mondrian was made for IT; packets are encrypted and authenticated; Security management is centralized; Compatible with 62443-3-2	Architecture	[25]
Railway	PERA	Shows what are the threats to railway; evaluates the 62443 and shows the potential risks when connecting to the cloud	Risk	[60]
n/a	n/a	Shows the potential of IT/OT convergence	Data	[101]
Manufacturing	RAMI 4.0	Discuss the opportunities of new architectural models, such as RAMI 4.0	Architecture	[62]
n/a	Archimate	Proposes an extension to Archimate to draw architectures for IT/OT Integration	Architecture	[63]
n/a	n/a	Introduces the OT technology and business objectives; says that risk evaluation are a priority	Risk	[47]

[16] Although paper's original language is German, the english abstract has been taken

Application Domain	Architecture used	Keywords	Scope	Ref
n/a Oil & Gas	n/a Enterprise Architecture	Notices that if the cybersecurity risks cannot be addressed, Industry 4.0 cannot be achieved Authors tackle the problem that a proper architectural metamodel is lacking in OT, in particular in oil and gas. They provide an OT metamodel	Risk Architecture	[97] [64]
n/a	n/a	Need to share cybersecurity from IT to OT to let the IT staff to understand the complexity of OT and viceversa; organized a workshop with a DT	Cybersecurity; OT Skills	[69]
n/a	n/a	Highlights network threats when converging, stating that the cyber attack may have physical impacts, and lateral movements may also endanger intellectual property.	Cybersecurity	[51]
Manufacturing	n/a	Authors concentrates in IoT in manufacturing, and how the adoption of such IoT is due to the IT/OT Convergence. Their survey is based on hypotheses on on concepts that may positively influence the convergence. As example, Effective IT Governance, Resilient IT Infrastructure and interoperability have such positive effects. Authors interviewed manufacturing firms, and propose managerial implications, including the use of EA	OT Skills; Architecture	[32]
Ad Hoc with Gateway	Manufacturing	The paper presents a novel architecture, based MQTT and OPC UA	OT Skills; Architecture	[15]
Smart Grids	n/a	The paper focuses on smart grid. It tackles the point that Smart Grid are, by definition, a case of convergence. The point is that protocols were not made to converge. Authors survey both standards and protocols, in order to gain information that can help to create cybersecurity plans.	Data	[81]
Manufacturing	n/a	Defined an ontology of OT data for integration on motor winding; Integration relying on the meaning of the data (semantic integration between OT and IT)	Data	[85]
n/a	AdHoc	Highlights the problem of converging IT and OT in terms of network protocols. OT is full of Time Sensitive networks. Authors survey the existing protocols, find their limitations, and then introduce a Ethernet Extension for a backbone network. . Their extension is transparent for underlying technology	Architecture	[65]
n/a	AdHoc	Authors say that there are several issues to solve in order to harness the widespread dissemination and adoption of the IoT paradigm. Authors considers the IoT paradigm holistically, including the datacenter. They say that today there exists non standard way to implement OT/IT convergence as a whole. They focus on bringing together seamlessly the IT and OT, proposing an ontology which also encompasses the Software-Defined Data Center. Include security as a concern.	Architecture	[59]
n/a	n/a	Defines a methodology for avoiding human errors in risk analysis, based on IEC 62443. They consider both 62443 and 61131 standards . The methodology automates and ISO 31000 risk assessment applied to ICS. The methodology is divided in three part: threat modeling using STRIDE, generation of safety-compromising cyberattack scenarios, and building a risk matrix. New RA methodology, but aligned with standards, automatize it.	Risk	[22]
Manufacturing	n/a	Provides an analysis focused on manufacturing for IT/OT Convergence. Authors found that despite the investments, companies are not ready to extract data from all its production equipment. Authors present recommendations on how to perform OT/IT convergence projects. Authors conclude that open standards and API are key requirements for interconnectivity. Their results are that smart manufacturing (I4.0) is embraced by companies to tackle supply chain disruptions, but that the method that should be followed to implement IT/OT Integration is often unclear, because there are not many holistic studies on it. Moreover, authors claim that the business case for IT Convergence is often lacking.	Data	[68]
n/a	Enterprise Architecture	The paper presents a governance framework for Industry 4.0. It considers mainly IoT. Define a Data-Governance as a system, based on TOGAF and IEEE 42010	Architecture	[104]
n/a	AdHoc	IT/OT Convergence may face disturbances, and the system shall be able to reconfigure itself to deliver the service. Defines the IT/OT System as a loosely-coupled SOA, then represents it as a bipartite graphs, with process steps and available service instance. Provide a lab instance.	Architecture	[33]
End of Table				

Table 5. Detailed analysis of the commercial studies.

Commercial / Internet Resources				
Application Domain	**Architecture used**	**Keywords**	**Scope**	**Ref**
Manufacturing	62443	Shows the benefits of IT OT Convergence of data, where data flows from OT to IT	Data	[92]
Manufacturing	62443	Digital transformation can't be avoided; Digital Twins are complex; Most important concepts are network segmentation protection of zone boundaries securing the communication between the security zones	Cybersecurity	[91]
Smart Buildings	62443	Perform a Cybersecurity Assessment; Introduces BACNet/SC, that is a security-first approach	Cybersecurity	[95]
n/a	BACNet	*similar to [95]*	[94]	
n/a	n/a	Concerns about cybersecurity; Security automation tools should be leveraged whenever possible to help ensure a strong security posture of the ICS infrastructure	Cybersecurity	[93]
n/a	61499	Shows that 61499 can be a standard for defining a common way to attain convergence; 61499 defines an object-oriented method to define data	n/a	[88]
Critical Infrastructure	n/a	Brings use cases: Enabling real-time decision making through edge computing (moving from SCADA to Edge when need for data), Eliminating unplanned downtime through predictive maintenance, Deploying wireless technology in all environments, Providing cybersecurity for a new world of connected operations	Data	[17]
n/a	62443	Proposes a Converged Plantwide Ethernet (CPwE) that helps to enable IACS network and security technology convergence using standard Ethernet; Gold architecture use TLS Proxies	Cybersecurity	[19]
n/a	PERA	Defines cybersecurity concerns: malware, lack of visibility, lack of segmentation, lack of defined workflow. They put the DMZ in the cloud;	Cybersecurity	[18]
n/a	n/a	The need for IT is increasing, as new paradigm may arise (AI/ML); many products are being used as a service (the paper doesn't consider the costs)	Data	[16]
Manufacturing	n/a	Report on 10 years of digitalization; show that the convergence is more in oil and manufacturing; use cases of predictive maintenance, remote monitoring (IoT more than OT).	Maintenance	[20]
n/a	n/a	Converged SOC; SOC shall have OT skills; Stress the fact that with convergence comes risks	Skills	[39]
n/a	ZTNA	Airgap is not effective; Cybersecurity concern; Use onnly firewalls	Operational Efficiency; Maintenance	[40]
n/a	PERA	Safety is a key component to evaluate; Consider Cybersecurity when integrating	Cybersecurity	[41]
n/a	PERA	IT/OT convergence will give competitive advantage for companies	Operational efficiency	[45]
n/a	n/a	Introduces the concept of ET, engineering technology. OT/IT convergence is a must-do, without cybersecurity implications	Opportunities	[43]
n/a	MQTT	Introduces the use of MQTT Sparkplug b, from ECLIPSE. The security section is non-normative. Cites RAMI 4.0.	n/a	[44]
n/a	n/a	OT and IT are siloed operations; defines the need of a common governance to achieve the project; use case of predictive maintenance; RISK of having a single operating model. Against the standards	Operational Efficiency	[72]
n/a	n/a	Notices that the majority of companies are still in pilot phase (2018-2020); Pilot fails to anticipate critical requirements to scale to the enterprise; problem of integrating different automation software, bought over the years and stratified; Says that convergence is a security concern.	Cybersecurity	[75]
n/a	n/a	Considers cybersecurity countermeasures; suggests data without considering the standards; Full of grey literature	Cybersecurity	[74]
n/a	PERA; Edge	Proposes a methodology to attain convergence, divided in business, organization, and technology. Proposes an architecture based on Edge Nodes	Cybersecurity	[76]
n/a	n/a	Defines the need to prioritize use cases	Cybersecurity	[78]
n/a	n/a	Prioritize use cases	Cybersecurity	[73]
n/a	AdHoc	Proposes a set of techniques, not following the standards, with foggy terms (zero trust, visibility, awareness)	Cybersecurity; Operational efficiency	[77]
n/a	n/a	Defines some steps to attain convergence, not based on the standard; defines roles and responsibilities, asset inventory	Organization	[27]
n/a	PERA	IT/OT Convergence is risky; Shows not-standard steps to secure the mining industry; considers a compromised IT	Cybersecurity	[26]
Manufacturing	n/a	IT/OT shows growth, and competitiveness; Key technologies are Cloud Computing, AI, and MES	Cybersecurity; Operational Efficiency	[28]
n/a	AdHoc	Notices that if IT/OT are not converged, AI cannot advance. Poses the SCADA in the convergence layer;	Cybersecurity; Data	[11]
n/a	n/a	Concentrates on lacking of cybersecurity talents	Skills	[12]
n/a	PERA + Edge	Mapping of the ISA 62443 into AWS stack; Uses IIoT Cloud services on prem (Edge Network)	Cybersecurity; Data	[4]
n/a	PERA + Edge	Following the standard and the PERA (as AWS), uses Edge computing on prem.	Cybersecurity; Data	[80]
n/a	PERA + Edge	Concentrates on OT/IT convergence for data.	Cybersecurity; Data	[79]
End of Table				