The Information Technology (IT) and Operational Technology (OT) Convergence in Industrial World

Sawatsakorn Chaiyasoonthorn
Electronics Technology, Faculty of Science,
Ramkhamhaeng University, Huamark
Bangkapi Bangkok Thailand
sawatsakorn_c@hotmail.com

Somsak Mitatha
Smart City innovation Research Academy
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand
somsak.mi@kmitl.ac.th

Surapong Siripongdee
College of Innovation and Industrial Management
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand
surapong.si@kmitl.ac.th

Montri Wiboonrat*
KMITL Business School
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand
montri.wi@kmitl.ac.th*

Theeraporn Sriudomsilp
Ph.D.h.c. Candidate in Morality and Development Technology (Safety Engineering and Technology),
BRIC Graduate Institute,
UMKC-BRIC Asia Region.
sriudomsilp.tuu@gmail.com

Abstract— **Cyber Vision plays a crucial role in fostering a collaborative workflow that improves synergy between IT and OT, ensuring the secure production of operations. In collaboration with Cisco (Thailand), this study focuses on strengthening cybersecurity measures within the oil and gas (O&G) industry to defend against external cyber threats. Researchers intend to employ Cyber Vision for protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis, offering valuable insights into the industry's security posture. Following IEC 62443 and NIST 800-82 standards, Cyber Vision ensures the continuous, resilient, and safe operation of industrial processes by providing constant visibility into Industrial Control Systems (ICS). Cyber Vision comes pre-integrated with leading security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms.**

Keywords—information technology (IT), operational technology (OT), system integration, industrial control systems

I. INTRODUCTION

IT/OT convergence entails the seamless integration of information technology (IT) systems and operational technology (OT) systems. IT systems excel in data-centric computing, while OT systems excel at monitoring events, processes, and devices, facilitating adjustments in both enterprise and industrial operations. In the modern business landscape, organizations grapple with the coexistence of two distinct realms. Firstly, there's the traditional physical domain comprising machinery, electromechanical equipment, manufacturing systems, and other industrial assets. Secondly, there's the more recent digital realm housing servers, storage, networking infrastructure, and other devices that power applications and process data. Historically, these two realms remained largely isolated, sharing minimal, if any, data or control capabilities, and relying on business staff with disparate skill sets. Today, a pivotal transformation is underway as the worlds of IT and OT converge. Technological advancements like the Internet of Things (IoT) and sophisticated big data analytics systematically enable the digital information sphere to perceive, comprehend, and influence the physical operational world. When executed adeptly, IT/OT convergence amalgamates business processes, insights, and control mechanisms into a unified and harmonious environment. Like numerous other global industries, the O&G sector has navigated through multiple crises in recent times. These challenges encompassed the repercussions of the COVID-19 pandemic, volatile price fluctuations, and the repercussions of the Russian-Ukrainian conflict. In response to these adversities, many industries turned to cutting-edge technologies for both reaction and mitigation. In this context, the convergence of IT/OT stands out as a burgeoning trend within the O&G domain. It holds the potential to bridge the divide between conventional systems supporting OT and the contemporary layers of IT.

The primary focus of this research is to address the prevalent challenges associated with safeguarding the IT/OT ICS environment against cyber threats. These challenges encompass issues such as limited network visibility and monitoring capabilities, the exposure of devices to the internet without adequate safeguards, deficiencies in perimeter security defenses, vulnerabilities within unsecured systems and devices, and a notable lack of cybersecurity awareness among key stakeholders including operators, maintenance engineers, and automation engineers.

The convergence of IT and OT serves as a valuable tool for O&G operators, allowing them to harness the wealth of data generated through the integration of Internet of Things (IoT) devices with operational equipment. This data holds the potential to yield invaluable insights throughout the different phases of operation and production. According to an article published on Birlasoft, it presents itself in the form of time series data, which can be analyzed using artificial intelligence (AI) and machine learning (ML) techniques to preemptively identify potential damage or technical issues. Achieving the integration of IT and OT systems can be accomplished through a three-stage process. Initially, the OT layer, comprising supervisory control and data acquisition (SCADA) systems or distribution control systems (DCS) or programmable logic controller (PLC), and facility-installed sensors, must be seamlessly connected to the appropriate network technology for data transmission to IT systems. Subsequently, this data is aggregated by advanced platforms and stored in data silos, primed for utilization across various scenarios. Finally, through the application of AI and ML tools, this data can be leveraged to provide predictive analyses, thereby facilitating automated operations and industrial control systems (ICS). This integration also holds the promise of enhancing production, reducing incidents, and facilitating precision production planning. This research has been conducted with Cisco (Thailand) for the O&G industry to protect and prevent cyberattacks from outside. The researchers' purpose Cyber Vision for protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to provide insights into your security posture.

II. Background

A. What is IT/OT Convergence?

The concept of technological convergence is not a novel one. By facilitating the seamless integration and efficient interoperability of diverse technologies into a unified system, businesses can typically enhance efficiency, minimize errors, reduce costs, streamline workflows, and gain a competitive edge. Historically, enterprise IT has been a primary focus of convergence initiatives, aiming to unite often-disparate data center technologies and support flawless interconnectivity. An illustrative instance of convergence is the emergence of IT converged infrastructure, later evolving into hyper-converged infrastructure. These advancements consolidate traditionally segregated components such as servers, storage, networking, and management tools into a single, cohesive, centrally managed product.

The notion of IT/OT convergence, on the other hand, seeks to bridge the divide between physical (OT) equipment and devices and the digital (IT) domain. This transformation has been made feasible through innovations like machine-to-machine communication and the introduction of sophisticated IoT sensors and actuators that can be seamlessly integrated into physical equipment. These devices harness wireless communication through standardized networking protocols to relay pertinent data from each physical system to a central server for monitoring and analysis. The findings of this analysis can subsequently be fed back to the physical system to enable more autonomous operation, enhance precision, facilitate maintenance, and improve uptime. Consider the impact of this convergence on everyday technologies, such as vehicles. The incorporation of sensors, actuators, and standardized communication enables a vehicle to transmit real-time information about its position, movement, and condition to a central data repository for analysis [5]. Simultaneously, instructions and real-time data, such as traffic and weather conditions, can be relayed to the vehicle. This empowers a human driver to make informed driving decisions, such as choosing alternate routes or scheduling vehicle maintenance before breakdowns occur. Notably, this type of IT/OT convergence serves as the foundation for autonomous (self-driving) vehicle technology as well.

B. Types of IT/OT Convergence

Convergence is not a singular, one-size-fits-all endeavor. Depending on the unique requirements and objectives of each organization, convergence initiatives can manifest in various ways. There are three primary categories of IT/OT convergence:

- Process Convergence: This category pertains to the harmonization of workflows. IT and OT departments need to revise their processes to align with each other and ensure that vital projects are effectively communicated. It's essentially an organizational convergence that addresses the internal business structure. For instance, a business may have established procedures for storing and safeguarding IT data, which may need to be adapted or expanded to accommodate the convergence of OT systems.
- Software and Data Convergence: This facet revolves around optimizing front-office software and data to meet the needs of OT. It involves technical convergence and focuses on the network architecture of the organization. For instance, IT may need to introduce new tools to gather OT data and integrate OT and IT data for analysis.
- Physical Convergence: In this category, physical devices are either consolidated or retrofitted with updated hardware to accommodate the integration of IT into traditional OT systems. This represents an operational convergence, where the hardware itself undergoes updates and maintenance over time. It could involve procuring new OT systems or incorporating aftermarket devices to facilitate data communication and control.

C. IT/OT Convergence Straegies and Best Practices

What's the optimal approach to undertake an IT/OT convergence initiative? Given the diversity of OT systems and industries considering convergence, there isn't a one-size-fits-all path that guarantees a successful convergence strategy. Nevertheless, several general principles can significantly enhance an organization's chances of success:

1) *Clear Goal Communication:* Start by articulating the overarching objectives and ensure that both IT and OT teams comprehend the goals associated with convergence.

2) *Highlight Overlaps:* Illustrate how IT and OT will intersect for each team, particularly concerning systems management and security.

3) *Define Roles and Responsibilities:* Clearly outline the roles, responsibilities, objectives, and duties for IT and OT teams, emphasizing opportunities for collaboration.

4) *Provide Cross-Training:* Encourage cross-training to foster a deeper understanding of each other's domains and needs. Additionally, consider leveraging IT/OT convergence certifications to enhance project management capabilities.

5) *Select Appropriate Tools:* Collaboratively identify and implement tools that offer the necessary visibility and control over IT/OT assets. These tools should encompass discovery, configuration, management, and security aspects.

The journey toward an effective IT/OT strategy typically comprises three distinct phases: organizational, technical, and operational.

1) *Organizational Phase:* This phase aims to facilitate collaboration and communication by fostering cooperation between IT and OT teams, often under the guidance of a senior manager or a convergence advocate.

2) *Technical Phase:* In this stage, the actual convergence architecture, including IoT and other infrastructure components, is designed and developed. This phase addresses management and security concerns and usually involves some degree of proof-of-principle validation.

3) *Operational Phase:* Here, the converged environment is deployed and maintained, which includes periodic infrastructure updates and refreshes as technology evolves.

With these overarching principles in place, an organization can concentrate on more practical aspects of IT/OT integration. There are typically three recognized approaches:

- Separate Networks: Establishing distinct networks for IT and OT.
- Network Partitioning: Dividing IT and OT networks with controlled access points.
- Full Integration: Integrating OT traffic seamlessly into the IT environment.

Each approach comes with its unique challenges and trade-offs because IT and OT systems have distinct requirements that necessitate careful consideration, particularly when dealing with legacy OT systems.

III. IT/OT Convergence Role in Industrial Operational Efficiency

IT/OT convergence techniques represent a significant leap forward for the petroleum sector. By facilitating predictive analysis through IT/OT convergence, operational costs can be significantly reduced, particularly in terms of maintenance expenditures. Moreover, this approach plays a crucial role in maintaining consistent production levels, allowing workers to anticipate and address issues before they disrupt operations. Furthermore, the implementation of remote and automated control systems not only saves valuable time but also minimizes travel expenses, enabling personnel to manage operations from their offices without the need to visit field locations.

However, it's important to acknowledge that IT/OT convergence is not without its challenges. One notable concern is the potential vulnerability to cybersecurity threats posed by hackers. To mitigate this risk, O&G companies must establish stringent cybersecurity protocols and adopt zero-trust security paradigms. Additionally, the successful implementation of IT/OT convergence necessitates the availability of equipment and devices capable of seamless integration with these new systems. When O&G companies proactively address these challenges, they stand to reap countless benefits from this innovative technique. It not only enhances operational efficiency but also supports the sector's ongoing digital transformation while minimizing overall costs.

IT/OT convergence in the O&G industry offers a multitude of business advantages. For instance, asset-intensive upstream and midstream operations can attain peak uptime levels, strategically plan maintenance downtimes, optimize oil well operations at minimum viable levels, and enhance the overall efficiency of revenue generation at production plants. Below are some key benefits of IT-OT convergence within the O&G sector, as illustrated in Fig. 1 [1];

Cost Efficiencies
1
Safer Workplaces
2
Better Production Uptime
3
Environmental Compliance
4
IT-OT Convergence Benefits In Oil & Gas Industry
5
Innovation
6
Higher Production Levels
7
Improved Collaboration
8
Better Asset Visibility

Fig. 1. IT/OT convergence benefits in O&G industry.

- Cost efficiencies
- Safer workplaces
- Better production uptime
- Environmental compliance
- Innovation
- Higher production levels
- Improved collaboration, and
- Better asset visibility

A. *IT/OT Convergence Strategy*

The oil and gas (O&G) industry is gradually embracing digital-driven practices, following the lead of industry giants such as Royal Dutch Shell, ExxonMobil, and BP. These pioneers are introducing innovative approaches that deliver unparalleled value to both their stakeholders and the market. Nevertheless, smaller and mid-sized O&G companies may lack the substantial resources required for large-scale transformation. For these organizations, adopting an incremental strategy that harnesses end-to-end use cases to simultaneously impact their bottom line will be the key to a financially viable IT/OT convergence strategy.

Furthermore, the industry faces a shortage of digital-savvy talent in areas such as data engineering, networking expertise, cloud computing, IoT proficiency, and modernized IT teams. Consequently, forming partnerships with established technology leaders with a proven track record in the industry will be a critical determinant of success. Lastly, securing support and commitment from upper management will be essential to orchestrate concerted efforts that are instrumental in the successful execution of digital transformation initiatives.

B. *IT/OT Convergence Challenges*

Purchasers, installers, and operators in both IT and OT have encountered enduring obstacles, including issues of interoperability and equipment maintenance. Cybersecurity has historically posed significant challenges for IT, and as the Industrial Internet of Things (IIoT) continues to connect more physical OT assets to the internet, OT is increasingly grappling with cybersecurity concerns as well. The majority of IIoT devices remain online at all times, offering round-the-clock access through multiple entry points (Data Management). Consequently, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and IT departments across the globe are collaborating to develop systems and networks that deliver robust and effective protection for every connection within both IT and OT systems. While IT/OT convergence offers significant business advantages, the transformation process within the oil and gas (O&G) sector has encountered notable challenges, contributing to a slower pace of adoption. Below are some key obstacles that have arisen over the years; IT/OT cybersecurity, data management, and change management, as shown in Fig 2.

1) *IT/OT Cybersecurity:* The convergence of IT and OT introduces several network security challenges as it involves transmitting data from remote sites to the core IT systems of the business. Additionally, maintaining high network availability while preserving access integrity is paramount

due to the potential safety risks and losses associated with breaches. While networking technology providers emphasize the importance of best practices to address many security concerns, organizations can mitigate security risks arising from digital transformation efforts by focusing on securing network perimeters, selecting the appropriate networking protocols at a device level, and adopting a modular approach to implement zero-trust security paradigms.Highlight Overlaps: Illustrate how IT/OT will intersect for each team, particularly concerning systems management and security. As per Statista [11], the O&G industry encountered 21 ransomware attacks worldwide in 2022, ranking it as the fifth most impacted sector by ransomware within the past year. Given its reliance on digital systems for tasks like extraction, transportation, and refinement of O&G products, the industry becomes a vulnerable target for cyber threats.

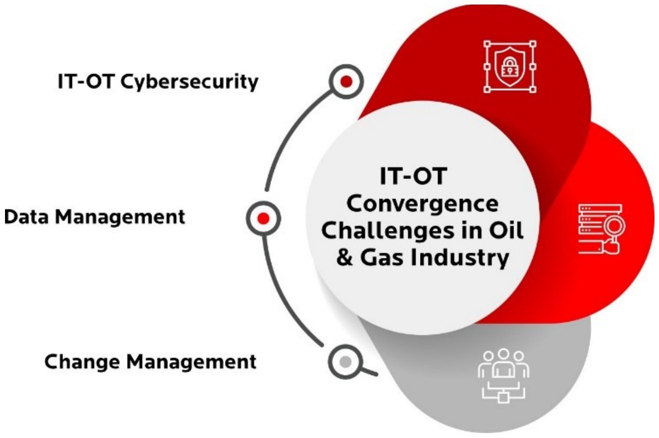


Fig. 2. IT/OT convergence challenges.

2) Data Management: Establishing an operational data platform stands as a primary objective in the pursuit of an IT-OT convergence initiative. However, the practical implementation of such a platform necessitates careful attention to numerous considerations. The value derived from data platforms becomes tangible only when the data within them is meticulously cleansed, appropriately tagged, traceable, and provided with context, rendering it readily usable as engineers embark on constructing new use cases. Furthermore, striking a balance between internalizing the correct access protocols and deploying them for high-availability, low-latency use cases is crucial while also being mindful of associated costs. Lastly, constructing a robust data platform demands a level of data engineering expertise that the industry currently finds in short supply.

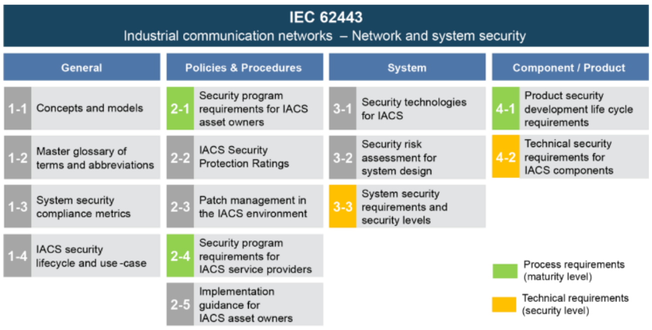
3) Change Management: Ultimately, the true business benefits of IT/OT convergence materialize only when the use cases it enables are effectively implemented. However, the success of these use cases hinges on the way they are introduced and managed within the organization, particularly at the individual practice level. For instance, the widespread adoption of wearable safety device alarms and triggers plays a pivotal role in enhancing site safety. Likewise, the implementation of remote orchestration entails numerous on-site changes, such as reducing human presence and equipping control room engineers with the necessary guidelines to oversee processes effectively. This also necessitates the promotion of cross-functional expertise, as many processes, such as drilling, tracking, and exploration, intersect with multiple disciplinary contexts.

IV. Security Model Construction

The O&G industry depends on technology to oversee an extensive network of global energy assets and operations. This technology streamlines laborious tasks, enhances safety measures, optimizes profits, and ensures the industry remains at the forefront of advancements and efficiency. Nevertheless, this reliance on technology exposes the industry to various cybersecurity risks.

A. IEC 62443 industrial communication networks

The fundamental objective of the IEC 62443 [6] series is to establish a versatile framework that enables the systematic identification and mitigation of existing and future vulnerabilities in Industrial Automation and Control Systems (IACS). This is achieved in a defensible and organized manner. It is crucial to recognize that the intent of the IEC 62443 series is to extend enterprise security principles, adapting them to the specific requirements of Business IT systems, and integrating these with the distinct demands for robust availability essential in IACS, as demonstrated in Fig 3.



IEC 62443
Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	🟩 2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	🟩 4-1 Product security development life cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 IACS Security Protection Ratings	3-2 Security risk assessment for system design	🟨 4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	🟨 3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use -case	🟩 2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

🟩 Process requirements (maturity level)
🟨 Technical requirements (security level)

Fig. 3. IEC 62443 industrial communication networks – network and system security [2].

This section of the IEC 62443 series offers in-depth technical control system requirements (SRs) aligned with the seven foundational requirements (FRs) outlined in IEC 62443-1-1. This includes the specification of requirements for control system capability security levels, denoted as SL-C (control system). These requirements are intended for utilization by diverse stakeholders within the industrial automation and control system (IACS) community, in conjunction with the specified zones and conduits for the system under consideration (SuC). They play a crucial role in formulating the appropriate control system target SL, referred to as SL-T (control system), for a specific asset.

B. SIEM and SOAR

a) Security information and event management (SIEM): The industrial sector is actively seeking methods to optimize incident response procedures, aiming for quicker resolutions to security incidents. These distinctions become particularly evident, especially when examining metrics such as mean time to detection (MTTD) and mean time to respond (MTTR). Security information and event management (SIEM) tools provide a centralized mechanism for gathering crucial log and event data from diverse sources such as security, network, server, application, and database systems. Subsequently, SIEMs identify and issue alerts for security events [7]. The practical application of SIEM occurs when a system recognizes an unusually high number of login attempts on a specific system. Following detection, the SIEM notifies the security operations (SecOps) team about the incident, enabling them to explore the possibility of a compromised system or compromised user credentials. SIEMs gather data from various sources, including firewalls, intrusion prevention systems, antivirus and antimalware software, DNS servers, data loss prevention tools, and secure web gateways [10].

b) Security orchestration, automation, and response (SOAR): SOAR represent a software solution designed to empower security teams by integrating and coordinating disparate tools into efficient threat response workflows. Through the optimization of alert triage and the seamless collaboration of various security tools, SOARs contribute to reducing mean time to detect (MTTD) and mean time to respond (MTTR), thereby enhancing the overall security posture [8]. The ability to detect and respond to security threats more rapidly can mitigate the impact of cyberattacks. As an illustration, notifications originating from the SIEM system and additional security technologies create opportunities for incident analysis and triage, utilizing a blend of human expertise and machine capabilities. This approach aids in establishing, prioritizing, and steering standardized incident response activities. SOAR tools further enable organizations to articulate incident analysis and response procedures through a digital workflow format. Conventional SIEMs solely deliver alerts, leaving the SecOps team responsible for charting the course of an investigation. SOARs, which automate investigation path workflows, can markedly reduce the time needed to address alerts and offer insights into the skill set essential for completing an investigation path. Nevertheless, SIEMs excel in consolidating and analyzing data for threat alerting. Consequently, numerous enterprises opt to implement both SIEM and SOAR. When utilized in tandem, these technologies yield significantly reduced mean time to detect (MTTD) and mean time to respond (MTTR) outcomes.

The integration of SIEM and SOAR leverages the strengths of both systems, offering a comprehensive and proactive cybersecurity approach, as shown in Fig 4. This synergy results in a shortened time frame for detecting and responding to threats. Collaboratively, they improve visibility into the security landscape, streamline security operations, automate repetitive tasks, and implement preventive measures. This integration allows teams to redirect their focus toward more strategic initiatives.

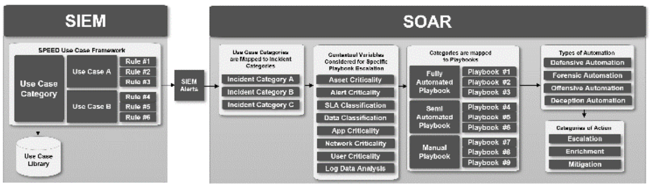


Fig. 4. The integration of SIEM and SOAR.

C. Purdue Model

The Purdue Enterprise Reference Architecture is rooted in a widely utilized architectural reference model established in the 1990s for control systems. This model served as a foundation for segregating industrial control system networks from corporate enterprise networks and the internet. It is a fundamental architecture for various industrial control system frameworks, including API 1164 and NIST 800-82. Originating from the Purdue Laboratory for Applied Industrial Control (PLAIC) at Purdue University, the Purdue Enterprise Reference Architecture (PERA) and its associated methodology were developed in December 1990 and published a year later. PERA is described as an informal means of guiding a user's application group through all phases of an enterprise integration program, from initial concept to final planned obsolescence [3].

A significant contribution of the Purdue Architecture lies in its detailed and practical approach to assimilating and integrating enterprises within standard industrial processes, manufacturing, and services industries. The architecture defines layers that represent connections between electronic or mechanical components facilitating specific functions. Interfaces between these layers serve as shared boundaries between entities, enabling interactions such as engineer or programmer to computer, plant worker or operator to computer, and computer to computer, as illustrated in Fig 5. In the energy sector, interconnected interfaces control information data flow, material and energy flow, and physical systems. Protocols are crucial in providing a common language across these interfaces, encompassing both standard Information Technology protocols and specialized Operations Technology protocols.

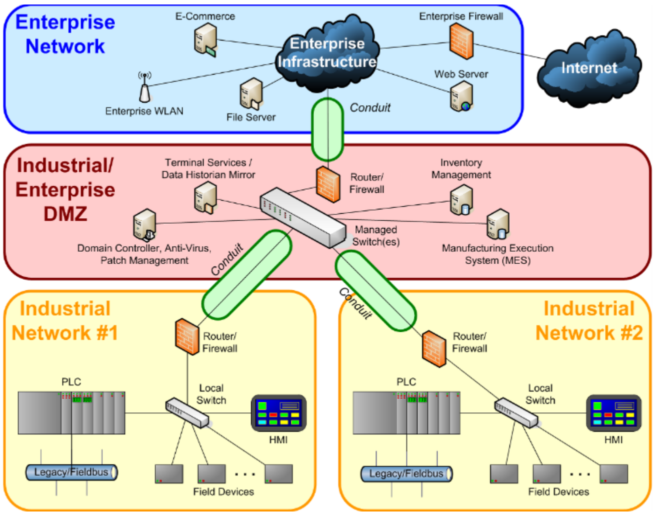


Fig. 5. Purdue Architecture.

While the difference in protocols between IT and Operations Technology (OT) is not substantial, it must be accurately represented when describing, identifying, and securing OT. NIST 800-82 [4] emphasizes the need for a cross-functional team of control engineers, control system operators, and IT security professionals to collaborate closely on understanding the potential implications of security solution installation, operation, and maintenance in conjunction with control system operations. IT professionals engaged with Industrial Control Systems (ICS) must grasp the reliability impacts of information security technologies before deployment, considering that some operating systems and applications within ICS may not align seamlessly with commercial-off-the-shelf (COTS) IT cybersecurity solutions due to specialized ICS environment architectures [9]. To comprehend the complexity of the OT environment, the Extended Purdue model was developed, derived from the generic ICS model and applying specific layers.

D. Cyber Vision Model

Ongoing technological advancements have elevated cyber-attacks to a pervasive threat in the modern world. The reliance on digital systems across various sectors has made them susceptible to cybercriminal activities, including critical infrastructure. Consequently, ensuring cybersecurity in the O&G industry has become imperative. Cisco Cyber Vision integrates a distinctive edge monitoring architecture with seamless compatibility with Cisco's premier security portfolio. Integrated into your Cisco industrial network equipment, it can be effortlessly deployed on a large scale to monitor industrial assets and their real-time application flows. This solution is optimal for providing your IT Security Operations Center (SOC) with OT context, facilitating the establishment of a unified IT/OT cybersecurity architecture. The distinctive edge computing architecture of Cisco Cyber Vision incorporates security monitoring components directly into our industrial network equipment. This eliminates the necessity for dedicated appliances and the complexities of installation. Moreover, there's no requirement to establish an out-of-band network for sending industrial network flows to a central security platform. Cyber Vision empowers industrial networks to gather essential information, facilitating comprehensive visibility, analytics, and threat detection. The simplicity and cost-effectiveness of the Cyber Vision architecture make it particularly advantageous for network managers when deploying OT security at scale. The network sensors of Cyber Vision offer flexibility in achieving scale-appropriate visibility without causing disruptions to network performance.

By leveraging the guidelines established in IEC 62443 and NIST 800-82 standards, Cyber Vision is committed to ensuring the uninterrupted continuity, resilience, and safety of industrial operations. This is achieved through the provision of continuous visibility into Industrial Control Systems (ICS), facilitating a holistic comprehension of the security landscape. The overarching objective is to optimize the efficacy of industrial networks, seamlessly extending robust information technology (IT) and operational technology (OT) security measures to envelop the entirety of industrial operations. IEC 62443 proposes a set of fundamental criteria for undertaking an initial zone and conduit segmentation prior to embarking on a comprehensive cyber risk assessment, commonly referred to as Cyber-PHA (Cyber Process Hazardous Analysis). This segmentation process is accompanied by a set of recommendations to ensure optimal outcomes. Every designated zone—Enterprise IT: Purdue Level 4, Industrial Demilitarized Zone (DMZ): Purdue Level 3.5, and Industrial Operations (Zone-1 and Zone-2): Purdue Level 0 - 3 as well as each conduit (Sensor), is allocated a Security Level Target (SL-T) signifying the necessary security level and a Security Level Achieved (SL-A) indicating the current security level.

It is important to note that these aspects are presented without delving into intricate technical details. Cyber Vision is pre-equipped with leading SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms, ensuring seamless transmission of Operational Technology (OT) events and alerts to any other tool via Syslog integration, as illustrated in Fig 6. The Next-Generation Firewall (NGFW) at Industrial DMZ, powered by AI, can detect malicious files at both the network level and endpoints. Cyber Vision offers advanced malware detection and protection, ensuring comprehensive and holistic defense against all threats with user-friendly operation. It swiftly and effectively mitigates any security threats.

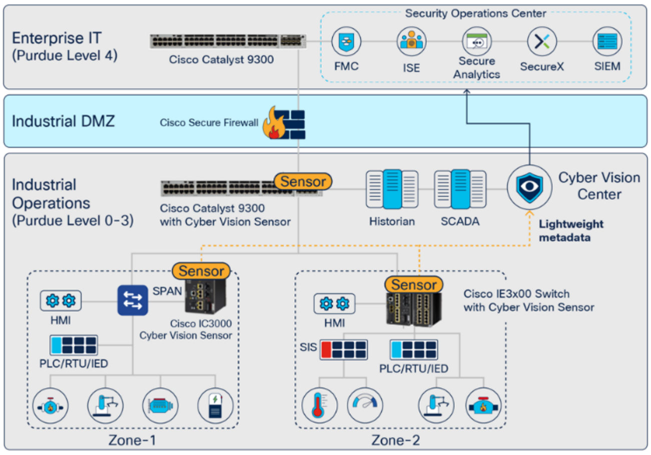


Fig. 6. Cyber Vision's network sensors.

Cyber Vision utilizes both passive and active discovery mechanisms to effectively identify all assets, their characteristics, and their communications. The active discovery queries are highly precise and non-disruptive, employing the semantics of the protocols in use to gather details about all industrial assets, including Windows-based systems. As these queries originate from Cyber Vision sensors embedded in Cisco network equipment within the industrial network, they are not impeded by firewalls or NAT boundaries, ensuring comprehensive visibility. This abundance of information, covering assets, communication maps, and operational and security events, is accessible to local OT and IT team members. Additionally, it can be centralized in a Cyber Vision Global Center, allowing large organizations to achieve global visibility across all sites, facilitating governance and compliance. Cyber Vision's nonintrusive edge architecture is instrumental in providing detailed information to both local and global stakeholders, as presented in Fig 7.

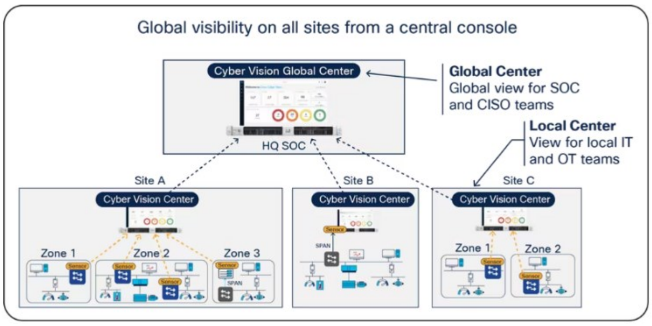


Fig. 7. Cyber Vision leverages a nonintrusive edge architecture.

Cisco Cyber Vision integrates protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to provide insights into your security posture. It automatically assigns risk scores to each component, device, and specific operational elements, highlighting critical issues for prioritized attention. Accompanying each score is guidance on how to mitigate exposure, enabling a proactive approach and the development of an improvement process to address risks.

The detection engine of Cyber Vision utilizes threat intelligence from Cisco Talos, a prominent cybersecurity research team and the official developer of Snort signature files. The Cyber Vision threat knowledge base is updated weekly to incorporate the latest list of asset vulnerabilities and intrusion detection systems (IDS) signatures. Moreover, Cyber Vision seamlessly integrates with prominent SIEM systems like IBM QRadar or SPLUNK, enabling security analysts to track industrial events within their current tools and initiate correlations between OT/IT events. With the robust API of Cyber Vision, IT and OT teams can effortlessly provide comprehensive insights into industrial assets, network traffic, and security posture to any existing tool. Leveraging technology, the O&G sector efficiently oversees a vast network of global energy assets and operations. This streamlines labor-intensive tasks, enhances safety measures, maximizes profits, and maintains the industry's cutting-edge efficiency. Nevertheless, this reliance on technology also exposes the industry to various cybersecurity risks.

V. Conclusion

The critical infrastructure of the oil and gas (O&G) sector heavily depends on technology, rendering it susceptible to cyber-attacks, as outlined in the report. The document also attributes the vulnerability to outdated infrastructure, which may lack robust cybersecurity measures, such as antiquated surveillance systems and more. To enhance system functionalities and productivity, each Industrial Control System (ICS) consistently integrates new technologies and software across both Information Technology (IT) and Operational Technology (OT). The convergence of Information Technology (IT) and Operational Technology (OT) offers enterprises enhanced integration and visibility into the supply chain, encompassing critical assets, logistics, plans, and operational processes. Cyber Vision allows the grouping of assets into zones, such as production cells, buildings, substations, etc., facilitating the sharing of logical network information between operational teams and IT. This enables the construction of security policies aligned with IEC 62443 standards. Cyber Vision comes pre-integrated with prominent SIEM and SOAR platforms and can seamlessly transmit OT events and alerts to any other tool through Syslog. To prevent event fatigue, it provides the flexibility to select which types of events should be shared.

References

[1] S. Bajaj and L. Vaz, “IT-OT Convergence in the Oil and Gas Industry: Top Strategies and Benefits,” birlasolf. CK BIRLA Group. https://www.birlasoft.com/articles/it-ot-convergence-in-oil-and-gas-strategies-benefits, August 2023.

[2] M. Weidele, “IEC 62443 – You should know these basics as the operator of an automation solution,” Sichere Industries. https://www.sichere-industrie.de/iec-62443-grundlagen/, August 2023.

[3] C. Smith, and T. Williams, Mathematical Modelling, Simulation and Control of the Operation of a Kamyr Continuous Digester for the Kraft Process; Purdue Laboratory for Applied Industrial Control, Schools of Engineering, Purdue University: West Lafayette, IN, USA, 1974.

[4] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, Guide to Industrial Control System (ICS) Security, Revision 2 Final Public Draft (NIST SP 800-82), February 2015.

[5] M. Wiboonrat, "Cybersecurity of Industrial Automation and Control System (IACS) Networks in Biomass Power Plants," 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE), Helsinki, Finland, 2023, pp. 1-6, doi: 10.1109/ISIE51358.2023.10228108.

[6] J. -H. Wang, C. -Y. Huang, H. -Y. Chou, C. -Y. Wang, H. -J. Kuo and V. Ting, "Security Service Architecture Design Based on IEC 62443 Standard," 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), Taichung, Taiwan, 2023, pp. 483-486.

[7] M. Cinque, D. Cotroneo and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Memphis, TN, USA, 2018, pp. 95-99.

[8] R. Vast, S. Sawant, A. Thorbole and V. Badgujar, "Artificial Intelligence based Security Orchestration, Automation and Response System," 2021 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2021, pp. 1-5.

[9] C. Zhou, B. Hu, Y. Shi, Y. -C. Tian, X. Li and Y. Zhao, "A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems," in Proceedings of the IEEE, vol. 109, no. 4, pp. 517-541, April 2021, doi: 10.1109/JPROC.2020.3034595.

[10] M. Sun, Y. Lai, Y. Wang, J. Liu, B. Mao and H. Gu, "Intrusion Detection System Based on In-Depth Understandings of Industrial Control Logic," in IEEE Transactions on Industrial Informatics, vol. 19, no. 3, pp. 2295-2306.

[11] Sangfor, Igniting Attacks: Cybersecurity in the Oil and Gas Industry, Sangfor Technologies, 18 October, 2023. https://www.sangfor.com/blog/cybersecurity/cybersecurity-in-the-oil-and-gas-industry/.