TSARKA SCIENCE

Volume 1 (2025)
Issue 1

A PRAGMATIC DECISION-TREE BASED APPROACH FOR OT NETWORK SEGMENTATION FOR SMALL AND MEDIUM BUSINESSES

Z. Supeyev[1]*, Zh. Yeskendir[2]
[1]Aydin Systems R&D , Astana, Kazakhstan
[2]AIMI Automation, Almaty, Kazakhstan
*Corresponding author: zakir@aydin.kz

Abstract

Industrial operators face pressure to connect operational technology (OT) to business systems, partners, and cloud analytics—often without the staff or budget to implement expansive standard frameworks. We present a concise decision framework that maps business dataflow needs to four pragmatic outcomes for network segmentation: air-gapping, next-generation firewalls (NGFW) with deep packet inspection (DPI), constrained serial links, or data diodes. The guiding principle is pragmatic risk reduction: fit controls to real dataflows, operational maturity, and lifecycle cost. Testing the framework on two hypothetical Small and Medium Business (SMB) scenarios demonstrated its effectiveness: 1) For a small manufacturer with low security maturity and no automatic data transfer needs, the framework determined that Air-Gap was the optimal choice, yielding zero CAPEX and maximum risk reduction. 2) For a medium enterprise requiring only one-way cloud analytics export from a low-maturity OT environment, the framework correctly selected a Data Diode, providing physical security guarantees and superior long-term OPEX efficiency compared to implementing an NGFW.

Keywords: *cybersecurity, data diode, decision making network segmentation, operational technology.*

1. Introduction

Operational Technology (OT) is defined as “hardware and software that detects or causes change by directly monitoring and/or controlling industrial equipment, assets, processes, and events” [1]. The main difference between OT and Information

Technology (IT) is that OT deals with physical processes, while IT focuses on the processing, storage, and distribution of data [2].

In the past, OT systems relied on security through obscurity. In most cases, this was sufficient because the level of connectivity was low (i.e., systems were more isolated), and various systems were managed manually or through their own management tools [3].

This situation has changed dramatically with the convergence of OT and IT and the emergence of networked industrial control system (ICS) known as the Industrial Internet of Things (IIoT) [4, 5]. Differences in the characteristics of OT and IT have led to different cybersecurity requirements. Modern ICS, which incorporate both OT and IT, require high availability, as critical infrastructure (e.g., power grids, nuclear power plants, and water/gas systems) and manufacturing require near-zero downtime [5]. Another imperative is prioritizing the safety of employees and the environment due to physical aspects [6].

Awareness of OT cybersecurity has increased dramatically following a series of high-profile incidents demonstrating the potential for physical attack via cyberspace. The Stuxnet attack (2010) targeted Iran's Natanz Nuclear Power Plant and damaged approximately 25% of its uranium enrichment centrifuges, becoming the first publicly known cyberweapon to cause physical destruction [7]. In 2012 the Shamoon malware attacked Saudi Aramco, the state oil company of Saudi Arabia, and RasGas, the natural gas company of Qatar. It destroyed data and made the infected systems unusable [8]. A cyberattack on Ukrainian power distribution companies in 2015 resulted in the loss of power to over a quarter of a million people [8]. In 2021, an attack on water systems in Oldsmar, Florida, occurred when an attacker exploited a vulnerability in an outdated operating system and gained access to the water treatment plant's computer system. The attacker then attempted to alter the amounts of chemicals used to treat the water [7]. Although the hack was detected before it caused significant damage, it exposed vulnerabilities in operational technology (OT) cybersecurity systems [9].

Thus, in many critical sectors, such as manufacturing, power grids, and water treatment, the cybersecurity of OT systems is crucial to managing industrial operations. As OT and IT networks converge, they become increasingly vulnerable to cyber threats and, therefore, require sophisticated security measures.

This convergence of IT and OT environments complicates the task of ensuring and maintaining network security. Vulnerabilities in IT networks can lead to security incidents not only within the IT perimeter; they must also be prevented from spreading throughout the OT network. Therefore, the development and implementation of effective approaches to OT network segmentation adapted to technological convergence and the Industrial Internet of Things is currently a pressing issue.

The relevance of the study is also driven by the need to integrate OT systems into overall business processes in the context of digital transformation, and the simultaneous lack of resources among small and medium-sized businesses (SMBs) to fully implement comprehensive segmentation standards such as IEC 62443 [10].

The goal of this study is to develop a pragmatic, resource-oriented decision-making methodology for selecting optimal OT network segmentation tools for SMBs.

Standards such as IEC 62443 offer valuable direction, yet many sites lack the capacity to execute full zoning programs based on HAZOP/PHA [11]. In practice, well-intentioned efforts can become protracted consulting projects with modest operational outcome. The alternative is a prudent, resource-aware approach: pick controls that measurably reduce risk, are operable by the existing team, and preserve process determinism.

We convert this concept into a decision tree-based framework. Beginning with specific business data flow requirements, the framework directs operators towards one of four justifiable outcomes, accompanied by implementation guidelines that ensure deployments remain efficient and verifiable. The proposed methodology is implemented in the form of a decision tree based on three key criteria: the need for software interaction with OT, the level of security maturity, and the need for bidirectional data exchange.

2. Methods

2.1 A Decision Framework Based on Real-Life Experience

Our framework is a binary tree (see Figure 1), developed based on an expert assessment of the risks and operational feasibility of small companies. The tree includes three sequential decision nodes, each of which clearly determines the transition to the next step or the final technical solution.

Node 1 asks the question, “Is software interaction with the OT system required?” A positive answer (or if the condition is met) indicates the need to use software for data transfer, commands, and remote administration.

Node 2 checks whether the OT environment demonstrates basic security maturity. Basic maturity is defined as (to be defined): the presence of an asset inventory, regular patching, designated firewall rule owners, and functioning basic monitoring (SOC/SIEM) for the segment.

Node 3: Is bidirectional data exchange required? This node is activated only at low maturity (the answer is “No” in Node 2). In this case, a bidirectional flow (commands/acknowledgement) is selected for a critical business process.

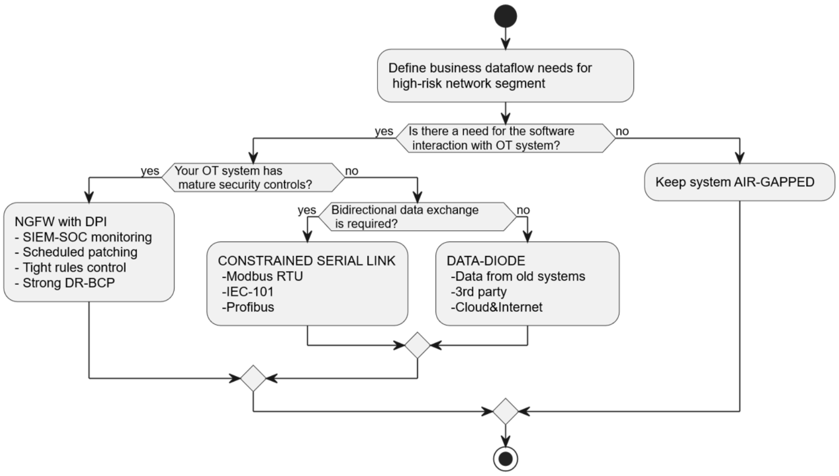

Figure 1. Decision-tree framework for OT networks segmentation

2.2 Decision making workflow

To systematize the process of selecting a technical solution for OT network segmentation, the algorithm presented in Table 1 is proposed. It is based on three key decision nodes that take into account business needs, cybersecurity maturity level, and data exchange requirements.

Air-gapping maximizes isolation [12]. While remains safest option it still demands disciplined operational practices: backups, physical/administrative controls, controlled scheduled maintenance windows, and integrity evidence media handling, (e.g., cryptographic hashes for transferred Monitoring remains essential, but the attack surface is minimized.

Where software interaction with OT interaction is necessary, the site's security maturity determines whether rich, policy-driven IP connectivity is viable or whether narrow, bounded conduits are safer. Maturity is not ultimate, in most cases the indicator of maturity is the presence of patched and inventoried assets, named rule owners, SOC monitoring, backups, and tested recovery.

Table 1. Decision-making algorithm for OT network segmentation

Algorithm step/decision node	Description	Recommendations for implementation
1	2	3

Table 1. Continued

1	2	3	
Scope First	Define Business Dataflows into High-Risk Segments	Before any connectivity, specify who and what communicates, in which direction, over which protocols, how often, and why. Name the assets that constitute "high-risk" (safety systems, Level 2 controls, recipe/Batch management, laboratory systems, time sources etc.).	
Decision Node 1:	Is Software Interaction with OT Required?	If interaction is required, continue to the maturity check; interaction increases the potential for unsafe states and calls for stronger governance.	If software interaction is not required, an air gap is the safest and often cheapest option.
Decision Node 2:	Does the OT System Have Mature Security Controls?	If the answer is yes, NGFW with DPI at natural choke points commonly between Purdue Levels 3 and 3.5 - becomes the primary control.	If the answer is no, the framework defers broad IP bidirectionality and asks whether truly bidirectional exchange is required.
Decision Node 3	Is Bidirectional Data Required?	For minimal two-way needs, bounded serial protocols-Modbus RTU, IEC-101, Profibus-limit scope and exposure by design.	For a unidirectional data gateway, it is recommended to use a data diode.

Next-Generation Firewalls (NGFWs) with industrial DPI enables default-deny approach and explicit documented allow lists. They support granular policies, logging, and change control without breaking process determinism. Operationally, success depends on SIEM/SOC monitoring that is scoped to a small set of high-value alerts, scheduled patching and configuration hygiene, rule ownership and a review cadence, and resilient DR/BCP: tested backups, failover procedures, and versioned configurations.

Policy discipline matters. Avoid “write-up” flows (from lower-trust to higher-trust zones) except for narrowly justified historian use cases with integrity guards. Keep ICMP within the same Purdue level or zone where possible. Group rules by purpose and direction; standardize boilerplate rules and vary only host lists. Every rule must have a named owner, an explicit rationale, and an expiration or review date. Handle exceptions through a brief risk note with an explicit owner, defined scope and a default expiry; otherwise, exceptions proliferate.

Bidirectionality implies commands or acknowledgments crossing the boundary. If required, choose the narrowest possible control that preserves safety. If not required, prefer one-way export.

Data diodes provide one-way export from weak or sensitive segments without inbound exposure [13]. We as a company offering data diodes are particularly interested in correct implementation and considering below as a key diode use cases:

1) pulling data from low-maturity networks;
2) working with untrusted third parties;
3) accessing cloud\Internet for digital transformation & AI.

Example for case (1): early-2000s equipment, minimally maintained, unpatched, but business-valuable. A diode solves two problems: Enables access to data without direct inbound access to the vulnerable network. Prevents intentional (intrusion/attack) and unintentional (active discovery, broadcast storms, high traffic) interactions back into that network. The diode also acts like a protective “dam,” allowing staged modernization and maturity uplift without introducing new risks.

For second case when you must deliver information outward without granting a two-way channel into your network (e.g., utilities data to water/electric providers; sharing with technology partners for equipment monitoring or process integration).

Since big compute and AI/Big-Data tools largely reside with cloud providers, there’s pressure to connect OT directly to the Internet — which raises compromise risk. As in (1), a diode lets you export data without exposing sensitive segments to inbound Internet access.

After notable regional Trysis cyber incidents [14], many chose to separate IT and OT with a diode. However, highly digitalized, tightly integrated “order-to-cash-to-production-to-shipment” plants couldn’t use a hard one-way split between IT and OT. For them, firewalls (with careful policy) are required.

Practical design emphasizes simple mediation (brokered telemetry, file drops with integrity metadata), queueing/buffering sized for outages, and cryptographic integrity/freshness (hashes, MACs, timestamps). Treat diode endpoints as zones with owners, patch plans, and monitoring. Plan for local administration; do not re-introduce two-way paths via side channels (portable media, misconfigured jump hosts).

3. Results: Testing of the proposed approach

To verify and validate the pragmatic decision tree (see Figure 1), two hypothetical small and medium business (SMB) scenarios with different needs, maturity levels, and resources are presented in Table 2. The analysis demonstrates how the proposed algorithm leads to an objective selection of the optimal technical solution.

The rationale for Case 1 is based on risk, operational feasibility, and cost. This solution provides maximum risk mitigation by eliminating remote attack vectors and IT perimeter compromise (no network connectivity). The operational model (manual migration) is already in place and requires no additional staff training or network security specialists. There are zero capital expenditures (CAPEX) on network equipment and minimal operating expenses (OPEX). Compared to implementing and maintaining an NGFW (which would not be required but would cost between $5,000 and $15,000 initially), Air-Gap is the most cost-effective choice for this SMB.

Choice Rationale for Case 1 (Qualitative and Quantitative):

- a data diode provides a physical guarantee of unidirectional data flow; this minimizes the risk of compromise through the IT network for a weakly protected OT environment (low maturity);
- the solution fully meets a critical business need (cloud analytics);
- although a data diode is more expensive than a simple firewall, it optimizes OPEX in the long term because it does not require constant configuration, updates, or monitoring as intensively as an NGFW, making it suitable for SMBs with limited IT staff;
- the risk of compromise through the IT network is reduced to virtually zero, making this solution the most effective in this situation in terms of residual risk.

Table 2. Decision-making algorithm for two SMB scenarios

Case	SMB Characteristics	Decision Tree Walk-through	Result:
1	2	3	4
1	*Business Type:* Small, local concrete production facility.	*Node 1:* Is software interaction with the OT system required?	No need to move to Nodes B and C.

Table 2. Continued

1	2	3	4
1	*OT Environment:* Legacy, 15-year-old programmable logic controllers (PLCs) with no internet connection. *Need:* The accounting department must manually import batch quantity data once a week. *Security Maturity Level:* Low. There is no asset inventory, patches are not applied (due to the risk of failure of the legacy equipment), and there is no centralized monitoring. *Budget:* Extremely limited; allocating funds for IT staff is not possible.	*Node 1:* Is software interaction with the OT system required? *Answer:* NO. Interaction is accomplished solely by manually transferring data on a USB drive.	*Optimal Solution:* Air-Gap (Physical isolation).
2	*Business Type:* Medium-sized packaging manufacturing company. *OT Environment:* Modern PLCs and sensors connected to a local SCADA system. *Need:* It is necessary to upload (export) telemetry in real time (or near real time) to a cloud platform for predictive analytics and production optimization. Feedback from the cloud is not required and is prohibited. *Security Maturity Level:* Low. Management has only just begun the process of inventorying and implementing basic procedures (no regular patching, no functioning SOC/SIEM). *Budget:* Sufficient to purchase and install specialized, but not overly complex, equipment	*Node 1:* Is software interaction with the OT system required? *Answer:* YES. *Node 2:* Does the OT environment demonstrate basic security maturity? *Answer:* NO (low maturity). *Node 3:* Is bidirectional data exchange required? *Answer:* NO (only unidirectional export is required).	*Optimal Solution:* Data Diode.

4. Conclusion

There is no segmentation pattern that is simultaneously the most cost-effective and the universally correct choice. For most small and medium OT asset owners, sustained progress comes from pragmatic judgment: define real dataflows, select the smallest control that safely enables them, and operate that control with discipline. Data diodes safely publish value from weak zones; NGFWs with DPI govern necessary two-way flows; constrained serial links bound minimal command/ack needs; and airgaps remain valid when interaction is unnecessary. The practical efficacy of the methodology was proven through two hypothetical SME case studies, illustrating its capacity to identify the most economical and secure solution.

The created method functions as a practical reference for operators, security engineers, and OT system architects, facilitating informed decision-making about the implementation of network segmentation mechanisms. Further study may concentrate on amalgamating this methodology with lifecycle costing (LCC) models to enhance its financial precision.

Thanks. The authors thank the reviewers for their constructive feedback and helpful suggestions, which have enhanced the quality of this paper.

Financing. This work was conducted without external funding.

Conflict of interest. The authors declare that there is no conflict of interest.

References

1. Gartner. "Definition of operational technology (OT)." Accessed: August 22, 2025. URL: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.
2. Sonkor, M.S., García de Soto, B. (2021). Operational technology on construction sites: A review from the cybersecurity perspective. Journal of Construction Engineering and Management, 147(12), 04021172.
3. Kampa, T., Müller, C.K. and Großmann, D. (2024). Interlocking IT/OT security for edge cloud-enabled manufacturing. Ad Hoc Networks,154, 103384.
4. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. Journal of Manufacturing Systems, 57, 367-378.
5. Tange, K., De Donno, M., Fafoutis, X., & Dragoni, N. (2020). A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, 22(4), 2489-2520.
6. Hahn, A. (2016). Operational technology and information technology in industrial control systems. In Cyber-security of SCADA and other industrial control systems, 51-68. Cham: Springer International Publishing.

7. Piggin, R. (2014). Industrial systems: cyber-security's new battlefront [Information Technology Operational Technology]. Engineering & Technology, 9(8), 70-74.
8. Hemsley, K. E., Fisher R. E. (2018). History of industrial control system cyber incidents. Accessed: August 22, 2025. URL: https://www.osti.gov/servlets/purl/1505628.
9. Margolin, J., and I. Pereira. 2021. "Outdated computer system exploited in Florida water treatment plant hack." Accessed: August 22, 2025. URL: https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550.
10. Shaaban, A. M., Kristen, E., & Schmittner, C. (2018). Application of IEC 62443 for IoT components. In International Conference on Computer Safety, Reliability, and Security (pp. 214-223). Cham: Springer International Publishing.
11. Koelemij, S. (2020). ISA 62443-3-2 an unfettered opinion. URL: https://otcybersecurity.blog/2020/08/07/isa-62443-3-2-an-unfettered-opinion/
12. Hamada, R., & Kuzminykh, I. (2023). Exploitation Techniques of IoST Vulnerabilities in Air-Gapped Networks and Security Measures—A Systematic Review. Signals, 4(4), 687-707.
13. Ginter, A. (2019). Secure Operations Technology (SEC-OT). Abterra Technologies Inc. 6, 51-66.
14. The National Cyber Security Centre UK (2017). TRITON Malware Targeting Safety Controllers. Accessed: August 22, 2025. URL: https://www.ncsc.gov.uk/information/triton-malware-targeting-safety-controllers

Information about authors

Supeyev Zakir Sagitovich - Master of Science in Cybersecurity Management, Aydin Systems R&D, Astana, Kazakhstan.

e-mail: zakir@aydin.kz

ORCID: https://orcid.org/0009-0007-6913-3214

Zhanibek Yeskendir – Master of Science Appliance building (electronics), Satbayev University, Almaty. Founder AIMI Automation.

e-mail: sales@aimi-automation.com

ORCID: https://orcid.org/0009-0002-3005-7705