IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

The Operational Technology Exposure Budget: A Business Value Model for Industrial Connectivity Decisions

Daniel Ward

Department of Computer Science, Southern New Hampshire University, United States

ORCID: 0009-0002-4466-6739

Abstract: Industrial organizations increasingly connect operational technology (OT) to enterprise analytics, remote access platforms, maintenance systems, cloud services, and artificial intelligence pipelines. These connections may provide operational visibility, but they can also create control-path exposure in systems that monitor or control physical processes. This paper proposes the Operational Technology Exposure Budget, a design-science decision model for evaluating whether OT connectivity and industrial data flows are justified by measurable business value. The model separates business-value scoring from exposure-burden scoring and classifies connectivity decisions into four outcomes: approve, re-architect, reduce, or remove. Using public OT security guidance, secure-connectivity principles, data governance literature, AI-in-OT guidance, and synthetic industrial connectivity scenarios, the paper demonstrates how organizations can preserve useful telemetry while minimizing unnecessary exposure. The contribution is a practical engineering-management artifact that challenges unjustified OT connectivity before organizations attempt to secure it after the fact.

Keywords: business value, industrial connectivity, industrial control systems, operational technology, OT exposure budget, telemetry governance

I. INTRODUCTION

Operational technology (OT) environments support physical processes in manufacturing, energy, water, transportation, building automation, and other industrial sectors. These systems differ from ordinary enterprise information technology because they monitor or control equipment, processes, and events that may affect safety, reliability, quality, production, and environmental outcomes. NIST SP 800-82 Revision 3 defines OT broadly as programmable systems and devices that interact with the physical environment or manage devices that do so, while emphasizing the unique performance, reliability, and safety requirements of OT security [2].

The growth of industrial data platforms, cloud dashboards, remote access, enterprise reporting, and artificial intelligence creates a recurring architectural tension. Organizations want more operational visibility, but each new connection can create additional exposure. This paper argues that OT cyber risk is often created before a security tool is ever selected: it is created when industrial data flows and connectivity paths are approved without a clear business-value test.

The central research problem is therefore not only how to secure connected OT, but also how to secure it. A prior question must be asked: Should this OT connection exist in the first place? Connectivity that supports a defined maintenance decision, compliance requirement, production-quality outcome, safety review, or measurable business process may be justified. Connectivity that exists only because data are available, dashboards are desirable, or analytics teams want unrestricted access to live tags may create more exposure than value.

This paper proposes the Operational Technology Exposure Budget (OT Exposure Budget) as a structured decision model for evaluating industrial connectivity. The model treats exposure as a finite organizational burden that must be justified by business value. It does not categorically reject industrial analytics, artificial intelligence, remote monitoring, or IT/OT integration. Instead, it provides a scoring method for deciding whether a connection should be approved, re-architected, reduced, or removed.

A. Purpose and Contribution

The purpose of this paper is to develop a practical model for value-based OT connectivity decisions. The contribution is a non-human-subjects design artifact that links business value, exposure burden, safer data-plane patterns, and synthetic scenario scoring. The model is intended for plant managers, OT engineers, cybersecurity leaders, reliability engineers, data engineers, and executives who must decide which OT data flows are worth maintaining.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026
DOI: 10.17148/IJIREEICE.2026.14703

This work extends the author's prior research stream in ICS/OT cybersecurity by shifting attention from security-control deployment to connectivity justification. Prior dissertation research identified compatibility issues, limited resources, inadequate professional knowledge, infrastructure constraints, and performance concerns as barriers to the adoption of new OT cybersecurity capabilities [1]. This paper moves one layer earlier and asks whether some of the connections that create later cybersecurity burdens should be subjected to a business-value and exposure-burden test before they are built.

B. Research Questions

Four research questions guide the paper:

RQ1. What criteria should determine whether an OT data flow or industrial connectivity path is business-justified?
RQ2. How can organizations score the business value and exposure burden of OT connectivity decisions?
RQ3. Which connectivity patterns preserve the value of industrial data while reducing control-path exposure?
RQ4. How does the OT Exposure Budget classify common industrial connectivity scenarios?

II. BACKGROUND AND RELATED WORK

A. OT Connectivity as a Risk and Value Problem

OT connectivity is usually justified through promises of efficiency, remote monitoring, production visibility, predictive maintenance, energy optimization, and business intelligence. Those goals can be legitimate. However, industrial data are not automatically valuable simply because they exist. Data become valuable only when they support a defined decision, action, compliance obligation, safety review, maintenance outcome, production improvement, or financial result.

Recent guidance on secure connectivity from CISA, the FBI, NCSC-UK, and international partners frames OT connectivity as a design, security, and management problem. The guidance lists principles such as balancing risks and opportunities, limiting exposure to connectivity, centralizing and standardizing network connections, using standardized and secure protocols, hardening the OT boundary, limiting the impact of compromise, logging and monitoring connectivity, and establishing an isolation plan [4]. This aligns directly with the premise of an exposure budget: connectivity should not be assumed; it should be justified and governed.

NIST CSF 2.0 is also relevant because it frames cybersecurity as an organizational risk-management practice that supports governance, identification, protection, detection, response, and recovery [3]. For OT connectivity, that means the decision to connect should be treated as a risk-governance activity, not merely a network-engineering task. IEC 62443-2-1:2024 similarly emphasizes asset-owner security program policy and procedure requirements for industrial automation and control systems in operation [5].

B. Industrial Data Governance and Business Value

A value-based connectivity model also depends on data governance. Recent data-governance research emphasizes that organizations need methods for aligning data quality, assurance, governance frameworks, and maturity with enterprise value creation [9]. For OT, this point is especially important because industrial data can have very different value profiles. Some telemetry is necessary for operations. Some supports maintenance or compliance. Some feeds are dashboards that are rarely used. Some is collected speculatively for future analytics without a defined consumer or decision process.

The OT Exposure Budget, therefore, treats industrial data as a governed asset. A data flow should have a named owner, business consumer, decision use, latency requirement, retention requirement, and measurable outcome. Without those attributes, the organization may be accepting exposure without knowing what value it is receiving in return.

C. Read-Only Telemetry and Parallel Data Planes

A major design implication is that enterprise systems rarely need direct access to live controllers. When sharing useful industrial data is necessary, safer patterns include historian replicas, edge collectors, schema-limited brokers, one-way transfer paths, delayed aggregation, and publish-subscribe telemetry. The OPC Foundation describes OPC UA PubSub as an alternative to direct client-server exchange in which publishers send messages to message-oriented middleware, and subscribers process messages of interest without knowing where the data originated [8]. Eclipse Sparkplug provides a specification for MQTT clients to integrate data from applications, sensors, devices, and gateways into the MQTT infrastructure. It defines topic namespaces, payload formats, and session-state management for IIoT and SCADA/HMI contexts [7].

These technologies do not eliminate cybersecurity risk. They do, however, support an architectural principle that is central to this paper: useful industrial data should move outward through governed, read-oriented patterns whenever possible, while the control function remains local, segmented, and protected from arbitrary enterprise queries or write-back paths.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

D. Artificial Intelligence and OT Data Access

Artificial intelligence increases the importance of connectivity discipline. AI may provide useful recommendations for maintenance, alarm review, energy analysis, anomaly detection, and root-cause exploration. Yet AI does not automatically require live control-network access. Joint guidance on secure AI integration in OT emphasizes understanding AI risks, considering the business case for AI use in OT, establishing governance and assurance mechanisms, and embedding safety and security practices into AI-enabled OT systems [10]. The same guidance cautions that active AI influence over critical OT functions should account for safety concerns, latency limitations, oversight, and failsafe practices [10].

The OT Exposure Budget uses this principle to distinguish analytical access from control access. AI systems should consume replicated, approved, delayed, or read-only data unless an organization can demonstrate that live access is required and that operational safety, human oversight, rollback, and governance requirements have been satisfied.

III. MATERIALS AND METHODS

A. Research Design

This study uses design science supported by qualitative document analysis and synthetic scenario evaluation. Design science is appropriate because the output is an artifact intended to solve a practical engineering-management problem: how to decide whether OT connectivity is justified. Qualitative document analysis is appropriate because the model is derived from public standards, guidance, and prior research rather than human subjects, private operational data, or live industrial systems.

The paper does not involve human participants, interviews, surveys, focus groups, proprietary telemetry, or live critical infrastructure. It should therefore be treated as a non-human-subjects design and document analysis paper. Later studies could validate the model through expert review, field application, cyber ranges, or retrospective assessment of actual industrial data flows.

B. Source Corpus

The source corpus was selected to represent OT security constraints, cybersecurity risk governance, industrial control system security program requirements, publish-subscribe telemetry patterns, data governance concepts, and AI-in-OT risk considerations. Table I summarizes the analytic role of each source category.

TABLE I SOURCE CORPUS AND ANALYTIC ROLE

Source category	Analytic role	Reason for inclusion
Prior OT adoption research	Problem context	Identifies compatibility, resource, knowledge, infrastructure, and performance barriers that shape OT cybersecurity decisions [1].
NIST OT guidance	Operational constraint baseline	Defines OT security around physical-process monitoring and control, reliability, performance, and safety requirements [2].
Cybersecurity risk frameworks	Governance baseline	Frames cybersecurity as risk governance, communication, and prioritization across organizational functions [3].
Secure connectivity guidance	Connectivity principles	Provides principles for balancing connectivity benefits against OT exposure and resilience requirements [4].
IEC 62443 security program requirements	Asset-owner program context	Supports policy, procedure, legacy-system, and compensating-control considerations for IACS operators [5], [6].
Data governance literature	Value justification context	Links data governance and data quality to enterprise value creation and maturity assessment [9].
Industrial telemetry specifications	Alternative architecture patterns	Supports publish-subscribe and schema-limited data exchange concepts for industrial environments [7], [8].
AI-in-OT guidance	AI connectivity constraint	Supports business-case, governance, oversight, safety, and human-in-the-loop considerations for AI-enabled OT [10].

C. Model Development Procedure

The model was developed in four steps. First, common OT connectivity patterns were identified, including remote access, live tag access, historian connections, cloud analytics, maintenance reporting, MES integration, vendor access, and AI pipelines. Second, each pattern was decomposed into business-value and exposure-burden factors. Third, the factors were converted into scoring categories that can be applied consistently across scenarios. Fourth, synthetic scenarios were scored to demonstrate how the model produces practical decisions.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

The model is intentionally simple. It does not attempt to replace formal risk assessment, safety analysis, threat modeling, or compliance review. Its purpose is to provide a first-pass decision artifact that forces organizations to connect industrial data flows to business purpose before accepting added exposure.

IV. OPERATIONAL TECHNOLOGY EXPOSURE BUDGET MODEL

The OT Exposure Budget evaluates each proposed or existing connectivity path using two scores: Business Value Score and Exposure Burden Score. Business Value Score estimates whether the connection deserves to exist. The Exposure Burden Score estimates the risk and operational costs created by the connection. Each factor is scored from 0 to 3. Higher business value supports approval; higher exposure burden supports redesign, reduction, or removal.

A. Business Value Score

Business Value Score is based on five factors: decision linkage, actionability, latency justification, outcome measurability, and owner accountability. The score ranges from 0 to 15. A high score means the connection supports a defined operational or business outcome. A low score means the data flow is speculative, unused, weakly owned, or disconnected from measurable value.

TABLE II BUSINESS VALUE SCORING CRITERIA

Factor	Score 0	Score 1	Score 2	Score 3
Decision linkage	No defined decision	General visibility only	Supports a recurring decision	Supports a critical business or operational decision
Actionability	No named action	Occasional informal action	Named action by defined role	Action is routine, documented, and measured
Latency justification	Real-time requested without reason	Convenience latency only	Near-real-time supports operations	Latency requirement is operationally or financially justified
Outcome measurability	No metric	Qualitative benefit only	Metric exists but weakly tracked	Benefit is tied to cost, downtime, safety, quality, compliance, or risk
Owner accountability	No owner	Technical owner only	Business or process owner identified	Owner funds, reviews, and accepts risk for the data flow

B. Exposure Burden Score

Exposure Burden Score is based on five factors: control-path potential, directionality, privilege burden, external dependency, and monitoring/lifecycle burden. The score also ranges from 0 to 15. A high score indicates that the connectivity path creates strong exposure, especially where it allows inbound access, privileged credentials, remote access, cloud dependency, or unclear operational ownership.

TABLE III EXPOSURE BURDEN SCORING CRITERIA

Factor	Score 0	Score 1	Score 2	Score 3
Control-path potential	No possible write or command path	Indirect influence only	Potential command path with controls	Direct or unclear command path to OT assets
Directionality	Offline or manual export	One-way outbound	Bidirectional through broker or API	Inbound or interactive access to OT
Privilege burden	No credential exposure	Low-privilege service identity	Shared or elevated service identity	Privileged, persistent, or vendor-controlled access
External dependency	Local and isolated	Internal enterprise dependency	Cloud or third-party dependency	Multiple external or unmanaged dependencies

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

Monitoring and lifecycle burden	Fully logged and owned	Logged but review is manual	Partial visibility or unclear review	Poor logging, weak ownership, or no retirement process

C. Connectivity Decision Matrix

The two scores are interpreted through a four-outcome decision matrix. High value and low exposure supports approval. High value and high exposure support re-architecture because the data are useful, but the current path is too risky. Low value and low exposure supports reduction, aggregation, or scheduled export. Low value and high exposure supports removal.

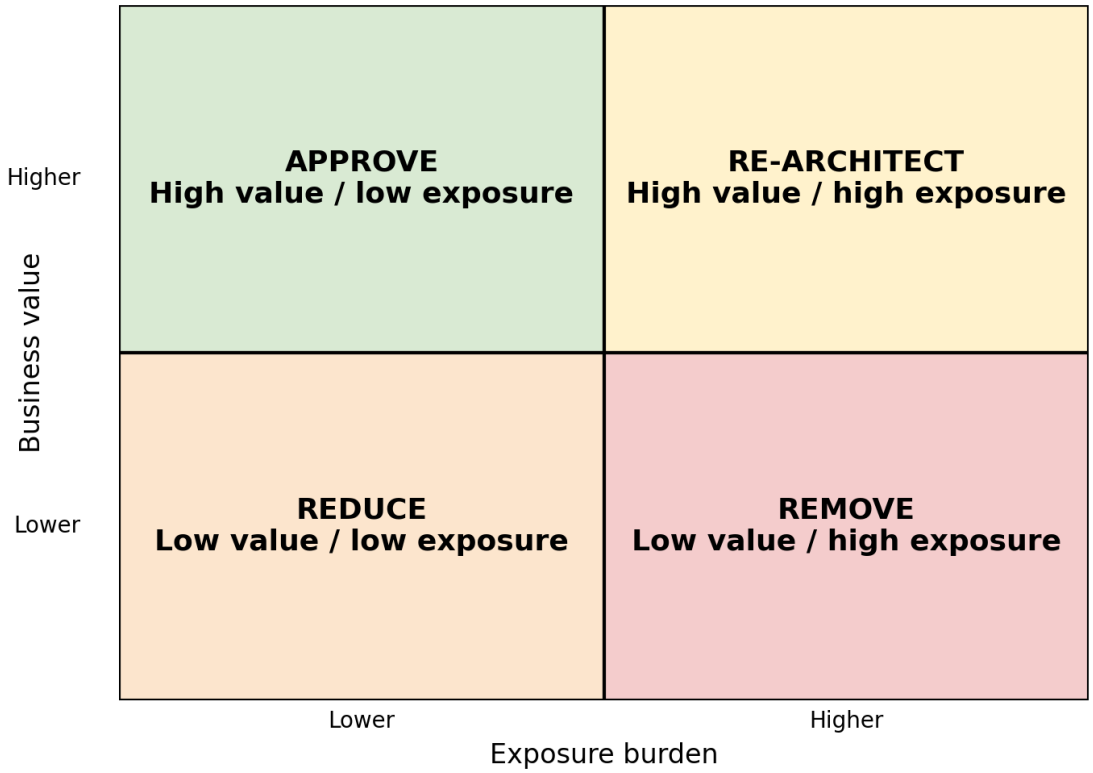

Fig. 1 OT exposure budget decision matrix.

The matrix is intentionally conservative. In OT environments, a high-value use case does not automatically justify a high-exposure connection. It may justify a safer pattern. The most important output of the model is therefore not the score itself, but the decision conversation it forces: what value is created, what exposure is introduced, and what architecture can preserve value while reducing risk?

D. Preferred Connectivity Patterns

When a data flow has value, but the existing path creates unnecessary exposure, the model points toward re-architecture. Preferred patterns include historian replicas, OT outbox mechanisms, push-only telemetry, one-way transfer, delayed aggregation, schema-limited brokers, and human-approved writeback. These patterns separate data consumption from control authority.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

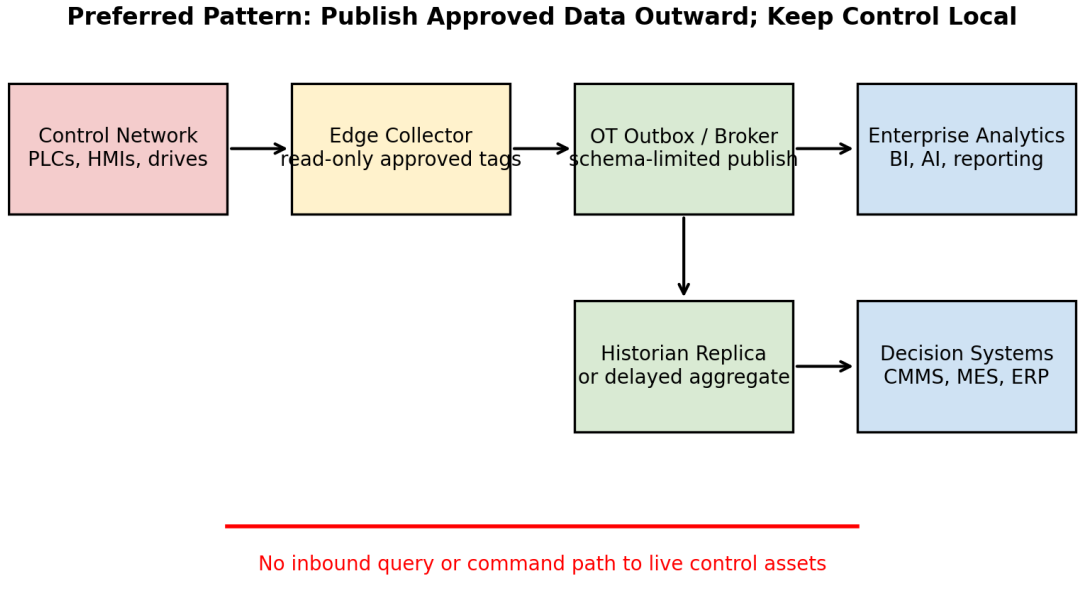

Fig. 2 Preferred read-only data plane for industrial telemetry.

TABLE IV PREFERRED PATTERNS FOR RE-ARCHITECTING OT DATA FLOWS

Pattern	Purpose	Exposure reduction principle
Historian replica	Allows enterprise reporting and analytics to consume copied data	Avoids routine enterprise queries against production historians or controllers
OT outbox	Publishes approved events or values outward	Prevents external systems from browsing or querying live assets
Push-only telemetry	Moves data outward from approved collectors	Reduces inbound sessions to control networks
One-way transfer	Enforces directional separation where justified	Blocks command, query, or malware paths back into OT
Delayed aggregation	Provides summaries when real-time access is unnecessary	Reduces data volume, latency pressure, and attack surface
Schema-limited broker	Publishes only approved tags and metadata	Prevents arbitrary namespace browsing
Human-approved writeback	Allows recommendations but requires OT change control	Separates analytics from direct process control

V. SYNTHETIC SCENARIO EVALUATION

To demonstrate the model, eight synthetic but realistic connectivity scenarios were scored. The scores are illustrative rather than universal; organizations should tailor the model to their risk appetite, process criticality, industry, safety requirements, and regulatory context. The purpose of the evaluation is to show how the model distinguishes valuable telemetry from unjustified exposure.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026

DOI: 10.17148/IJIREEICE.2026.14703

TABLE V SYNTHETIC OT CONNECTIVITY SCENARIO SCORING

Scenario	BVS	EBS	Decision	Rationale
Executive dashboard polling PLC tags directly	4	14	Remove	Low decision value and high control-path exposure; use aggregate reporting instead.
Maintenance system receiving daily pump runtime summaries	11	4	Approve	Clear maintenance action, delayed latency, and low exposure through aggregation.
Cloud analytics reading from a historian replica	12	7	Re-architect	Value is strong, but exposure depends on identity, logging, replica design, and cloud controls.
AI model using weekly exported historian data	9	2	Reduce/approve	Offline data supports analytics without live OT access; value should be tied to a measurable decision.
Enterprise BI tool browsing live tag namespace	6	13	Remove	Broad namespace browsing creates high exposure without proportional value.
Persistent vendor VPN to engineering workstation	8	12	Re-architect	Support value may exist, but persistent access and privileged exposure require redesign.
MES receives production counts every 15 minutes via broker	12	5	Approve	Clear process integration value with limited telemetry and controlled broker pattern.
AI optimization engine with direct writeback to process setpoints	12	15	Re-architect/deny	Potential value is high, but direct control influence requires safety case, oversight, and change control.

The scenario scoring illustrates three patterns. First, direct access to live controllers or tag namespaces is difficult to justify unless the connection is operationally necessary and tightly controlled. Second, useful data can often be preserved through historian replicas, delayed summaries, brokers, or outbox mechanisms. Third, AI and analytics should be treated as data consumers unless a formal safety and governance case supports active control influence.

VI. DISCUSSION

A. Connectivity Should Be a Budgeted Decision

The OT Exposure Budget changes the starting point for OT cybersecurity. Rather than asking how to secure every new connection after it is created, the model asks which connections deserve to exist. This is a more rigorous position because it recognizes that every connection consumes some combination of engineering time, identity-management effort, monitoring capacity, risk acceptance, incident response planning, and lifecycle maintenance.

A budget metaphor is useful because exposure is not unlimited. Many organizations have limited OT engineering staff, limited maintenance windows, legacy equipment, unclear ownership boundaries, and incomplete monitoring. In that context, each connection should be required to justify itself. The budget should favor connections that support measurable outcomes and penalize connections that create control-path risk, privileged access, unmanaged dependencies, or unclear ownership.

B. Implications for AI and Industrial Analytics

The model is especially relevant to AI adoption. Many AI use cases can operate on replicated, delayed, or exported data. Maintenance recommendations, root-cause exploration, energy analysis, alarm rationalization, asset documentation, and configuration review generally do not require live command access to controllers. The OT Exposure Budget, therefore, provides organizations with a way to separate AI decision support from AI control authority.

When AI is proposed for closed-loop optimization, setpoint adjustment, or direct control, the exposure burden should be scored high by default. Such use cases require safety validation, human oversight, fallback states, change control, explainability, logging, and incident-response integration. The issue is not whether AI is useful. The issue is whether the same value can be obtained without creating a new control path.

C. Implications for Governance

The model also creates practical governance artifacts. A connectivity request can include a business-value score, exposure-burden score, data owner, approved architecture pattern, latency requirement, control-path assessment, monitoring plan, and sunset date. These artifacts can support review by OT engineering, cybersecurity, enterprise architecture, safety, compliance, and executive leadership.

This makes the model useful beyond cybersecurity teams. A plant manager can use it to challenge unnecessary dashboards. A data team can use it to request only the data needed for a defined analytic purpose. An OT engineer can use it to reject unnecessary inbound access. A CISO can use it to translate technical exposure into business-risk language. An auditor can use it to determine whether connectivity has ownership and evidence.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2026
DOI: 10.17148/IJIREEICE.2026.14703

D. Relationship to Existing Standards

The OT Exposure Budget does not replace NIST SP 800-82, NIST CSF 2.0, IEC 62443, or secure-connectivity guidance. It operationalizes a decision that those sources imply: connectivity must be justified, risk-informed, monitored, and governed. Its contribution is to convert that principle into a usable scoring artifact that can be applied before architecture hardening begins.

VII. LIMITATIONS AND FUTURE WORK

This paper develops and demonstrates a decision model; it does not validate the model in a live industrial environment. The synthetic scenario scores are illustrative and should not be interpreted as universal scoring values. Different sectors may assign higher exposure to certain connections based on safety criticality, regulatory requirements, process hazards, or adversary threat models. The model also assumes that organizations can identify data consumers and data owners, which may be difficult in environments where connectivity was added incrementally over time.

Future research should validate the OT Exposure Budget through expert review, industrial case studies, cyber range exercises, and retrospective review of existing plant data flows. Additional work should also refine the weighting of business value and exposure factors, especially for safety instrumented systems, remote operations, vendor-managed assets, and AI-enabled OT systems. A later empirical study could compare the model against actual connectivity inventories to determine how many existing OT data flows are approved, reduced, re-architected, or removed under a formal exposure-budget process.

VIII. CONCLUSION

OT cybersecurity should not begin with the assumption that every connection must be defended. It should begin with the question of whether the connection should exist. The OT Exposure Budget provides a practical model for answering that question by separating business value from exposure burden. The model classifies connectivity decisions into approve, re-architect, reduce, or remove, and encourages organizations to preserve useful industrial data through read-only, push-oriented, schema-limited, and governed data-plane patterns.

The paper's central conclusion is that industrial data has value only when it supports a defined decision, action, compliance need, safety function, maintenance result, or business outcome. Connectivity that does not meet that standard should not automatically become another security burden. By budgeting exposure before connectivity is implemented, organizations can reduce unnecessary attack surface, preserve useful telemetry, and support industrial analytics and AI without granting needless access to live control environments.

ACKNOWLEDGMENT

No external funding was received for this paper.

REFERENCES

[1] D. Ward, "Enhancing Security: A Comprehensive Study on Deception Technology Integration in Manufacturing and Critical Infrastructure," Ph.D. dissertation, University of the Cumberlands, 2025. ProQuest Dissertations & Theses.
[2] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev. 3, Sep. 2023. doi: 10.6028/NIST.SP.800-82r3.
[3] C. Pascoe, D. R. Dempsey, N. B. Lefkovitz, J. M. Marron, V. Y. Pillitteri, R. T. Shapiro, and K. A. Stouffer, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
[4] CISA, FBI, NCSC-UK, ASD ACSC, Canadian Centre for Cyber Security, BSI, NCSC-NL, and NCSC-NZ, "Secure Connectivity Principles for Operational Technology (OT)," Jan. 2026. Available: https://www.cisa.gov/resources-tools/resources/secure-connectivity-principles-operational-technology-ot.
[5] International Electrotechnical Commission, "IEC 62443-2-1:2024, Security for Industrial Automation and Control Systems - Part 2-1: Security Program Requirements for IACS Asset Owners," Aug. 2024. Available: https://webstore.iec.ch/en/publication/62883.
[6] International Society of Automation, "ISA/IEC 62443 Series of Standards." Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
[7] Eclipse Foundation, "The Sparkplug Specification." Available: https://sparkplug.eclipse.org/specification/.
[8] OPC Foundation, "OPC Unified Architecture - Part 14: PubSub," OPC 10000-14, Release 1.05.06, Oct. 2025. Available: https://reference.opcfoundation.org/specs/OPC-10000-14.

DOI: 10.17148/IJIREEICE.2026.14703

[9] B. Bernardo, H. São Mamede, J. M. P. Barroso, and V. Santos, "Data Governance & Quality Management: Innovation and Breakthroughs Across Different Fields," Journal of Innovation and Knowledge, vol. 9, no. 4, Article 100598, 2024. doi: 10.1016/j.jik.2024.100598.

[10] CISA, ASD ACSC, NSA AISC, FBI, Canadian Centre for Cyber Security, BSI, NCSC-NL, NCSC-NZ, and NCSC-UK, "Principles for the Secure Integration of Artificial Intelligence in Operational Technology," Dec. 2025. Available: https://www.ic3.gov/CSA/2025/251215.pdf.

[11] NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, Jan. 2023. doi: 10.6028/NIST.AI.100-1.