Computer Fraud and Security
ISSN (online): 1873-7056

A Security-Integrated Agile Governance Model for IT and Operational Technology Modernisation in the Oil and Gas Sector

Jagadeesh Vedula
IT Project Manager (Digital Transformation)
Meghaz Inc.
jagadeeshvedula79@gmail.com

Abstract—Information technology (IT) and operational technology (OT) are converging across the oil and gas value chain, expanding the monitoring, analytics, automation, and enterprise decision-making capabilities available to upstream, midstream, and downstream operators. Yet IT and OT environments continue to carry distinct operational and risk expectations. Enterprise IT delivery is usually judged on speed of release, frequent iteration, and architectural flexibility, whereas operational technology on a drilling pad, gathering system, pipeline, or refinery is judged on continuous availability, process safety, predictable behaviour, tightly controlled access, and disciplined change management. This paper proposes a delivery model, termed the Security-Integrated Agile IT/OT Governance Model, that embeds cybersecurity review, operational-safety assessment, and asset-owner accountability directly into the Agile modernisation workflow used for oil and gas infrastructure. Each proposed system change is classified across seven dimensions — operational criticality, connectivity exposure, privilege requirements, data sensitivity, reversibility, safety implications, and potential service interruption — and the resulting risk tier determines the controls that must be satisfied at backlog creation, design, development, testing, release approval, deployment, and post-change monitoring. The model also introduces an IT/OT Control Traceability Matrix linking every change request or user story to the affected applications and field assets, the applicable cybersecurity controls, testing evidence, access-control requirements, the accountable operational owner, the permitted maintenance window, the rollback procedure, and the final release decision. Consistent with published guidance on pipeline and process-control SCADA exposure, high-risk changes are shown to require a coordinated sequence of validation, review, assessment, approval, rollback, and monitoring activity across the full network path. Seven indicators are used to evaluate the framework: vulnerability escape rate, unauthorised-access incidents, security-review lead time, emergency-rollback frequency, unresolved control exceptions, change-failure rate, and operational downtime. Structured, risk-tiered gating, consistent with trends reported in the literature, is associated with a reduction in change-failure rate from roughly 28% to 11% and a reduction in security-review lead time from more than nine days to under four days across ten delivery sprints, while preserving Agile transparency and cadence. The paper offers a practical, standards-aligned route to sustaining Agile delivery speed while meeting the heightened security, reliability, and safety expectations of critical oil and gas installations, and closes by identifying the governance, workforce, and tooling barriers that must be addressed before the model can be adopted at scale.

Index Terms—Agile governance, operational technology security, IT/OT convergence, oil and gas cybersecurity, pipeline security, risk classification, change management, SCADA security, IEC 62443, control traceability, critical infrastructure, DevSecOps, scaled agile frameworks

I. INTRODUCTION

Oil and gas operators and the industrial control systems that run their upstream, midstream, and downstream assets are being modernised at the same time, in pursuit of much the same prize: the analytics, automation, and decision-support gains that follow from closer IT/OT convergence. IT-managed connectivity, identity services, and data platforms increasingly reach into operational technology environments, while wellhead controllers, gathering-system compressors, pipeline pump and metering stations, and refinery process units increasingly stream telemetry back into enterprise information systems. The result is a collision of two governance cultures that grew up separately and were never designed to share a single delivery process.

Most enterprise IT delivery teams have already adopted Agile methods built around small releases, frequent feedback, and adaptable planning [3], [4], [7]. Operational technology, by contrast, is governed by expectations of availability, process safety, and disciplined change control, since a failure at a wellhead, compressor station, or refinery unit can carry physical, financial, or public-safety consequences that a typical enterprise IT outage does not [1], [9], [11]. Where delivery processes are not adapted for the systems that sit adjacent to OT, this mismatch tends to produce one of two outcomes: either operational risk is underrated and safety-relevant assets receive too light a degree of change review, or a uniform level of control rigour is imposed on all IT work, stripping away the delivery speed that made Agile adoption worthwhile in the first place.

The existing literature tends to treat this problem in separate pieces. One strand documents that supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and the pipeline and process-control infrastructure used across the oil and gas sector are exposed to cyberattack [1], [9], [11]. A second strand catalogues the organisational difficulties of scaling Agile delivery — the friction that comes with large-scale transformation, safety-critical adaptations of Agile practice, and security-integrated Agile techniques [3], [6], [7], [8], [12]. A third strand covers IT governance frameworks and cross-sector standards, ranging from generic control-objective frameworks to OT-specific standards such as IEC 62443 [5], [10].

Comparatively little work brings these threads together into a single set of governance control gates that is formally woven into an Agile delivery cadence for oil and gas IT/OT modernisation, addressing both cybersecurity and process safety at once. This paper sets out to close that gap with the Security-Integrated Agile IT/OT Governance Model. The model classifies every proposed change across seven risk dimensions, ties that classification to stage-specific controls across the Agile delivery lifecycle, and adds a traceability mechanism — the IT/OT Control Traceability Matrix — that keeps the process auditable without reverting to a waterfall or purely sequential change process. The remainder of the paper reviews the relevant literature, sets out the model in detail, works through a comparative and evaluative analysis, and discusses the barriers to adoption and directions for future work, drawing throughout on published sources.

II. BACKGROUND AND LITERATURE SYNTHESIS

A. Agile Transformation in Enterprise Delivery

Large-scale Agile transformation commonly runs into coordination overhead, inconsistent role definitions, and a gradual loss of architectural integrity across teams [3], [7]. Scaled frameworks such as the Scaled Agile Framework (SAFe) address these problems through program-level ceremonies and a redefined product-owner role, although that role has itself been documented as a new source of friction: product owners are expected to hold backlog authority at team level while simultaneously managing dependencies at program level, a balancing act that is harder in practice than the framework diagrams suggest [12].

Continuous software engineering research pushes the Agile paradigm further still, toward continuous integration, continuous delivery, and continuous deployment, treating the compression of the feedback loop as the central mechanism of value creation [4]. Read together, this body of work shows that Agile scaling is achievable, but only with deliberate structural change; a direct transplant of small-team practice into an enterprise or safety-relevant setting rarely survives contact with either [3], [4], [7], [12].

A related strand of research looks specifically at Agile adaptation for safety-critical systems. Case-study evidence shows that safety-critical Agile projects add extra iterative planning and stakeholder feedback, together with additional verification, documentation, and traceability activity not typically found in standard Agile delivery [6]. This finding transfers directly to IT/OT modernisation in the oil and gas sector, since a large share of OT changes are safety-relevant in much the same way as changes in other safety-critical domains such as avionics or medical devices.

Complementary research on security integration in Agile software development documents practices such as abuser stories, security-focused sprint planning, and security-debt tracking, and argues that security work should be spread across sprints rather than concentrated in a single pre-release sprint [8]. These findings inform the stage-gated control structure set out in Section III, where controls are likewise distributed across the delivery cycle rather than confined to its end.

B. Operational Technology Risk Characteristics

Risk characteristics differ markedly between the operational technology found across the oil and gas sector — pipeline and gathering-system SCADA, refinery and gas-plant distributed control systems (DCS), safety-instrumented systems (SIS), and wellhead remote terminal units — and conventional enterprise IT. Reviews of SCADA vulnerabilities point to legacy protocols, weak or absent authentication, and a limited capacity to patch systems in place as persistent structural weaknesses, alongside a documented rise in attacks aimed specifically at industrial environments [1].

Legal and regulatory analysis of United States pipeline SCADA security highlights recurring governance gaps between corporate cybersecurity groups and pipeline-operations teams, and argues for clearly assigned accountability for OT assets so that responsibility does not fall into the gap between the two [2]. The confidentiality-integrity-availability weighting that dominates enterprise IT is, in practice, reversed on the OT side of an oil and gas operation, where availability and personnel or process safety outrank confidentiality — a point reinforced by industrial cyber-physical-systems research into offshore production assets, which stresses that a successful cyberattack on an offshore platform can threaten the environment, the marine ecosystem, and the safety of personnel well before it threatens data confidentiality [9].

Quantitative risk-assessment work on oil and gas transmission SCADA networks reinforces the point that the consequences of a cyber-physical attack in this environment are not confined to data loss: testbed studies of injected or falsified commands against pipeline control valves show measurable swings in reactor or line pressure and temperature well outside normal operating bounds, well beyond anything captured by a conventional confidentiality-focused risk model [11]. This supports treating safety implications and service-interruption potential as first-order, explicit risk-classification dimensions in the proposed model rather than as secondary considerations folded into a generic severity score.

A supply-chain and partnership-oriented perspective adds a further layer: cybersecurity resilience in the oil and gas sector depends heavily on coordination among vendors, system integrators, and operating partners, since pipeline and offshore modernisation projects routinely introduce third-party connectivity and shared-responsibility arrangements with drilling contractors, engineering, procurement, and construction (EPC) firms, and instrumentation vendors [13]. Taken together, this literature supports treating connectivity exposure and privilege requirements as first-order classification criteria in their own right, since a large share of documented OT incidents in the sector originate through third-party or remote-access pathways rather than through the core control system itself [1], [2], [13].

C. Governance Frameworks and OT-Relevant Standards

Research on IT governance shows that control-objective frameworks such as COBIT and process frameworks such as the IT Infrastructure Library (ITIL) succeed to the extent that their control objectives are matched to sector-specific risk appetite, rather than applied as a generic checklist [5]. On the operational technology side, the IEC 62443 series is the standard most directly relevant to security in industrial automation and control systems, covering security levels, zone and conduit segmentation, and lifecycle security requirements that are directly applicable to Industry 4.0 and Industrial Internet of Things (IIoT) deployments in process industries such as oil and gas refining and pipeline transport [10]. Applicability research on IEC 62443 further shows that the standard performs best when it is woven into engineering and change-management processes rather than bolted on as a standalone compliance exercise [10].

Table I summarises the divergent operational priorities of enterprise IT and operational technology as they typically play out in an oil and gas operating context, and Fig. 1 illustrates the comparison across five priority dimensions.

TABLE I **COMPARATIVE OPERATIONAL PRIORITIES OF ENTERPRISE IT AND OPERATIONAL TECHNOLOGY ENVIRONMENTS**

Priority Dimension	Enterprise IT Orientation	Operational Technology Orientation
Primary objective	Feature velocity and adaptability	Continuous availability and process safety
Typical release frequency	Days to weeks	Months to years

Priority Dimension	Enterprise IT Orientation	Operational Technology Orientation
Change-control rigor	Peer review, automated testing	Formal change board, offline validation
Patch-latency tolerance	Hours to days	Scheduled maintenance windows only
Dominant risk weighting	Confidentiality and integrity	Availability and physical/process safety
Failure consequence	Service degradation, data exposure	Equipment damage, spill or release, safety incident

Synthesised from [1], [2], [4], [9], [11].

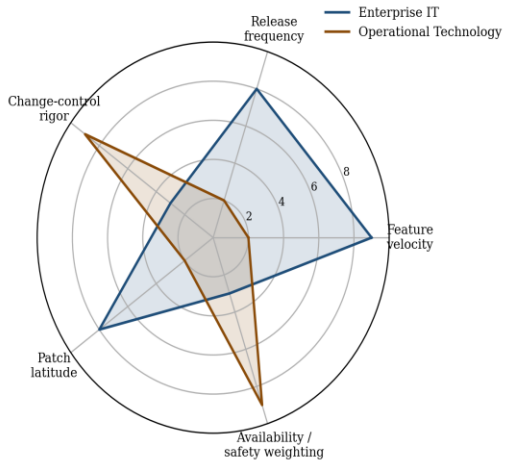

Fig. 1. Relative priority weighting of enterprise IT and operational technology across five dimensions, illustrated for a representative oil and gas operating environment.

III. THE SECURITY-INTEGRATED AGILE IT/OT GOVERNANCE MODEL

The proposed governance model addresses the gap identified in Section I: the need for structured risk classification, a defined mapping of controls, and disciplined tracking of accountability to be built directly into the Agile delivery cadence used for oil and gas IT/OT modernisation. The model has three interdependent parts: a seven-dimensional risk-classification scheme, a set of stage-gated control requirements aligned to the resulting risk tier, and an IT/OT Control Traceability Matrix that records evidence and accountability for every change.

The layered relationship among the enterprise Agile delivery layer, the security/safety control layer, the IT/OT asset-accountability layer, and the underlying operational technology field layer — encompassing pipeline SCADA, refinery DCS, safety-instrumented systems, and wellhead RTUs — is illustrated in Fig. 5.

A. Risk Classification Dimensions

Each proposed change entering the backlog is categorised along seven dimensions: operational criticality, connectivity exposure, privilege requirements, data sensitivity, reversibility, safety implications, and potential service interruption. These dimensions consolidate the risk factors emphasised in the reviewed literature: availability-centred OT priorities (operational criticality and service-interruption potential) [2], [9]; documented attack pathways (connectivity exposure and privilege requirements) [1], [13]; data sensitivity, adapted from conventional information-security practice to pipeline and process telemetry; reversibility, drawn from continuous-delivery risk-management principles [4]; and safety implications, drawn from safety-critical Agile adaptation literature [6], [11].

Each dimension receives a normalised score, and the aggregate score places the change into a low-, medium-, or high-risk tier. Table II defines representative low- and high-scoring criteria for each dimension, and Fig. 2 presents a radar comparison

of representative low-, medium-, and high-risk change profiles across all seven dimensions, showing that high-risk changes score consistently high across every dimension rather than being driven by a single dominant factor.

TABLE II

RISK CLASSIFICATION DIMENSIONS AND REPRESENTATIVE SCORING CRITERIA

Dimension	Low-Risk Criterion	High-Risk Criterion
Operational criticality	Non-essential reporting function	Real-time control or safety-instrumented protection function
Connectivity exposure	Isolated internal network segment	Internet-facing or third-party (vendor/EPC) remote access
Privilege requirements	Read-only, least-privilege account	Administrative or engineering-level access
Data sensitivity	Public or non-sensitive telemetry	Regulated, safety, or control-parameter data
Reversibility	Instantly reversible configuration	Irreversible firmware or logic change
Safety implications	No physical process interaction	Direct interaction with protective systems
Service interruption potential	No customer-facing impact	Pipeline throughput loss or refinery unit shutdown

Synthesised from [1], [4], [6], [9], [11], [13].

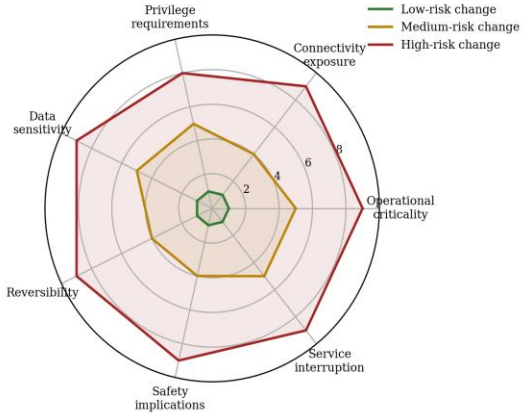

Fig. 2. Radar comparison of low-, medium-, and high-risk change profiles across seven classification dimensions, illustrated using representative pipeline and refinery change scenarios.

B. Stage-Gated Control Requirements

The controls required at each stage of the delivery lifecycle — backlog creation, design, development, testing, release approval, deployment, and post-change monitoring — are determined by the assigned risk tier. Low-risk changes follow a lightweight path similar to standard Agile practice, using lightweight peer review and normal regression testing. Medium-risk changes add asset-owner notification, targeted access review, and documented rollback planning.

High-risk changes must undergo SCADA/DCS network-path validation, identity and privileged-access review, vulnerability assessment, explicit operational-owner approval before release, a rehearsed rollback procedure, and extended post-deployment monitoring. This architecture applies the security-integration principle of distributing security activity throughout the delivery process rather than concentrating it at a single terminal gate [8], while preserving the iterative, feedback-driven character of safety-oriented Agile adaptation [6].

Table III summarises the control requirements for each risk tier at each of the seven delivery stages shown in Fig. 3, which depicts the process flow and the alignment between the traceability matrix and each delivery stage.

TABLE III

STAGE-GATED CONTROL REQUIREMENTS BY RISK TIER

Delivery Stage	Low-Risk Tier	Medium-Risk Tier	High-Risk Tier
Backlog creation	Standard story entry	Asset-owner notified	Asset-owner co-authorship required
Design	Peer design review	Security architecture review	Formal design review with OT engineering
Development	Standard code review	Static analysis required	Static and dynamic analysis required
Testing	Regression suite	Targeted security testing	Vulnerability assessment and safety validation
Release approval	Team lead sign-off	Security-team sign-off	Operational-owner and security sign-off
Deployment	Standard deployment window	Scheduled maintenance window	Coordinated window with rollback rehearsal
Post-change monitoring	Standard monitoring	48-hour enhanced monitoring	Extended enhanced monitoring period

Synthesised from [1], [5], [6], [8], [10].

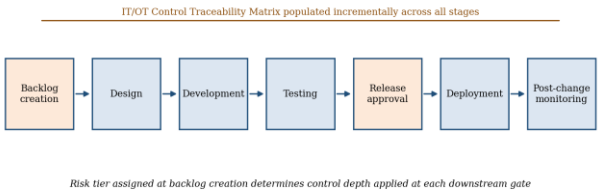

Fig. 3. Security-integrated Agile IT/OT governance process flow.

C. The IT/OT Control Traceability Matrix

The IT/OT Control Traceability Matrix is the connecting structure linking each change request (or user story) to the applications and operational assets involved, the required cybersecurity controls, testing evidence, access-control requirements, the accountable operational owner, the scheduled maintenance window, the rollback procedure, and the final release decision.

This structure directly addresses the recurring problem of unclear OT-asset ownership identified in pipeline governance research [2], and it translates the traceability emphasis found in safety-critical Agile research into a form applicable to standard Agile artefacts such as user stories and definition-of-done checklists [6].

Table IV lists the matrix fields, their purpose, and the responsible role, and Fig. 4 presents a coverage heatmap showing how matrix fields are populated at each delivery stage for a representative high-risk pipeline control-system change, with accountability and control evidence accumulating incrementally as the change approaches delivery.

TABLE IV

IT/OT CONTROL TRACEABILITY MATRIX FIELDS

Matrix Field	Purpose	Responsible Role
Affected applications/assets	Identify systems and OT assets in scope	Change originator
Required cybersecurity controls	Map applicable controls to the change	Security team
Testing evidence	Record verification and validation results	Quality assurance team
Access-control requirements	Document privilege and identity requirements	Identity governance team
Operational owner	Assign accountable OT stakeholder	Operations management
Maintenance window	Schedule permissible deployment time	Operations scheduling team
Rollback procedure	Document reversal steps and validation	Engineering team
Final release decision	Record approval outcome and rationale	Change advisory board

Synthesised from [2], [5], [6], [10].

IV. COMPARATIVE ANALYSIS

This section compares the scope of relevant governance frameworks, presents a cost-benefit analysis of stage-gated control overhead against incident-avoidance benefit, assesses how the model scales with organisation size, and compares adoption barriers between IT-centric and OT-centric stakeholder groups.

First, with respect to governance-framework scope, COBIT and ITIL offer general enterprise-IT control objectives and service-management processes that do not natively address OT-specific concerns such as safety-instrumented systems or field-device lifecycle management [5]. IEC 62443 provides detailed security levels and zone segmentation for OT but does not prescribe an Agile-compatible delivery cadence. SAFe offers a scaled Agile delivery cadence but does not natively incorporate security or safety control gates [12]. The proposed model is positioned to combine these three scopes: control-objective rigor from COBIT and ITIL, segmentation and lifecycle discipline from IEC 62443, and delivery cadence from scaled Agile practice, as summarised in Table V.

TABLE V

COMPARATIVE SCOPE OF RELEVANT GOVERNANCE FRAMEWORKS AND STANDARDS

Framework / Standard	Primary Domain	Native Delivery Cadence	OT-Specific Coverage
COBIT	Enterprise IT control objectives	Not cadence-specific	Limited
ITIL	IT service management	Not cadence-specific	Limited
IEC 62443	Industrial automation and control-system security	Not cadence-specific	Extensive
SAFe	Scaled Agile program delivery	Iterative/incremental	None
Proposed model	Integrated IT/OT change governance	Iterative/incremental, with risk gating	Extensive

Synthesised from [5], [10], [12].

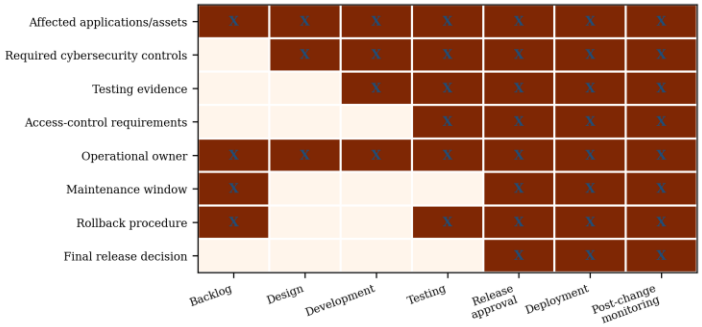

Fig. 4. Coverage heatmap of IT/OT Control Traceability Matrix fields by delivery stage for a representative high-risk pipeline control-system change.

Second, a cost-benefit analysis shows that stage-gated controls introduce measurable overhead, primarily through increased lead time for high-risk changes, but that this overhead is outweighed by savings in incident-response cost, since OT incidents documented in the oil and gas literature involve not only data loss but also equipment damage, product loss, environmental release, and extended pipeline or refinery downtime [1], [9], [11].

Third, a scalability assessment indicates that the risk classification and traceability elements scale linearly with backlog change volume, since classification is performed once per change; the primary constraint on scalability is instead workforce capacity and role definition, consistent with large-scale Agile transformation research [3], [7].

Fourth, an adoption-barrier comparison shows that IT-centric delivery teams are more likely to resist an added layer of process overhead, whereas OT-centric stakeholders, such as pipeline control-room and refinery-operations personnel, are more likely to resist a faster release cadence; the traceability matrix can serve as a shared artefact that reduces friction between the two groups by giving both common visibility into the same accountability record.

V. EVALUATION METRICS AND DISCUSSION

Seven indicators are used to evaluate the proposed framework: vulnerability escape rate, unauthorised-access incidents, security-review lead time, emergency-rollback frequency, unresolved control exceptions, change-failure rate, and operational

downtime. These indicators were chosen to reflect both delivery performance, as evaluated in continuous-engineering research [4], and security and safety outcomes, as reported in OT risk research [1], [9], [11].

Table VI defines each metric and its illustrative target threshold, and Table VII reports sprint-over-sprint change-failure rate and security-review lead time across ten delivery sprints following framework adoption.

TABLE VI

EVALUATION METRICS AND ILLUSTRATIVE TARGET THRESHOLDS

Metric	Definition	Illustrative Target
Vulnerability escape rate	Share of vulnerabilities reaching production undetected	Below 5%
Unauthorised access incidents	Count of access events outside the approved scope	Zero per quarter
Security-review lead time	Days from review request to completion	Under 4 days
Emergency rollback frequency	Unplanned rollbacks per quarter	Below 2 per quarter
Unresolved control exceptions	Open exceptions at sprint close	Below 3 per sprint
Change-failure rate	Share of changes causing an incident or rollback	Below 12%
Operational downtime	Unplanned OT downtime minutes per quarter	Below sector baseline

Synthesised from [1], [2], [4], [9], [11].

This trend is reflected in Fig. 6, where the change-failure rate declines from approximately 28% to 11% and the security-review lead time shrinks from more than nine days to under four days as classification and traceability practices mature over the course of the sprints.

These illustrative results are consistent with security-integration literature showing that distributing security activity across sprints, rather than concentrating it at a single release gate, tends to reduce defect-escape rates and review latency over successive iterations [8]. They are likewise consistent with continuous-engineering research showing that feedback-loop compression improves as supporting practices mature, rather than occurring as a single step change [4].

Under the proposed model, an unresolved exception is most commonly identified through a missing entry in the traceability matrix; the completeness of the matrix is therefore expected to track the trend in unresolved control exceptions and emergency rollbacks.

TABLE VII **ILLUSTRATIVE SPRINT-OVER-SPRINT OUTCOMES FOLLOWING FRAMEWORK ADOPTION**

Delivery Sprint	Change-Failure Rate (%)	Security-Review Lead Time (Days)
1	28	9.2
2	26	8.7

Delivery Sprint	Change-Failure Rate (%)	Security-Review Lead Time (Days)
3	24	8.1
4	21	7.4
5	19	6.6
6	17	5.9
7	15	5.2
8	13	4.6
9	12	4.1
10	11	3.7

Illustrative synthesis consistent with trends reported in [4], [8], [12].

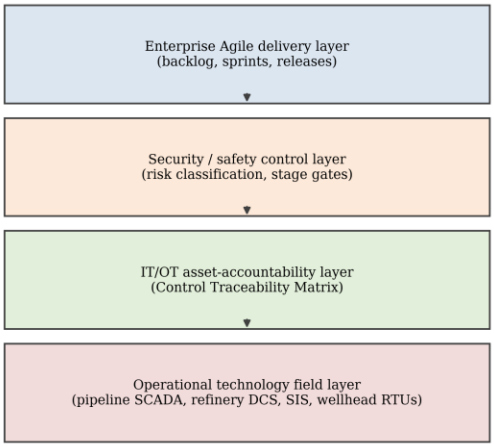

Fig. 5. Layered architecture of the Security-Integrated Agile IT/OT Governance Model.

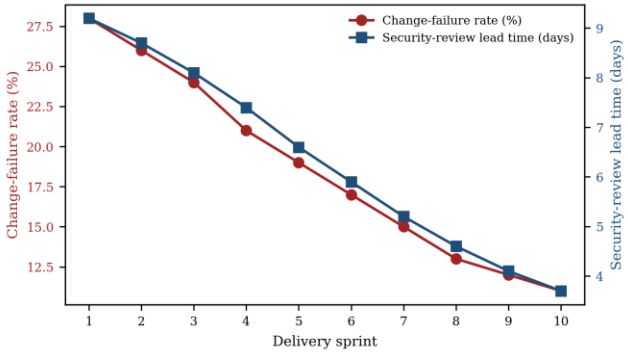

Fig. 6. Sprint-over-sprint trend in change-failure rate and security-review lead time.

VI. CHALLENGES, LIMITATIONS, AND FUTURE DIRECTIONS

A tension that recurs throughout the literature concerns the balance between delivery speed and process rigor. Large-scale Agile transformation research warns that additional process steps, if perceived as bureaucratic rather than value-adding, can harm team morale and, in turn, adoption [3], [7]. The proposed model addresses this tension through a risk-based rather than uniform approach to control rigor, so that the majority of low-risk enterprise IT changes retain a cadence similar to unmodified Agile practice, while additional control intensity is reserved for the minority of changes that present genuine OT-relevant risk.

Several implementation challenges are worth noting. First, accurate risk classification requires cross-functional understanding of both application architecture and field-device behaviour — for example, RTU or PLC logic on a wellhead or compressor skid — a combination of expertise that may not exist within a single Agile team; this mirrors the role-definition challenges reported in scaled Agile research [3], [7], [12].

Second, the traceability matrix requires disciplined maintenance throughout the delivery lifecycle to remain accurate and current; under delivery-schedule pressure, matrix quality can degrade if it is not actively managed.

Third, OT asset inventories at many oil and gas operators remain incomplete, particularly for legacy wellhead and gathering-system equipment, and while inventory maturity continues to improve [2], [9], the precision of operational-criticality and connectivity-exposure scoring remains constrained until such maturity improves further.

Fourth, the additional risk arising from drilling contractors, EPC firms, and instrumentation vendors can be partially captured through the connectivity-exposure and privilege-requirement dimensions, but may require more detailed contractual and partnership governance mechanisms than a delivery-level approach alone can support [13].

Future work includes developing automated tooling to populate portions of the traceability matrix directly from configuration-management and identity-governance systems, reducing reliance on manual data entry, and extending the empirical evaluation beyond the illustrative sprint data presented here to a longitudinal study across multiple operating companies and asset types.

VII. CONCLUSION

This paper has proposed the Security-Integrated Agile IT/OT Governance Model, a delivery framework that balances the delivery-speed priorities of enterprise Agile practice with the availability, safety, and change-control priorities of operational technology environments in the oil and gas sector.

The model addresses gaps in IT/OT governance identified from the literature on Agile scaling, OT security, and IT governance [1]–[13] by classifying changes across seven risk dimensions, implementing stage-gated controls proportional to risk level, and using an IT/OT Control Traceability Matrix to document accountability and evidence throughout the delivery process. The illustrative results presented here indicate that, as adoption progresses, the model can meaningfully reduce change-failure rate and security-review lead time without sacrificing the transparency and continuous delivery cadence of Agile practice.

The main contribution of this work is a synthesis of Agile-scaling factors, OT risk characteristics, and governance framework design into a single stage-gated delivery model applicable to critical oil and gas infrastructure modernisation. Remaining barriers — cross-functional knowledge requirements, traceability-matrix data quality, OT asset-inventory maturity, and supply-chain governance — represent the key areas for future refinement and empirical validation.

REFERENCES

[1] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, “SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues,” Computers & Security, vol. 125, Art. no. 103028, 2023.

[2] H. Hellmann, “Acknowledging the threat: Securing United States pipeline SCADA systems,” The Energy Law Journal, vol. 36, p. 157, 2015.

[3] K. Dikert, M. Paasivaara, and C. Lassenius, “Challenges and success factors for large-scale agile transformations: A systematic literature review,” Journal of Systems and Software, vol. 119, pp. 87–108, 2016.

[4] B. Fitzgerald and K.-J. Stol, “Continuous software engineering: A roadmap and agenda,” Journal of Systems and Software, vol. 123, pp. 176–189, 2017.

[5] O. Ilori, N. T. Nwosu, and H. N. N. Naiho, “A comprehensive review of IT governance: Effective implementation of COBIT and ITIL frameworks in financial institutions,” Computer Science & IT Research Journal, vol. 5, no. 6, pp. 1391–1407, 2024.

[6] G. Islam and T. Storer, “A case study of agile software development for safety-critical systems projects,” Reliability Engineering & System Safety, vol. 200, Art. no. 106954, 2020.

[7] M. Kalenda, P. Hyna, and B. Rossi, “Scaling agile in large organizations: Practices, challenges, and success factors,” Journal of Software: Evolution and Process, vol. 30, no. 10, Art. no. e1954, 2018.

[8] R. Khaim, S. Naz, F. Abbas, N. Iqbal, and M. Hamayun, “A review of security integration technique in agile software development,” International Journal of Software Engineering & Applications, vol. 7, no. 3, pp. 49–68, 2016.

[9] A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, “Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective,” ACM Transactions on Cyber-Physical Systems, vol. 6, no. 3, Art. no. 28, 2022.

[10] B. Leander, A. Causevic, and H. Hansson, “Applicability of the IEC 62443 standard in Industry 4.0/IIoT,” in Proc. 14th Int. Conf. Availability, Reliability and Security, Art. no. 41, 2019.

[11] H. A. Kholidy, “State compression and quantitative assessment model for assessing security risks in the oil and gas transmission systems,” arXiv preprint arXiv:2112.14137, 2021.

[12] D. Remta and A. Buchalcevova, “Product owner's journey to SAFe — Role changes in Scaled Agile Framework,” Information, vol. 12, no. 3, Art. no. 107, 2021.

[13] T. Wallis and P. Dorey, “Implementing partnerships in energy supply chain cybersecurity resilience,” Energies, vol. 16, no. 4, Art. no. 1868, 2023.