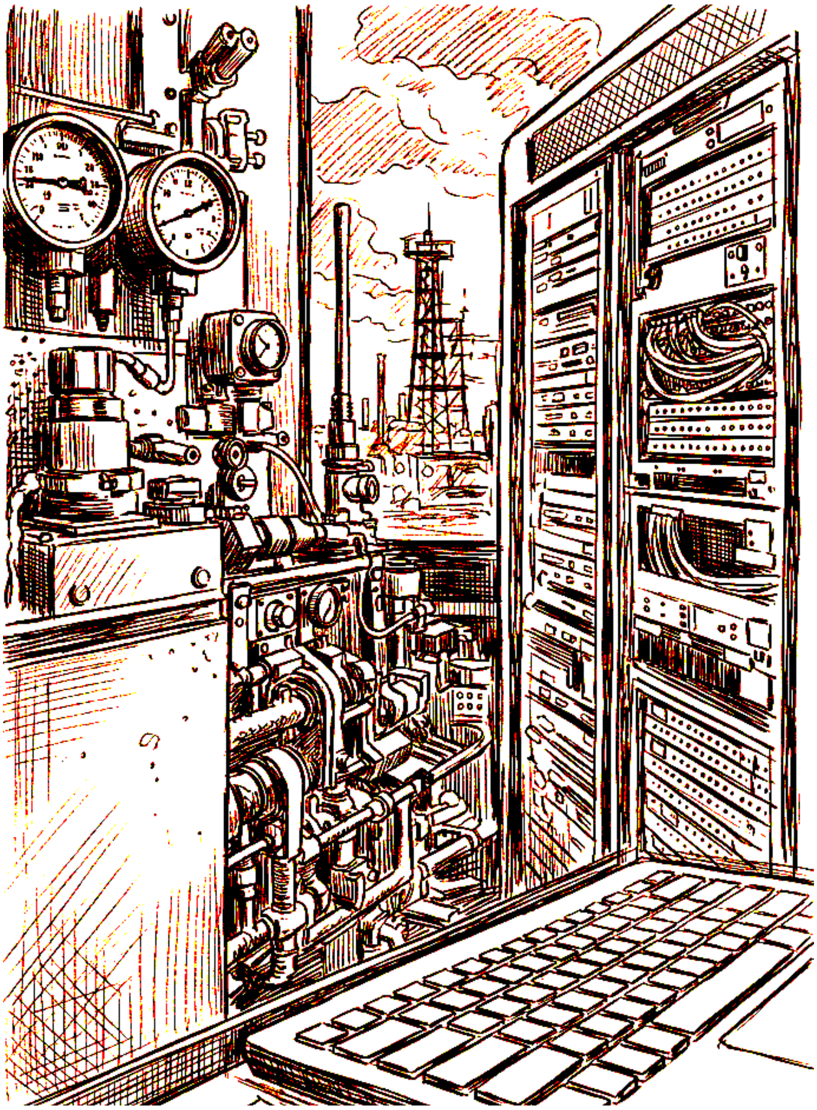

OT-IT Convergence Kill Chain

A progression model of enterprise driven operational risk.
v.0.1

Zafani Baixa Security
Operational Intelligence and Risk Research
July 2025

Index

Executive Premise

Incidents impacting critical infrastructure are increasingly described as Operational Technology (OT) events. In practice, they rarely begin there. Across energy, utilities, manufacturing, and industrial environments, the most consequential operational disruptions are the downstream result of conditions established far upstream in enterprise IT and cloud ecosystems.

Compromise does not emerge suddenly inside control systems. It progresses gradually across identity, trust, and organizational boundaries that were never designed to withstand adversarial pressure. This is a systemic progression that is often overlooked by domain focused security models and control centric risk programs..

Modern enterprises operate in environments where IT, cloud, and OT are deeply interconnected through identities, vendors, remote access, shared tooling, and operational workflows. These connections are essential for efficiency and scale. They are also the mechanisms through which enterprise compromise becomes operational risk. Most security programs are structured around domains. However, adversaries are not.

They move through organizations by exploiting time, legitimacy, and assumptions of trust. They rely on approved access paths, operational urgency, and the expectation that systems behaving normally are systems behaving safely. By the time anomalous behavior is visible at the operational layer, the conditions enabling impact have often existed for months or years.

As a result, organizations frequently experience OT incidents that cannot be clearly explained by a single vulnerability, control failure, or malicious action. Controls appear intact. Segmentation exists. Monitoring is in place. Yet confidence in operational integrity erodes, and leadership is forced to make decisions under uncertainty, often too late in the progression to act without disruption.

From Enterprise Access to Operational Risk

The OT IT Convergence Kill Chain provides a structured way to reason about how enterprise compromise evolves into operational and physical risk over time. It focuses on progression rather than events, on failure modes rather than threat actors, and on decision points rather than tools. The intent is not to replace existing cybersecurity or industrial security standards, but rather to complement them by addressing a question they were not designed to answer.

➢ *How does legitimate enterprise access, when combined with time, trust, and organizational structure, become an operational threat?*

Answering this question is the difference between managing risk and reacting to consequences.

Scope, Assumptions, and Non-Goals

This section defines the intended scope of the OT IT Convergence Kill Chain, the assumptions under which it is designed to operate, and the objectives it deliberately does not pursue. Clear boundaries are essential to ensure the framework is applied correctly and interpreted consistently.

Scope

The OT IT Convergence Kill Chain applies to organizations operating environments where enterprise IT, cloud services, and operational technology are interconnected as part of normal business operations. The framework is intended for use in sectors where operational integrity, safety, and continuity are critical, including but not limited to energy generation and distribution, utilities, manufacturing, oil and gas, transportation, and other industrial environments.

Within these contexts, the framework focuses on the progression of risk across converged domains, specifically:

- Enterprise IT environments, including identity systems, endpoints, corporate networks, and SaaS platforms.
- Cloud environments that support enterprise and operational functions.
- OT environments where digital systems influence physical processes.
- The organizational and operational interfaces that connect these domains.

The framework is designed for security leadership, risk owners, and operational decision makers responsible for governing converged environments. It is not limited to technical security teams.

Assumptions

This framework is built on the following assumptions, which reflect observed conditions in modern industrial enterprises.

- **Organizations operate converged environments by necessity.**
    - Separation between IT, cloud, and OT exists conceptually, but practical operations depend on shared identities, vendors, tooling, and workflows.
- **Most consequential incidents rely on legitimate access.**
    - The framework assumes that valid credentials, approved access paths, and operationally justified exceptions are primary mechanisms through which risk progresses.
- **Adversaries are patient and adaptive.**
    - Progression is expected to occur over extended periods, often without triggering clear technical alarms.
- **Security controls exist but are unevenly governed.**
    - The framework assumes that controls may be present, yet misaligned with decision authority, operational realities, or organizational incentives.

- **Operational continuity is a dominant constraint.**
  - Decisions affecting OT environments are influenced by safety, uptime, and regulatory obligations, which shape how and when security actions can occur.

Non Goals

The OT IT Convergence Kill Chain is not intended to replace existing cybersecurity or industrial security standards. It is designed to complement them by addressing a specific analytical gap related to convergence and progression.

The framework does not attempt to provide:

- Tactical guidance, playbooks, or procedures for attacking or defending systems.
- Tool specific recommendations or vendor aligned architectures.
- Threat actor profiles, campaigns, or attribution analysis.
- Prescriptive implementation steps or configuration instructions.
- Compliance checklists or audit criteria.

The framework is also not a maturity model, risk scoring system, or control catalog. While it informs such efforts, its primary purpose is to support structured reasoning about progression, failure modes, and decision points.

Intended Use

This framework is intended to be used as:

- A lens for understanding how enterprise compromise can evolve into operational risk.
- A common language between IT, OT, security, and leadership.
- A foundation for decision making under uncertainty.
- A complement to existing standards, assessments, and risk management programs.

It should not be used as a standalone measure of security posture or as a substitute for domain specific technical analysis.

The Model (OT–IT Convergence Kill Chain v0.1)

The OT IT Convergence Kill Chain describes the structured progression through which enterprise compromise evolves into operational and physical risk in converged environments. The model captures recurring failure patterns that allow risk to accumulate and propagate over time.

The model reflects how modern organizations actually operate, how trust is distributed, and how legitimate capabilities are accumulated and misused over time. Each phase represents a condition in which risk increases not because a system is broken, but because assumptions remain unchallenged.

Progression through the kill chain is not linear, deterministic, or inevitable. However, once multiple phases are present simultaneously, the organization enters a state where operational impact becomes increasingly difficult to prevent without disruption.

Model Structure

The model consists of seven phases. Each phase represents a distinct risk condition with clear entry characteristics, observable indicators, and potential intervention points. The phases are cumulative, earlier phases do not disappear as later phases emerge.

The **seven** phases are:

1. **Enterprise Exposure Accumulation**
2. **Initial Trust Breach**
3. **Identity and Access Drift**
4. **OT Adjacent Visibility and Mapping**
5. **Convergence Pivot**
6. **Operational Influence Establishment**
7. **Physical Process Impact**

Phase 1: Enterprise Exposure Accumulation

This phase reflects the gradual formation of enterprise conditions that expand the space in which compromise can occur.

Exposure develops over time through unmanaged identities, long standing vendor access, undocumented technical dependencies, inherited exceptions, and fragmented accountability across IT, cloud, and operational environments. These elements rarely appear risky in isolation. Together, they form a durable condition of permissive access and limited oversight. At this stage, no adversarial presence is required.

Risk exists independently of intent, embedded in how the enterprise operates. Failure at this phase is rarely recognized because these conditions are treated as normal operational complexity rather than as sources of risk.

Phase 2: Initial Trust Breach

The initial trust breach occurs when an adversary gains legitimate access to enterprise systems. This access is typically achieved through enterprise IT or cloud environments, not through OT systems. The breach does not require elevated privileges. Presence alone is sufficient.

The defining characteristic of this phase is that access appears valid. Systems behave as designed. Security controls may remain intact. The organization experiences no immediate operational impact, yet trust boundaries have been crossed.

Phase 3: Identity and Access Drift

Identity and access drift describes the gradual expansion of effective capability through accumulated permissions, inherited roles, and organizational blind spots.

Privilege increases not through overt escalation, but through normal enterprise processes. Access justified for one purpose becomes reusable for others. Ownership becomes unclear. Review cycles lag reality. At this phase, the convergence of IT and OT becomes organizational rather than technical. Authority is gained implicitly, not seized.

Phase 4: OT Adjacent Visibility and Mapping

In this phase, the adversary develops an understanding of OT environments without interacting directly with control systems. Visibility is obtained through documentation, architecture artifacts, support tooling, monitoring platforms, engineering workflows, and historical operational data accessible from enterprise contexts.

- ➢ OT is analyzed as a business system rather than a technical target.
    - ○ Critical processes become legible.

This phase significantly reduces uncertainty while remaining difficult to distinguish from legitimate enterprise activity.

Phase 5: Convergence Pivot

The convergence pivot represents the transition from enterprise environments into operationally adjacent systems. This transition does not rely on exploitation. It relies on designed access paths such as remote support, engineering workstations, shared services, and operational tooling.

The defining failure at this phase is not the absence of segmentation, but the absence of meaningful control over how segmentation is used. The boundary between IT and OT exists, but it does not function as a security boundary.

Phase 6: Operational Influence Establishment

Rather than immediate disruption, adversaries at this phase seek to establish influence over operational conditions. This may include subtle changes to visibility, timing, configuration, or automated decision making processes. Actions are deliberately small, reversible, and operationally plausible. Operations continue to function, yet confidence in their integrity quietly erodes.

- Detection is difficult because changes do not violate expected system behavior in isolation.

Phase 7: Physical Process Impact

Physical process impact represents the realization of operational risk.

Impact may take the form of disruption, degradation, safety exposure, or strategic leverage. In some cases, the demonstrated ability to cause impact is sufficient to achieve adversarial objectives without execution. At this phase, leadership is required to act with incomplete information. Confidence in system behavior is reduced, timelines are compressed, and decisions must balance safety, continuity, and trust with limited options remaining.

As impact unfolds, attribution becomes contested. It is often unclear whether the event is the result of malicious action, operational error, mechanical failure, or an interaction of all three. This ambiguity delays decisive action and shifts focus toward containment rather than understanding.

- **The incident is frequently framed as an isolated OT failure.**
  - In reality, it reflects the cumulative effect of enterprise level conditions that progressed unchecked over time.
  - By the time physical impact is visible, the opportunity for low cost intervention has passed. What remains is risk acceptance under pressure.

Model Implications

The OT IT Convergence Kill Chain reframes operational risk as a progressive condition rather than a discrete event. It emphasizes that the most effective interventions occur before OT systems are directly affected, when trust, identity, and organizational boundaries can still be adjusted without physical consequence.

The model is intended to support earlier recognition, clearer decision making, and more deliberate governance across converged environments.

Systemic Failure Modes (SFM) Library

This section documents recurring failure modes observed across converged IT, cloud, and OT environments. These failures are systemic in nature. They emerge from organizational structure, operational incentives, and long lived design decisions rather than from individual technical weaknesses.

Failure modes described here are not hypothetical. They represent patterns that consistently precede operational impact across critical infrastructure sectors. Each failure mode is independent. Multiple failure modes often coexist.

Phase 1 SFM

Enterprise Exposure Accumulation

- ***Diffuse Asset Ownership***
  - Assets, identities, and integrations exist without clear ownership. Responsibility is implied rather than assigned. Risk accumulates silently because no single function perceives it as theirs to manage.
- ***Exception Permanence***
  - Temporary access and architectural exceptions remain in place indefinitely.
  - Operational urgency overrides review. Over time, exceptions become part of the baseline.
- ***Shadow Operational Dependencies***
  - OT supporting systems rely on enterprise services that are undocumented or poorly understood. These dependencies are discovered only during incidents.
- ***Vendor Access Normalization***
  - Third party access is treated as operational infrastructure rather than as a dynamic risk condition. Credentials persist beyond contractual or functional necessity.
- ***Complexity Without Visibility***
  - The organization accepts architectural complexity as inevitable. Visibility into how systems connect degrades faster than the systems themselves.

Phase 2 SFM

Initial Trust Breach

- ***Implicit Trust in Authentication***
  - Authenticated access is equated with legitimacy. Context, behavior, and intent are secondary considerations.
- ***Identity Overload***
  - Security teams manage volume rather than meaning. Anomalous access blends into background noise.
- ***Third Party Trust Inheritance***
  - Trust extended to vendors propagates across internal systems without reevaluation.
- ***Access Without Operational Context***
  - Security monitoring detects access events without understanding business relevance. Risk remains abstract.

Phase 3 SFM

Identity and Access Drift

- ***Privilege Accumulation***
    - Access grows incrementally through role changes, temporary needs, and inherited permissions. Removal lags acquisition.
- ***Role Reality Mismatch***
    - Access reflects historical responsibility rather than current function. Identity represents what someone was, not what they do.
- ***Review Fatigue***
    - Access reviews exist but lack depth. Approval becomes routine. Risk acceptance is implicit.
- ***Non Human Identity Expansion***
    - Service accounts and automation gain authority without proportional governance. Visibility into their effective reach erodes.

Phase 4 SFM

OT Adjacent Visibility and Mapping

- ***Operational Transparency Bias***
    - Documentation and diagrams are broadly accessible to support efficiency. Sensitivity is underestimated.
- ***Monitoring Tool Overexposure***
    - Operational monitoring platforms are accessible from enterprise contexts without segmentation of insight.
- ***Knowledge Centralization***
    - Critical OT knowledge is stored in shared repositories without contextual access controls.
- ***Historical Data Normalization***
    - Incident reports and post event analysis are accessible without restriction. Past failures inform future compromise.

Phase 5 SFM

Convergence Pivot

- **Boundary Convenience**
    - IT and OT boundaries are designed for usability. Security enforcement is secondary to operational flow.
- **Bidirectional Trust Paths**
    - Access designed for support and monitoring allows influence to flow in unintended directions.
- **Shared Management Infrastructure**
    - Enterprise systems manage both IT and OT assets. Administrative separation exists on paper.
- **Change Authority Ambiguity**
    - Responsibility for approving cross domain changes is unclear. Decisions default to availability.

Phase 6 SFM

Operational Influence Establishment

- **Plausible Change Acceptance**
  - Small operational changes are assumed to be benign. Patterns emerge slowly.
- **Baseline Absence**
  - Normal operation is understood intuitively rather than formally. Deviation lacks reference.
- **Tool Authority Concentration**
  - Centralized platforms gain influence over operational outcomes without corresponding oversight.
- **Alert Desensitization**
  - Frequent low severity anomalies reduce confidence in signals. Subtle manipulation persists.

Phase 7 SFM

Physical Process Impact

- **Delayed Recognition**
  - Early indicators are rationalized until impact becomes unavoidable.
- **Decision Paralysis Under Uncertainty**
  - Leadership hesitates due to incomplete information. Safety and continuity compete for priority.
- **Incident Framing Collapse**
  - Events are labeled technical failures rather than systemic outcomes. Learning is localized.
- **Recovery Bias**
  - Restoration of service takes precedence over root cause understanding. Conditions enabling impact remain.

Use of the Failure Modes Library

This library is intended to support:

- Identification of latent risk conditions
- Cross domain dialogue between IT, OT, and leadership
- Prioritization of early intervention points
- Structured post incident learning

Failure modes should be reviewed collectively rather than in isolation. Their presence indicates progression risk even in the absence of active compromise.

Signals & Telemetry Model

This section defines the types of signals and telemetry that indicate progression across the OT IT Convergence Kill Chain. The model emphasizes interpretation over volume and context over precision.

- Signals described here are not indicators of compromise in the traditional sense. They are indicators of condition. Individually they may appear explainable. Collectively they describe drift toward operational risk.

Risk can accumulate without producing obvious signals. Subtle and persistent conditions often carry more significance than isolated high severity events.

Signal Categories

Signals are grouped by domain of observation. Convergence risk emerges when signals from multiple domains align.

The framework considers five primary signal categories:

- Identity and access
- Endpoint and workload behavior
- Network and connectivity patterns
- Operational and process signals
- Organizational and governance signals

No single category is sufficient on its own.

Phase 1 Signals

Enterprise Exposure Accumulation

- **Identity and Access**
  - Growth in identities without corresponding business justification. Persistent third party access that outlives operational needs. Service accounts with expanding scope.
- **Endpoint and Workload Behavior**

  - Systems supporting OT functions appear in enterprise inventories without clear classification. Cloud workloads operate with unclear ownership.
- **Network and Connectivity**
  - New integrations and pathways emerge gradually. Dependencies are discovered reactively.
- **Organizational Signals**
  - Unclear accountability for shared systems. Risk discussions focus on complexity rather than exposure.

Phase 2 Signals

Initial Trust Breach

- **Identity and Access**
  - Authenticated access that deviates from historical patterns while remaining policy compliant. Logins that align with credentials but not with role expectation.
- **Endpoint and Workload Behavior**
  - Enterprise systems accessed successfully without subsequent operational activity. Sessions that persist longer than typical workflows require.
- **Organizational Signals**
  - Security events are acknowledged but deprioritized due to lack of immediate impact.

Phase 3 Signals

Identity and Access Drift

- **Identity and Access**
  - Incremental expansion of access across domains. Permissions inherited through role changes rather than explicitly requested.
- **Endpoint and Workload Behavior**
  - Accounts access systems adjacent to their primary function. Automation interacts with broader scopes over time.
- **Organizational Signals**
  - Access reviews are completed without substantive challenge. Ownership of permissions is unclear.

Phase 4 Signals

OT Adjacent Visibility and Mapping

- **Identity and Access**

- Enterprise identities access documentation, monitoring platforms, or support systems related to OT environments.

- **Endpoint and Workload Behavior**
  - Queries and interactions with operational data that are informational rather than functional.
- **Network and Connectivity**
  - Read oriented access to OT adjacent systems from enterprise contexts.
- **Organizational Signals**
  - OT knowledge is widely shared for efficiency. Sensitivity is assumed to be low.

Phase 5 Signals

Convergence Pivot

- **Identity and Access**
  - Enterprise identities appear in operationally adjacent systems through approved access paths.
- **Network and Connectivity**
  - Consistent traffic across IT and OT boundaries during non operational windows.
- **Operational Signals**
  - Remote support or engineering access is used outside of standard maintenance cycles.
- **Organizational Signals**
  - Boundary controls are viewed as operational constraints rather than security mechanisms.

Phase 6 Signals

Operational Influence Establishment

- **Operational Signals**
  - Small configuration changes that align with acceptable ranges. Timing adjustments that do not trigger alarms.
- **Endpoint and Workload Behavior**
  - Increased interaction with systems that influence operational visibility rather than control.
- **Organizational Signals**
  - Anomalies are explained individually. Patterns are not examined collectively.

Phase 7 Signals

Physical Process Impact

- **Operational Signals**
    - Process instability, unexpected degradation, or safety related alerts without clear mechanical cause.
- **Organizational Signals**
    - Escalation occurs under time pressure. Decision authority becomes centralized late.
- **Post Event Signals**
    - Investigation focuses on immediate triggers. Upstream conditions receive limited attention.

Interpreting Signals

Signals should be evaluated for persistence, alignment, and progression. Single events rarely justify action. Repeated conditions across domains indicate movement along the kill chain. The most valuable signals often appear explainable until viewed in aggregate. Effective interpretation requires collaboration between IT, OT, security, and operational leadership. No single function holds sufficient context.

Model Intent

This telemetry model is intended to:

- Enable earlier recognition of convergence risk
- Support cross domain interpretation rather than alert escalation
- Inform decision thresholds before operational impact
- Shift detection from event based to condition based reasoning

Signals are a means to understanding system state. They are not an end in themselves.

Control Objectives

This section defines the control objectives associated with the OT IT Convergence Kill Chain. Control objectives articulate intent. They describe the conditions an organization seeks to maintain, rather than the mechanisms used to achieve them.

Controls are evaluated by their ability to reduce uncertainty, constrain progression, and preserve decision space. Presence alone is insufficient. Alignment with operational reality is decisive.

Control Philosophy

Control objectives within this framework are designed to:

- Constrain the misuse of legitimate enterprise capability
- Reduce the accumulation of ungoverned trust
- Preserve early intervention options
- Support decisions under operational constraint

Controls are expected to function across IT, cloud, and OT environments without assuming uniform technical capability or authority.

Phase 1 Control Objectives

Enterprise Exposure Accumulation

- **Asset and Identity Accountability**
  - Every identity, system, and integration supporting operational outcomes is associated with a clear owner accountable for its continued necessity and risk.
- **Exception Lifecycle Governance**
  - Operational exceptions are explicitly time bound, reviewed, and retired. Permanence is treated as a failure condition.
- **Third Party Access Discipline**
  - External access reflects current operational need and contractual scope. Access continuity is actively justified.
- **Dependency Awareness**
  - Critical operational functions maintain documented awareness of enterprise and cloud dependencies that influence availability or integrity.

Phase 2 Control Objectives

Initial Trust Breach

- **Contextual Trust Evaluation**
  - Authentication and access decisions incorporate behavior, role expectation, and historical context.
- **Access Purpose Clarity**
  - Enterprise access reflects defined operational intent. Unexplained presence is treated as a risk condition.
- **Third Party Trust Containment**
  - Trust extended to external entities is constrained to the minimum scope required to deliver service outcomes.

Phase 3 Control Objectives

Identity and Access Drift

- **Privilege Alignment**
  - Access reflects current responsibility rather than historical entitlement.
- **Identity Scope Visibility**
  - The effective reach of identities, including non human identities, is understood and reviewed.
- **Access Review Integrity**
  - Access validation processes emphasize challenge and justification over completion.

Phase 4 Control Objectives

OT Adjacent Visibility and Mapping

- **Operational Information Sensitivity**
  - OT related documentation, monitoring views, and historical data are treated as sensitive operational assets.
- **Contextual Access to Insight**
  - Visibility into operational environments aligns with role and function. Broad access is not assumed.
- **Knowledge Distribution Awareness**
  - Critical operational understanding is shared deliberately rather than implicitly.

Phase 5 Control Objectives

Convergence Pivot

- **Boundary Intent Enforcement**
  - Connections between enterprise and operational environments reflect explicit security intent, not only operational convenience.
- **Directional Trust Control**
  - Access paths support required operational flows without enabling unintended influence.
- **Change Authority Definition**
  - Responsibility for approving cross domain access and configuration is explicit and enforceable.

Phase 6 Control Objectives

Operational Influence Establishment

- **Operational Baseline Confidence**
  - Normal operational behavior is formally understood, documented, and reviewed.
- **Influence Visibility**
  - Systems and tools capable of shaping operational outcomes are governed with heightened oversight.
- **Change Pattern Awareness**
  - Incremental changes are evaluated collectively rather than in isolation.

Phase 7 Control Objectives

Physical Process Impact

- **Decision Readiness**
  - Authority to act under uncertainty is established before operational impact occurs.
- **Integrity Preservation Priority**
  - Confidence in operational correctness is treated as critical to safety and continuity.
- **Recovery Discipline**
  - Restoration efforts incorporate validation of upstream conditions that enabled impact.

Use of Control Objectives

These control objectives are intended to guide architectural decisions, governance design, and operational oversight.

They are not prescriptive requirements. They define the outcomes that controls should support, regardless of implementation approach. Organizations should evaluate control effectiveness based on whether these objectives are consistently met across converged environments.

Decision Thresholds

This section defines decision thresholds associated with progression across the OT IT Convergence Kill Chain. Decision thresholds describe the conditions under which leadership must reassess posture, authority, and acceptable tradeoffs.

They are designed to preserve decision space while it still exists. Decision thresholds do not rely on certainty. They rely on alignment of signals, persistence of conditions, and erosion of trust.

Purpose of Decision Thresholds

- Decision thresholds exist to address a recurring failure in converged environments.
- Organizations often detect signals yet delay action while seeking confirmation. By the time certainty is achieved, available options have narrowed and operational disruption becomes unavoidable.
- Decision thresholds formalize when uncertainty itself becomes a risk condition.

Decision Principles

Decision thresholds within this framework adhere to the following principles:

- Decisions are triggered by conditions, not by single events
- Authority is established before escalation is required
- Safety and operational integrity are prioritized over convenience
- Early action preserves optionality
- Delay compounds consequence

Thresholds are intended to support judgment, not replace it.

Phase Based Decision Thresholds

Phase 1: Enterprise Exposure Accumulation

- **Threshold Condition**
    - Accumulated exposure exceeds organizational visibility or ownership capacity.
- **Decision Implication**
    - Leadership must determine whether operational complexity is being accepted knowingly or by default.
- **Required Decision**
    - Whether to pause expansion, consolidate exposure, or assign explicit ownership before further integration.

Phase 2: Initial Trust Breach

- **Threshold Condition**
    - Legitimate access occurs outside of historical or functional expectation while remaining policy compliant.
- **Decision Implication**
    - Trust can no longer be assumed to align with intent.
- **Required Decision**

    - Whether to increase scrutiny, restrict scope, or temporarily constrain access despite lack of confirmed impact.

Phase 3: Identity and Access Drift

- **Threshold Condition**
    - Effective access exceeds role clarity across domains.
- **Decision Implication**
    - Organizational authority has become ambiguous.
- **Required Decision**
    - Whether to realign privileges proactively or accept increased risk in favor of continuity.

Phase 4: OT Adjacent Visibility and Mapping

- **Threshold Condition**
    - Enterprise identities gain sustained visibility into operational environments without operational responsibility.
- **Decision Implication**
    - Operational knowledge has become decoupled from accountability.
- **Required Decision**
    - Whether to constrain visibility or redefine responsibility for operational insight.

Phase 5: Convergence Pivot

- **Threshold Condition**
    - Approved access paths enable interaction with operationally adjacent systems beyond defined maintenance or support windows.
- **Decision Implication**
    - The boundary between enterprise and operational environments no longer constrains influence.
- **Required Decision**
    - Whether to restrict pathways temporarily or accept reduced boundary assurance.

Phase 6: Operational Influence Establishment

- **Threshold Condition**
    - Incremental operational changes accumulate without clear attribution or consolidated review.
- **Decision Implication**
    - Confidence in operational integrity begins to erode.

- ❖ **Required Decision**
    - ➢ Whether to slow operations, increase validation, or escalate authority despite absence of overt failure.

Phase 7: Physical Process Impact

- ❖ **Threshold Condition**
    - ➢ Operational behavior deviates in ways that challenge confidence in safety, correctness, or predictability.
- ❖ **Decision Implication**
    - ➢ Risk extends beyond digital systems into physical consequence.
- ❖ **Required Decision**
    - ➢ Whether to prioritize integrity validation over continuity, even at the cost of disruption.

Authority and Timing

Decision thresholds are ineffective without clear authority. Organizations must define in advance:

- ➢ Who has authority to act at each threshold
- ➢ What tradeoffs are acceptable at each phase
- ➢ How decisions are communicated across IT, OT, and leadership

Authority established early reduces the likelihood of delayed action under pressure.

Use of Decision Thresholds

Decision thresholds are intended to:

- ➢ Enable earlier intervention without requiring certainty
- ➢ Support alignment between technical signals and executive action
- ➢ Reduce escalation friction during critical moments
- ➢ Shift response from reactive to deliberate

Decision thresholds support alignment between technical signals and executive authority. They provide a shared reference point that allows security, operations, and leadership to act cohesively rather than in parallel or in conflict. They reduce escalation friction during critical moments by pre establishing when action is expected, who holds authority, and what tradeoffs are acceptable. This clarity limits hesitation and prevents last minute decision making under pressure.

Decision thresholds also shift organizational posture from reactive response to deliberate intervention. Action is taken based on progression and persistence, not solely on confirmed impact.At their core, decision thresholds function as commitment points for leadership. They formalize when uncertainty itself is treated as a risk condition and when the organization chooses to act despite incomplete information.

Appendix A

Standards Mapping Overview

This appendix provides a conceptual alignment between the OT IT Convergence Kill Chain and widely adopted cybersecurity and industrial security standards. The purpose of this mapping is to support interpretation and integration. It is not intended to prescribe implementation, define compliance requirements, or replace existing standards.

Purpose of the Mapping

Cybersecurity and industrial security standards are designed to define outcomes, controls, and governance expectations. They establish what organizations should manage and protect. The OT IT Convergence Kill Chain addresses a different, complementary need. It provides a structured way to reason about how risk progresses across converged enterprise and operational environments over time, particularly when that progression relies on legitimate access, organizational structure, and accumulated trust rather than discrete technical failures. This mapping exists to help organizations place the kill chain within their existing standards based programs without disruption.

Conceptual Alignment

The mapping presented in this appendix is intentionally conceptual. It aligns kill chain phases with the intent and focus of existing standards rather than with specific clauses, controls, or technical requirements. This approach reflects how the framework is designed to be used in practice. The kill chain does not introduce new control requirements. It provides a lens through which existing controls can be evaluated for timing, effectiveness, and decision relevance. In particular, the mapping highlights where existing standards provide coverage and where they assume conditions that may no longer hold in converged environments.

Relationship to Existing Standards

The OT IT Convergence Kill Chain does not replace cybersecurity or industrial security standards. Standards such as NIST CSF, ISA IEC 62443, and NIST SP 800 82 define foundational expectations for governance, protection, detection, response, and recovery. These remain essential. The kill chain complements these standards by focusing on progression, failure modes, and decision points that emerge specifically from IT, cloud, and OT convergence. It is designed to be used alongside existing frameworks to enhance early recognition of risk and to support leadership decisions before operational impact occurs.

Use of the Mapping

Organizations may use this mapping to:

- ➢ Interpret existing control programs through a progression based lens
- ➢ Identify where controls are present but ineffective due to timing or governance gaps
- ➢ Support cross domain discussions between IT, OT, and leadership

- Inform risk scenarios and tabletop exercises
- Strengthen alignment between technical signals and executive decision making

The mapping should not be used as a compliance checklist or as evidence of control sufficiency.

Scope and Limitations

This appendix does not attempt to provide exhaustive mappings or detailed correspondence between standards and kill chain phases. Such mappings are context dependent and vary significantly by sector, architecture, and regulatory environment.

Appendix B

Conceptual Mapping to NIST Cybersecurity Framework 2.0

This appendix provides a conceptual alignment between the OT IT Convergence Kill Chain and the NIST Cybersecurity Framework 2.0. The mapping is intended to support interpretation and integration within existing CSF based programs. It does not imply control equivalence, compliance coverage, or implementation guidance.

NIST CSF defines what organizations should manage across governance, protection, detection, response, and recovery. The OT IT Convergence Kill Chain complements this by describing how risk conditions progress over time in converged IT, cloud, and OT environments.

OT IT Convergence Kill Chain Phase	Primary CSF Functions	Conceptual Alignment
Enterprise Exposure Accumulation	Govern, Identify	Governance gaps, unclear ownership, and incomplete asset understanding enable latent risk to accumulate before detection is possible
Initial Trust Breach	Protect, Detect	Legitimate access challenges preventive assumptions and requires detection informed by context and behavior
Identity and Access Drift	Govern, Protect	Privilege expansion reflects erosion of alignment between authority and responsibility
OT Adjacent Visibility and Mapping	Identify, Protect	Operational information becomes accessible without corresponding accountability or sensitivity controls
Convergence Pivot	Protect, Detect	Approved enterprise to operational pathways allow unintended influence across boundaries
Operational Influence Establishment	Detect, Respond	Subtle integrity degradation requires detection based on persistence and response readiness
Physical Process Impact	Respond, Recover	Leadership decisions focus on containment, recovery, and restoration of operational confidence

This alignment is intended to help organizations:

- Apply CSF functions across time rather than as static control domains
- Identify where CSF aligned controls exist but fail due to timing or governance gaps
- Support executive discussions on progression and early intervention
- Integrate convergence risk scenarios into CSF based risk management programs

The mapping should not be used to infer CSF compliance or control sufficiency.