

# Foundations of IT/OT for Measurement & Control Integrity: Backup & Recovery from Field to Back Office

Wayne Sallee

Octave

## Abstract

Backup and recovery in Information Technology and Operational Technology (IT/OT) environments is not only about preserving data. It is about preserving the trusted operating state of measurement and control systems from the field edge to the back-office. Natural gas measurement and control environments depend on the reliable interaction of field instrumentation, monitoring devices, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, historians, communication networks, and back-office measurement platforms. As these systems become increasingly interconnected, one of the most overlooked operational risks is the ability to preserve and recover the configurations, engineering logic, setpoints, calculations, data records, and system relationships that support trusted measurement and control (Stouffer et al., 2023).

This paper provides a foundational overview of IT/OT backup and recovery principles as they apply to measurement and control integrity. The discussion compares traditional IT backup practices with OT recovery requirements, including the challenges associated with proprietary device configurations, real-time control systems, field changes, communication dependencies, operational constraints, and safe return-to-service expectations.

Topics include the identification and prioritization of critical recovery assets such as field instrument configurations, flow computer parameters, RTU/PLC logic, SCADA applications, alarm and event records, historian databases, engineering workstation files, server images, and business-layer measurement systems. The paper also addresses Recovery Time Objective (RTO) and Recovery Point Objective (RPO) concepts in a measurement context, where recovery must account for operational continuity, measurement accountability, regulatory compliance, and validation before return to service (National Institute of Standards and Technology, n.d.-a, n.d.-b).

Common governance gaps include undocumented control system configuration baselines, inconsistent version control, unmanaged field changes, unclear backup ownership, and limited restore testing. Practical strategies are presented for establishing defensible backup practices and recovery validation methods that help confirm system integrity before systems and assets are returned to service.

## Key Takeaways

- Understand fundamental differences between IT and OT backup and recovery requirements.
- Identify critical configuration and data assets across the field-to-back-office continuum.
- Apply RTO/RPO concepts to measurement continuity, operational visibility, and recovery accountability.
- Recognize common governance gaps such as undocumented baselines, unmanaged changes, unclear ownership, and untested restores.
- Use recovery validation practices to confirm measurement and control integrity before returning systems and assets to service.

## 1. Introduction

Industrial measurement and control environments rely on a continuous chain of trusted data, configurations, logic, calculations, communications, and system relationships segmented via various network layers of the Industrial Control System (ICS) zones, managed within the Purdue Model. From field instruments and flow computers to RTUs, PLCs, SCADA systems, historians, databases, and back-office reporting platforms, each layer depends on the accuracy and recoverability of the layer before it. If any part of that chain is lost, corrupted, undocumented, overwritten, or unrecoverable,

an organization may struggle to restore safe operation, validate measurement accuracy, or reconstruct the operating state after an abnormal event.

In natural gas measurement and control environments, backup and recovery practices must therefore protect more than files and applications. They must generate an offline digital twin of the trusted configuration, calculation, logic, communication, and data relationships that support measurement accuracy, operational continuity, regulatory compliance, and safe return to service. A backup may capture data, but recovery requires the ability to restore a known-good operating condition and validate that the restored system reflects the intended measurement and control state.

This distinction is especially important in OT environments. In traditional IT systems, recovery is often measured by whether applications, servers, files, and user access have been restored. In OT environments, recovery is complete only when the restored system can be trusted to support safe operation, reliable control, accurate measurement, and return to service. This distinction is consistent with OT security guidance that emphasizes physical process impact, safety, availability, and reliability as defining characteristics of operational environments (Stouffer et al., 2023).

During a disruption, whether caused by equipment failure, physical damage, severe weather, cyber activity, unauthorized change, technology obsolescence, or human error, the organization must be able to answer practical questions: What was running? What changed? What was trusted? Which backup represents the approved operating state? What dependencies are required for restoration? What must be validated before the asset, system, or process is returned to service?

Based on field experience supporting industrial control system technologies, digitized OT asset programs, engineering work practices, and disaster recovery readiness efforts, this paper outlines practical considerations for protecting measurement and control integrity across the IT/OT stack. The central message is straightforward: backup and recovery programs should not be judged only by whether backup files exist. They should be judged by whether the organization can use those backups to confidently restore trust.

## 2. IT/OT Foundations in Measurement and Control

Natural gas measurement and control environments operate at the intersection of IT and OT. IT systems typically support business applications, databases, reporting, user access, enterprise connectivity, and data management. OT systems support the monitoring and control of physical processes, including field instrumentation, flow measurement, RTUs, PLCs, safety systems, SCADA platforms, historians, and operator interfaces. In measurement and control environments, these domains cannot be treated as fully separate because each layer depends on the accuracy, availability, and integrity of the layers beneath it (Stouffer et al., 2023).

In simple terms, IT manages information, while OT manages operation. A field device may measure pressure, temperature, flow, or gas quality. A flow computer or RTU may apply calculation logic and communicate values to SCADA. A historian or database may retain operational and measurement data. A back-office system may use that data for reporting, allocation, custody transfer support, compliance, or business decision-making.

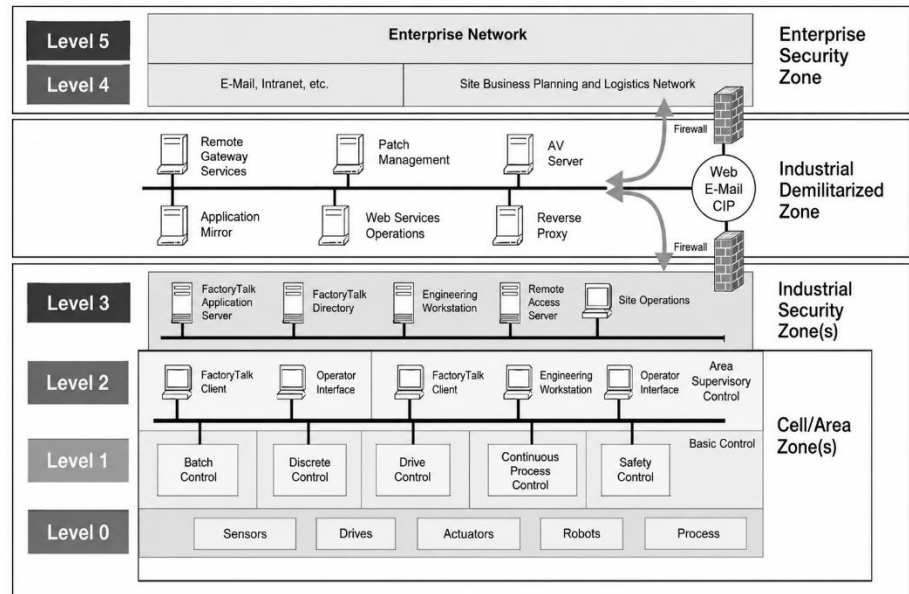


**FIGURE 1. The Purdue Model Segmented with an Industrial Demilitarized Zone (IDMZ).** Adapted from Securely Traversing IACS Data Across the IDMZ Design and Implementation Guide (p. 23), by Rockwell Automation & Cisco Systems, 2022. Copyright 2022 by Rockwell Automation, Inc. and Cisco Systems, Inc.

Although IT and OT environments may use similar technologies, their priorities are often different. IT environments generally prioritize data availability, application access, confidentiality, business continuity, and enterprise service restoration. OT environments prioritize safety, reliability, process stability, measurement accuracy, control continuity, and safe return to service. In OT, a restore point is only meaningful if the recovered system supports the intended operating state of the physical process.

Modern IT/OT governance has become a shared responsibility. Virtualization, domain services, segmented networks, remote access, historians, SCADA applications, and database-backed control systems can improve recoverability, but they also introduce dependencies on hypervisors, storage systems, authentication services, licensing, network segmentation, and documented restore procedures. Industrial automation and control system security guidance similarly treats secure operation as a lifecycle and cross-functional responsibility (International Society of Automation, n.d.; Stouffer et al., 2023).

| Layer                           | Examples                                                                                                                             | Backup and Recovery Relevance                                                                 |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Field instrumentation           | Transmitters, analyzers, meters, valves, Highway Addressable Remote Transducer (HART)/Fieldbus devices                               | Device parameters, calibration context, communication settings, firmware, configuration files |
| Measurement and control devices | Flow computers, RTUs, PLCs, DCS controllers, SIS controllers                                                                         | Calculation parameters, logic, I/O configuration, setpoints, interlocks, project files        |
| Supervisory systems             | SCADA, Human Machine Interface (HMI), operator stations, engineering workstations                                                    | Graphics, alarms, user settings, communication drivers, project files, software versions      |
| Data systems                    | Historians, SQL/Oracle databases, alarm/event databases                                                                              | Trend data, event records, measurement history, configuration history, transaction logs       |
| Infrastructure                  | Servers, virtual machines, network devices, domain services, remote access                                                           | Server images, snapshots, access control, network configuration, application dependencies     |
| Back-office systems             | Measurement reporting, accounting, compliance, Enterprise Asset Management (EAM) / Computerized Maintenance Management System (CMMS) | Reporting continuity, data reconciliation, audit records, asset hierarchy, workflows          |

TABLE 1. Measurement and Control System Layers

A mature approach should define which assets are critical, what configuration and data relationships must be preserved, where backups are stored, who owns them, how they are protected, what tools are required to restore them, and how the recovered state is validated before return to service.

### 3. Measurement and Control Integrity

Measurement and control integrity refers to the ability to trust that industrial measurement values, control strategies, calculations, configurations, communications, historical records, and system relationships accurately represent the intended operating state of the process. In natural gas environments, this integrity is essential because operational, commercial, safety, and compliance decisions are made from a connected chain of field data, control system logic, historian records, and business-layer reporting.

For backup and recovery, this integrity can be understood through five trust elements: configuration, calculation, logic, communication, and data relationships. Configuration includes setup, device settings, project files, and system definitions. Calculation includes formulas, meter factors, gas quality inputs, compensation values, and derived measurements. Logic includes control strategies, interlocks, function blocks, safety logic, sequences, permissives, and automation rules. Communication includes protocols, interfaces, addressing, polling structures, tag paths, and data exchange methods. Data relationships link field devices, flow computers, controllers, SCADA points, historians, alarms, reports, asset records, and back-office systems.

| Backup and recovery trust elements |
|------------------------------------|
| Configuration                      |
| Calculation                        |
| Logic                              |
| Communication                      |
| Data relationships                 |

FIGURE 2. Backup and Recovery Trust Elements.

Measurement integrity begins at the field level. Pressure, temperature, differential pressure, flow, level, density, gas composition, vibration, and other values may originate from transmitters, analyzers, meters, flow computers, RTUs, PLCs, DCS platforms, or specialized monitoring devices. A measurement value is only as

trustworthy as the configuration, calculation, and communication path supporting it. If a flow computer is restored from an outdated backup, or if a transmitter is replaced without restoring the correct configuration, the system may resume operation while producing questionable measurement results.

Control integrity refers to the ability to trust that control systems are operating according to the approved strategy, logic, configuration, and safe operating expectations of the facility. Restoring PLC, DCS, RTU, SIS, or flow computer files is only one part of the process; the organization must also confirm that the restored logic matches the approved baseline, that the correct version is used, that Input/Output (I/O) is mapped correctly, and that operations can safely return the system to service. Functional safety standards for the process industry emphasize lifecycle requirements for safety instrumented systems, reinforcing the need for disciplined validation when safety-related logic or configuration is restored (International Electrotechnical Commission, 2016).

Historians, alarm/event databases, Structured Query Language (SQL) or Oracle databases, and reporting platforms preserve operational context. They help teams review process trends, investigate abnormal conditions, evaluate key performance indicators, support measurement analysis, and reconstruct what occurred before, during, and after an event. If historical records are lost or restored incompletely, the organization may lose the ability to understand the event timeline or validate whether recovered systems are performing as expected.

Measurement and control integrity also depend on disciplined management of change. Changes to logic, configuration, setpoints, calculations, communication paths, historian tags, alarm limits, security settings, or reporting relationships should be traceable and aligned with approved work practices. In process environments, management of change is a recognized process-safety discipline for controlling changes that may affect safe operation (Occupational Safety and Health Administration, n.d.-a).

*The purpose of backup and recovery is not only to restore systems. It is to restore trust in the measurement and control environment.*

## 4. Field-to-Back-Office Architecture

A successful backup and recovery strategy depends on understanding the architecture that connects field devices, control systems, supervisory systems, data platforms, infrastructure, and business applications. In natural gas measurement and control, this architecture can be viewed as a field-to-back-office chain. Each layer creates, consumes, transforms, or stores information that may be required during recovery.

At the field level, instruments and devices generate measurement and operating data. At the control level, flow computers, RTUs, PLCs, DCS controllers, SIS platforms, vibration systems, turbine controls, and other automation platforms apply logic, calculations, alarming, and control strategies. At the supervisory level, SCADA, HMI, engineering workstations, historians, and application servers provide visibility, configuration, trending, and operator interaction. At both infrastructure and business layers, databases, reporting platforms, asset management systems, maintenance systems, and enterprise tools support analysis, compliance, accounting, planning, and decision-making.

This architecture matters because backup and recovery requirements exist across every layer. A facility may have strong server backups but weak controller project-file governance. It may have historian backups but incomplete field-device configuration records. It may have flow computer files but lack the software, communication path, or version history needed to restore them. Recovery confidence depends on the full chain, not only the most visible systems (Stouffer et al., 2023).

## Field-to-Back-Office Recovery Architecture

Recovery confidence depends on preserving both system files and the context needed to restore trusted operation.

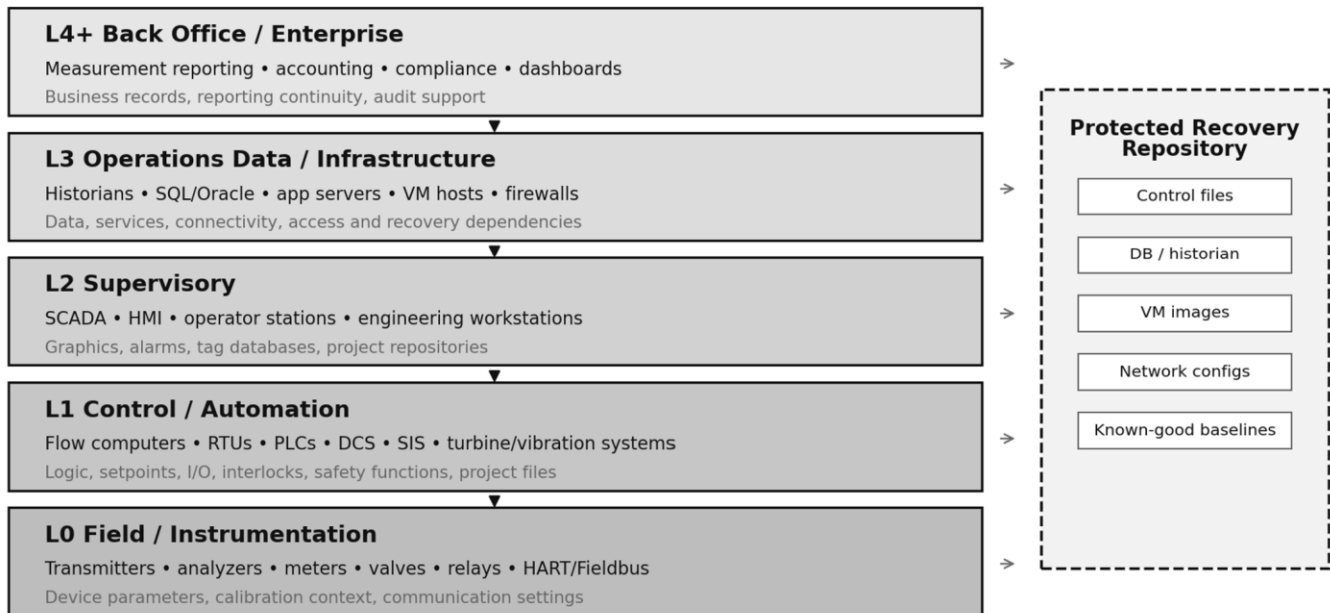


**FIGURE 3. Field-to-Back-Office Recovery Architecture, Back-Office Systems to Field Devices**

| Architecture Layer                            | Example Assets                                                                                                                              | Recovery Relevance                                                                                                           |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| L4+ Back-office and enterprise systems        | Measurement reporting, accounting, compliance systems, EAM/CMMS, enterprise dashboards                                                      | Business records, reporting continuity, audit support, asset hierarchy, decision support                                     |
| L3 Operations data and infrastructure systems | Historians, SQL/Oracle databases, alarm/event systems, application servers, virtual machines, switches, routers, firewalls, domain services | Trend data, event records, application databases, server images, network configurations, access records, system dependencies |
| L2 Supervisory systems                        | SCADA, HMI, operator stations, engineering workstations, configuration stations                                                             | Graphics, alarm configuration, operator interface files, application settings, project repositories                          |
| L1 Control and automation                     | Flow computers, RTUs, PLCs, DCS controllers, SIS controllers, turbine controls, vibration monitoring systems                                | Logic, setpoints, I/O configuration, control strategies, interlocks, safety logic, project files                             |
| L0 Field instrumentation                      | Transmitters, analyzers, meters, valves, relays, wireless devices, HART devices, Foundation Fieldbus devices                                | Device configuration, calibration context, communication settings, firmware, measurement parameters                          |

**TABLE 2. Field-to-Back-Office Architecture and Recovery Relevance**

Traditional IT visibility often focuses on servers, workstations, operating systems, databases, users, network devices, and enterprise applications. These are important, but they represent only part of the OT recovery picture. Much of the recovery-critical information exists below the traditional IT waterline, inside controllers, I/O modules, flow computers, field devices, instrumentation networks, safety instrumented systems (SIS), and proprietary automation platforms.

## OT Visibility Below the Waterline

Traditional IT visibility may see the platform; trusted OT recovery depends on the production-specific context below it.

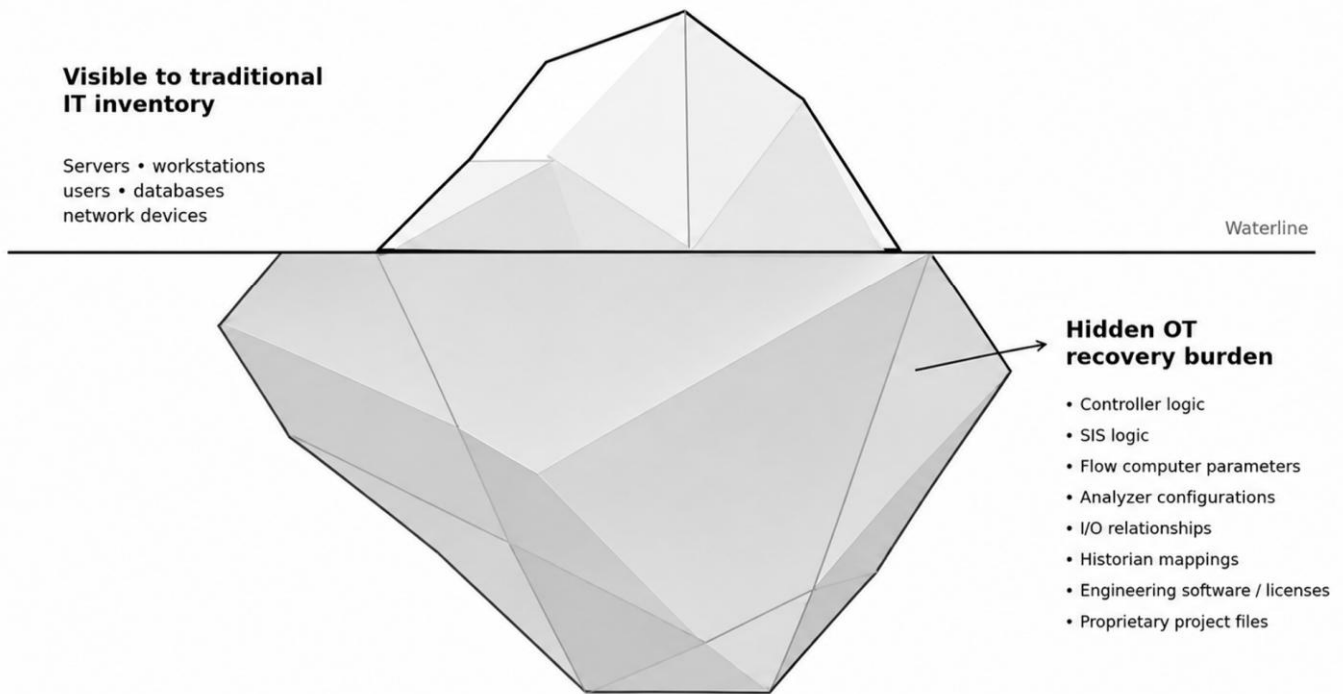


**FIGURE 4. OT Endpoint and Configuration Backup Visibility Below the Waterline**

Infrastructure systems provide the technical foundation that allows the OT environment to operate, communicate, and store information. Automation systems directly support measurement, control, safety, and process operation. Both categories are required for recovery. A historian may require both a database restore and correct tag/interface configuration. A PLC may require both a project-file backup and the correct engineering software version. A flow computer may require both calculation parameters and the communication pathway to SCADA.

Accurate inventory is also a recovery asset. The right inventory is not merely a list of devices. It is an operational map of hardware, software, firmware, I/O, communication paths, control strategies, configuration files, backup locations, and system relationships. Cybersecurity and resilience guidance similarly emphasizes asset inventory as a foundational capability for identifying known, unknown, and unmanaged assets (Cybersecurity and Infrastructure Security Agency, n.d.).

*A backup strategy is only as strong as its understanding of the architecture it is intended to recover.*

## 5. Backup Types Across the IT/OT Stack

In instrumentation and control environments, backup and recovery practices support one primary operational objective: returning a system, unit, asset, or process to a trusted and stable operating state following a failure, disruption, cyber event, equipment replacement, unintended configuration change, or disaster recovery scenario. Backups are not merely file copies. They are recovery assets that preserve logic, configuration, relationships, parameters, and system context.

Backups exist in many forms across instrumentation, control, measurement, SCADA, historian, infrastructure, and enterprise environments. A complete backup and recovery strategy should recognize that different systems produce different types of recoverable data and that each type may require a different collection, storage, validation, and restoration process. This layered approach is consistent with OT guidance that emphasizes the unique reliability, safety, and operational requirements of systems that monitor or control physical processes (Stouffer et al., 2023).

Control systems commonly rely on vendor-specific configuration files, project files, controller logic, graphics, databases, and engineering artifacts. These files may include control strategies, process parameters, I/O configuration, tag references, safety logic, alarm settings, setpoints, and tuning parameters. The practical question is not simply, Do we have a backup? The better question is whether the organization has the correct backup, in the correct format, tied to the correct asset, supported by the correct software, and validated against the intended operating state.

| System or Asset Type        | Representative Backup Form                                            | Recovery Consideration                                                                                      |
|-----------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| DCS                         | Engineering databases, project exports, tag databases, graphics files | Requires correct engineering environment, database restore process, software version, and compatibility     |
| PLC                         | Project files, ladder/function block logic, controller exports        | Requires programming software, firmware compatibility, controller model, and communication access           |
| SIS                         | Safety project files, logic libraries, configuration exports          | Requires validation, approval, and safety lifecycle discipline before return to service                     |
| Flow computers and RTUs     | Configuration files, calculation parameters, communication settings   | Requires device utility, communication path, calculation validation, and measurement review                 |
| HMI and SCADA applications  | Project files, graphics, tag databases, alarms, drivers               | Requires application software, server dependencies, graphics/tag validation, and historian/interface checks |
| Field devices and analyzers | Device parameters, calibration context, firmware, diagnostics         | Requires vendor utility, license or handheld tool, communications, and field validation                     |
| Network and infrastructure  | Switch/router/firewall configs, VLANs, AD/GPO, server images          | Restores connectivity, access, and system dependencies                                                      |

**TABLE 3. Representative OT Backup Forms and Recovery Considerations**

Database, historian, and alarm/event backups preserve data structures, transaction history, event records, trend records, and application configuration. Recovery may require more than restoring the database file; the application services, database engine, schema, user permissions, interfaces, patches, and server dependencies must also be restored or validated. This aligns with contingency planning guidance that emphasizes recovery strategies, testing, and dependent information system components (Swanson et al., 2010).

Image-based backups and virtual machine snapshots can preserve the operating environment around a control application, including operating system files, installed software, drivers, licensing components, local databases, user profiles, services, and system configuration. However, an image may not include later field changes, controller updates, modified setpoints, updated historian interfaces, or recent application configuration changes. Image-based recovery can restore the environment, but configuration-level backups confirm whether the environment reflects the intended control and measurement state.

One of the most important lessons across the IT/OT stack is that backup files alone are not enough. Restoration may require vendor engineering software, the correct software version, product-specific licenses, firmware compatibility, controller hardware compatibility, communication drivers, adapters, network access, user credentials, vendor documentation, trained personnel, and approved restoration procedures. Backup retention is not enough; organizations must also preserve restore capability.

| Concept                        | Traditional Meaning                        | Measurement and Control Interpretation                                                                                                        |
|--------------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Recovery Time Objective (RTO)  | How quickly a system must be restored      | How quickly measurement visibility, control capability, historian access, or reporting must return to support safe operation                  |
| Recovery Point Objective (RPO) | How much data loss can be tolerated        | How much configuration, measurement history, event data, logic change, or transaction history can be lost without compromising accountability |
| Known-good backup              | A usable backup from a prior point in time | A backup tied to an approved and validated operating baseline                                                                                 |
| Recovery success               | Server or application is restored          | The system is restored and validated as accurate, safe, and fit for service                                                                   |

**TABLE 4. RTO and RPO in Measurement and Control Context**

NIST defines RTO and RPO in the context of mission or business impact and the point in time to which data must be recovered after an outage (National Institute of Standards and Technology, n.d.-a, n.d.-b). In OT, these concepts must be interpreted alongside change management, version history, last known-good baselines, validation, and operational acceptance before return to service.

*A backup file is only valuable if the organization can identify it, protect it, restore it, and prove that it returns the asset or system to the intended operating state.*

## 6. E&I Work Practices and Repository Discipline

Effective backup and recovery depend not only on technology, but also on the work practices used by Engineering and Instrumentation (E&I), automation, control systems, operations, maintenance, vendors, and IT/OT support teams. Many critical recovery assets are created, modified, exported, or maintained by personnel working directly with field devices, controllers, safety systems, SCADA platforms, analyzers, relays, or engineering software. If those work practices are inconsistent, the official backup record may become incomplete, outdated, or difficult to trust.

Project files and configuration backups may be created during commissioning, troubleshooting, routine maintenance, turnaround work, capital projects, vendor support, or emergency response. The person making the change is often closest to the asset, but the recovery need belongs to the entire organization. If an updated file is not captured, versioned, documented, and stored in the proper repository, the organization may not be able to recover that change later.

Repository discipline means maintaining an official, governed location for backup files, configuration exports, project files, and known-good baselines. The repository may be an automated asset management platform, a dedicated configuration management system, a secured network location, a controlled document repository, or a disciplined manual structure. The purpose remains the same: to establish a trusted system of record.

- Which backup belongs to which asset?
- Which version is currently approved?
- Who created or modified it, and why?
- Was the change authorized and validated?
- Where is the file stored, and who may restore it?

*Engineering laptops are valuable tools, but they should not become the system of record for control strategy backups.*

A consistent check-in and check-out process is one of the most practical ways to maintain backup integrity. Before work begins, the technician or engineer should identify the current approved version of the project file or configuration record. After work is completed, the updated file should be saved, reviewed, versioned, checked back into the official repository, linked to the work order or management-of-change record, and validated where required.

Clear file naming and versioning standards are essential for recovery confidence. A repository should allow users to distinguish between a current approved project file, a temporary troubleshooting copy, an emergency rollback version, a vendor export, and an obsolete file. The goal is not simply to store files, but to make them understandable under pressure.

Transient devices such as E&I laptops, vendor laptops, and portable engineering workstations are often necessary, but they create risk when they become unofficial storage locations for critical backups. These devices should be treated as work tools, not permanent repositories. When a change is completed, the resulting file should be transferred into the governed backup process and linked to the affected asset.

Backup and recovery work practices should align with management of change. A configuration change that affects logic, measurement, control, alarming, safety, communication, historian mapping, or reporting should be documented in a way that supports future recovery. In process environments, management of change is a recognized process-safety discipline for controlling changes that may affect safe operation (Occupational Safety and Health Administration, n.d.-a).

*A backup that cannot be found, trusted, or restored is not a recovery asset.*

## 7. Backup Governance Gaps

Backup governance gaps often begin with a poor backup philosophy. Technology, staffing, and funding can strengthen a program, but they cannot compensate for unclear methodology, inconsistent work practices, weak ownership, or poor execution. A facility may own advanced tools and still have unreliable backups if personnel bypass the process, fail to check in project files, ignore version control, or do not validate recovery.

The most common governance failure is not simply the absence of a backup(s). It is an absence of confidence in the backup. A mature backup philosophy defines how backups are created, named, stored, protected, updated, tested, and restored. It also defines who owns each backup, which version is approved, where the official system of record resides, and how field changes become part of the recovery record.

One common failure is the floating file problem. A technician, engineer, vendor, or contractor may make a legitimate change using a field laptop, but the updated file remains only on that laptop or in a local folder. Multiple project files then exist across engineering workstations, technician laptops, shared folders, vendor devices, and outdated archives. During recovery, the organization may not know which file is current, approved, downloaded, temporary, or known-good.

| Governance Gap                           | Practical Consequence                                                                                            |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Poor backup philosophy                   | No consistent understanding of what should be backed up, where it should be stored, or how it should be restored |
| Unclear ownership                        | Personnel assume another group, vendor, or department is maintaining the backup record                           |
| Transient laptop dependency              | Latest project files exist only on field laptops, vendor devices, or unsupported workstations                    |
| Inconsistent naming and folder structure | Teams struggle to identify the correct backup during recovery                                                    |
| Weak version control                     | Approved, temporary, obsolete, and emergency files become difficult to distinguish                               |
| Lack of MOC alignment                    | Backup files do not reflect approved changes or known-good baselines                                             |
| Technology obsolescence                  | Backup files exist but cannot be opened or restored with available tools                                         |
| Untested restore procedures              | Backups are assumed to work but have never been proven                                                           |
| Local-only storage                       | Backups are lost when the workstation, server, laptop, or network segment fails                                  |
| Overreliance on vendors                  | The owner/operator lacks direct access to the official recovery record                                           |

**TABLE 5. Common Causes of Backup Governance Failure**

Funding and staffing matter, but lack of funding is not always the root cause of poor backup governance. A disciplined process can succeed even in a resource-constrained organization if it includes clear naming standards, defined folder structures, controlled access, backup logs, check-in/check-out discipline, preserved prior versions, periodic review, and restore testing. A well-funded program can still fail if the backup and recovery solution is not used, used incorrectly, or field changes remain outside the official backup record.

A strong backup philosophy should answer what the organization considers a critical backup, what the official system of record is, how a known-good backup is defined, how emergency changes are captured, how vendor-created files are transferred into owner/operator control, how backups are protected from the same failure domain as production systems, who has authority to restore systems, and what validation is required before return to service. This aligns with contingency planning guidance that emphasizes documented procedures, recovery roles, testing, and maintenance (Swanson et al., 2010).

*A backup program fails when it cannot prove which backup is trusted, where it resides, how it is restored, and whether it represents the intended operating state.*

## 8. Disaster Recovery Scenarios: Why Backup Integrity Matters

Backup and recovery practices are often discussed as routine maintenance activities, cybersecurity controls, or disaster recovery requirements. Their value becomes most visible during abnormal operating conditions, physical disasters, malicious activity, equipment failure, or major infrastructure loss. In these scenarios, the organization must quickly determine the last known-good state, which logic and configurations were active, which assets were damaged, which backups are trusted and restorable, and what must be validated before restart. These examples align with broader contingency planning and incident response guidance, which emphasizes preparedness, documented recovery procedures, testing, response coordination, and recovery effectiveness (Nelson et al., 2025; Swanson et al., 2010).

### Scenario 1: Storm Surge and Infrastructure Loss

In one representative scenario, a storm surge flooded a below-grade server room, damaging server cabinets, hardware, and supporting infrastructure. The event also affected portions of the control system environment, creating concern around operating logic, system state, and the ability to return safely to normal production. Physical replacement alone was not enough. Even when replacement hardware could be procured, recovery depended on restoring the correct operating environment, application state, database records, and control-system dependencies.

The facility benefited from coordinated database backup and recovery procedures and recent backups that included current operational changes. This reduced recovery time and supported safer production ramp-up. The scenario highlights the importance of protected backups outside the affected area, documented recovery ownership, current server and database backups, and validation of logic, setpoints, and application function before restart. CISA guidance similarly emphasizes offline, encrypted backups and regular testing of availability and integrity (Cybersecurity and Infrastructure Security Agency, 2023).

### Scenario 2: Internal Risk and Unauthorized Access

A second representative scenario involved trusted insider misuse or unauthorized post-employment access. During a transition period, remote access pathways were created or modified in a way that later allowed unauthorized access after employment ended. Operations personnel eventually observed abnormal process values, valve positions, pressure readings, gauge values, and operating thresholds. Investigation determined that unauthorized access had been used to manipulate control-related values.

The broader lesson is that weak change management, incomplete inventory visibility, and lack of trusted configuration baselines can delay detection and complicate recovery. A stronger process may have helped identify unauthorized account creation, access-policy changes, remote access modifications, abnormal configuration drift, and differences between the current operating state and the approved baseline. OT security guidance emphasizes access control, system monitoring, and configuration awareness in operational environments (International Society of Automation, n.d.; Stouffer et al., 2023).

*Recovery is difficult when the organization cannot prove what normal looked like before the event.*

### Scenario 3: Physical Damage and Field Asset Recovery

A third representative scenario involved an explosion that affected operating areas, field devices, and instrumentation assets. Although no fatalities or serious injuries occurred, the incident created immediate questions around damaged equipment, instrumentation replacement, control system recovery, and safe return to service. In fire, explosion, or equipment-loss events, recovery often requires replacing or recommissioning transmitters, valves, analyzers, controllers, I/O, junction boxes, marshalling cabinets, network devices, and supporting infrastructure.

The facility benefited from mature backup and recovery practices, including OT-relevant inventory, device tracking, and change management capabilities. These records helped identify affected assets, determine device types and locations, and support reimplementation against expected operating baselines. The lesson is that physical recovery depends on both system-level backups and field-level asset context. Organizations cannot confidently recover what they cannot identify, locate, configure, or validate (Cybersecurity and Infrastructure Security Agency, n.d.).

| Scenario                              | Primary Risk                                                             | Backup and Recovery Lesson                                                            |
|---------------------------------------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Storm surge or infrastructure damage  | Server room flooding, equipment loss, control system disruption          | Backups must be protected from the same event that damages production systems         |
| Insider misuse or unauthorized access | Configuration manipulation, abnormal operating values, delayed detection | Trusted baselines and change visibility are essential for detection and recovery      |
| Explosion or field asset damage       | Instrumentation loss, device replacement, recommissioning complexity     | Field inventory, device configuration, and control relationships must support restart |

TABLE 6. Summary of Scenario Lessons

## Operational Impact Lens: Establishing Operational Trust from Backup Integrity

The financial, operational, and safety impact of poor backup governance is best evaluated at the site or asset level. Broad loss estimates can be difficult to apply directly because each facility has different production value, process criticality, staffing, recovery maturity, and operational constraints. However, practical exposure is straightforward.

*Site-level recovery exposure = lost operating time + recovery labor + validation effort + measurement reconciliation + delayed return-to-service risk.*

| When Backup Integrity Fails                 | Practical Consequence                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Trusted backup cannot be found              | Additional downtime while teams search for the correct file, repository, or version history.                                                                                                                                                                                                                                        |
| Restore tools are unavailable               | Recovery is delayed while locating software, licenses, cables, drivers, or legacy workstations.                                                                                                                                                                                                                                     |
| Backup is stored in the same failure domain | Recovery assets may be encrypted, deleted, corrupted, or physically lost with production systems.                                                                                                                                                                                                                                   |
| Baseline cannot be proven                   | Teams must spend time comparing current logic, setpoints, communication paths, and field conditions.                                                                                                                                                                                                                                |
| Validation is incomplete                    | Operations may delay returning to service or accept additional measurement, safety, or reliability risk.                                                                                                                                                                                                                            |
| Cyber recovery depends on exposed backups   | CISA recommends offline, encrypted backups and regular testing; Dragos documented 1,693 ransomware attacks targeting industrial organizations in 2024, with 75% of incidents Dragos responded to leading to partial OT shutdown and 25% to full OT shutdown (Cybersecurity and Infrastructure Security Agency, 2023; Dragos, 2025). |

**TABLE 7. Backup Failures and Unintended Operational Impacts**

These calculations or failed measures do not require inflated global statistics. It asks a practical question: if a critical controller, analyzer, historian, SCADA server, or flow computer had to be restored today, how long would it take to identify the trusted backup, restore it, validate it, and return the system to normal operation?

Across all three scenarios, the common thread is that the organization must know what existed, what changed, what was trusted, what was damaged, and what can be safely restored. A backup may restore data, but only a governed recovery process can restore trust.

## 9. Recovery Validation Before Return to Service

A strong backup and recovery program improves the organization's ability to restore systems after a failure, disruption, or disaster recovery event. However, the existence of a backup, even a recent and well-governed backup, should not be taken as proof that the system is ready for safe operation. In measurement and control environments, restoration must be followed by validation.

A backup may restore a file, database, controller program, server image, or configuration record, but the organization must still confirm that the restored system accurately represents the intended field condition, control strategy, measurement state, and safe operating expectation.

# Backup-to-Validation Recovery Lifecycle

A restored system is not necessarily a trusted system

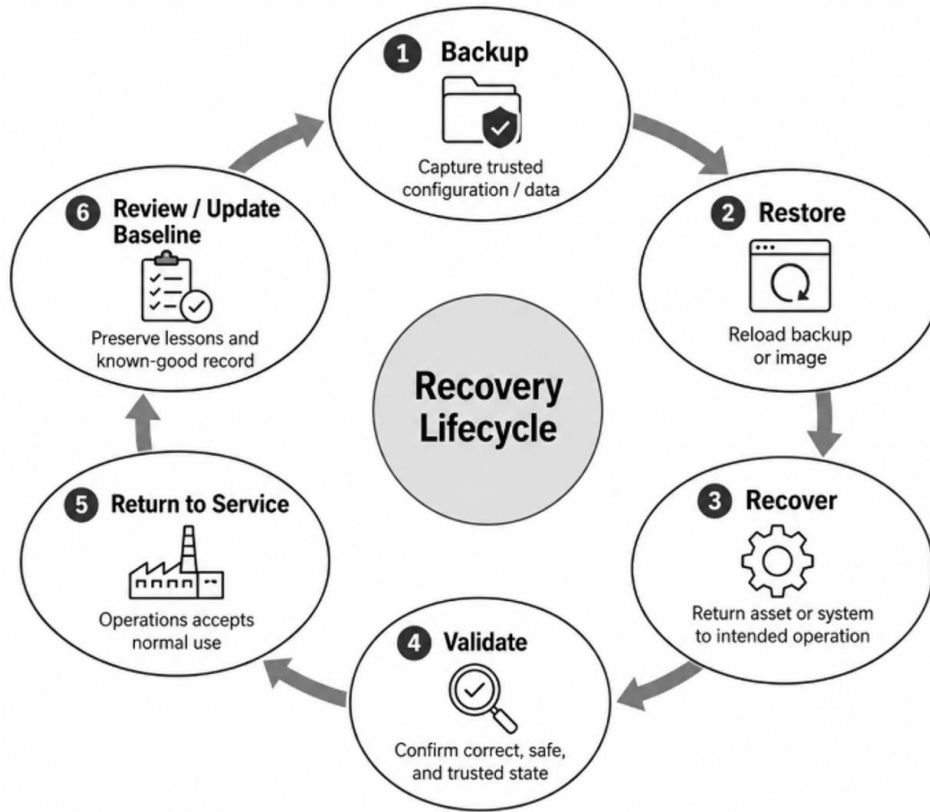


**FIGURE 5. Circular Backup-to-Validated-Recovery Lifecycle.**

| Step              | Meaning                                                                      |
|-------------------|------------------------------------------------------------------------------|
| Backup            | Capturing the configuration, logic, data, image, or file                     |
| Restore           | Reloading or reapplying the backup                                           |
| Recovery          | Returning the asset or system to intended operation                          |
| Validation        | Confirming that the recovered state is correct, safe, and trusted            |
| Return to Service | Operational acceptance and placing the validated system back into normal use |

**TABLE 8. Backup, Restore, Recovery, Validation, and Return to Service**

In practical terms, validation means comparing the restored digital representation against the expected field and operating condition. The values shown in a software interface, engineering tool, SCADA screen, historian display, analyzer program, flow computer configuration, or PLC/SIS logic file should be checked against what the field device, instrument, controller, or process is expected to represent.

If an analyzer program configuration is restored after equipment replacement or software recovery, the team should confirm that the analyzer program, measurement ranges, calibration context, communication settings, and reported values align with installed field equipment and process expectations. If a flow computer, SCADA application, PLC program, or safety logic file is restored, the organization should confirm that the correct version was loaded, that setpoints and calculation parameters

are appropriate, that I/O and communication paths are aligned, and that operations personnel accept the system before return to service. Safety-related restoration should follow appropriate lifecycle, testing, and validation expectations (International Electrotechnical Commission, 2016).

This approach is similar in philosophy to lockout/tagout practices used during physical maintenance and turnaround activities. Equipment is not reenergized simply because repair work appears complete; it is returned to service only after proper checks, clearances, and readiness confirmations. OSHA's lockout/tagout standard reinforces the importance of established procedures for controlling hazardous energy during service and maintenance activities (Occupational Safety and Health Administration, n.d.-b). The same discipline should apply to restored OT systems.

- The correct backup version was restored.
- The backup belongs to the correct asset, device, controller, or system.
- Critical setpoints, parameters, calculations, and logic are appropriate.
- Field values and software values align as expected.
- Communication paths to SCADA, historian, or reporting systems are functioning.
- Alarms, events, and operator visibility are restored where applicable.
- Operations, engineering, E&I, or responsible owners accept the system for return to service.

*A restored system is not necessarily a trusted system. Trust is established through validation before returning to service.*

## 10. Practical Backup and Recovery Maturity Model

A mature backup and recovery program begins with a well-defined philosophy. Technology can strengthen the process, but it cannot replace clear ownership, disciplined work practices, repeatable procedures, and validation. Even the best technical model(s) can become ineffective if the people expected to maintain it do not understand it, follow it, or trust it during abnormal operating conditions.

This is similar to alarm management philosophy in process operations. A site does not achieve effective alarm management simply by installing an alarm system. The organization must define how alarms are prioritized, categorized, rationalized, managed, reviewed, and improved over time. This lifecycle approach is consistent with alarm management guidance for the process industries (International Society of Automation, 2016). Backup and recovery require the same type of operating philosophy.

Maturity should not be judged solely by whether a site uses a specific commercial backup repository or automated change management platform. A facility with advanced tooling may be mature, but a facility with a disciplined manual process may also be mature if the process is well designed, consistently followed, and auditable. The key question is whether the organization has a reliable, repeatable, governed, and validated method for preserving and restoring the trusted operating state.

## Backup and Recovery Maturity Ladder

Maturity increases when backup practices become repeatable, governed, protected, validated, and resilient

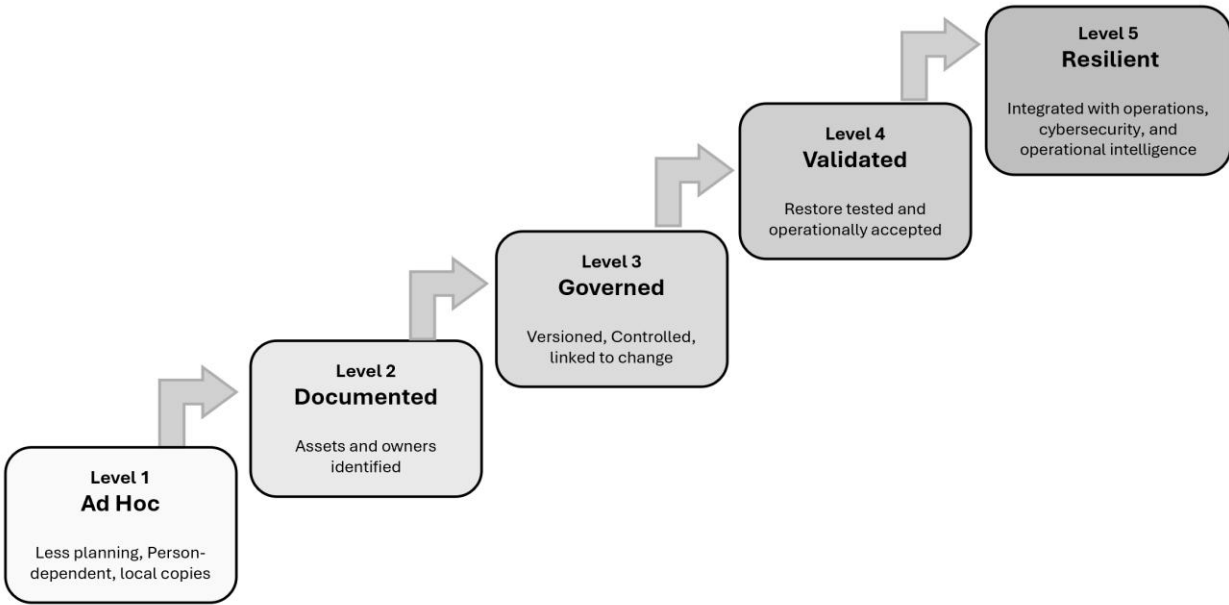


FIGURE 6. Backup and Recovery Maturity Ladder.

| Maturity Level       | Description                                                                                                        | Characteristics                                                              | Recovery Risk                                                     |
|----------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Level 1 — Ad Hoc     | Backups exist inconsistently and are often person-dependent                                                        | Files stored on laptops, shared drives, vendor devices, or old workstations  | High risk of missing, outdated, or incorrect backups              |
| Level 2 — Documented | Critical systems are identified and backup expectations are documented                                             | Asset list, backup owners, basic folder structure, manual logs               | Moderate risk if the process is not followed or tested            |
| Level 3 — Governed   | Backups are versioned, access-controlled, and tied to change management                                            | Naming standards, approval records, check-in/check-out, protected storage    | Reduced risk, but restoring confidence depends on validation      |
| Level 4 — Validated  | Backups are periodically tested against expected operating state                                                   | Restore tests, comparison to known-good baseline, operational signoff        | Lower risk: recovery confidence improves                          |
| Level 5 — Resilient  | Backup and recovery are integrated with data intelligence, cybersecurity, operations, measurement, and maintenance | Segmented/offline storage, role-based access, recovery drills, asset linkage | Lowest practical risk an organization can restore with confidence |

TABLE 9. Backup and Recovery Maturity Model

The most important message is that maturity is not defined by whether the process is automated or manual. Maturity is defined by whether the process is reliable, repeatable, governed, protected, validated, and sustainable. Contingency planning guidance similarly emphasizes documented recovery strategies, defined roles, testing, training, and plan maintenance as part of effective recovery readiness (Swanson et al., 2010).

*The best backup strategy is the one people actually follow — and the one the organization can prove works.*

## 11. Network Segmentation and Protected Backup Storage

Network segmentation and protected backup storage are important components of a mature backup and recovery strategy. In OT environments, segmentation is often discussed in the context of cybersecurity, access control, and network governance. However, segmentation also plays a direct role in recovery survivability. A backup strategy is incomplete if the backup can be lost, encrypted, corrupted, deleted, or destroyed by the same event that compromises the production system.

Modern industrial control system architectures increasingly use structured network segmentation to separate business systems, industrial demilitarized zones, SCADA and historian environments, control networks, safety systems, vendor access pathways, and field-device communication layers. These controls support cybersecurity and access governance, but they also help define where recovery assets should reside and how they should be protected. OT security guidance commonly emphasizes segmentation, controlled access, and architecture design as methods for reducing risk in connected operational environments (International Society of Automation, n.d.; Stouffer et al., 2023).

*The purpose of segmentation in backup and recovery is not only security. It is survivability.*

A common weakness occurs when backups are stored within the same failure domain as the system they are intending to recover. A failure domain may be physical, logical, or administrative: the same server, disk volume, workstation, network segment, user credential path, server room, storage array, or access group. If ransomware, insider misuse, fire, flood, disk failure, or accidental deletion affects both the production system and its backup, the backup may no longer function as a recovery asset.

- Backups should *not* reside only on the same server, disk, storage volume, or engineering workstation.
- Backups should *not* be writable or erasable from compromised production accounts.
- Backups should *not* exist only in the affected room, cabinet, site area, or network segment.
- Backup modification and deletion rights should be *limited, logged, and reviewed*.
- Owner/operators *should* retain the official backup record when vendors or contractors transition.

A protected repository should provide a clear and trusted location for critical backup assets, including control system project files, flow computer configurations, analyzer files, relay settings, SIS logic, PLC programs, SCADA applications, historian backups, SQL or Oracle backups, virtual machine snapshots, server images, and engineering workstation recovery files. CISA ransomware guidance similarly emphasizes offline, encrypted backups and regular testing of backup availability and integrity in disaster recovery scenarios (Cybersecurity and Infrastructure Security Agency, 2023).

Backup repositories should not be open file shares where any user can modify, overwrite, delete, or move critical recovery files. Access should be aligned with job responsibility, operational need, and recovery authority. Strong access control reduces the risk of accidental deletion, unauthorized modification, malicious activity, or confusion over who is allowed to restore critical systems.

Database, historian, and image backups require special attention because they may contain operational history, alarm and event records, measurement data, reporting relationships, configuration records, and application dependencies. If these backups remain only on the same production server or storage array, they may be lost during a disk failure, ransomware event, server compromise, or physical disaster.

*In OT environments, backup storage location is part of the recovery strategy.*

## 12. Technology Obsolescence as a Recovery Risk

Technology obsolescence is an often-overlooked recovery risk in measurement and control environments. Many industrial facilities continue to operate legacy systems because those systems perform a specific task reliably, support a critical process, or depend on vendor software that is difficult to replace. In these cases, the system may continue to provide operational value even after the operating system, hardware, software, drivers, or vendor support have reached end-of-life.

From a backup and recovery perspective, the risk is not only that the system is old. The greater risk is that the organization may have backup files but no longer have the practical ability to restore them. OT security guidance recognizes that industrial environments often include legacy systems, long equipment lifecycles, and vendor-specific dependencies that affect security, maintenance, and recovery planning (Stouffer et al., 2023).

- A legacy operating system
- Vendor-specific engineering software
- A license tied to old hardware
- A serial communication adapter or proprietary cable
- A database version or driver that no longer operates on modern systems
- A workstation image that cannot be restored to replacement hardware
- A technician or vendor who understands the legacy restore process

*The organization may possess the backup file, but not the ecosystem required to use it.*

For example, an industrial facility may operate a critical process using legacy servers or workstations because those systems support a dedicated production function. If one or more systems fail and no tested replacement image, spare server, virtual conversion, or recovery procedure exists, the organization may spend days locating hardware, reinstalling obsolete software, restoring network settings, reloading applications, and validating communication. Production may remain offline even though backup files technically exist.

A similar issue can occur in gas measurement and analyzing environments. A gas analyzer, meter-reading system, flow computer utility, or calibration workstation may depend on older software, an obsolete operating system, or a specific communication method. If the configuration is backed up but the site no longer has the software, license, cable, driver, or compatible workstation required to reload it, the backup may not support timely recovery.

Technological obsolescence can also affect image-based recovery. A server image or virtual snapshot may preserve operating system and application files, but it may not fully preserve hardware dependencies, licensing behavior, communication cards, serial interfaces, or field connectivity. The image may be restored successfully in a technical sense but still fail to communicate with field equipment or application dependencies.

- Can the backup still be opened?
- Can the software still be installed and licensed?
- Is compatible hardware, cabling, adapter, and driver support available?
- Has the restore process been tested?
- Is there a replacement or virtualization strategy?
- Does the restored system still communicate with field equipment?
- Has the recovered system been validated before returning to service?

*Backup retention is not enough. Organizations must also preserve restoration capability.*

## 13. Conclusion and Practical Checklist

Backup and recovery in natural gas measurement and control environments must be understood as more than a technical file-management activity. These practices support measurement accuracy, control reliability, operational continuity, regulatory confidence, and safe return to service. A backup may preserve data, logic, configurations, images, or project files, but the true value of that backup is realized only when the organization can use it to restore a trusted operating state.

Throughout the IT/OT stack, critical recovery information may reside in many locations and formats. Field devices may contain measurement parameters and calibration context. Flow computers, RTUs, PLCs, DCS controllers, and safety systems may contain logic, setpoints, I/O relationships, calculation parameters, and control strategies. SCADA systems, historians, databases, engineering workstations, network devices, and back-office reporting platforms may contain operational data, event records, configuration history, and system relationships needed to understand and recover the process.

The central lesson is that recovery confidence depends on more than the existence of backup files. It depends on whether those files are current, protected, traceable, restorable, and validated. It also depends on whether the organization has the software, licenses, hardware, communication paths, personnel, procedures, and governance required to use those backups under real recovery conditions.

*A backup may restore data, but only a governed recovery process can restore trust.*

| Area                                 | Key Questions                                                                                                                                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Asset and system identification      | Have critical measurement and control assets been identified? Are field devices, controllers, SCADA, historians, databases, and back-office dependencies included? Is there accurate inventory of hardware, software, firmware, I/O, network, and communication dependencies? |
| Backup scope and content             | Are logic, configurations, setpoints, calculations, I/O relationships, alarms, graphics, historian mappings, reporting dependencies, flow computer parameters, analyzer files, and field-device parameters preserved where applicable?                                        |
| Repository and version control       | Is there an official system of records? Are backups asset-linked, versioned, timestamped, protected from overwrite, and able to distinguish approved, temporary, obsolete, and emergency versions?                                                                            |
| E&I and field work practices         | Do engineers, technicians, vendors, and contractors follow check-in/check-out discipline? Are field changes captured after work is completed and linked to work orders or MOC records?                                                                                        |
| Protected storage and access control | Are backups stored outside the same failure domain? Are read, write, delete, and restore permissions controlled? Are repositories segmented, encrypted, offline, offsite, or otherwise protected where appropriate?                                                           |
| Restore capability                   | Can the organization still open, interpret, and restore the backup files? Are required software versions, licenses, drivers, cables, adapters, hardware, and legacy dependencies available?                                                                                   |
| Recovery validation                  | Does the restored state belong to the correct asset and align with expected field conditions? Are SCADA, historian, alarm, reporting, and operator visibility functions validated before acceptance?                                                                          |

TABLE 10. Practical Backup and Recovery Checklist

Backup and recovery programs are strongest when they preserve both the technical file and the operational meaning behind the file. In measurement and controls environments, the goal is not simply to bring systems back online. The goal is to restore confidence that the recovered system accurately reflects the intended process, measurement, control, and safety condition.

*The purpose of backup and recovery is not only to restore systems. It is to restore trust in the measurement and control environment.*

## References

- Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity performance goals: Asset inventory. U.S. Department of Homeland Security. <https://www.cisa.gov/cybersecurity-performance-goals>
- Cybersecurity and Infrastructure Security Agency. (2023). StopRansomware guide. U.S. Department of Homeland Security. <https://www.cisa.gov/stopransomware/ransomware-guide>
- Dragos. (2025). Dragos's 8th annual OT cybersecurity year in review is now available. <https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available>
- International Electrotechnical Commission. (2016). IEC 61511-1:2016: Functional safety—Safety instrumented systems for the process industry sector—Part 1: Framework, definitions, system, hardware and application programming requirements.
- International Society of Automation. (n.d.). ISA/IEC 62443 series of standards. <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
- International Society of Automation. (2016). ANSI/ISA-18.2-2016: Management of alarm systems for the process industries.
- National Institute of Standards and Technology. (n.d.-a). Recovery point objective. Computer Security Resource Center Glossary. [https://csrc.nist.gov/glossary/term/recovery\\_point\\_objective](https://csrc.nist.gov/glossary/term/recovery_point_objective)
- National Institute of Standards and Technology. (n.d.-b). Recovery time objective. Computer Security Resource Center Glossary. [https://csrc.nist.gov/glossary/term/recovery\\_time\\_objective](https://csrc.nist.gov/glossary/term/recovery_time_objective)
- Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-61r3>
- Occupational Safety and Health Administration. (n.d.-a). 29 CFR 1910.119—Process safety management of highly hazardous chemicals. U.S. Department of Labor. <https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119>
- Occupational Safety and Health Administration. (n.d.-b). 29 CFR 1910.147—The control of hazardous energy (lockout/tagout). U.S. Department of Labor. <https://www.osha.gov/control-hazardous-energy>
- Rockwell Automation & Cisco Systems. (2022). *Securely Traversing IACS Data Across the IDMZ: Design and Implementation Guide* (Publication ENET-TD009G-EN-P). Rockwell Automation.
- Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-34r1>