



CROSSROADS • ISSUE 6 • OCTOBER 5, 2026 • ~16 MIN READ

Backups Are Not Recovery: Building a Recovery Process That Actually Works in OT and ICS Environments

1. A backup file is not a recovery capability
2. Recovery starts with knowing what you have
3. Determine what actually needs to be backed up
4. The latest backup matters
5. Recovery instructions are as important as the backup
6. Technology changes; instructions must change with it
7. Test the procedure, not just the backup job
8. What could force an organization to recover?
9. Real incidents show why this matters
10. Build a recovery matrix
11. Recovery priority matters
12. Seven questions a backup program should answer
13. Final thought and field takeaway
14. Sources

A backup file does not mean an organization can recover.

A backup file is not a recovery capability

That distinction becomes especially important in Operational Technology (OT) and Industrial Control System (ICS) environments, where recovering a system can involve far more than restoring files to a server.

A Control Center may depend on dozens of interconnected servers, databases, network devices, authentication services, virtualization platforms, communication systems, and security appliances. A transmission substation or generating facility may contain protective relays, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human Machine Interfaces (HMIs), switches, firewalls, gateways, and other devices whose configurations may be difficult — or sometimes impossible — to recreate quickly.

When one of those systems fails, organizations need more than a backup. They need a tested recovery capability.

NIST reinforced this concept on June 17, 2026 with the release of [NIST SP 1339, OT Backup Quick Start Guide](#)¹, which states that effective OT backup management involves integrating backups into the change and risk management processes, creating them regularly, testing them, and reviewing them during recovery exercises — starting with identifying the assets that require backups.



For electric utilities subject to NERC CIP, the concept is also well established in [CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems](#)², which addresses documented recovery plans, backup information, recovery testing, and maintenance of those plans as technologies and responsibilities change.

Version note. CIP-009-6 is the version in effect today. NERC's [Weekly Regulatory Updates \(September 28, 2026\)](#)³ lists CIP-009-7.1, part of the virtualization revisions, with a U.S. effective date of July 1, 2028.

But meeting a regulatory requirement should not be the end goal. The real question is much simpler:

If this system disappeared tonight, could your organization rebuild it tomorrow?

Recovery starts with knowing what you have

One of the most important parts of a recovery program happens before a backup is ever created. The organization must identify the systems supporting the operational environment and understand their dependencies. For many utilities and industrial organizations, that inventory extends across several layers.

Control Centers

Control Centers can contain some of the most complex recovery dependencies within an OT environment. Systems may include:

- Energy Management Systems (EMS)
- SCADA servers
- Distribution Management Systems
- Generation management systems
- Historians
- Operator workstations
- Engineering workstations
- ICCP servers
- Application servers
- Database servers
- Active Directory or other authentication infrastructure
- DNS and time synchronization systems
- Patch-management infrastructure
- Antivirus or endpoint-security management servers
- Logging and SIEM infrastructure
- Electronic Access Control or Monitoring Systems
- Firewalls
- Routers and switches
- Remote-access infrastructure
- Virtualization platforms
- Storage platforms



Recovering the SCADA application while overlooking the database, authentication system, licensing server, virtual infrastructure, or network configuration it depends on may still leave operators without a functional system. That is why recovery planning must identify systems and dependencies, not simply individual computers.

Data Centers and virtual infrastructure

Modern OT environments increasingly depend on virtualized systems hosted within centralized or regional Data Centers. That creates another layer of recovery considerations. Backing up a virtual machine is valuable, but organizations should also understand what would be required if the underlying infrastructure were lost. Recovery may depend upon:

- VMware ESXi or other hypervisor configurations
- vCenter or management platforms
- Storage configurations
- Virtual switches
- VLAN assignments
- Network interfaces
- Backup infrastructure
- Authentication services
- Certificates
- Licensing
- Firewall rules
- DNS
- NTP
- SAN or NAS configurations

A perfectly valid SCADA virtual-machine backup may provide little value if the organization cannot rebuild the platform required to run it. Recovery planning should therefore examine the infrastructure underneath the application, not only the application itself.

Do not forget the field devices

One of the largest gaps in traditional backup programs can occur outside the Data Center. OT environments contain hundreds or thousands of devices whose configurations may be essential to restoring operations.

[NIST SP 1339⁴](#) specifically names PLCs, switches, firewalls, transmitters, actuators, DCS components, SCADA servers, VFDs, and HMIs as examples of OT assets to identify for backup. For an electric utility, the list may extend further:

- Protective relays
- RTUs
- Substation gateways
- PLCs
- Intelligent electronic devices
- Managed Ethernet switches



- Routers
- Firewalls
- Serial gateways
- Protocol converters
- Automation controllers
- Station HMIs
- Engineering workstations
- Telecommunication devices

Consider a failed substation firewall:

- Does the organization have the latest configuration?
- Does it know the exact hardware model and firmware version?
- Are certificates required?
- Are VPN configurations documented?
- Are interfaces, routing tables, access-control rules, NAT rules, objects, services, and security policies included?
- Could a replacement firewall be installed and configured by someone other than the engineer who originally deployed it?

Those questions determine whether a configuration backup is truly a recovery capability.

Determine what actually needs to be backed up

Different systems require different types of recovery information. There is rarely one universal backup approach for an OT environment.

System	Recovery information typically required
Server	Full image, operating-system configuration, application installation packages, databases, licenses, certificates, and configuration files
PLC	Current logic program and the associated engineering project
Firewall	Running configuration, firmware information, licenses, certificates, security policies, objects, interfaces, VPN parameters, and routing configuration
Network switch	Configuration, VLAN assignments, trunk configuration, access ports, spanning-tree settings, authentication configuration, and firmware information
Protective relay	Latest approved relay settings and associated configuration files

The objective should be to answer one question:

What information would be required to take replacement hardware or a clean system and return it to its approved operational state?

That information becomes the true recovery package.



The latest backup matters

Having a backup is not necessarily sufficient. Organizations also need to determine whether they have the right backup from the right point in time.

Suppose a firewall configuration was backed up six months ago. Since then, new substations were commissioned, network routes changed, access-control rules were modified, certificates were replaced, VPN tunnels changed, and firmware was upgraded. The six-month-old backup may technically be valid, but restoring it could recreate a configuration that no longer matches the operational environment.

This is where backup management and change management should intersect. When significant configuration changes occur, organizations should determine whether a new backup should be generated as part of the change. [NIST SP 1339⁴](#) specifically recommends using the organization's change-management process to review and approve backup-impacting changes. That creates a straightforward lifecycle:

1. Change
2. Validate
3. Approve
4. Implement
5. Verify
6. Backup
7. Update recovery documentation

That final backup step can prevent an organization from discovering during an emergency that its most recent recoverable configuration predates several major changes.

Recovery instructions are just as important as the backup

Imagine having the latest PLC program but nobody knows which engineering software version is required to load it. Or having a server image but discovering during recovery that the application requires a license key stored on the failed server. Or having the correct firewall configuration but discovering that the replacement firewall is running firmware that cannot accept it.

This is why recovery instructions should accompany critical backups. Depending on the system, recovery documentation may need to identify:

- Required hardware
- Required firmware
- Operating-system version
- Required software
- Engineering software version
- Software installation order
- Licensing requirements
- Certificate requirements
- Service accounts
- Required network connectivity
- IP addressing



- Dependencies
- Backup location
- Restoration procedure
- Validation steps
- Expected communications
- Cybersecurity controls that must be restored
- Responsible personnel
- Vendor support contacts
- Escalation procedures

The documentation should be written so that a qualified individual who did not originally build the system can reasonably execute the recovery. If recovery relies entirely on one engineer remembering how something was installed five years ago, the organization's recovery capability has a single point of failure.

Technology changes. Recovery instructions must change with it.

One of the biggest dangers with recovery documentation is that it ages quietly. The document may still exist. The backup may still exist. The instructions may even look correct. But the environment surrounding them has changed:

- A server may have moved from physical hardware to VMware, and VMware may since have been upgraded.
- Windows Server may have changed versions, and the application may have been upgraded.
- The firewall vendor may have changed.
- Authentication may have moved to a new Active Directory environment.
- The backup repository may have changed, and a service account may no longer exist.
- The engineer named in Step 4 may have left the company three years earlier.

This is one reason recovery documentation must be treated as a living operational document, not something produced for an audit and forgotten.

CIP-009-6² explicitly addresses this problem. For applicable systems, a representative sample of recovery information must be tested to confirm it remains usable and compatible with current configurations, and the plan must be updated when changes to roles or responsibilities, responders, or technology affect the organization's ability to execute it. The standard's technical guidance further explains that testing should provide assurance that recovery information is usable and current.

That is an important distinction:

A backup test should not simply prove that a file can be opened. It should help demonstrate that the information can actually be used to recover the system.

Test the procedure, not just the backup job

Many organizations can demonstrate that a backup job completed successfully. That answers one question: did the backup software copy something? It does not answer the more important one: can we use what was copied to restore the system?

Testing should periodically move beyond backup-job success messages. Depending on operational risk and available test environments, organizations can conduct, roughly in order of increasing assurance:



1. Documentation reviews
2. Tabletop exercises
3. Representative backup validation
4. Configuration restoration
5. Virtual-machine restoration
6. Isolated laboratory recovery
7. Bare-metal recovery
8. Simulated hardware replacement
9. Full recovery exercises

CIP-009-6 testing requirement	Applies to	Minimum interval
Test each recovery plan (R2.1)	High impact BCS; medium impact BCS at Control Centers	Once every 15 calendar months
Test a representative sample of recovery information for usability and compatibility with current configurations (R2.2)	High impact BCS; medium impact BCS at Control Centers	Once every 15 calendar months
Operational recovery exercise in an environment representative of production (R2.3)	High impact BCS	Once every 36 calendar months, subject to the standard's provisions

Source: [NERC CIP-009-6](#)². Even organizations outside the formal applicability of CIP-009 can benefit from the same principle: recovery should be exercised before the emergency.

What could force an organization to recover?

Recovery procedures should not be designed exclusively around ransomware. There are many circumstances in which an organization may suddenly need its recovery documentation and most recent backup.

- Ransomware or destructive malware. Servers, workstations, databases, or shared infrastructure could become encrypted or otherwise unusable. CISA's [#StopRansomware Guide](#)⁵ recommends maintaining offline, encrypted backups and regularly testing their availability and integrity, because many ransomware variants attempt to find and delete or encrypt accessible backups.
- Failed security patch or software upgrade. A patch intended to reduce cybersecurity risk may unexpectedly prevent an OT application or supporting service from functioning correctly.
- Firmware upgrade failure. A router, firewall, PLC, switch, or other OT device could fail during a firmware upgrade and require replacement or reconfiguration.
- Hardware failure. Servers, storage arrays, firewalls, routers, industrial computers, controllers, and network switches eventually fail.
- Configuration error. An engineer could accidentally deploy a configuration that interrupts communications or makes a device unreachable.
- Database corruption. SCADA, historian, or application databases can become corrupted and require restoration.
- Virtualization failure. A hypervisor, management platform, or storage failure can affect multiple critical applications simultaneously.
- Cybersecurity containment. Incident responders may intentionally isolate, wipe, or rebuild systems after discovering that an attacker obtained privileged access.



- Physical disaster. Fire, flooding, hurricane damage, electrical failures, cooling failures, or other facility events can damage technology supporting Control Center or Data Center operations.
- Device replacement. A failed relay, RTU, PLC, firewall, switch, or gateway may need to be replaced rapidly with available spare hardware.

In every one of these scenarios, the recovery team benefits from having both current recovery information and tested instructions.

Real incidents show why this matters

The risk is not theoretical.

Norsk Hydro, 2019. The global aluminum producer was hit by a targeted ransomware attack, reported as the LockerGoga variant, that disrupted operations across its enterprise. Some operations reverted to manual methods while systems were restored, and the company did not pay the ransom ([WIRED](#)⁶). The incident became an important industrial cybersecurity example of the value of resilience, manual operating capability, and recoverable systems.

City of Tulsa, 2021. A [CISA SAFECOM-NCSWIC meeting summary](#)⁷ recounts that responders had to shut down the city's backup system as part of mitigation, which made restoring and rebuilding systems from backups more difficult. Participants emphasized backup redundancy and training personnel to use backup plans when networks are compromised.

Colonial Pipeline, 2021. After the DarkSide ransomware attack, CISA and the FBI's joint advisory [AA21-131A](#)⁸ urged critical infrastructure owners to segment IT and OT networks, regularly test manual controls, implement frequent backups on both IT and OT networks, test those backups regularly, and isolate them from network connections that could enable the spread of ransomware.

These incidents illustrate an important point: during a major cyber event, the normal infrastructure used to perform recovery may itself be unavailable or untrusted. Recovery procedures should account for that possibility.

Build a recovery matrix

One practical approach is to maintain a recovery matrix for critical systems. The illustrative example below shows the shape; the exact structure will vary by organization.

SCADA server

Criticality	Critical
Backup required	VM + database + configuration
Backup frequency	Daily
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested



OT firewall

Criticality	Critical
Backup required	Full configuration
Backup frequency	After approved changes
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested

Substation RTU

Criticality	High
Backup required	Configuration / database
Backup frequency	After approved changes
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested

Managed switch

Criticality	High
Backup required	Running configuration
Backup frequency	After approved changes
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested

Engineering workstation

Criticality	High
Backup required	Image + software + project files
Backup frequency	Defined interval
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested



PLC

Criticality	Critical
Backup required	Logic + engineering project
Backup frequency	After approved changes
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested

Protective relay

Criticality	Critical
Backup required	Approved settings
Backup frequency	After approved changes
Recovery documentation	Yes
Last backup	Current
Last restore test	Tested

The matrix forces several questions to be answered: What is critical? What needs to be backed up? How frequently? Where is it stored? Who owns it? When was it last updated? And most importantly:

When was someone last able to prove that it could be restored?

Recovery priority matters

During a major incident, everything cannot always be restored simultaneously. Organizations should establish a recovery sequence based on operational dependencies. For example:

1. Infrastructure
2. Authentication
3. Networking
4. Core SCADA services
5. Databases
6. Operator applications
7. Supporting applications

The actual sequence will differ by environment. A Control Center may need DNS and authentication before several applications can function. A SCADA application may require its database. A historian may depend on communications infrastructure. A firewall configuration may have to be restored before systems can communicate. Understanding these dependencies before an incident can dramatically reduce recovery time.

CISA's [#StopRansomware Guide](#)⁵ similarly recommends prioritizing restoration based on a predefined critical-asset list that includes the systems those critical services depend on.



A backup program should answer seven questions

A mature OT recovery program should be able to answer:

1. What do we need to recover?
2. Where is the latest approved recovery information?
3. Is that information protected from the incident we are recovering from?
4. What systems must be recovered first?
5. What dependencies must exist before recovery can begin?
6. Who knows how to perform the recovery?
7. When did we last prove that the process works?

If any of those answers are unknown, the organization may have backups — but it may not yet have reliable recovery capability.

Final thought: the worst time to test recovery is during the incident

The value of a recovery plan is difficult to measure on a normal day. Everything is operational. The SCADA system is communicating. The servers are running. The firewalls are forwarding traffic. The PLCs are controlling the process.

Then something fails.

At that moment, the organization's backup and recovery program stops being documentation and becomes an operational capability.

The organizations that recover most effectively will not necessarily be those with the most expensive backup platform. They will be those that have identified what matters, captured the information needed to rebuild it, protected that information, documented the recovery process, tested the process, corrected what did not work, and repeated the process as their technology changed.

A backup provides data. A tested recovery process provides resilience.

For organizations reviewing their OT backup and recovery programs, start with three actions:

1. Identify. Build an inventory of critical systems across Control Centers, Data Centers, network and security infrastructure, and field OT devices.
2. Validate. Confirm that current backups and configuration files exist and that they reflect the environment operating today.
3. Recover. Periodically prove that the organization can use those backups and its documented procedures to restore functionality.

Because the question that ultimately matters is not “Did the backup complete successfully?” It is: “Can we recover?”

Sources

- NIST — SP 1339, OT Backup Quick Start Guide (June 17, 2026), publication page¹
- NIST — SP 1339, OT Backup Quick Start Guide (PDF)⁴
- NERC — CIP-009-6, Cyber Security — Recovery Plans for BES Cyber Systems²
- NERC — Weekly Regulatory Updates (September 28, 2026), CIP effective-date table³
- CISA — #StopRansomware Guide⁵



- CISA and FBI — AA21-131A, DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (May 11, 2021)⁸
- CISA — SAFECOM-NCSWIC Spring 2021 Joint Meeting Highlights (City of Tulsa ransomware discussion)⁷
- WIRED — The Norsk Hydro cyber attack is about money, not war (March 2019)⁶

Editorial note: Opinions are the author's own. This issue is based on publicly available NIST, NERC, and CISA guidance and public reporting on the incidents cited. The recovery matrix is illustrative, not a template endorsed by any regulator. Nothing in this piece is compliance or legal advice; registered entities should confirm applicability of CIP-009 requirements against their own BES Cyber System categorization.

Sources & references

1. NIST SP 1339, OT Backup Quick Start Guide
<https://www.nist.gov/publications/ot-backup-quick-start-guide>
2. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems
<https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-009-6.pdf>
3. Weekly Regulatory Updates (September 28, 2026)
https://www.nerc.com/globalassets/programs/compliance/bulletins/2026_09_28_weeklyregulatoryupdates.pdf
4. NIST SP 1339
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1339.pdf>
5. #StopRansomware Guide
<https://www.cisa.gov/stopransomware/ransomware-guide>
6. WIRED
<https://www.wired.com/story/norsk-hydro-cyber-attack/>
7. CISA SAFECOM-NCSWIC meeting summary
https://www.cisa.gov/sites/default/files/video/21_05_safecom-ncswic_spring2021_highlights_21_0804_tech-edit%20%28FINAL%29_508c.pdf
8. AA21-131A
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>