Power and Water Cybersecurity Suite – System Backup & Recovery

Features

- Supports compliance for NERC CIP-009 backup and restore requirement
- Provides a solution for disaster recovery
- Implements and restores image backups of control systems
- Offers disk-level protection
- Provides full, incremental or differential backups
- Executes scheduled, event triggered or manual backup schemes with conditions
- Offers universal restore of system workstations and servers

Overview

Unplanned power generation outages can be costly events due to lost revenue, purchasing replacement power, incurring environmental penalties and a loss of public confidence. An interruption to water or wastewater treatment processes can endanger community trust as well as cause property loss (including data) and potential environmental damage. Process disruptions can be caused by several factors from equipment failures and human errors to cyber incidents or natural disasters. A well-thought-out contingency plan with rapid restoration capabilities can minimize losses. The most important step of a viable contingency plan is creating a strategy for efficient and effective control system recovery following a disruption.

A traditional recovery plan includes finding suitable replacement equipment with the proper operating system, sourcing the original application software with correct licensing keys and then reloading the customer-specific software with validation – a process that is very delicate and time consuming.

Rapid recovery requires capturing and archiving dynamically changed control system data before any unanticipated incident occurs.

A comprehensive contingency plan can accelerate the recovery process by reapplying the target station’s image extracted from the archives and returning the station or whole system back to normal operation. The contingency plan should also include a disciplined backup procedure that manages system development and routine maintenance.
Solution

Backup & recovery is included with every Ovation™ system to restore the database software server. Additional Ovation and non-Ovation full system protection can be provided as a standalone solution or by installing the Power and Water Cybersecurity Suite’s system backup & recovery module. The functions included in this module enhance the user’s ability to elaborate the process of regular backup, the validation of the correct backup files and the location of available storage.

The functionality can be further configured so that the backup can be triggered by events and any corrupted data can be retained for further analysis and diagnosis.

The fundamental significance of CIP-009 is to ensure a rapid recovery of the control system from any disaster; regardless if it is caused by cyber, natural or human-error incidents. The imaged-based backup technology addresses this need by providing a full disk image of the control system that is readily available for restoration.

The Benefits of Emerson’s Solution

Emerson’s system backup & recovery incorporates easily into a control system’s architecture and facilitates the creation and restoration of image-level backups of system assets. Emerson’s solution includes full support for “bare metal” restoration for both disaster recovery and limited point-in-time restoration purposes.

System backup & recovery is distinguished from out-of-the-box third-party products in that it incorporates Acronis Backup & Recovery (a trusted, proven and recognized industry-leading software package) along with integrated Emerson software that provides a solution tailored to the flexibility and capabilities of the Ovation product line.

Emerson’s system backup & recovery is fully tested by Emerson and actively maintained to expand capabilities and software support. Additionally, the solution is formally supported with current Windows versions and a wide range of Emerson add-on modules. The solution is delivered with documentation that details the installation, configuration, operation and maintenance within the control system’s environment.

In regards to Ovation, system backup & recovery handles numerous areas of sensitivity and reliability that are not available from stand-alone third-party solutions separately connected to an Ovation system. These actions include software mechanisms that assess and intelligently react to the state of Ovation HMIs and controllers at the time of both backup and restoration. Additionally, these mechanisms take into consideration other areas of the Ovation product line including integration with various databases and active directory.

Functionality

Backup

The control system backup & recovery module consists of a single management server with agents loaded on each Windows workstation and server, along with a network attached storage that provides various fault tolerance capabilities for storage. The management server provides the following functions:

- Single entry to the overall infrastructure
- Easily protects data on numerous machines using centralized backup plans
- System-wide monitoring and reporting functionality
- Centralized catalog of all data stored on the storage nodes
- Can be backed up in the same manner as any other client machine, such that its failure would not prevent the ability to restore other machines

Backups can be accomplished using two different methods:

- **Full backup** - stores all data selected for backup and forms the base for incremental and differential backups. It can be used to roll back the system to its initial state.
- **Incremental backup** - stores changes to the data against the latest backup. This is useful when data changes tend to be small and there is a need to roll back to any one of multiple saved states.
In addition to ad hoc backups, a well-thought-out backup plan for the entire control system is recommended. A thorough backup plan considers the following factors:

- **What to backup** - select the type of data to back up and specify the data items
- **Where to backup** - specify a path to the location where the backup archive will be stored and named
- **How to backup** - specify when and how often to back up; define how long to keep the created backup archives; set up the schedule for the archive cleanup procedure; use well-known or create a custom backup scheme

Default backup options are pre-defined with values stored in each agent. These values can be modified specific to each backup plan.

### Recovery

Default recovery options are pre-defined with values stored in each agent. These values can be modified specific to each recovery plan.

### Storage

Storing backup archives requires a designated location or a vault for ease of use and administration. The network attached storage module is configured as the vault for the backup archives. Once the vault is selected, the following management operations can be performed:

- Receive a list of backups included in each archive
- Recover data from a backup
- Examine backup content
- Validate all archives in the vault or individual archives or backups
- Mount a volume backup to copy files from the backup to a physical disk
- Safely delete archives and backups form the archives

### Operations

#### Management Server Software

The management server software drives data protection to the targeted system or systems. This server software can be loaded on a standalone Microsoft® Windows® station and is capable of servicing multiple systems in a multi-network environment. The server software can also be loaded on a virtual machine within the Power and Water Cybersecurity Suite. The built-in network capability of the suite allows the station to support multiple systems within the same plant.

#### Agents

An agent is loaded on each Windows station that is resident on the system network. The agent is responsible for performing disk- or file-level data backup and recovery, and enables other management operations, such as task management and operations with hard disks.

#### Vault

A vault is a location for storing backup archives. A separate network attached storage location is designated as the centralized vault for the system. Multiple vaults can be created if needed. Each vault can be managed or unmanaged by storage node. The storage node enables the administrator to:

- Use a single centralized catalog of data stored in the managed vaults
- Relieve managed machines of unnecessary CPU load by performing cleanup, validation and other operations with backup archives
- Prevent access to the backup archives by using encrypted vaults

#### Management Console

The management console enables users to perform server-specific or agent-specific operations. It contains three sections:

- **Menu Bar**: Lists user activities; dynamically changes depending on the items selected in the navigation tree and from the main area.
- **Navigation Pane**: Contains the navigation tree with short-list views of the dashboard, machines with agents, backup plans and tasks, vaults and alerts; and full-list views showing data catalogs, storage nodes, tape management, licenses, reports and logs.
- **Main Area**: Creates, edits and manages backup plans and recovery tasks; dynamically changes depending on the item selected in the menu or navigation tree.
Backup Plan
A comprehensive backup plan is suitable for a long-term backup strategy. The strategy may include schedules, conditions and the timely deletion of backups or moving them to different locations. The backup schedule is triggered by an event or multiple events, such as time, time passed since the last successful backup, user logon or logoff, system startup, free space change, or an event in the Windows event log. In addition to the events, additional conditions can be specified such as a user being idle, available host or all users logged off. After the backup file is created and stored in the primary location, it can be replicated to a second location for a retention period specified in the backup plan. It can be additionally replicated to up to five different locations (including the primary one) or be deleted.

Recovery Task
A recovery task can be created for restoring disk, volume or file data. The steps include the following:
- What to recover
- Where to recover
- When to recover

Reports can be generated with either predefined or customizable templates. Templates are available for the following reports:
- Registered machines
- Local and centralized tasks existing on the registered machines
- Local and centralized backup plants existing on the registered machines
- Archives and backups stored in the centralized managed vaults
- Statistics about centralized managed vaults
- Task activities history

Alerts and logs can greatly assist with regular operations. An alert is a message that warns about actual or potential problems. The alert can be active if the issue has not been resolved or inactive if the issue has been resolved or self-healed. The centralized event log stores the history of operations performed by the management server, the storage nodes and the registered machines.

Power and Water Cybersecurity Suite
The established Power and Water Cybersecurity Suite infrastructure can be leveraged for supporting multiple systems. In the event of a disaster, system recovery is available from multiple disk images across multiple systems.

The backup files may be sent to several locations, although the network attached storage is the preferred selection, as it provides an easy-to-use and high-performance storage solution conveniently installed in the Power and Water Cybersecurity Suite cabinet.

Compliance Summary

<table>
<thead>
<tr>
<th>NERC Standard</th>
<th>Requirement</th>
<th>Emerson Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-009-6 R1 Part 1.3</td>
<td>One or more processes for the backup and storage of information required to recover bulk energy system cyber system functionality</td>
<td>Regular backups can be automatically scheduled and executed. Each backup can be set for full, incremental or differential backup</td>
</tr>
<tr>
<td>CIP-009-6 R1 Part 1.4</td>
<td>One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures</td>
<td>Error logs during backups are available through the system backup &amp; recovery application or the Windows event log</td>
</tr>
</tbody>
</table>