

A Large Petrochemical Company Utilizes AutoSave in its Goal to Achieve Cyber Immunity

THE CHALLENGE

A large multi-national petrochemical company seeking to harden its cyber-defenses (or said another way, seeking cyber immunity) realized the need to protect their controls environment against the inevitability of cyber-attacks. To accomplish this, they needed a way to track and control all of their programmable automation devices to protect them from unauthorized access. History has shown not managing these devices well results in downtime, product errors and safety issues.

Specifically, the customer needed to protect the data in thousands of automation devices in their upstream operations in the Permian Basin in the U.S. They are aware that one of the most dangerous ways to attack their operation is to gain access to control systems that operate and/or automate industrial processes, such as programmable logic controllers (PLC.) It was vital to find a solution for identifying and eliminating hazardous situations while controlling risks to production that can result from cyber-attacks targeting OT systems.

THE SOLUTION

The customer selected the market-leading solution that captures all automation device programmatic changes in support of the goal of cyber immunity = AutoSave. AutoSave provides the ability to:

- ☑ Back up data (configurations, logic, code, etc.) from industrial controls to a central repository with appropriate access protection/management, for both networked and non-networked devices.
- ☑ Authenticate users' access to workstations
- ☑ Manage workstation backup/images
- ☑ Identify firmware and software versions for risk mitigation

These features enabled the company to prepare for an attack by securing program intellectual property, detecting unauthorized program changes, and rapidly restoring and recovering the correct program after an attack.

MDT AutoSave Portal | AutoSave Program

Summary Revisions Server Commands

Program Revisions

/Line8/workcell-b/HMI2

ID: 2 Version: Current Created: 2015-08-28 12:05:55

Show 10 entries Columns Copy CSV Print Search:

Anc. Num.	File Date	Store Date	Comment	Method	User	Client
41	2019-02-07 20:43:15	2019-02-07 20:43:15	local to current	Local to Current	RickM	RT-7x-2
40	2019-02-07 20:42:53	2019-02-07 20:42:53	launch program change	Launch	RickM	RT-7x-2
39	2019-01-28 10:08:14	2019-01-28 10:08:15	this is a new comment from the field client	Local to Current	RickM	RT-7x-2
38	2019-01-02 09:51:31	2019-01-02 09:51:31	updated from field work	Local to Current	RickM	LAP-RAG-3
37	2018-12-14 00:43:54	2018-12-14 00:43:55	test	Upload	RickM	RT-7x-2
36	2018-12-03 23:31:11	2018-12-03 23:32:17	make revision 34 current again	Ancestor to Current	RickM	LAP-RAG-3
34	2018-12-03 23:31:11	2018-12-03 23:31:11	launch change - updating the current	Launch	RickM	LAP-RAG-3
33	2018-11-28 23:48:23	2018-11-28 23:48:23	upload current	Upload	RickM	RT-7x-2
32	2018-11-28 14:56:01	2018-11-28 14:56:01	upload current from device via agent	Upload	RickM	RT-7x-2
35	2018-10-12 14:24:52	2018-12-03 23:31:57	downloading revision 28	Ancestor to Current	RickM	LAP-RAG-3

Showing 1 to 10 of 30 entries Previous 1 2 3 Next

PREPARE:
AutoSave saves a copy of each program revision in a central repository. Access to program folders and programs is managed via a flexible privileging system.

DETECT:
AutoSave compares the latest program copy on file in AutoSave with the program running in each device to identify any differences. If differences are found, the appropriate people are notified with an email highlighting the differences.

MDT AutoSave Compare Report

Command group: ConveyorGroup_2

Actual Start: 2019-02-25 08:01:21
Actual Finish: 2019-02-25 08:01:52
Alert remaining at: 2019-02-25 08:30:21

SUMMARY

Completed:	11	Errors:	0
Save:	4	Program timed out:	0
Different:	5	Group time exceeded:	0
Auto updates:	0	Program disabled:	1

DETAILS

All Programs: 12

Program Path	Scheduled Command	Upload		Compare		Auto	Agent	Remarks
		Start	Stop	Start	Stop			
\\hmi\workcell\conveyor08	Compare current to device	08:00:22	08:00:25	08:00:25	08:00:27	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\conveyor08	Compare current to version (master)	08:00:28	08:00:30	08:00:30	08:00:32	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\hmi2	Compare current to device	08:00:33	08:00:45	08:00:45	08:00:56	N/A	RT-7x-2	No differences were detected
\\hmi\workcell\conveyor08	Compare current to device	N/A	N/A	N/A	N/A	N/A	RT-7x-2	This program has been disabled for use by the command schedule
\\hmi\workcell\hmi2	Compare current to version (master)	N/A	N/A	08:00:58	08:01:00	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\hmi2	Compare current to version (master)	N/A	N/A	08:01:00	08:01:03	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\hmi2	Compare device to version (master)	N/A	N/A	08:01:03	08:01:14	N/A	RT-7x-2	No differences were detected
\\hmi\workcell\hmi2	Compare device to version (master)	08:01:14	08:01:16	08:01:16	08:01:19	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\hmi2	Compare device to version (master)	08:01:19	08:01:21	08:01:21	08:01:23	N/A	RT-7x-2	Differences were detected
\\hmi\workcell\hmi2	Compare device to version (master)	08:01:24	08:01:36	08:01:36	08:01:47	N/A	RT-7x-2	No differences were detected
\\hmi\workcell\hmi2	Upload current	08:01:47	08:01:50	N/A	N/A	N/A	RT-7x-2	The upload completed successfully
\\hmi\workcell\hmi2	Download Current to Processor	N/A	08:01:51	08:01:51	08:01:52	N/A	RT-7x-2	The upload completed successfully

MDT AutoSave version 7.08.00.34 www.MDT-Software.com

Program Editor Connected: AutoSave Data/Modules/Unity_a/quantum13.1

File Program Revision View Help

Add Feedback View Contents Delete Contents

Restore (Download) To Compare To

Modify Current Device Disk Local Version Device Local Revision

User: mass Client: RT-8X-1 Server: 10.16.100.81

Explore

- language
- Line-1
- Modules
- Mitsubishi
- Q&A Module
- rs5k_c
- Step 5
- step7_a
- step7tia_d
- step7tia_e
- unity_a
 - quantum13.1
 - test
- Univ
- rag
- Regulated
- sab
- sync-server-test
- Templates

Version List

Main (Current)	00019	AutoSave System Account	2021-10-29 2:55:47 PM	local to current
master	00018	AutoSave System Account	2021-10-27 9:27:42 PM	backup from the agent
	00017	AutoSave System Account	2021-10-27 1:44:58 AM	local to current
	00016	AutoSave System Account	2021-10-27 1:41:59 AM	local to current
	00015	AutoSave System Account	2021-10-27 1:38:52 AM	local to current
	00014	AutoSave System Account	2021-10-27 1:29:06 AM	etestset

Add Feedback

- Compare to Device via Client
- Compare to Device via Agent
- Compare to Local via Client
- Compare to Local via Agent
- Compare via Client to ...
- Compare via Agent to ...
- Restore (Download) via Client**
- Restore to Main (Current)
- Save as Version
- Restore to Local
- Restore to Disk
- Delete
- View Contents

8:00:85.00

RECOVER:
With an archive of all program revisions, using AutoSave, users can quickly restore the latest approved program after an unauthorized change.

THE RESULTS

This customer is now using AutoSave to manage all program configurations. AutoSave is authenticating users that have permission to make a change to the program. However, if a change is made outside of the AutoSave, they have greatly increased their resiliency against a breach to the controls system simply by knowing right away that a breach has occurred and being able to quickly revert systems back to the state they were in prior to the breach. To restore operations, the latest approved program can now be downloaded to the device very quickly. For operations to maintain uptime when faced with normal hazards, such as power outages, human error and equipment failure, AutoSave enables users to quickly retrieve the most current copy of the program and resume operations. When the change is malicious and unauthorized, AutoSave becomes even more vital in reaching cyber immunity.



MORE INFORMATION

For more information about AutoSave Cyber Security Solutions, visit: www.mdt-software.com/autosave-protection-and-recovery-solutions/.

Petrochemical Industry Article: "[A cyberattack on a U.S. gas pipeline has us asking: Are utilities prepared for a rise in cybersecurity attacks and what can be done about it?](#)"

