Gone are the days when engineering staff have easy, unlimited access to control rooms in industrial facilities. In today’s world, onsite access to industrial control rooms can be quickly constrained due to global health issues, such as the COVID-19 pandemic, as well as due to travel restrictions, threats to industrial facility physical security, severe weather, or other geopolitical conflict. Due to recent global events, remote operations planning and implementation, already underway in many critical infrastructure companies, has now accelerated.

PAS SOLUTIONS SUPPORT BUSINESS-CRITICAL REMOTE OPERATIONS

Effective remote operations require access to real-time asset, process, and plant information from anywhere at any time. Engineers and operators can use this information to improve process safety, asset utilization, and cybersecurity. They are also more prepared to prevent – or quickly recover from – downtime.

PAS software solutions support remote operations capabilities for many of the world’s leading industrial organizations, providing business-critical visibility to reduce process safety risks, remediate cyber threats, and make more confident decisions that rely on OT data – regardless of physical location.

• PlantState Integrity™ analyzes data from disparate sources to provide critical safety and production information.
• Cyber Integrity™ delivers comprehensive inventory, vulnerability, configuration, compliance, backup and recovery, and risk management for OT assets.
• Automation Integrity™ collects and contextualizes OT/ICS configurations and automates change management.
• Decision Integrity™ enables trusted data for decision-making.

MAINTAINING VISIBILITY INTO DAY-TO-DAY OPERATIONS DURING A GLOBAL PANDEMIC

A global Fortune 10 multinational integrated oil & gas company uses PlantState Integrity reports as a part of their daily operations and to maintain their master alarm database. They also send events from their instrumented protective systems (IPS) to PlantState Integrity for monitoring safety instrumented functions (SIFs) performance. Of particular value is their ability to identify critical SIFs with bypass durations greater than 24 hours.
When faced with an unprecedented health crisis which included quarantines, curfews, and other travel restrictions, PlantState Integrity enabled their engineers, many of whom were suddenly required to work from home, to continue to perform their jobs. This ensured plant operations continuity and a reliable global energy supply.

PROVIDING CONTINUOUS VISIBILITY INTO ALARM SYSTEM PERFORMANCE

For one of the largest petrochemical companies in the world, PlantState Integrity is essential to operations, providing insight into critical safety and production data engineers require for their daily work processes. PlantState Integrity reports deliver vital visibility into current operations for remote staff, who typically do not have access to systems running below the Demilitarized Zone (DMZ), guaranteeing business continuity even when physical access to facilities is limited.

IDENTIFYING PROCESS ANOMALIES

A global Fortune 500 multinational chemical company recently implemented a “lean” model, where half of the workforce now works remotely. PlantState Integrity enables this model by allowing engineers to analyze frequent, standing, and chattering alarms, and examine average versus peak rates. Additionally, engineers are able to review operator changes to critical settings, such as reconfiguring control loops from manual to automatic, shelving alarms, and disabling alarms. The data PlantState Integrity provides helps process control engineers quickly identify process anomalies, as well as address nuisance alarms without physical access to facilities.

ENSURING DAY-TO-DAY CONTROL SYSTEM OPERATIONAL INTEGRITY

A Fortune 500 integrated energy company needed to give control system engineers working remotely the ability to securely analyze and troubleshoot configuration changes when physical access to facilities was constrained.

OT security policies prohibited remote connections to the control systems or the process control network (PCN). However, engineers needed visibility into existing configurations and planned and unplanned control system configuration changes to ensure day-to-day operational health and safety.

With Automation Integrity running in a Level 3 DMZ, engineers are able to collect control system inventory and configuration information across all Level 2 through Level 0 OT assets. They then use this data to detect and troubleshoot configuration issues, ensuring safe, reliable operations.
MAINTAINING OT ASSET CYBER RISK VISIBILITY REGARDLESS OF LOCATION

During the COVID-19 pandemic, a large specialty chemical company suddenly limited on-site engineering staff, causing a surge in remote work. At the same time, the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom’s National Cyber Security Centre (NCSC) issued an alert (AA20-099A) regarding COVID-19 related malicious cyber activity targeting critical infrastructure companies.

The OT cybersecurity team uses Cyber Integrity OT asset inventory, vulnerability management, configuration management, and risk analytics as the foundation for their OT cybersecurity program. This enables them to quickly pivot from using Cyber Integrity on site to using Cyber Integrity remotely.

It also allows them to continuously assess their current level of cybersecurity risk, monitor for unauthorized changes, and drive appropriate remediation actions without interruption during a time of amplified threats.

ADDITIONAL REMOTE OPERATIONS USE CASES

Additional remote operations use cases enabled by PAS solutions include:

- Shifting from local to remote daily production “standup” meetings facilitated by KPIs and reports from PAS software
- Generating reports to demonstrate NERC CIP compliance for transient cyber assets (TCA)
- Identifying safety instrumented function (SIF) dependencies prior to approving maintenance work orders
- Conducting daily reviews of control system configuration changes to identify issues that could lead to production upsets
- Identifying control loop problems and scheduling remediation tasks
- Monitoring critical security settings (open ports, failed logins, etc.) for changes that materially increase risk

For more information about how PAS solutions can enable remote operations for your industrial facilities, contact us.

About PAS

PAS, the OT Integrity company, delivers software solutions that prevent, detect, & remediate cyber threats; reduce process safety risks and optimize profitability; and enable trusted data for decision-making. PAS helps industrial organizations Ensure OT Integrity including 13 of the top 15 refining, 13 of the top 15 chemical, 4 of the top 5 pulp and paper, 3 of the top 5 mining, and 7 of the top 20 power generation companies.

For more information, visit www.pas.com.