Why is Tracking all Industrial Control System Changes Critical for Pharmaceutical Manufacturers?

The Coronavirus pandemic has had some effect on just about every business in the world, including industrial manufacturing. Pharmaceutical manufacturers have an extra complication in that the world is depending on them and the stakes are even higher to avoid errors and production interruptions. The increased need for certain drugs and therapies also requires that plants be more agile to meet changing demands. Adding to these challenges is the continued regulatory scrutiny on the life sciences industry and the unfortunate, but still very real risk, of cyber-attacks.

Protection from Errors and Downtime

Industrial control system (ICS) devices such as PLCs, HMI/SCADA systems, robots, etc. and their logic programs are vital to manufacturers in ensuring pharmaceuticals are produced consistently, reliably, and safely. They also must function exactly as intended. An inadvertent program change can result in downtime and contaminated products.

Managing program changes is necessary to:

- "Undo" an undesirable change by restoring a prior, good working version within seconds.
- Detect any unknown or unauthorized changes and notify the appropriate personnel of the rogue change.
- Control who can edit programs with user permissions and collect information on the who, what, when and where of a change.

Change is an inherent part of the life cycle of a pharmaceutical product but when change is not properly managed, it can have consequences for the plant's processes, people, and end-products. Due to the severity of some of these outcomes, pharmaceutical plants must comply with regulations that require the ability to trace process changes and ensure processes have not been altered without approval or documentation.

Regulatory Requirements

The regulatory environment under which a facility is governed can have a number of impacts on ICS operations. FDA regulations, such as FDA 21 CFR 11, have specific rules around electronic signatures. Other regulations address secure program access, audit trails and version control. However, these automation control systems don't include built-in tools that can manage all these requirements. In the past, many regulatory requirements were managed by manual, paper-driven processes, resulting in inaccuracies and inefficiencies. A Change Management System (CMS) contains tools that can significantly streamline the process of making changes in a validated environment and help to ensure that proper change processes are followed. For instance, a CMS with electronic signature and workflow capability can route proposed changes to appropriate personnel, manage the use of the proposed change during testing phases so that produced product is appropriately quarantined, and capture approval of the change for use in production. A CMS used in a regulated manufacturing environment should have all the following features:

- Electronic Signature approvals (21CFR11 compliant)
- Multiple review statuses

- Additional security features: password control, electronic log messages, configurable approval messages and more
- Electronic Signature and audit trail support for documents

Not only will a CMS help plants meet pharmacopeia standards and regulations, it will also help address the increasing threat of cyber-attacks.

Cybersecurity

While pharmaceutical companies have long been a primary target of criminals attempting to steal intellectual property, cyber-attacks have increased in the past year as some have focused on stealing COVID-19 vaccine research data. Not only are these manufacturers at risk of losing valuable assets but a breach can also lead to downtime, dangerous and expensive product errors, and hazardous situations for employees. One of the most effective, and common, methods to attack a manufacturing plant is to gain access to control systems and their logic programs. A robust CMS helps manufacturers prepare in case an attack happens, detect unauthorized changes and rapidly recover after an attack.

To help prepare, device programs are stored in the CMS in a central location where there is a privileging system set-up to manage access to plant-floor devices. No USB should get anywhere near the OT network and workstation access should be authenticated by a CMS. Also, automation device manufacturers regularly update their firmware to address new threats. It is, therefore, a major benefit if the CMS can track data such as firmware, software, and CPU versions in automation devices throughout the facility so they can be compared against published threat reports.

A CMS can compare the programs running in devices with reference copies. It will detect changes by comparing the latest approved program copy on file with the program running in each device and identify any differences and notify the appropriate personnel. Because all program changes in a pharmaceutical environment should be done through the CMS, rogue changes should be investigated immediately.

A post-attack strategy will leverage the CMS repository to restore operations. After an attack, the latest approved programs can be easily accessed and downloaded to the automation devices. A CMS maintains an archive of all program revisions so plants can restore operations or maintain uptime even when facing normal hazards, such as power outages, human error and equipment failure. It is also integral that the CMS selected supports a wide range of devices and any PC-based application, so that the entire OT environment is protected.

The risks facing pharmaceutical manufacturers are not likely to go away, or even decrease, and during a pandemic, the stakes have never been higher.