

The following article first appeared in the Resource Center of Control Engineering Magazine, February 1, 2005 issue:

Back to Basics

PLC change management

By Joe J. Colletti Jr., president of MDT Software; www.mdtsoft.com. February 1, 2005

Automation control systems often involve an array of PC workstations, programmable logic controllers (PLCs), robotic controllers, and HMI (human machine interface) workstations. Control logic is stored either in the device or on an associated workstation and can involve a large number of associated files and executable programs grouped into 'projects.' This complexity poses a challenge to detecting unauthorized—and potentially hazardous—program changes, especially where systems from multiple vendors and the associated variety of program development and device management tools exist.

Until recently, proprietary protocols and network isolation provided adequate security from external threats. However, many vendors are abandoning proprietary communication mechanisms to lower costs and improve reliability. Similarly, more and more device management is moving to PC-based workstations and other open systems. This transition to standard protocols and operating systems is making modern devices and systems more vulnerable to attack.

Risk areas

Internal risks are present in several forms. Most visible is the disgruntled employee who has proper access and system knowledge. Although system design and interlocks can prevent most catastrophic events, it is far easier to make changes resulting in system downtime. The role of the change management system in detecting and preventing such scenarios lies in how these threats typically manifest: someone with malicious intent will often modify a program to perform an undesirable action at some time in the future, not at the moment of the change. In the time between the planting of the malicious code and its triggering, a change management system can detect the damage, alert appropriate individuals, and prevent a harmful situation.

The second form of internal risk is the case of someone making an incorrect change to a system parameter, damaging properly running code. Though training and data backups are helpful, they are not enough. Even the best-trained personnel make mistakes. Data backup systems usually focus on server data and rarely backup the logic in proprietary devices. The role of the change management system in this case is to make available a previously verified and documented version of the program.

A third form of internal risk lies in the lack of an approval process prior to making system changes. This problem is made more acute when contractors are brought in and allowed to

make changes or downsizing decreases plant-floor systems expertise. Role of the change management system in this case is to provide an approval process and audit trail of changes.

Much has been written recently about the external threats posed by those with malicious intent. Proper use of firewalls, DMZs (demilitarized zone: computer or small subnetwork that sits between a trusted internal network), and access restrictions are key to securing mission-critical systems. However, these steps do not track actual changes made to control systems. To achieve this level of security requires a change management system to compare the logic currently in use to a reference copy.

Another challenge in detecting changes in automation devices lies in the design of the devices themselves. Many allow direct connection to the processor, as with a PLC, bypassing network security and validation. To detect these changes in a timely manner, it is necessary to look for them frequently. Automating this process is a far more precise way to achieve this goal than periodic, cursory reviews.

Type of change to control system Authentication	Real-time changes	Time-delayed changes
Using Proper Authentication	<ul style="list-style-type: none"> • Change management system would contain a copy of the last authorized version of code. 	<ul style="list-style-type: none"> • Change management system would contain a copy of the last authorized version of code.
Bypassing Authentication	<ul style="list-style-type: none"> • Change management system works in conjunction with other vendor applications to capture change history and audit trail. • Change management system would contain a copy of the last authorized version of code. 	<ul style="list-style-type: none"> • Change management system works in conjunction with other vendor applications to capture change history and audit trail. • CMS Periodically conducts scan and comparison of device logic to reference files. Alerts personnel when changes are detected.
	<ul style="list-style-type: none"> • In certain cases the CMS could detect direct communication with plant devices and signal an alert. 	

Note: CMS=change management system Source: Control Engineering with data from MDT Software