Saving and Securing PLC Code

In the "SCADA world," we often relate security to how secure our networks are or how complex of a password we can make to ensure we are following the best practices to prevent unauthorized access to our critical infrastructure. These policies secure our servers and PCs that run our SCADA software, providing the proper credentials from municipal staff members, typically based on their responsibilities for the organization. The SCADA software also communicates to Programmable Logic Controllers (PLCs), which then has programming that is designed to make decisions based on various water or wastewater process conditions. While PLC programming "lives" in a PLC, a backup copy should also be saved in files that a systems integrator will create. Upon completion of a project or a change, the programming files should be turned over to the owner to serve as reference for modifications made as well as a backup in the event of a PLC failure. The question is, where and how do we save these files securely? The following will review how to ideally save and secure PLC code.

Saving PLC Code

Let's say a project or substantial change has just been completed at a pump station, the programming has been approved, and the facility has been turned over to the owner. Any time programming is finalized or a project has been completed is typically a good time for the owner to ask their system integrator for the complete, commented programming for storage purposes. The systems integrator now has a few options for providing the programming:

- **E-mail** – Email is not preferred as email is typically not encrypted or secured. If you must send PLC programming files via email, encrypting the attached or linked file would be recommended and see your IT staff for how to best encrypt a file attachment.
- **CD, DVD, or Flash Drive** – While many portable storage options have been popular in recent years, they can often get lost in a file cabinet or on someone's desk, and they often are read-only or not updated, making them less than ideal for permanent storage.
- **Secure file transfer (e.g. OneDrive, SFTP, etc.) combined with server-based storage** – The secure/server-based storage of data is preferred as it helps to ensure the data is encrypted in transit, and saved on a server within your agency that has the proper credentials required for access.

So now we understand how to securely transmit and ideally save a PLC backup file, but managing access to the file and making sure we have the right version if and when we need to restore it can be nearly as important as having a backup copy.

Securing through Change Management and Managed Access

In most cases, PLCs stick around for 10-20 years after they are installed without major modifications. Within that time, the facilities that the PLCs control may undergo modifications that require the programming to be updated along the way. In order to provide the quickest, safest, and most efficient modifications to existing programming, having commented archived PLC programming saved on a server

that is backed up by your IT staff can be a great thing. In addition, having simple permissions as to who can access the PLC code as well as a simple procedure for how to keep track of changes to the code can also be very beneficial. From experience, having a record of what has been changed and being able to revert back to an older version of the programming can save a lot of time and frustrations when things don't go exactly as planned. One suggestion to keep track of PLC versions might be to append the PLC filename with a version suffix at the end (e.g. – "Panel_B_v8.acd" and the next would be "Panel_B_v9.acd"). If you already do a good job of managing change and access to your code and are interested in taking change management to the next level, PLC manufacturers can provide software that can manage the changes and access of PLC programming for you in ways that add additional auditing and security features.

So whether you are a public works director, a superintendent, an IT professional, a member of maintenance staff, or an operator, start the conversation internally about where your PLC code is stored, how previous versions are saved, and where it is backed up. Then ask your systems integrator what level of security is appropriate for your PLC code. Doing so will save time, improve the security of your code, and help with overall operational stability.

Nicholas A Paradiso, PE
Lead Automation Engineer
Concentric Integration