Backup and Restore:

A GUIDE FOR CREATING INDUSTRIAL BACKUP PROCEDURES

Shawn Perkins, P.E.

It's 10PM and you just got a call from the plant that a critical PLC has failed and can't be revived. A replacement PLC is on hand so all the technician needs now is the backup file to get everything back up and running. You know where that is, right? It's up to date and has all the latest set point values included, doesn't it? There aren't any supporting files that you need and don't have, are there?

If you’re able to sleep at night then you are probably doing a good job of backing up your critical operating files. But knowing where the backup files are located is just half the battle. Ideally you should have a comprehensive Backup and Restore Procedure available to guide you, or any other qualified personnel, through the steps needed to recover from this type of situation in a timely fashion.

Who, What, When, Where, How?

Those are the type of questions that should be answered in your Backup and Restore Procedure, although not necessarily in that order. Let's tackle the What question first.

What to back up

The first things that comes to mind when we think about backing up industrial source code are the PLC files and the HMI (SCADA) code. But to be complete there are many other files and settings that are equally as important. Regarding the PLC files, it is imperative to have not only the bits and bytes of the code, but also the documentation that goes along with it. Code written today is more complex than that of the past, which makes it even more important to have well-documented code with tag names, symbols, rung comments, and other documentation within the code. A few modern controllers allow this important documentation to be stored on the PLC in a separate memory area so it is readily available and saved along with the code, but this is the exception not the norm. So before you upload and save the PLC file, make sure you start with a current file that has the documentation included.

PLCs do not get over-the-air updates like your smartphone, but there are periodic firmware updates made available by manufacturers that can be installed. Some firmware updates address critical operational or security aspects, while others may add features that do not apply to your equipment so they can be skipped. You should have an inventory list of all the PLCs in your plant, with model numbers, series information, and firmware level. This will make it easier to evaluate when new firmware is available to help determine if you should install it or not. In addition to the firmware code itself, you should retain a copy of the software tool needed to update the firmware and a written procedure detailing how to go about the process.

You may also have advanced function cards in your PLC system that require setup and configuration outside of the PLC code itself. These advanced communication or similar type cards may have their own configuration software and files that should be backed up. Be sure to include the application installation files along with the configuration file generated.

If your HMI (SCADA) systems are not integrated with Windows domain user accounts, then you likely would want to backup user account settings to a more secure location. Maybe you cannot or do not want to drill all the way down to the user account and password level, but if you have any groups or group permissions set up you would want to detail that information at a minimum. Do not forget to include copies of the HMI system install disks and also any license files, keys or codes, or management tools that you need.

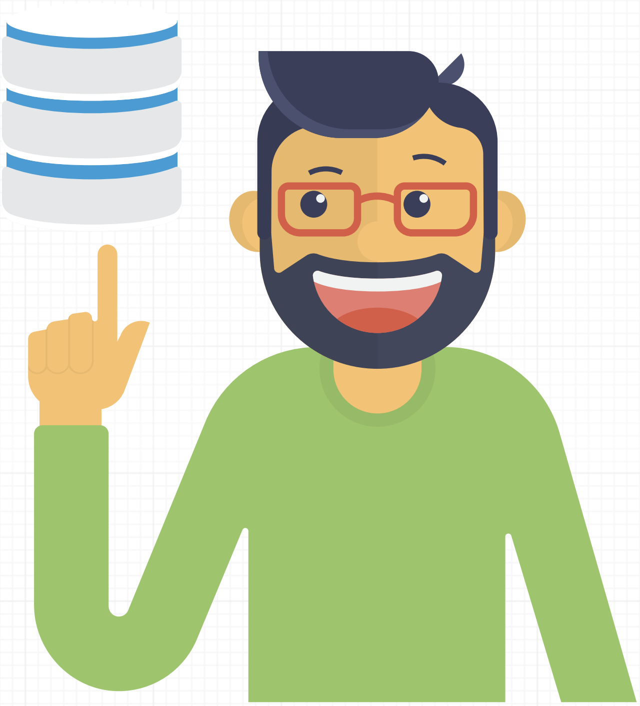
At the hardware level often overlooked but highly important components are the network switches. It is likely that the switches in your plant had some configuration changes made to them after they were installed, so be sure to backup this configuration. If a tool does not exist to backup and restore this configuration, be sure to document any settings that differ from the default, out-of-box condition.

Similarly, adjustable speed drives have hundreds of parameters that can be configured, so include these files in your overall backup and restore procedure. This applies to other hardware as well. Include any DIP switch settings, jumpers, dials, etc. for the drives and hardware devices. Configuration settings for display panels, meters, transmitters, or any other instrumentation should be recorded, including calibration information and scaling for engineering units. Alternatively some of this information can and should be included on your electrical drawings. But whatever approach you take, be consistent. Having some information in the backup and restore procedure and other information on the drawings will be confusing, especially if the same information is recorded in two places and not consistent.

And while not technically part of the backup and restore topic, if you do not have accurate and available electrical drawings for all of your systems, including the field wiring, you should work toward that goal.

How to Backup and Restore

After detailing what should be backed up, the next important topic in the procedure should be how to create the backups and, perhaps more importantly, how to restore from these backups. Fortunately equipment manufacturers typically do a good job of detailing both the backup and restore procedures in the supplied (or online) documentation. It is acceptable to just point to specific instructions in this documentation from your Backup and Restore Procedure, provided this information is stored along with your document, preferably as an attachment. If you do not have the full-blown programming or configuration software for the PLC or other equipment in your facility, keep in mind that many



programs now have Lite, Mini, or Service additions with scaled back functionality that may fit your need. Outside of the PLC and HMI development and runtime software, usually any other software programs or tools that you would need can be downloaded for free or are provided at a minimal cost.

For PC based HMI systems, your procedure needs to address backup and restore at two levels. How to restore just the HMI portion of the system should be one level, while a complete restore of the computer should be the other level. For the complete computer rebuild, you will want to detail the important hardware requirements, including specialty cards needed and all pertinent settings. For this level of backup and restore there are many off-the-shelf tools available at little or no cost. Look for something that allows for “bare-metal” restore capability, which is more flexible in the event that you need to restore to hardware that does not match exactly what you had before.

Who and When

The Who question somewhat overlaps with security in general, which is beyond the scope of this guide. However, the Backup and Restore Procedure should briefly address not only who is responsible for creating backups, but also who is authorized to restore the code, and even who is allowed access to the folder where backup files are located.

The When question is easier to tackle. It is almost impossible to make backups too frequently, with a few caveats. First of all, you do not want to make a backup today and overwrite the backup you made yesterday. At some point you will want to review a backup version that is weeks or months old. Your backup procedure should address how this is going to be managed, by either appending the date or a sequential number to each version of the backup, and/or by using folders to keep archived backups separate from the most current backup. It should be unquestionably obvious to anyone looking for the backup files which are the most recent. And at all costs avoid words like _new, _old, _good, _bad, etc. appended to the filename. While these terms may make sense at the time, someone else looking at these a year down the road may not be able to decipher this secret code. The second caveat regarding backing up files is that you may be backing the code up while it is in an undesirable state. For well-written code this usually is not a problem, but it is better to save the code in a "safe" or "initial" state if at all possible. For example, if you saved the Filter Control PLC code when it happened to be in a backwash state, a poorly written program may initiate a backwash cycle as soon as you restore the code, which may not be desirable.

It is vital to create a new backup after, and before, any changes to the system. The after is intuitive, but the before is perhaps more important. Having a backup that was created immediately before the downloaded changes has saved my bacon many times. This can be used to quickly fall back to this old code in the worst scenarios, or more frequently to “synchronize” states or settings between the old and new code.

Backups should also be created on a periodic basis, approximately every month or so, depending on the type of file and how critical or dynamic the source code is. There are advanced software packages available that can not only backup your code for you on a regular basis automatically, but can also monitor and compare the actively running code with the last approved backup file and let you know if there are any discrepancies. A Backup and Restore Procedure that is thorough and adhered to can work equally as well, especially if there are limited changes to your systems.

Where

Now that you understand the importance of having good backups and know what to back up and how to back everything up, the question remains of where to put all of this critical information. Obviously on-site backups should be readily available to authorized personnel and this location should be documented in the

procedure, but what about backups to the backups? At first this may look like a recommendation from the Department of Redundancy Department, but in fact it is very important.

If a virus takes out your SCADA computer it may likely take out the computer sitting next to it or on the same network at the same time. Other unfortunate events such as fire or water damage, or even theft, could render your single on-site backup useless. External hard drives and cloud storage are two common solutions to this problem. The amount of data that you have to backup may dictate which option is best for you.

If you go the external hard drive route, make sure the hardware you select is robust and made for portable devices. Cloud storage may have a small recurring cost, requires reasonably large internet bandwidth, and is only as reliable as your provider, but it is definitely worth considering.

Whether you use external hard drives, cloud storage, or any other form of backup redundancy, these details should also be included in your Backup and Restore Procedure. For example, in the case of external hard drives the procedure should address the type of hardware needed, type of software used, frequency of backups, where the offsite backup hard drive(s) are to be stored, and all other pertinent data.

Conclusion

Once your procedure is written do not let it collect dust and become outdated. You should review the document on an annual basis to make sure the information is correct and current. Also, where possible you should try and test or dry-run your procedures ahead of time to make sure they are complete. If you have a spare PLC or HMI on hand, see if a coworker can follow your procedure and install the firmware and source code onto this equipment. If the procedure needs corrections or improvements it is better to find that out during a test run and not when process equipment is actually down.

There is no one-size-fits-all implementation when it comes to the backup and restore process in an industrial atmosphere. Many of the tools that are used in the office IT world can be utilized and included in a comprehensive industrial backup procedure. However, many aspects and challenges on the industrial automation side of things require unique and customized solutions. Hopefully this guide helps you think about the procedures that you already have in place or motivates you to begin developing this important safety-net document.

If you would like to discuss this topic further or are interested in an evaluation or study of your plant or procedure, please contact me at the phone number or email listed below.

Shawn Perkins, P.E.

ShawnP@wesslerengineering.com

317-788-4551

WESSLER
ENGINEERING

More Than a Project™

We can help.

CONTACT

Wessler Engineering
6219 South East Street
Indianapolis, Indiana 46227
P: 317.788.4551
F: 317.788.4553

Wessler Engineering is a civil and environmental engineering firm, specializing in wastewater, drinking water, and stormwater projects, providing services ranging from master planning and design to construction administration and process energy audits. Founded in 1975 and based in Indianapolis, Indiana, we have branch offices in Evansville, West Lafayette, and Fort Wayne.