

Industrial plants are increasingly becoming automated, leading to shortages of staff skilled in the management of automation and associated control software.

Increasing plant and workforce efficiency

by Claude Agostinetti, Systems Automation Management

With these systems becoming more complicated, the control software is constantly being blamed for plants tripping and outages. How do we ensure that we minimise these trips, speed up the disaster recovery times and release our technicians and engineers from mundane tasks such as backing up software while increasing plant availability?

Data management, back-up and version control software tools have been available in the IT industry for many years, but in the automation industries these tools have only become mature and accepted products in the last couple of years. Systems Automation and Management (SAM) has been implementing these tools at various blue chip companies, in order to ensure that the correct backups of the programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) and other micro-processor based devices are systematically done. There have been several products available on the market, which claim to be able to do this, however they have been very cumbersome to install and manage. Thus many clients become disillusioned after spending vast amounts on these products which they are unable to use.

From many years of experience, SAM has managed to find and use back-up, data management and version control software that is not only easy to install and manage but has been successfully employed and accepted by their clients. From experience SAM has found that most clients with back-up software systems, whether manual or automatic, find these do not work and

approximately 60% of the back-ups do not match the software on the plant. Thus the technician/engineer does not know which backup is the latest backup. This leads to many man-hours being wasted while the technicians try to establish which version of software is the latest before reloading any software. Furthermore, there have been many cases where the software reloaded was not the latest and the technician had to figure out what was changed and implementing these changes again before getting the plant up and running. Many plant production hours have been lost due to not having the latest version

of the automation software available during plant disaster recovery.

Another major problem on plants is ensuring that the changes implemented on site by the technicians are managed and documented correctly. Typically, faults occur at the plant late at night and the technician arrives on site, bypassing the faulty equipment in the software to get the plant running. He leaves the site to go home and forgets to document and backup these changes. No one is notified of the changes and he is the only one with copy of the latest software. Regular backups of the automation

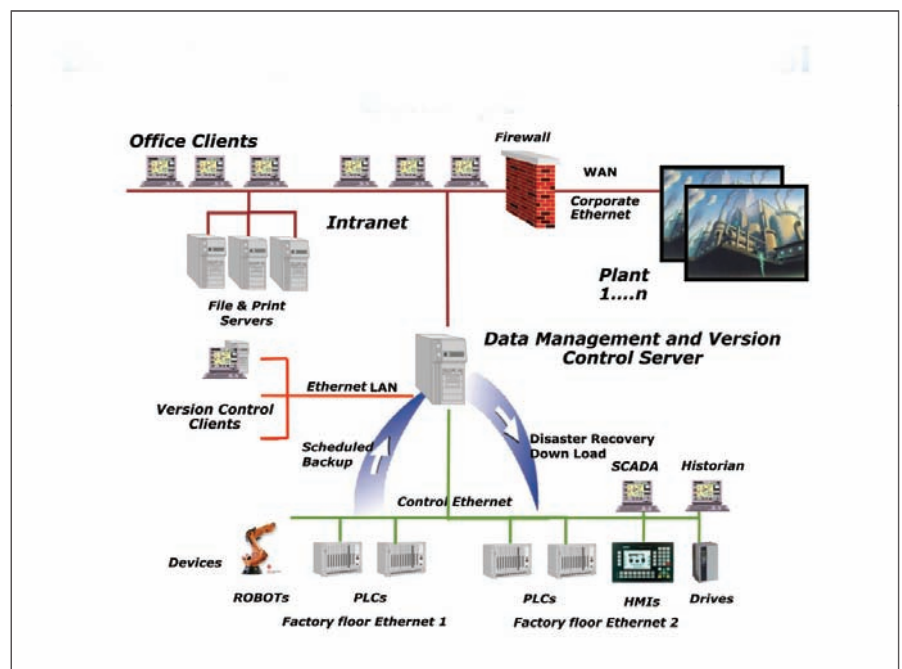


Fig. 1: Data management and version control concept.

software are usually done manually by the technicians and this is labour-intensive and boring. Thus, one finds that this task is normally left to the last minute and not done for several months, which means that the time between the day that the plant trips and the last software backup can be several months and no one knows exactly what has changed since the last backup. This makes disaster recovery very tedious and time-consuming. Many production hours are lost due to this factor and the cost is normally not recorded.

Skilled technical staff are sought after and retaining them is not easy, especially in the maintenance departments. Often staff turnover is high, with plant knowledge moving on with them. This necessitates rigorous version control, software backup and data management systems installed to minimise the impact of staff turnover and maximise knowledge retention.

The question must be asked, how do we minimise the impact of the above-mentioned issues as well as maximise the utilisation of the plant, equipment and skilled staff?

The concept is very simple. A central back-up server (CBUS) is installed on the process or office local area network (LAN) which can access all the PLCs, drives, human-machine interfaces (HMIs) and SCADA systems via the network. The data management, back-up and version control software is then able to address, connect to these devices and download the control software from the corresponding device (see Fig.1). The CBUS server is initially loaded with all the latest copies of the automation software. The configuration of the CBUS file manager reflects the logical plant process, and each section of the logical tree will have the automation software, drawing, manuals etc. stored together. This makes it easy for the technician to copy all the associated documentation as well as the automation software on to his notebook/programming unit before going to site and implementing any changes in the PLC, SCADA etc.

The data management, backup and version control software records who downloaded the software and the notebook/programming tool used. This makes it very easy to track who, when and why the changes were made to the automation software. The technician can book out any particular software exclusively, so that any other technician wanting to do changes is advised of who has the current software and that he cannot do any changes until the

software is booked back onto the CBUS. This prevents changes being done simultaneously on the same software by two different users. The technician is forced to record the reasons for the changes to the software. This ensures that anyone subsequently wanting to know why the changes were made, can easily understand these changes. This also allows one to obtain statistics of all the reasons that cause the changes to the software. By using the Pareto (80/20) principle, one can then determine the major causes of software changes and take corrective action to minimise changes. As the changes, comments and actions of the technicians are recorded, various audit reports can be created for analysis and further action.

Email reports

The data management and backup software can be configured to email all changes to the respective plant supervisor so that he is informed of all changes to the plant software. This also ensures that "finger trouble" is minimised and thus increases the availability of the plant.

The software back-ups of all plant devices that are on the LAN can now be scheduled automatically. Most clients elect to do their back-up once a day, late at night when data traffic is low. However, one can elect to do the back-ups per plant shift and even if the system is bypassed the changes will be detected per shift and this makes it easier to monitor who is changing the software. From experience, bandwidth on the network has never been compromised due to the fact that software is always zipped before being downloaded. The automatic backing up of the software now alleviates the technicians of this task, which when one has many devices to back up each time, can add up to many man-hours saved. All of which makes the investment into the data management, back-up and version control software feasible. For PLCs and devices that are not connected to the LAN, a utility is provided that allows less skilled workers to do the backups and store them on the CBUS.

With more devices becoming micro-processor-based, the software in these devices needs to be centrally managed. Devices like drives can take several days to commission and optimise, but the final optimised configuration is seldom saved. This means that every time the drive has to be replaced, it has to be re-commissioned and optimised. By having

the drives networked and accessible to the CBUS, these issues can now be eliminated.

Data management and back-up software has become mandatory in the food, beverage and pharmaceutical industries. With the ever-increasing threat of sabotage by disgruntled employees and terrorists, one needs to ensure that recipes are not altered without authorisation and that product is not compromised which could cause injuries or even death. One can now save the recipes that are in PLC data blocks on the central server. Any manipulation of these recipes will be detected even if the technician has forgotten to back up the changes. The American Federal Drug Administration has now made it compulsory that pharmaceutical companies implement measures to ensure that software changes are tracked and only executed by qualified personnel.

Thus access to the automation software needs to be managed and monitored. By having a CBUS, access to the software can be limited to authorised personnel per plant area, plant equipment etc.

It has been found that increasing the availability of the plant and minimising the time to restore the plant after a trip will easily pay for the installation of the system when compared to the cost of downtime of capital-intensive plants such as mines, power stations, automotive factories etc.

With power failures becoming a major problem in South Africa, the data management, back-up and version control software has a utility to download the latest automation software back in to the automation devices (such as PLCs, SCADA, etc.) directly from the CBUS. This makes disaster recovery a lot quicker and minimises plant downtime.

With systematic management of all data and software changes, a knowledge base is automatically developed making it easier for new staff to get to grips with complex automation software. This also minimises the impact when skilled staff leave, thus ensuring that knowledge is retained in the company.

With ISO 9000 becoming ever more important, the quality assurance systems can be modified to include the management of all the automation software.

Contact Claude Agostinetti,
Systems Automation Management,
Tel 011 803-0570,
claude@sam.co.za