AUVESY.

Technical Article

A step towards achieving greater security - Data management as a part of your cybersecurity strategy

A step towards achieving greater security – Data management as a part of your cybersecurity strategy

When people used programmable logic controllers in the past to control and monitor manufacturing processes, they had to make do with PLCs that had, in comparison to today's standards, a much smaller memory capacity. Today, the memory capacity of PLCs has grown as has PLCs ability to process larger qualities of data. This is due, in part, to the rapid evolution and development of high-level programming languages. Nevertheless, the ongoing digitalisation and automation of production processes also necessitate additional programming. More and more controllers are being connected to a network and therefore they need to be safeguarded. In addition to this, they must also have the capacity to take on an extensive range of tasks. It goes without saying that the data volume continues to grow at an ever-increasing rate. The task of translating high-level programming languages into machine language has become faster. Compilers and interpreters have long since taken over the task of translating source code into machine code, thereby relieving employees of the work involved in that particular aspect, though they do not relieve employees of the task of managing and organising data and versions.

The many and varied software versions all need to be taken into consideration during the commissioning phase of a production facility. This is the point that involves the most data that automation technicians will be faced with having to coordinate in order to get the production facility running according to the wishes of the operators. The more data there is to coordinate, the greater the chance there is for errors to creep in. Data can be mixed up or contain incorrect blocks. These unwanted instances can occur as a result of miscalculations and changes made to data. Data can, however, be compromised as a result of external manipulation. This can be done is such a sophisticated way as to cause false data to be displayed so that it appears that everything is functioning normally, when it is not. The ever-increasing number of interconnections between automation systems and the internet increases the likelihood of unwanted network access occurring.

Some computer viruses lie dormant, waiting for the moment that an IP address of an automation controller appears in a network, as is suspected in the case with the malicious computer worm, Stuxnet. The malware was specifically designed to target particular industrial control systems devices such as certain Human Machine Interfaces (HMI) and Programmable Logic Controllers (PLCs). The malware looked for controllers that had been set up in a certain way, and once it had identified these, it began its takeover. The creators of the Stuxnet virus remain unknown to this day. One thing is clear though, the advent of Stuxnet represents a serious threat that has wide-reaching global implications where the safety of critical infrastructures, human beings, and environment are involved.

Data management as part of your cybersecurity strategy

It has become paramount to proactively secure industrial facilities with an effective cybersecurity strategy. One way of achieving this is by implementing a strategy known as defence in depth. This strategy involves using several diverse defensive strategies throughout an IT system so that if one layer is breached, another layer will help to prevent a full-breach. The use of different methods helps to increase

the effectiveness of cybersecurity. However, a comprehensive solution is not available as of yet. Several well-known and successful examples of defence in depth strategies include:

▸▸The classic Firewall: prevents a computer network from unauthorised network access
▸▸ SIEM (security information and event management): provides real-time analysis of security alerts generated by network hardware and applications and thus helps to safeguard data in the long-term
▸▸ An intrusion detection system: helps detect attacks
▸▸ An intrusion prevention system: helps prevent attacks
▸▸ A honeypot: a security mechanism that functions as a diversion in order mislead the attacker
▸▸ Awareness training: helps to ensure that personnel are well-informed when it comes to security awareness

Naturally, there are other methods of achieving effective cybersecurity, however, increasing the awareness of personnel is one of the foremost strategies that can be implemented, so as to reduce the likelihood of human error – brought about by inattention or ignorance.

Documenting and backing up data

What is the best strategy to use against a cyberattack? If all lines of defence have been breached, the only chance of reducing the damage wrought by a cyberattack is to be able to quickly restore the last unchanged, hence virus-free version (disaster recovery).
Critical programs and data from automation devices need to be safeguarded. Since people began to keep records of data, safety measures have been developed, so as to ensure that the data remains free from unauthorised changes. Performing backups is the most commonly used method. Data backups of automation devices in production facilities (such as robots, PLCs or a HMI operating station) often require an inordinate amount of effort in order to be accomplished. If the device has been networked, it is possible to schedule automatic backups of data. However, it is important that the different types of data are completely backed up at regular intervals.

Executing regular backups

A backup consists of four different parts that make up a data set (see Fig. 1), which is then saved as a complete and consistent backup:

1. The program of the controller that is responsible for the steps involved in the process of production. This is done by programming languages such as LAD (LAdder Logic), STL, and GRAPH

2. The setpoints and parameters (e.g. for temperature or fill levels) need to be carefully monitored. They are important for condition monitoring (though in some cases they may be sometimes excluded from some backups). In order to ensure a consistent backup, it is important that setpoints and parameters are clearly defined (initial values)

3. Configuration data is important for customised production. It can be extracted from receptors and energy values. This type of data is often specific to the customer

4. Device logic is the fourth part that makes up a complete backup. In order for disaster recovery to be effective the system (firmware) and the program both need to be compatible.

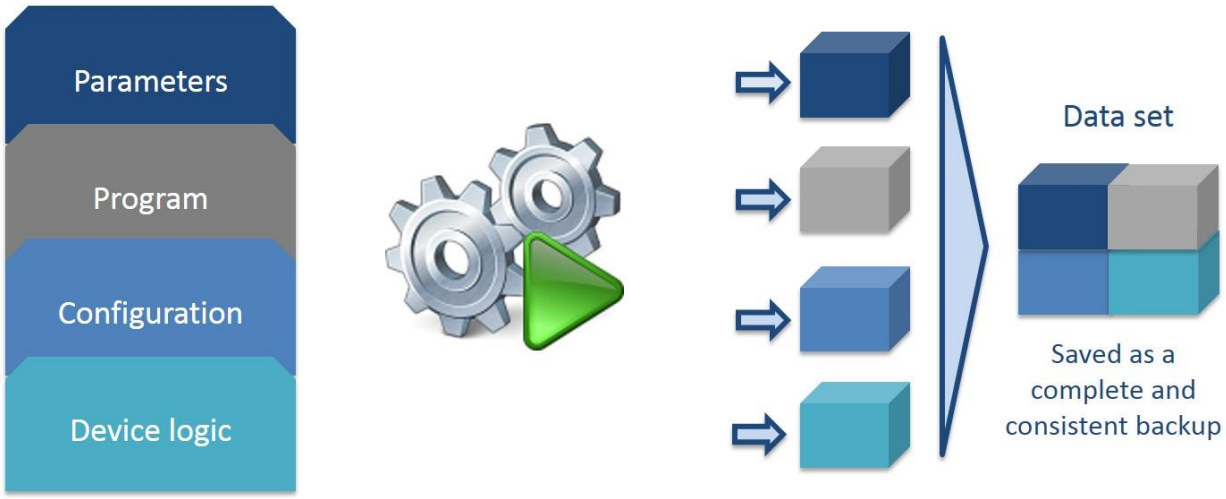

Fig. 1: How a complete backup taken from production can be used for disaster recovery (restoration of a previous version)

Classifying data backups is important for documentation. Generally, backups should be always be checked for completeness and accuracy each time data is transported. To be doubly sure, you can also compare checksum of the file(s). A checksum is a value that is derived from the sum of the correct digits in a piece of stored or transmitted data [3]. Checksums can also be used to detect errors in the data. Depending on how complex the rules for calculating checksums are, errors may be detected or ignored. If checksums are equal then the program has remained unchanged. When changes are documented, the version number, time and date, who made the changes, when and why are all included.

This is standard practice in production. However, it is often carried out manually by a technician, who goes from machine to machine, performing backups and comparisons of data, and making documentation. WHO changed WHAT, WHEN, WHERE, and WHY, are all questions which those who are involved in maintenance have to ask on a daily basis. In doesn't matter whether something has been changed between shifts, if a new machine has been integrated, or if a controller on a production line is being fine-tuned. The fact remains that each change that is not documented can lead to uncertainty, regardless of whether the change was authorised or not. It is thus of great importance to ensure the different data types used by a controller are completely and consistently backed up. If they are not, it is not possible to perform rapid disaster recovery.

How does disaster recovery work?

In order to get a better idea about the challenges involved in disaster recovery, we need look no further than a production facility. The maintenance department is almost always responsible for carrying out disaster recovery. That being said, maintenance is often treated as being separate from office IT, because it requires specific knowledge of how the machine code of a manufacturer works. The maintenance staff member goes around with their programming notebook in hand, which they use to connect to the many

and varied components involved in production. As a rule, the data taken from the last data backup is stored in the network, where it is only accessible to those who have been assigned the required rights.

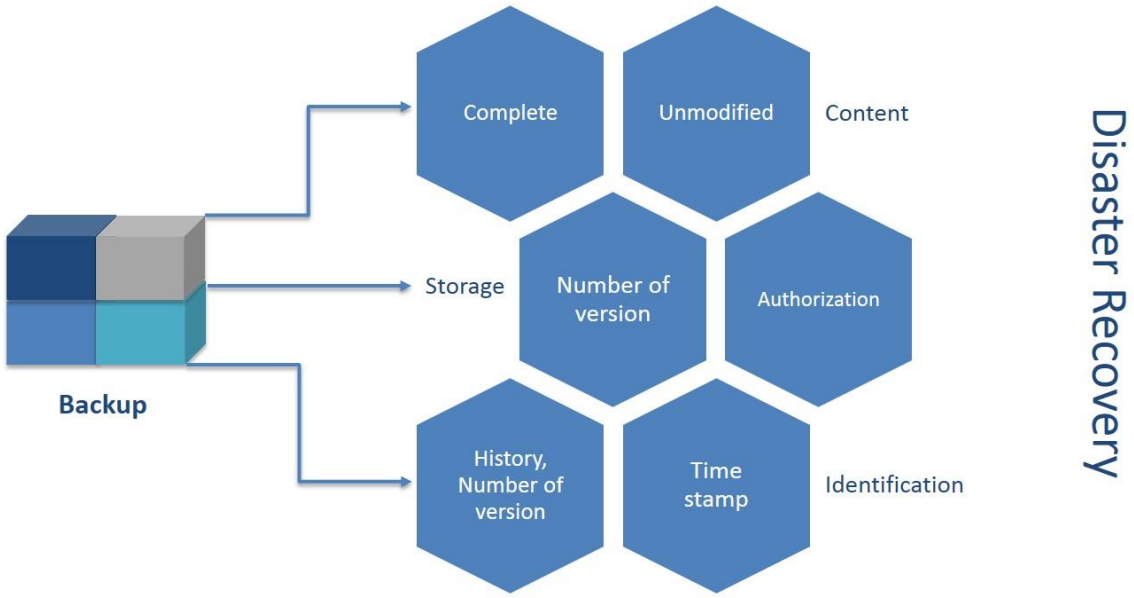

Fig. 2: Overview of a backup taken from production for disaster recovery. It is divided into parts based on content, storage and means of identification.

In instances where disaster recovery is required, the maintenance staff member copies the last unchanged version, and checks it for consistency, completeness. They also check to see WHO changed WHAT, WHERE, WHEN, and WHY (see Fig. 2). The maintenance staff member then connects to an automation device and downloads the version to the device. Whereupon they compare the version on the device with the last backup on the server. If both versions are identical, then the maintenance staff member knows that everything is as it should be and they document this. If both versions are not identical, differences will be displayed, which will have an effect on production (see Fig. 3). Despite all precautions, some errors do occur that are easy to explain, for instance: a physical defect or a battery outage. Undocumented changes can be the result of human error or, in the worst case scenario, the result of manipulated data.

If all lines of defence have been breached, performing a restoration from a backup can help

To be able to exploit the vulnerabilities of a system, on the scale of a zero-day threat, is an extraordinarily difficult and thus exceedingly rare task. Nevertheless, the cyberattacks that have occurred in the recent years, which targeted production facilities and critical infrastructures, have shown us just how dangerous such attacks have the potential to be. To safeguard data against such attacks will require a multi-modal cybersecurity strategy. No one single solution has as yet proven to be capable of achieving this. No virus scanner is capable of protecting production in real-time. No software update can be carried out, without the danger of data being manipulated.

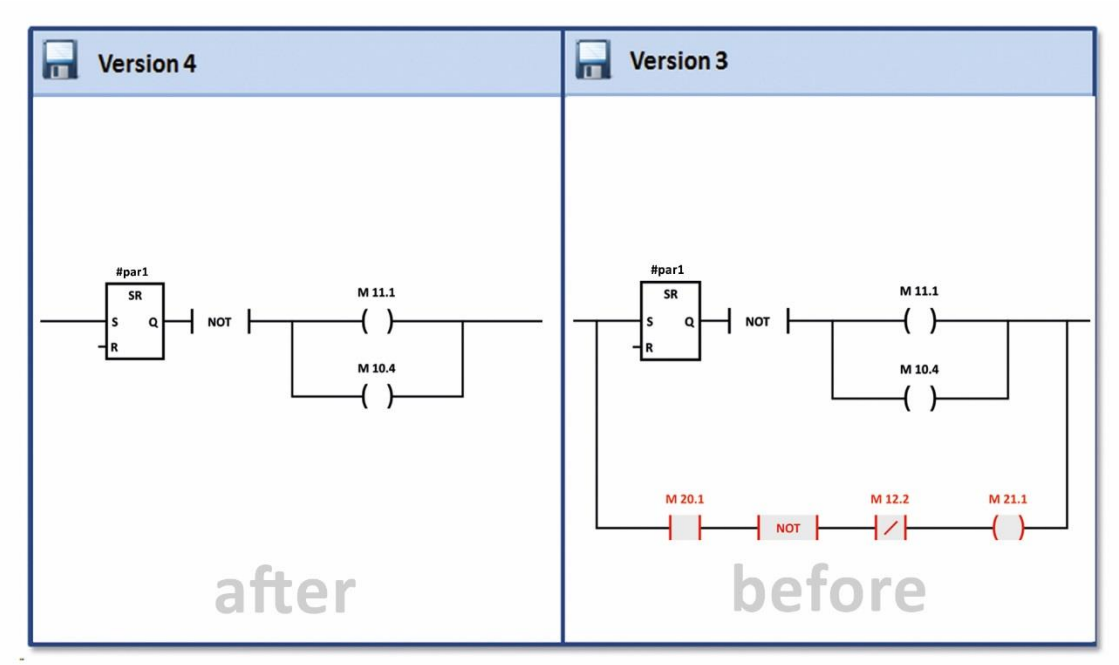

Fig. 3: Detailed analysis of differences between two software projects. Changes are highlighted in red.

Attempts have been made to strengthen the lines of defence and to close security gaps. In despite of these measures, new cyberattacks continue to be carried out. When such attacks succeed in breaching all defences, we have the solution of being able to perform a restoration of a system using the last unchanged (hence virus-free) backup version [2]. It is no wonder that cybersecurity is such a heavily discussed topic in context with the future of digitalisation. Our collective aim is clear: we need to further develop our defences against such attacks. There is still work to do, but for the moment data backups are a good starting point.

References:

[1] https://de.wikipedia.org/wiki/Pr%C3%BCfsumme

[2] In 2016 Deutsche Wasserwerke, http://www.spiegel.de/netzwelt/web/deutschland-sicherheitsluecke-wasserwerke-ungeschuetzt-im-internet-a-1103147.html In 2017 Ausnutzen einer Sicherheitslücke bei Windows-XP-Rechnern durch Wannacry-Virus, http://www.spiegel.de/wirtschaft/unternehmen/cyberangriffeauf-deutsche-firmen-verursachen-milliardenschaeden-a-1158975.html

[3] https://en.oxforddictionaries.com/definition/checksum

Authors

Dr. Thorsten Sögding,
Head of Business Development
AUVESY GmbH & Co KG

Stefan Schnackertz
Business Development
AUVESY GmbH & Co KG