SEPTEMBER 2017

International Cement review

polcid® – process control system

Process control system for the cement, lime and minerals industries
www.thyssenkrupp-industrial-solutions.com

engineering.tomorrow.together.

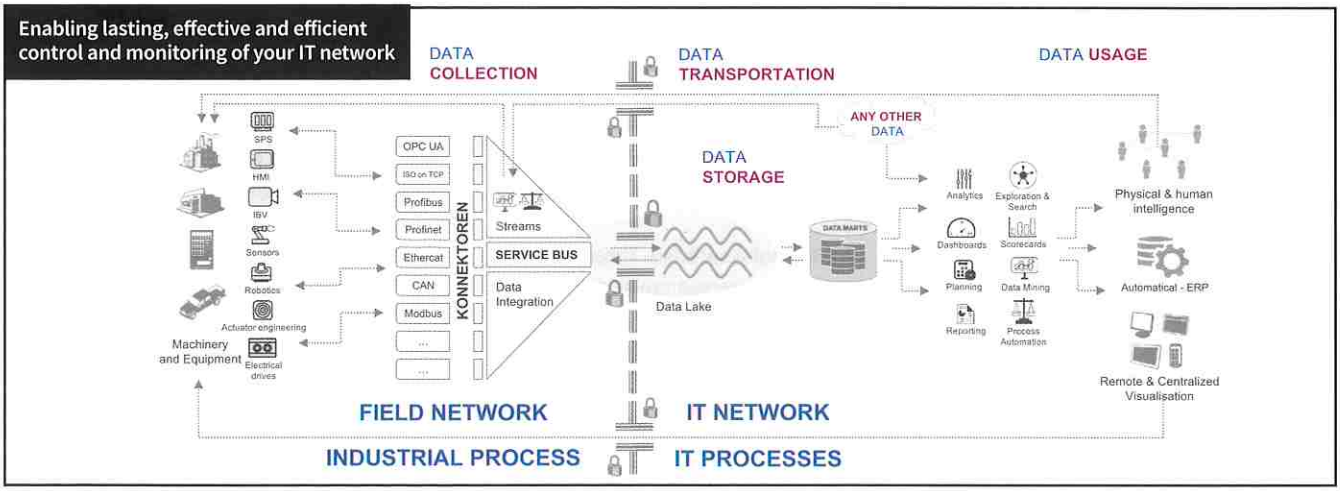
thyssenkrupp

Ensuring IT security

The role of security is becoming increasingly important for companies looking to gain control over their IT landscape. By identifying vulnerabilities in existing technical architecture, absolute control and security can be obtained to increase network safety.

■ *by* ***Oliver Kurtnacker,*** *Axians Industrial Applications & Services, Germany*

Enabling lasting, effective and efficient control and monitoring of your IT network



Picture the following scenario: you set up a network and subsequently don't pay any attention to its maintenance. Then imagine an acquaintance from your network empowers your contacts and plays them against you. Or imagine you are allowing users access to your network or other (unrecognised or unregistered) devices but do not pay attention to the type of access rights. Imagine you did not protect all URLs in your company with certificates and allowed easy access to your network. If all these points are taken together, or even looked at individually, control of your network is lost – a situation that you must face and counteract.

> *"The new business processes, which increasingly optimise operations are clearly no longer separated into the traditional fields of IT, production, finance and accounting. Companies have to take care and be aware of what happens in the 'field network' as well as the 'IT network'."*

Moreover, transferring these 'fears' to your network, imagine your company is running a web-based dispatch system and its URL is running 'http' instead of 'https', the situation becomes even more critical.

Furthermore, in smaller companies, it is often observed that employees can install any application they want. There are no restrictions in this regard and the installation is also only weakly controlled without any rules imposed by management or the IT department. The absence of these regulations make a network flawed and offers a large attack surface from the outside. They also question the position and responsibility of the network or system administrator. The administrator has no possibility of intervening in time.

New trends such as the IoT data linked into the classic world of automation – such as programmable logic controller (PLC) and supervisory control and data acquisition (SCADA) systems which are the backbone of production – combined with IT, are not only enabling a completely new world for business excellence but also raise a huge set of security topics.

Today, there are even viruses specifically targeted at PLC and automation equipment, such as STUXNET (a malicious computer worm) and similar dangers. This, combined with IoT devices that collect data and send it to the cloud, can cause considerable issues. It is mandatory to review this data on a regular basis.

The new business processes, which increasingly optimise operations are clearly no longer separated into the traditional fields of IT, production, finance and accounting. Companies have to take care and be aware of what happens in the 'field network' as well as the 'IT network' (see Figure 1). Data is collected from everywhere, transported to and used anywhere.

The perfect business process today follows intelligent rules to gather dedicated data to create the most beneficial outcome, which means, security becomes a critical issue for all areas of the business rather than an isolated topic.

Achieving absolute control

Therefore, achieving absolute control over the company's IT network by the administrator is key. To find the solution to this issue, three questions must be asked:

- What can lead to the threat of control over a network?

- What has caused the loss of control?
- Why is there no control at all?

To put these in context, let us assume that you have already integrated an automated and web-based system into your company and work successfully with it.

Various parameters are responsible for the lack or loss of control and must be investigated. A useful approach is to take into account three different threat levels: loss of existing control, eventuate loss of control and control does not exist.

1. Loss of existing control

Definition: you think you have control over your network, but there are few to no rules within the network. Under this scenario, the threats include:

- 'Third-party' users can access the network without defined user groups or access rights
- Access to the network can be obtained through unregistered hardware, without defined rights.
- Certificate management is deprecated or no attention is paid to it.
- Foreign components are integrated into the network, without more detailed examination in advance.
- Firewall is deprecated or does not exist: malware, email attachments are not checked.
- Passwords do not follow advanced encryption standard (AES) – the current standard of a 256-bit key.
- Passwords can be assigned arbitrarily without any rules.
- The use of static IP addresses – classic Alice Bob principle – allows very simple handling with all digital identities.
- Protected areas such as databases or tomcats have a weak password policy and can be viewed (and entered) by different user groups.

2. Eventuate loss of control

Definition: You experience the process of control loss or the result of the same.

- A virus has been successfully integrated into your network and accesses your system and the applications it contains.
- Data loss occurs.
- Access to services, network components, applications are denied, even though a user has the authorisation.
- Digital identities are not sufficiently protected due to expired certificates and lose their security.

3. Control does not exist

Definition: to have no control means that there is no discernible and predictable link between one's actions and the consequences that follow. That is, if my action to a process has only as little influence as if the process were controlled by itself, this means that influence or control is zero. In cases such as this, it could be that:

- The system is controlled from the outside and influenced by a third party.
- You have no knowledge about your own systems / system landscapes and the components and applications contained in it.

It is very quick and easy to see that the list of 'threatening dangers' is much longer in this third level than it is in the previous two.

This is not a surprise. Threatening dangers lurk everywhere and are omnipresent. In today's world, networks are predominantly transnational and allow hardware to communicate with other hardware from other countries with a foreign IP address. In many areas of our private life, we experience restrictions, such as not being able to access an American TV server with German IP addresses, to stream, for example, a US series or NFL games. Likewise, we can shop online worldwide, but selected products cannot always be imported from overseas sellers.

Transfer this example to your company and look at the exchange of data that takes place daily.

When and where does the moment occur when the question must be asked: who assumes the responsibility of data when it leaves the country? The question is: how do you ensure that foreign IP addresses do not pose a threat to your network?

To answer these two aspects, below is an explanation of what absolute control means and its resulting benefits.

What is control over a network?

From an economic sociological point of view, formal control is characterised by the imposition and monitoring of explicitly communicated rules and procedures, as well as the resulting penalties for non-compliance. Every process step can be monitored and there is absolute power over something or someone (eg, employees).

Additional security can be achieved by applying the Sarbanes-Oxley Act (SOX) regulations. Any system is SOX compliant, when external access to the applications is provided through a standard browser and authentication is secured by setting up password policies. It means that each password has to conform to one of the highest safety standards.

To ensure absolute control, it is essential that your network has the following six parameters:

1. Identity management

a. Each contact and user must be registered and maintained in an identity management system.
b. Each contact/user is assigned to a user group. The users in it have clearly-defined roles and are authorised to access selected components and data
c. All hardware must be registered and maintained. Each piece of hardware must identify itself with a certificate on the Remote Authentication Dial-In User Service (RADIUS). This Triple-A system (Authentication, Authorisation and Accounting) controls and allows users to dial into a computer system.
All hardware must be listed with the rating trust.

2. Certificate management

Certificates provide the basis for electronic identification and encryption of digital identities – online services, (peripheral) devices and machines. The establishment of certificate management and the maintenance of the certificates and keys is the responsibility of the data protection officer and their team.

3. Password policy

The creation of each password should follow a 256-bit encryption process, according to the Advanced Encryption Standard (AES). Any digital identity is linked to this password. Each user must change his domain password at regular intervals. Most of the issues arise due to a lack of understanding of employees. As well as by not paying attention to the secrecy of their passwords, it is a matter of educating the staff. The better the employees of a company are informed about the rules, the more secure the passwords are.

4. Interfaces

All components such as ERP, shipping system and peripheral devices must be accessible via secure interfaces.

5. Data exchange
Data exchange and data access may only be carried out if a correct inquiry is made to the database.

6. Deployment, management and maintenance strategy
With the help of a controlled software asset manager, applications and innovations are implemented throughout the entire network. A dedicated system administrator has absolute control over the entire network, providing access to all data and digital entities. The entire back-up scenario follows an efficient and sustainable plan, and always runs according to the same structure.

Advantages of absolute control

If these methodologies are taken into account and transferred to an example from everyday life, then control could look as follows. (Note: the example is based on the previously-set condition that a full-value dispatch automation system is already installed. Furthermore, it is the safest policy to pass these aspects through an audit process and certify their procedures.)

All automated processes can be timed and become integrated with further data of IoT and other business applications to gain full control of logistical processes. This means from the registration and arrival of the truck at the plant, up to its exit from the plant. An order (delivery note) must be assigned to a defined period. This ensures that no fraudulent activity can take place.

With secure pre-registration via an Internet disposition portal (iDispo), two things can be ensured:

1. Management can view a day-to-day report on cash inflows and outflows and is thus more quickly informed about the achievement of monetary targets. In addition, this enables precise evaluations that provide information on who has ordered what and when. This allows the transactions to be measured in relation to the frequency of a stakeholder and more concrete statements can be made about the forecast for the upcoming quarter.
2. Production knows all upcoming sales/purchase transactions in good time and can, if necessary, boost or reduce production at an early stage. This knowledge ensures optimal capacity utilisation. These evaluations have an impact on the planned energy consumption of equipment and enable optimised resource planning.

Monitoring of all bricks

Summed up, a properly-functioning network is based on a few manageable but fundamental bricks and rules. The uniqueness of a network is in absolute control of all components.

A true transparency of all business processes and transaction types of the complete supply chain as well as the database structures and all objects maintained in a proper identity management system enable lasting, effective and efficient control and monitoring.

Axian's aim is to educate and advise on each of these areas. It explains the consequences if even a partial aspect is not fully served. Together with its stakeholders, Axian creates dedicated specifications on business processes and the associated functionalities and system architectures in workshops on site. In addition to cost reduction, three of the main objectives are the acceleration and, if necessary, the simplification of relevant processes, a general increase in transparency and the introduction of an adequate safety standard. ■