SIEMENS
Ingenuity for life

Cybersecurity with 3WA air circuit breakers

Introduction

Communication in the context of Industry 4.0 enables more efficient use of plants and machinery and contributes to higher efficiency and lower costs. This results in advantages for both production operations as well as infrastructure facilities: Production in Industry 4.0 is networked right down to the field level, allowing machines to work in a more coordinated way. Status monitoring prevents downtimes in power distribution, energy flows become more transparent, and as a result, potential for streamlining and cost savings becomes more visible. The maintenance requirement becomes foreseeable, and measures can be planned in advance. Moreover, system components can be switched on and off according to requirements. Today, infrastructure systems can be monitored and maintained remotely.

The foundation for many innovative applications of Industry 4.0 and cloud applications are "intelligent devices", which communicate not only with one another but also with the internet. Access to communication-capable devices via the internet makes the protection of this access channel necessary: Effective cybersecurity measures ensure that systems can be operated securely, even in an environment that the relies on communication.

As core components of power distribution, communicative air circuit breakers enable added energy transparency. The 3WA circuit breaker opens up the advantages of network devices to operators, yet at the same time, it has been consistently developed with an eye towards cybersecurity. This white paper illustrates how integrated safety functions and operator-side safety measures make the 3WA air circuit breaker a secure solution for operators.

Contents

Safety in a networked business world

Wherever lots of data is transmitted, lots of data can potentially be intercepted. Wherever devices are remotely accessed, hackers can also exploit this remote access. Digitalization does not offer only advantages. More and more complex and professional cyber-attacks, precisely tailored to their target, represent a high damage potential for operators. Exploits in networks and devices offer an optimal opportunity to infect these very elements with malware.

Possible consequences

Cyber-attacks can impair or totally immobilize their target, be it the networks and the connected devices of a production hall, an office building or an infrastructure facility. In this, even supposedly "secure" components, such as communicative air circuit breakers in the power supply, can be attacked. This can result not only in high financial losses; the reputation of a company can also suffer damage. If infrastructure facilities are also affected, this may threaten to cause supply bottlenecks.

"Charter of Trust" for secure digital supply chains

In a globalized world, with complex merchandise and supply chains, cyber-attacks affect not only isolated companies but also numerous stakeholders along the value-chain. Consequently, cybersecurity must be understood as a universal concern – also by suppliers and business partners. That is why Siemens established the "Charter of Trust": A growing coalition of 16 major corporations (e.g. IBM, Daimler, Total) which came up with fundamental requirements for cybersecurity of digital supply chains and is consistently implementing them in own supply chains.

Exploits

- Programs that exploit the vulnerabilities of a system
- They do not cause damage on their own, but they could be used to infect a system with malware.

Malware

- Penetrates enterprise IT in order to carry out malware operations
- Is an integral part of many attack scenarios

Comprehensive approach for cybersecurity

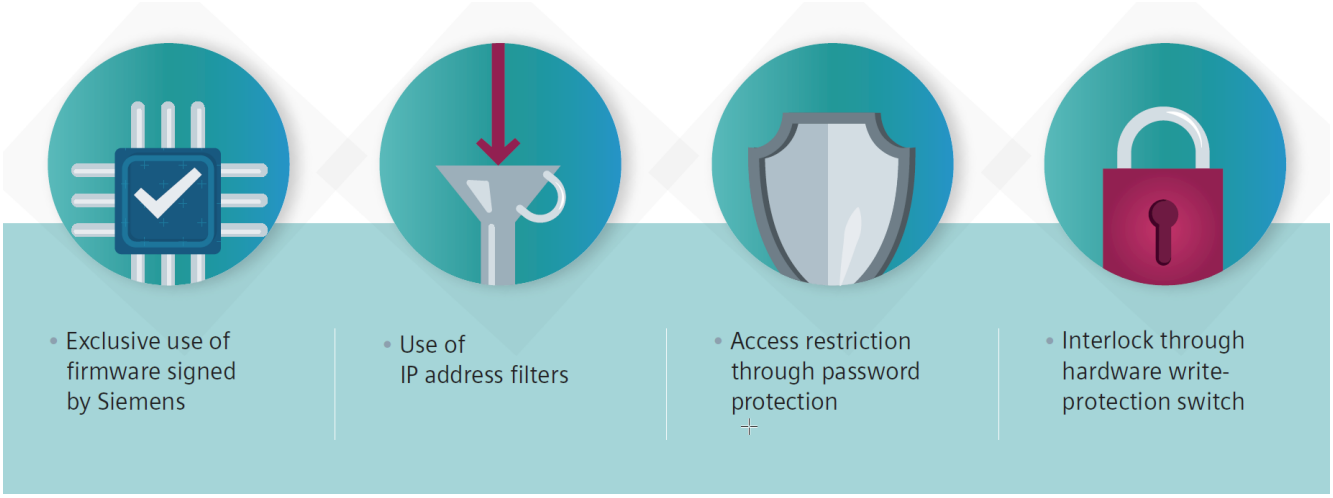
Cybersecurity encompasses the protection of the sum total of information technology connected with the internet or with a comparable network. Traditionally, this includes IT system such as computers, servers and networks, but in the IoT also all other devices connected to a network, right down to air circuit breakers. The protection of computer systems, networks and devices, along with their data, against manipulation, theft, unauthorized access and resulting faults, is the concern of cybersecurity.

Defense in depth creates integrated protection

Because cybersecurity is asynchronous, it poses a corresponding challenge during implementation: Whereas companies and infrastructure operators are required to protect themselves holistically, all that hackers need is one vulnerability for an attack on the system. In this, malware can proliferate throughout an entire enterprise via a single computer through so-called "lateral movement". For comprehensive protection from plant management to the field level, from access control to copy protection, Siemens uses the defense-in-depth concept. This involves a multi-layered information security concept, establishing plant safety, network security and system integrity.

Rapid countermeasures in case of security gaps

Part of the defense-in-depth strategy is ProductCERT, which advises customers and scans Siemens products for vulnerabilities and security gaps. If a gap is discovered during the course of analysis, the ProductCERT provide support with relevant countermeasures such as patches and security updates, and proactively communicates these to the customer.



The cybersecurity of communication-capable products from Siemens is built on four pillars.

Air circuit breakers for secure power distribution

Air circuit breakers are the centerpiece of power supply in every infrastructure and industry facility. Whether it be factories, high-rise buildings, airports or data centers – power distribution within the building begins everywhere with air circuit breakers. They deliver data for status monitoring, along with energy and maintenance management, and are used in many applications as switching, protection, measurement and display devices. Due to their positioning at the beginning of the energy chain of a building, unauthorized switching has the potential to impair the entire downstream power distribution. The resulting downtimes can create severe financial damage. Regardless of the application in which they are installed: Air circuit breakers are always neuralgic points in the power distribution and as such must be protected especially.

Protection thanks to secured service rooms – physical and virtual

There is indeed an awareness for the need to protect air circuit breakers. Operators know that access to them as a core component of power distribution must be strictly regulated. That is why physical access restrictions are long since the order of the day: By installing them in closed service rooms, the group of persons having access to the air circuit breaker is greatly restricted, and only selected specialist personnel receives access to such areas.

IT access rights only for selected persons

Digitalization and the associated use of communication-capable air circuit breakers, however, requires this protection to have a more comprehensive approach. In the Internet of Things, there are two rooms that need to be secured for effective protection of air circuit breakers: The service room in which the air circuit breaker is physically installed and the virtual room through which access is also possible. The latter requires equally strict regulation, however, as the closed service room. This means that access rights are restricted to ensure that only a designated group of persons has access to the air circuit breaker via IT systems. Only if both service rooms, the physical and the virtual, are consistently secured, is the air circuit breaker protected against unauthorized access.

Protection functions ideally already designed into air circuit breakers

In order to restrict virtual access, measures are needed to grant authorized users access to the air circuit breaker and thus utilize the advantages of a communication-capable air circuit breaker while blocking everybody else from access – both of receiving data from the air circuit breaker as well as of the input of data and commands into the air circuit breaker. For effective protection, measures of network technology are combined with protection functions, which in an ideal case are already integrated into the air circuit breaker. The type of security measures available to operators thus also depends on the air circuit breaker used.

Securing 3WA air circuit breakers against digital risks

The 3WA air circuit breaker is connected with the network via the communication module PROFINET IO/MODBUS TCP module COM190. It supports PROFINET for demanding industrial communication, as well as MODBUS TCP for power monitoring tasks. These two protocols, however, do not support cybersecurity functions as standard. Below is an illustration of how operators can nonetheless create a high level of cybersecurity when operating the 3WA air circuit breaker, using the IP network functions, along with integrated safety functions of the communication module. This also helps to create a security concept – independent from the concrete air circuit breaker.
There is no one-size-fits-all solution for cybersecurity. Depending upon the application, different threats need to be considered and corresponding measures developed. That is precisely what makes cybersecurity so demanding. The following applies: The mere awareness of digital risks offers no protection to operators. Only the development and implementation of a requirements-based security concept leaves them armed in case disaster strikes. And if there is no standard solution, the approach to implementing such a concept can be roughly divided into three phases:

Dependable protection thanks to a security concept

Uncovering vulnerabilities

Operators must identify potential points of attack and vulnerabilities in their IT and infrastructure. Based on the findings of this analysis, possible attack scenarios can be derived and evaluated. In the detection of vulnerabilities, as well as in the development and implementation of protective measures, external advisers can bring in a new perspective.

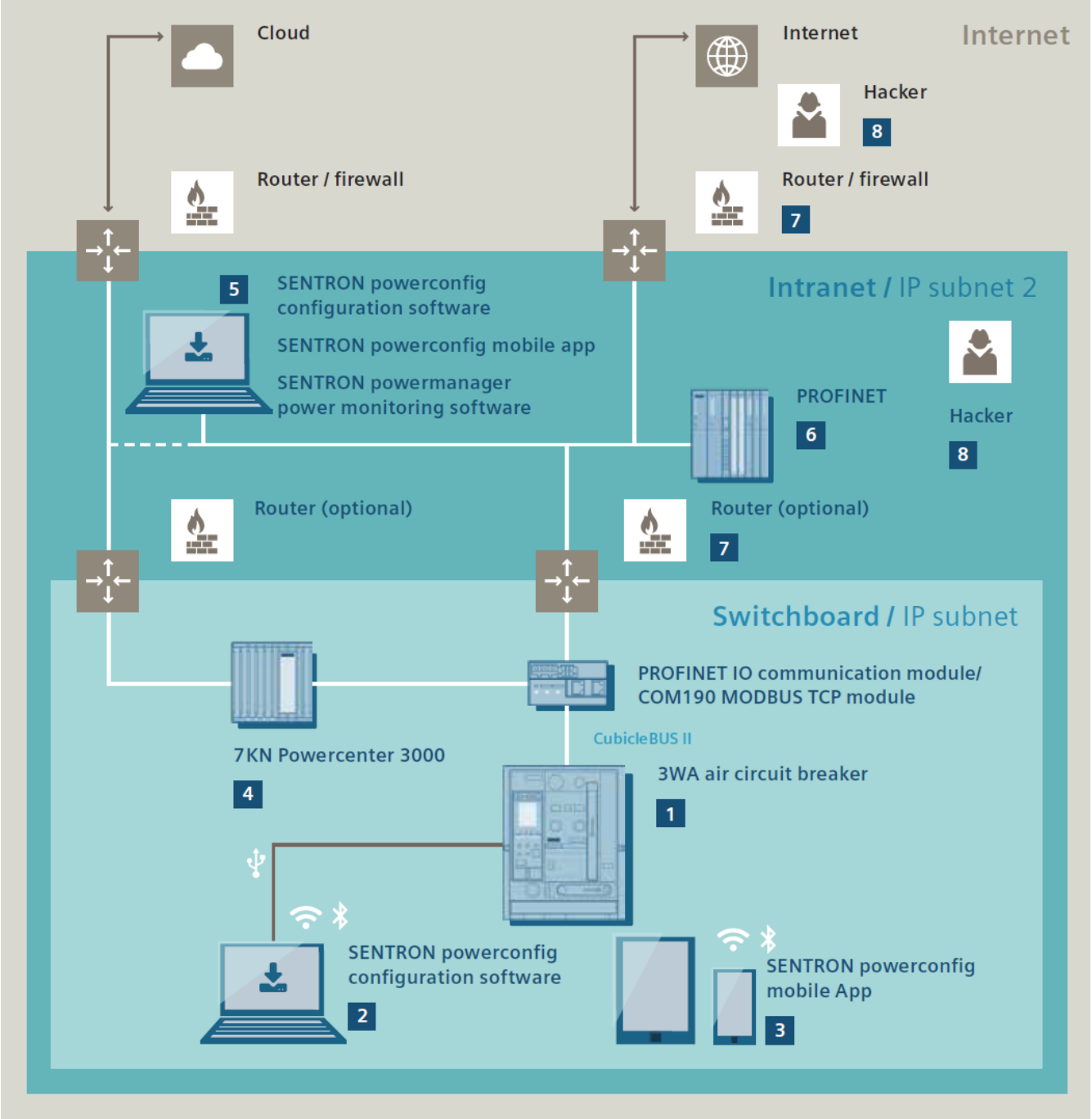
Defining and implementing effective measures

In the second phase, operators must review possible measures and their respective benefits, choosing the measures with which the identified attack scenarios can be fended off, and adapting them to their situation.

These security measures are based not only on the device and the related network nodes, which can be infected with malware, for example, but also on the prevention of social engineering and the avoidance of authentication that is too simple. In doing so, care should always be taken to ensure that cybersecurity does not rest solely on the shoulders of IT personnel. All employees must be trained accordingly in order to identify potential phishing emails as such, to prevent them from becoming a gateway for hackers.

Constantly adapting the security concept

Cybersecurity is never "finished". Because the starting situation is in constant flux, the protective measures also need to be dynamically adapted. That is why the security concept needs to be evaluated at regular intervals in terms of whether it still effectively fends off current risks. In addition, operators should always immediately install new security updates. Siemens communicates the publishing of updates actively on various channels, e.g. on Twitter at: *#ProductCERT*.



A cybersecurity concept using the 3WA air circuit breaker as an example.

1 3WA air circuit breaker: Protective measures in the 3WA air circuit breaker and the PROFINET IO/MODBUS TCP module COM190

2 SENTRON powerconfig configuration software: Safe and user-friendly interfaces

3 SENTRON powerconfig mobile app: Secure Bluetooth connection

4 7KN Powercenter 3000: Communication with the IoT data platform 7KN Powercenter 3000

5 SENTRON powerconfig configuration software, SENTRON powerconfig mobile app, SENTRON powermanager power monitoring software: The SENTRON powerconfig configuration software

6 PROFINET: Safe data exchange with PROFINET IO

7 Router (optional): Navigating safely in the network infrastructure

8 Hackers: Separate network for additional security

1

Protective measures in the 3WA air circuit breaker and the PROFINET IO/MODBUS TCP module COM190

Various safety features integrated into the 3WA air circuit breaker protect the circuit breaker against tampering attempts. For example, the PROFINET IO/MODBUS TCP module COM190 offers parameter writing and remote switching protection integrated directly into the hardware. This means that on parameter write protection, no parameters can be changed, whereas when remote switching protection is activated, switching on and off through any of the communication paths is prevented. Many functions are also always activated as a factory preset and must be manually and thus consciously switched off on the communication module itself. If the 3WA air circuit breaker is installed in an access-restricted service room, the write and remote switching protection parameter represents an insurmountable obstacle for unauthorized third parties when attempting to access the 3WA air circuit breaker.

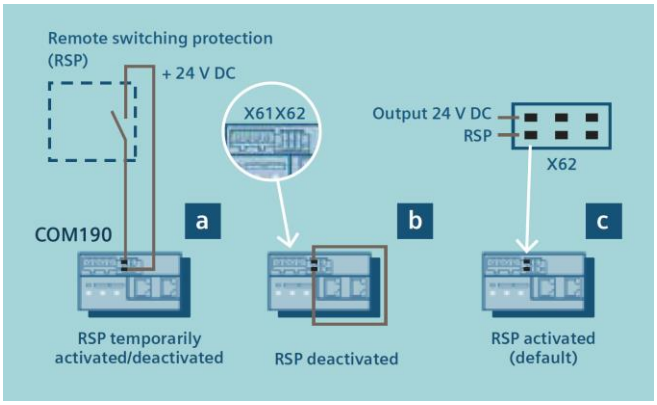
1.1 The parameter write protection of the PROFINET IO/MODBUS TCP module COM190

Via a DIP switch on the PROFINET IO/MODBUS TCP module COM190, the write protection parameter can be deactivated and activated. If write protection is activated, most of the parameters of the 3WA air circuit breaker cannot be overwritten via one of the communication connections.

The parameter write protection makes sophisticated circumvention solutions such as an adaptation of the rights assignments obsolete. A DIP switch that can only be actuated in a closed service room represents a solution that is as easy as it is secure. The parameter write protection only applies to the connection via MODBUS TCP and PROFINET IO of each communication module. If two communication modules COM190 are connected to the 3WA air circuit breaker, and if both are to remain blocked, the parameter write protection must be activated on both modules via the DIP switch.

1.2 The remote switching protection of the PROFINET IO/MODBUS TCP module COM190

Depending upon the application of the 3WA air circuit breaker, it can be useful to remotely control it or switch it off via the communication interface. In order to enable only remote switching, if the operator provides for it, the communication module COM190 is equipped with remote switching protection. This is indicated in the circuit diagrams by RSP (remote switching protection). It involves two terminals that need to be bridged in order to deactivate the remote switching protection. Like the parameter write protection, remote switching protection is activated as a factory default and has to be intentionally bridged where necessary.



Activation of remote switching protection (RSP) for the 3WA air circuit breaker.

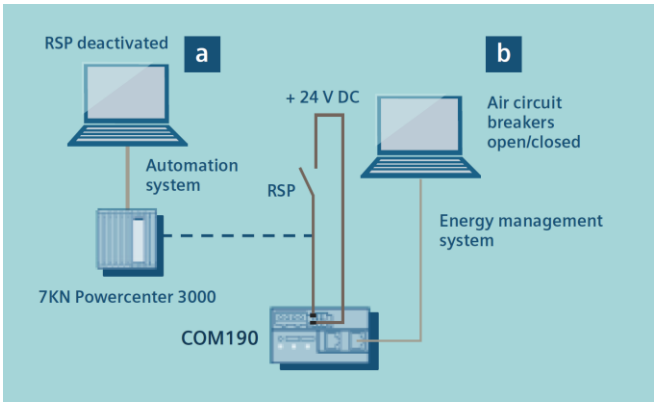
Remote switching protection, depending upon the requirements, can be used in various ways:

- Remote switching protection can be constantly activated or deactivated:

  To do so, the terminal is either left in its unbridged condition or constantly bridged.

- Remote switching protection can be temporarily activated and deactivated:

  In this case, the bridging is activated or deactivated by means of a selector switch, which is located on the outside on the control cabinet door, for example. Among other things, the procedure allows for increased safety during maintenance. The maintenance personnel can already activate remote switching protection on the door and therefore prevent unwanted remote switching during the maintenance work.



Temporary activation and deactivation of remote switching protection (RSP) for the 3WA air circuit breaker.

- Remote switching protection can be temporarily activated and deactivated via an independent path:

  Via a separate channel, for example a programmable controller (PLC), the remote switching is activated as needed and blocked afterwards. The remote switching itself occurs via another application, e.g. an energy management system. Remote switching is thus only possible by means of two independent paths, which makes unauthorized switching by hackers or malware significantly more difficult.

1.3 MODBUS TCP whitelist for secure access

For communications with the 3WA air circuit breaker via MODBUS TCP, access restriction can be set up with the help of a whitelist. In this whitelist, IP addresses or IP address blocks are stored that are allowed to communicate with the 3WA air circuit breaker. The communication module COM190 subsequently examines each connection build-up in terms of whether the IP address is in the whitelist. If it is not listed in the whitelist, no MODBUS TCP communication will occur.

The whitelist can be parameterized using the SENTRON powerconfig configuration software. An access restriction created in this way is exclusively limited to connections via MODBUS TCP, other connections are not controlled by it. In order for the access restriction through a whitelist to work reliably, the IP addresses of the devices with authorization must be in a defined range.

1.4 Signed firmware for secure updates

The 3WA air circuit breaker can be kept technically up to date and adapted to changing security risks with regular security updates. The installation of updates, however, represents a critical procedure, because in theory, third-parties could upload malware code with manipulated updates onto the 3WA air circuit breaker and as a result, deactivate safety functions, for example. In order to avoid this, Siemens signs firmware with a private key. An attempt to tamper with the code automatically causes the signature to change and the update from the communication module COM190 will be recognized as not trustworthy and not be installed.

1.5 Continuous risk assessment during development

In addition to the above-mentioned security features in the 3WA air circuit breakers and the PROFINET IO/MODBUS TCP module COM190, a repeatedly refined and adapted threat and risk assessment contributes to the 3WA air circuit breaker's being implemented safely from day one. Via regular Threat and Risk Assessments (TRA) throughout the entire development period, the 3WA air circuit breaker is continuously adapted to changing safety requirements. The results of the TRA flow into development. The security measures derived from this are also evaluated by various cybersecurity tests in terms of their suitability.

Potential points of attack can be immediately uncovered and remedied with a vulnerability scan. In parallel, an automated test for evaluating the robustness of the communication interface is carried out. Changing certain parameters of the IP communications controls the stability of the device.

2

Safe and user-friendly interfaces

In addition to the above-mentioned interfaces, the 3WA air circuit breaker is also equipped with USB-C and Bluetooth LE (Low Energy). During commissioning, the USB-C port serves as an external power source and at the same time provides the electronic release ETU600 of the 3WA air circuit breaker with power. In addition, it enables connection of a notebook for parameterization of the 3WA air circuit breaker. The approx. 800 different data points detected by the 3WA air circuit breaker are read out via this interface and evaluated with the SENTRON powerconfig configuration software.

There is a relatively low risk that the USB-C interface will offer unauthorized users access to the 3WA air circuit breaker. The installation in access-restricted service rooms ensures that the interface can only be reached and used by authorized persons. A sealable cover also offers additional protection against unauthorized access.

3

Secure Bluetooth connection

The Bluetooth functionality of the 3WA circuit breaker makes it possible to access it via the SENTRON powerconfig software. Because unlike the USB-C interface, the access-restricted service room is no longer needed as a protection level, many comprehensive security precautions are applied in the connection via Bluetooth.

The implemented Bluetooth standard offers powerful safety functions such as encryption. The transmission power was deliberately reduced to 4 dbm so that the effective range in the building is only a few meters. Moreover, the Bluetooth interface is deactivated by factory default and must be switched on via the display of the ETU600 electronic release. An active Bluetooth interface is intuitively recognizable by the ᛒ symbol on the display. After use, the Bluetooth interface switches itself off via a time-out in order to prevent improper access. For the pairing with the 3WA air circuit breaker, a one-time six-digit PIN is used, assigned by Siemens. It is newly generated for each 3WA air circuit breaker and loaded onto the respective unit during production. After the first pairing, the operator should change this PIN. In the course of operating the 3WA air circuit breaker, the Bluetooth interface can be kept technically up to date with signed security updates.

4

Communication with the IoT data platform 7KN Powercenter 3000

The IoT data platform 7KN Powercenter 3000 can be implemented as a gateway to the cloud. It collects information on energy levels from lower-level, communication-capable devices such as the 3WA air circuit breaker. This data is subsequently visualized and evaluated via Web interfaces (PC, smartphone, tablet), the SENTRON powermanager power monitoring software or cloud-based applications (e.g. MindSphere). The communication via an individual gateway protected with safety functions provides the necessary data security. In order to use the safety functions of the 7KN Powercenter 3000, the MODBUS TCP whitelist of the 3WA air circuit breaker must be utilized and the 7KN Powercenter 3000 entered in the list of the released IP addresses.

5

SENTRON powerconfig configuration software

SENTRON powerconfig configuration software is a software solution for commissioning and parameterization of 3WA air circuit breakers. Access can be restricted by means of SENTRON powerconfig with the help of the MODBUS TCP whitelist, as well as parameter write protection on the communication module COM190. The software can be installed on Windows systems and for mobile access on devices with Android and iOS. In this, the security of the system on which it is installed is decisive for the security of the app. Among other things, the anti-virus software, for example, prevents infection with malware and thus also protects the SENTRON powerconfig configuration software.

Siemens regularly publishes updates for SENTRON powerconfig configuration software. Operators should make sure to install them promptly and to consistently use the latest version of SENTRON powerconfig on all devices.

6

Safe data exchange with PROFINET IO

PROFINET is a standardized, manufacturer-independent industry standard and is constantly further developed: with respect to bandwidth, speed, performance, not to mention safety. As the leading industrial Ethernet standard for automation, it provides for quick and secure data exchange on all levels. Considering security mechanisms such as combined procedures for authentication, authorization and encryption PROFINET enables, for example, to implement new remote maintenance concepts.

7

Navigating safely in the network infrastructure

An inadequately protected network infrastructure runs the danger of unauthorized access to the 3WA air circuit breaker. The blocking of certain ports in an external firewall helps reduce this risk. For communications with the 3WA air circuit breaker, the following ports require a release.

Port type	Port number (decimal)	Service	Explanation
TCP	502 (default, but freely configurable)	MODBUS TCP	The MODBUS TCP port should be blocked when transferring to another network, if no MODBUS TCP connection to the 3WA air circuit breaker is desired on it.
UDP	161	SNMP	This service is required for operating the PROFINET IO interface.
	17008, 17009	Device detection and commissioning	These ports are used by SENTRON powerconfig and powermanager for commissioning the COM190 communication module. They should be blocked when transferring to another network (e.g. in a router firewall).
	34964	PROFINET RPC Endpoint mapper	These services are required for operating the PROFINET IO interface.
	49152 ... 49155	PROFINET RPC Device server	

Only services necessary for operation should be activated and, if possible, run in subnets. Network services such as VLAN (Virtual Local Area Network) or VPN (Virtual Private Network) enable operators to restrict access of 3WA air circuit breakers to necessary persons and applications.

8

Separate network for additional security

3WA air circuit breakers should not communicate directly with the internet, but rather with a closed network, which can be monitored more precisely. If communication via the internet is unavoidable in a special application, operations can also rely on services such as VPN in order to secure the data transfer with the 3WA air circuit breaker.

Summary

Extensive protective measures enable secure operation of communication-capable air circuit breakers like the 3WA air circuit breaker. This includes, on the one hand, functions that are already configured in the 3WA air circuit breaker: the exclusive installation of signed firmware updates, the protection of the MODBUS TCP interface with a whitelist and the parameter write protection and remote switching protection integrated into the communication module PROFINET IO/MODBUS TCP module COM190. The prerequisite for this, however, is that the 3WA air circuit breaker is installed in an access-restricted service room.

Precautions on the part of the operator protect the 3WA air circuit breaker against improper access by third parties. Only ports should be released that are actually necessary for communication with the 3WA air circuit breaker. Programs such as SENTRON powerconfig configuration software, which access the 3WA air circuit breakers, should be installed on secured systems. The communication via the IoT data platform 7KN Powercenter 3000 provides for additional security during data transfer. The protection of an 3WA air circuit breaker should never be seen in isolation, but always embedded in a comprehensive cybersecurity concept.

The 3WA air circuit breaker and other communication-capable devices promote more efficient and resource-saving workflows in Industry 4.0. The number of applications that build on communication are now continuously growing. A strong cybersecurity concept, which is supported in the safety functions installed in the devices, ensures that operators can safely and risk-free benefit from all the advantages.

Further information

All the latest information on 3WA open circuit breakers can be found at www.siemens.com/3wa

Published by:
Siemens AG
Smart Infrastructure
Electrical Products
Siemensstraße 10
93055 Regensburg, Germany

If you would like to obtain more information, please contact your Siemens Customer Support Center: www.siemens.com/lowvoltage/technical-support.