How to securely protect infrastructure?

End-to-end encryption is considered the optimal solution

Protecting public infrastructure against cyberattacks is of the highest priority and is compulsory for plant operators. However, when it comes to the mechanisms behind such protection, the question arises: What should and shouldn't be encrypted? There are contrasting views on this topic, which experts from Bachmann and Omicron discuss with the help of several case studies.

In principle, end-to-end encryption is considered the optimal solution for all internet use cases. For control systems, this means that only components directly in communication with one another hold the required decryption key, such as a smart device and Scada system. This maintains data content secrecy along the entire transmission route; attackers cannot obtain any information even after gaining access to network components or intercepting mobile communication transmissions.

The operational technology field – where IT resources are used in manufacturing – requires a more nuanced view of encryption. A distinction is made between authentication and encryption: Authentication ensures that the data connection has been established with the expected remote station. Further encryption is required to ensure tap-proof communication. The question therefore arises: Is the content of the communication confidential, or are anti-forgery protection and unique user authentication sufficient? The following two use cases show that both solutions have their place.

Use case 1: Access to wind turbine data

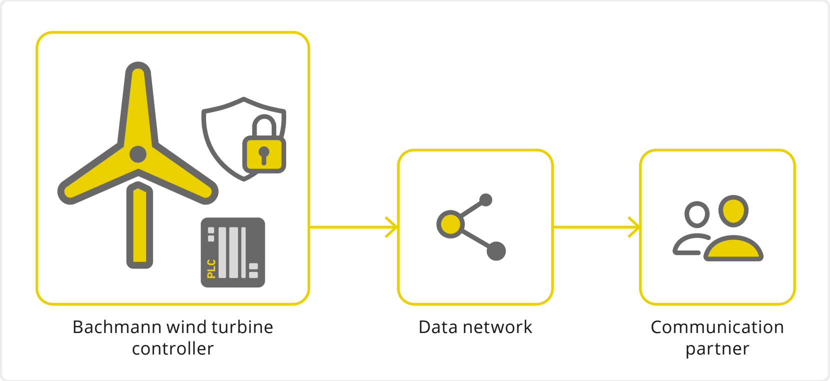

Fig. 1: End-to-end encryption of external plant communication with the Bachmann controller

Early on in wind power industrialization, the amount of data collected was very small and access was mostly only available to OEMs. Now however, with wind farms containing turbines from different manufacturers, when repairs are required, operators may enlist several additional, independent service providers. These service providers need to access operating hour meters and fault reports. In some cases, faults affect different specialist areas for plant protection, safety or feed-in guidelines, whereby additional information is also required.

At the same time, geographically distant direct marketers and energy brokers have access to power generation units to query available feed-in capacity and to transfer setpoint specifications and schedules for reactive and active power. This connection is also used to transfer billing data. In most cases, this access takes place via the existing internet connection or via satellite links and must be secured accordingly.

As security requirements continue to change, Scada systems for power generation units must be easily adaptable. Adding and removing users, changing access rights, or revoking certificates that are no longer required must be quick and simple, with changes being easy to implement.

The DIN EN IEC 61850 (VDE 0160-850)-certified MMS interface from Bachmann's controller portfolio enables secure communication via TLS certificates. Authentication and encryption can be separately configured. All settings are combined in an XML file and – provided the user has the required rights – easily distributed to all wind farm devices or to the park controller (Fig. 1). From this point on, only expected and intended users can send setpoints and switching commands and “listen in” on process data and events.

Fig. 2:
Omicron StationGuard
for monitoring internal
plant communication

Use case 2: Communication in protection and control technology

What are the disadvantages of encryption? Delayed reaction and transmission time comes up often. However, with protective relays on newer generation devices, times are usually within the required range for the signals contained in the message.

Another challenge is the potential for analysis: In switchgear automation, the readability of data traffic is critical. This is particularly true when operational faults have to be analyzed retrospectively. Encrypted network communication, however, makes analysis impossible. This is a particular problem for GOOSE messages, as they are often relevant for tripping protection.

Encryption can also be disadvantageous for security: Neither firewalls, nor attack detection systems, can scan encrypted communications for threats. Theoretically, it could be possible for security systems to open encryption, but this would in turn lead to other risks and efforts in the switchgear and control environment.

An intrusion detection system to monitor plant communications, such as Omicron's StationGuard (Fig. 2), offers numerous security advantages as well as plant diagnostics and monitoring: Individual activities in the MMS, GOOSE and IEC 60870-5-104 communication (DIN EN 60870-5-104) can be precisely distinguished and assessed. It is also possible to specify which devices are permitted to perform switching operations or configuration changes, for example, and which are not. StationGuard can also distinguish between maintenance situations and regular operation.

During normal plant operation, for example, the engineering PC does not usually perform switching operations. StationGuard configuration is kept simple and can be largely automated by importing SCL project files (Substation Configuration Language) or plant descriptions in CSV format. Due to detailed inspections by StationGuard, not only are threats to cyber security detected, such as manipulated packets or unauthorized control operations, but communication errors, issues with time synchronization, and thus potentially imminent device failures are picked up as well.

In this way, various security threats, as well as configuration errors in the control and network technology, can be detected during the initial StationGuard commissioning process. Omicron offers cyber security assessments to energy providers completely free of charge.

Conclusion

Authentication and integrity assurance for MMS and GOOSE communication is recommended across the board. The methods described in the DIN EN IEC 62351 (VDE 0112-351) standards can be used to ensure that the sender and recipient are the intended devices, and that messages have not been tampered with along the communication channel. The prerequisite is a system for key or certificate distribution, i.e. another server in the plant network, which must be made accessible to all switchgear, substation, power and control networks.

Encryption is optional but useful where communication content must remain confidential. This applies, for example, to confidential meter information, but may also be fundamentally necessary if communication crosses a public channel, such as a mobile network (5G). In this case, it is advisable to switch on channel encryption at the transition between private and public channel. This avoids the disadvantages of encryption in private networks, while preventing eavesdropping on public channels.

Details of the security standards series

The security standard series DIN EN IEC 62351 requires the use of secure transport protocols, by means of cryptographic methods, on all switching, protection, measuring and control devices. There is no way to avoid the authentication of communication participants by means of cryptographic certificates and message signatures. However, additional encryption of communications is optional and depends on the application.

A technical solution is proposed by the standards series with Transport Layer Security (TLS) in version 1.2, which allows the use of TLS with integrity checking, but without encryption. This is no longer possible in the current TLS 1.3 protocol, but there is an initiative in the Internet Engineering Task Force (IETF) (RFC 9150) that enables such "integrity-only cypher suites" for the successor TLS 1.3.

AUTHORS

Helmut Ritter
Product Line Manager Communication and Networking
Bachmann electronic GmbH in Feldkirch, Austria

Andreas Klien
Business Area Manager Power Utility Communication
Omicron Electronics GmbH in Klaus, Austria

FIND OUT MORE:

Telecontrol Protocol

CONTACT

Helmut Ritter
Product Line Manager
Communication
and Networking

info@bachmann.info

bachmann.

www.bachmann.info