BDEW White Paper in practice: IT security in the secondary systems

Dr.-Ing. Michael Conrad, IDS GmbH, D- 76275 Ettlingen, Germany
Dr.-Ing. Ralf Thomas, IDS-Gruppe Holding GmbH, D-76275 Ettlingen, Germany

Summary / Abstract

The extensive use of automation systems for monitoring / controlling hundreds of thousands of devices for the production, transport and distribution of energy is a result of the growth of the renewable energy sector in Germany. Exchange of data between field units and central control centers will be carried out on IP-based infrastructure. Those units are a new part of the critical infrastructure in terms of IT security.
This paper provides a practical insight into the implementation of IT security mechanisms for remote terminal units and SCADA systems (secondary equipment) in accordance with the BDEW white paper "Requirements for Secure Control and Telecommunication Systems" [1]. It also presents an evaluation of a variety of tools, protocols and procedures in terms of technical and organizational feasibility.

1 Introduction and Motivation

Smart Grid and smart metering are based on society's efforts to replace nuclear power, the development of renewable energy and the liberalisation of energy markets. High investments into decentralised power systems, substation automation and the monitoring of distribution networks are expected for the next years. This calls for the ability to control network components for the purpose of optimal power management, taking into account the volatility of the renewable energy systems. Therefore a comprehensive expansion of IP-based communication structures is necessary. Due to the requirement for low infrastructure costs, the use of existing public communication networks and protocols is recommended.
Secondary equipment of distribution network operators becomes part of the critical infrastructure and must be protected against manipulation by external attackers. In document [1], the basic requirements for IT security are defined by German energy suppliers. This leads to formal requirements for communication security, data security and system security for secondary equipment. The white paper does not provide instructions and concrete solutions (tools, protocols, procedures). Implementations made by manufacturers need to be evaluated by experts with particular emphasis on security, until standard specifications (e.g. ISO 27019 [2]) become available.

2 Structure of existing and future telecontrol systems

The significant increase in renewable and decentralized energy suppliers and the need for the monitoring and control of power systems is leading to changes in the structure of the associated telecontrol systems. The structure of "classical" and of future telecontrol systems is shown side by side in Fig. 1.

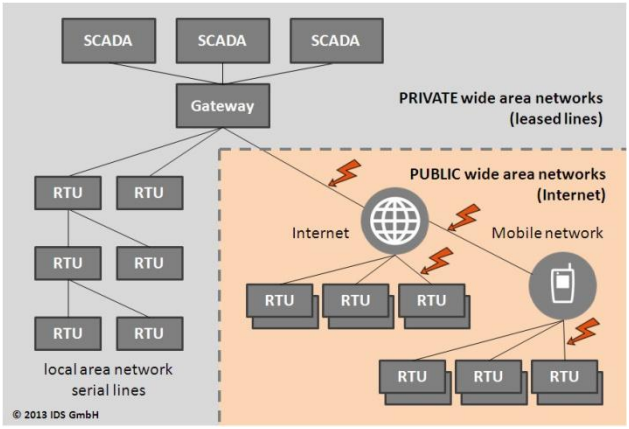

Figure 1 Structure of future telecontrol systems

Existing telecontrol systems, as shown on the left, for the monitoring and control of classic utility systems (electricity, gas, water) usually have a multi-layer and strictly hierarchical structure. At the head of the system are one or several SCADA systems which contain the central monitoring and control functions and which act as interface to humans. The SCADA systems are connected to the RTUs via one or several telecontrol gateways. A telecontrol gateway acts as communication link to the higher-level RTUs and carries out the aggregation of process data. There are usually several levels of RTUs below the telecontrol gateway. These levels are based either on the structure of the communication systems in use, or on functional interdependencies. A typical example of functional interdependencies is the substation automation of power grids: e.g. there are several RTUs in a transformer station which also exchange information amongst each other. Usually one RTU acts as data exchange frontend for all RTUs of the substation.
In the past, security requirements on the classic telecontrol systems were usually rather modest because those systems were installed and operated in a secure environment, using a purely private communication infrastructure

for data exchange. The current security discussion has highlighted the increasing security requirements even for those telecontrol systems; an upgrade of those systems in terms of security, however, has not yet been demanded.
The expansion of renewable energy and the concomitant emergence of distributed energy resources (DER) is increasing the likelihood of less complex telecontrol systems, as shown on the right-hand side of Fig. 1. Instead of a multi-layer hierarchical structure, the new telecontrol systems usually have a very flat structure. At the head, there are still SCADA systems; communication with the different RTUs also takes place via telecontrol gateways. Below these gateways, however, there is no further hierarchical grading – in terms of communication, all RTUs are arranged directly below the telecontrol gateway. Furthermore, there is no functional interdependence between the different RTUs.
In contrast to existing telecontrol systems, it is safe to assume – due to the high number and geographic distribution of distributed systems – that future telecontrol systems will include a considerably higher number of RTUs. For reasons of economy they will be based on public IP-based communication infrastructures (internet, mobile networks). One can expect that the demands on operation security for those systems will increase considerably. On the one hand, the distributed structure of RTU systems in some cases precludes their operation in a secure environment. On the other hand, the fact that communication between the telecontrol gateways and the different RTUs takes place via public communication infrastructure significantly reduces information security and renders it vulnerable to attacks.
Our analysis shows a high security demand for both types of telecontrol systems. Existing telecontrol systems operated in a secure environment have to be protected also against attackers as future large distributed telecontrol systems using public communication infrastructure.

3 BDEW White Paper

Subsequent to preparatory work by the energy supply company RWE AG, the German Association of Energy and Water Industries (BDEW) published the BDEW white paper "Requirements for Secure Control and Telecommunication Systems" [1] in 2008. This document contains security requirements from different realms (computer systems, communication, application and development). Additionally, it includes requirements on the documentation of various processes, such as data backup, data restoration and emergency planning [3].
Taking the requirements of this white paper into account, the owners of telecontrol systems shall be enabled to protect their systems against typical attacks and to issue controlled responses to security incidents [4]. In contrast to existing norms or standards, the BDEW white paper does not prescribe any special procedures or protocols, giving greater leeway for the fulfilment of the outlined security requirements.

3.1 Relevant aspects

Apart from general security demands on organization, documentation and emergency planning, especially paragraphs 2.2, 2.3 and 2.4 of the BDEW white paper contain a number of technical security requirements that are particularly important for RTUs and SCADA systems. These requirements, in terms of functionality, can be subdivided into three groups (see [1] section):

- Device security (2.2.1, 2.2.2, 2.4.1, 2.4.2)
- Communication security (2.3.1, 2.3.2, 2.3.3, 2.4.3)
- Data security (2.1.1.6, 2.1.1.10, 2.4.5, 2.4.6)

The term "device security" refers to the protection of the actual RTUs or the SCADA system. It is important to prevent attackers from obtaining unauthorized access to systems or subsystems. This applies both to process interfaces and to service and diagnostic interfaces. The device in question has to provide protective mechanisms against simple denial-of-service attacks, otherwise the attacker may be quick in preventing the execution of planned functions.
"Communication security" refers to protective measures for the exchange of data between RTUs or between RTUs and SCADA systems. The two foremost requirements are the integrity and authenticity of data; it must be possible to detect without a doubt whether data have been manipulated or whether data have been exchanged with unauthorized communication partners. Depending on the application scenario, the confidentiality of data may also be an issue.
Apart from device and communication security, data security will also play a major role in the future. Data security includes protection of data outside a secure transmission environment, which is the case, for instance, with the persistent storage of data or event logging. Similar to the protection of data during transmission, it is vital to ensure the integrity, authenticity and confidentiality of data.
Further security requirements, such as the availability and robustness of the communication infrastructure, are not highlighted in this paper because those security requirements have to be fulfilled by the respective infrastructure itself.

4 Device security

Device security is the main security objective. If device security is insufficient, even a high degree of communication or data security becomes useless. Attackers could compromise the respective device and directly read or manipulate data. To ensure a sufficient degree of device security, at least the following demands must be fulfilled:

- System hardening
- Access control
- Communication control

4.1 System hardening

The objective of system hardening is to minimize the vulnerability of RTUs or SCADA systems and to provide a maximum degree of basic security.

As part of the development process, it must be verified whether security gaps are known with regard to the application components to be installed; if this is the case, it must be checked whether a newer version for the component in question is available. This check should be carried out at recurring intervals and should therefore be included in the development process. Additionally, it is necessary to check for security gaps in operating system components. If desired, the typical server systems (Windows, Linux) automatically provide security updates of operating system components. However, these functions are often not available for embedded systems used by RTUs.

Prior to their application, all services there are not required for specific tasks within a telecontrol system must be deactivated on the respective devices. This includes, on the one hand, general services which are usually never required anyhow; on the other hand, it is also possible to activate or deactivate services depending on the respective application scenario.

Ensuring the system and application components and the active services are up to date, system hardening also includes making security-relevant system settings, such as, for instance, prescribed authentication procedures, permissible protocol versions or settings regarding the scope and complexity of user passwords.

For Windows-based systems, Microsoft offers different profiles of system settings with graded security settings which can be used as required or can be expanded in accordance with one's own regulations. Additionally, tools are available for standard server systems that enable the administration and integration into systems of the respective profiles.

4.2 Access control

Apart from system hardening, access control to all services provided by a device is an important aspect when it comes to ensuring a high degree of device security. The task of access control is to permit the utilization of a given service only to authorized persons or communication partners.

In the case of RTUs where no interactive access is made during normal operation, access control has to regulate access of other RTUs or SCADA components.

Unfortunately, the majority of telecontrol protocols that are in use nowadays are not include access control functions. Therefore, access control often can only be implemented in connection with additional security protocols (e.g. TLS). Furthermore, it is vital to ensure sufficient access control for the available service and diagnostic interfaces. With SCADA systems, access control of users is as necessary as is access control of other SCADA components. For the access control of users, it is important to ensure suitable authentication procedures.

Apart from ensuring a viable access control, it is of foremost importance to deactivate or delete unused service access to ensure a high degree of device security.

4.3 Communication control

In contrast to access control, communication control is another way of increasing device security. For this purpose, the communication capabilities of a device within a telecontrol system are reduced to such an extent that communication can be established only with specified communication partners. Although this no absolute protection against attackers, this measure makes attacks substantially more difficult because intruders can no longer initiate their attacks from any given position within the network.

The limitation of the communication capabilities of a device can be easily implemented by means of a packet-based firewall which is executed on the device itself. Configuration of the firewall can be done in two different ways. With a static configuration, and depending on the application scenario, access to specific services is limited using port numbers and network interfaces. If access to a service via a specific network interface is permitted, this service can be used by any given communication partner. With a dynamic configuration, services are enabled in the firewall only for the respective communication partners that are identified by means of their IP address. The benefit of this method is that the service in question cannot be used by any communication partner at will.

Moreover, a firewall can also be used to restrict access to insecure services which may not include a functional access control themselves.

5 Communication security

Unfortunately, the communication protocols used in current IP-based telecontrol systems (e.g. IEC 60870, IEC 61850, Modbus TCP) do not provide their own security functions which fulfil the requirements on authenticity, integrity and confidentiality. In order to ensure the required communication security despite these shortcomings, it is necessary to employ extra methods. One obvious method is therefore the use of existing and well-proven security protocols which ensure the secure transmission of data via insecure communication infrastructures.

Possible candidates to ensure the security of insecure communication procedures are the following protocols:

- IPsec
- OpenVPN
- TLS

The well-known and widely used point-to-point tunnelling protocol (PPTP), in connection with the authentication method MS-CHAPv2 was not considered in this paper due to security gaps with regard to authentication. The examined protocols hardly differ from the purely cryptographic methods. All those methods are capable of using standard algorithms (e.g. AES, SHA) for the encryption and security of data. However, these protocols differ with

regard to their scope of functions and the administrative effort.

5.1 IPsec

The security extension IPsec of the well-known Internet Protocol (IP) was introduced in 1998, last revised in 2005 and published as RFC 4301 [5]. In contrast to most other methods for secure data transmission, IPsec operates directly at the network layer of the ISO/OSI reference model and thus allows for a completely transparent approach to secure data communication. IPsec defines several protocol headers that are inserted after the IP protocol header.

IPsec supports secure data exchange between several IP networks to build a virtual private network (VPN), as well as the protection of individual communication connections. Due to the implementation within the network layer, there are problems in connection with NAT (Network Address Translation), which can be solved only by an additional encapsulation of IPsec traffic within a UDP communication connection. In addition to the IP protocol stack, the deep integration of IPsec requires an extensive administrative access to the operating system.

Unfortunately, IPsec itself does not contain mechanisms for the authentication of communication partners and negotiation of key material in establishing a secure connection. For this task, the Internet Key Exchange protocol (IKE) is normally used. It supports the negotiation of key material and the password- or certificate-based authentication. The older version IKEv1 in turn has problems with NAT scenarios, but in the current IKEv2 these problems have been remedied.

5.2 OpenVPN

OpenVPN provides an alternative to the rather complex combination of IPsec and IKE. OpenVPN also allows the construction of secure virtual private networks; however, it uses TCP or UDP for data exchange, therefore the NAT problem is eliminated. For the connection of secure communication channels, OpenVPN uses the TLS protocol, which is briefly introduced in the following section.

Through the use of the TLS protocol, OpenVPN - unlike IPsec - already includes mechanisms for authentication and key negotiation and therefore requires no additional components or protocols. Integration into the respective operating system takes place by means of a virtual network interface. For this purpose, administrative access to the operating system is needed; this procedure, however, is not as deep as when using IPsec.

5.3 TLS

Originally developed under the name Secure Socket Layer (SSL), this protocol has been developed since the late nineties by the IETF under the name of Transport Layer Security (TLS) and is currently available in version 1.2 in RFC 5246 [6].

Unlike IPsec and OpenVPN, the focus with TLS is on the protection of individual TCP-based communication connections; this protocol, however, does not enable the establishment of virtual private networks. For UDP-based communication, the protocol Datagram Transport Layer Security (DTLS) - based on TLS – is available.

TLS operates between the transport layer (TCP) and the application layer, thus protection extends only to the application data. However, this has the advantage that TLS can be implemented directly within the application and is not dependent on the support of the subordinate operating system. In addition, when using TLS, no administrative access to the operating system is required.

Therefore, TLS is ideally suited to upgrade existing telecontrol protocols to achieve the desired security features, without having to make major changes to the basic system. The use of TLS for TCP-based telecontrol protocols is described in the standard IEC 62351 [7].

When establishing a TLS connection, the two communication partners negotiate the cryptographic method to be used (so-called cipher suite) and authenticate to each other based on X.509 certificates. The authentication the server to the client is mandatory, the authentication of the client as against the server is optional. At the same time the connection-specific pre-master secret is generated during the negotiation. From this, the key material is derived subsequent to protect the application data.

5.4 Conclusion

To fulfil the requirements of communication security there are multiple options. The use of VPN tunnels to secure data transmissions is transparent to applications, but requires administrative access to the operating system. In contrast to VPN tunnel TLS or DTLS will be applied on application level and do not require administrative access to the operating system, but can only secures a dedicated communication channel.

At the beginning of implementing communication security for telecontrol components, it is easier to use VPN tunnels. All communication connections using the VPN tunnel will be protected and no changes to the different applications are necessary. For dedicated protocols (i.e. IEC 60870-5-104) an implementation of (D)TLS makes sense in a second step.

6 Data security

Even though data security currently is not regarded as important as device and communication security, its importance is expected to increase in the future. Data security refers to the protection of data that are stored or processed on the systems that are being considered. In contrast to device and communication security, there are practically no common procedures or standards for the implementation of data security, therefore scenario-specific solutions are usually employed.

In the application scenario of a telecontrol system, the following data requiring an increased degree of protection could be identified:

- Configuration data
- System and application files
- Event data

6.1 Protection of configuration data

In our present application scenario, configuration data are understood to mean information that is used for the configuration of an RTU or of a SCADA system. In order to ensure sufficient protection against attacks on configuration data, it is vital to ensure the authenticity and integrity of the data in question. In some instance, it may also be necessary to ensure confidentiality of the data.

There are two different approaches to ensure data authenticity and integrity. Exclusively on the basis of cryptographic hash functions, it is possible to use a simple approach which includes a secret in the calculation of the hash value (HMAC), thereby ensuring the authenticity and integrity of the data. A likelier approach, however, is based on asymmetric encryption methods. Here, the authenticity and integrity of data is ensured by means of a digital signature. In both cases, data confidentiality can be realized through the use of a symmetrical encrypting method.

6.2 System integrity

The concept of data security stipulated by the BDEW white paper is not limited to the data that are processed or stored in an RTU, but also applies to the RTU's software components because otherwise attackers would be able to able to modify the respective components without being noticed, and to successfully start and attack directly from the RTU.

For this reason, it is important to perform a periodical integrity check of software artefacts on the devices, for instance by means of the OSSEC software. This software is available for a number of operating systems, enabling – amongst others – integrity checks of system components. Moreover, it supports the secure transmission of integrity check results to a central system where these results can be further processed.

6.3 Event data protection

Apart from ensuring the security of configuration data and software components, the secure storage of event data is also of vital importance. Event data refer to incidents (e.g. failed log-in attempts) during normal operation. These data must be stored and secured against modification, since otherwise attackers are able to delete or modify them, thereby suppressing the registration of attacks.

Similar to the protection of configuration data, it is advisable to use digital signatures to ensure the authenticity and integrity of event data. For this purpose, event data are signed using the key material of the respective device, thus making sure that they can be unambiguously assigned at all times.

7 Implementation and experience

The following chapter provides a brief description of experiences made in the course of the preparation and auditing of a telecontrol system that consists of SCADA and telecontrol components, in accordance with the BDEW white paper. In the security audit an application scenario of a substation automation system consisting of several field units of type ACOS 750 and the SCADA system HIGH-LEIT from the company IDS GmbH was inspected. Furthermore, the findings made during this process and the future proceedings based on these findings are illustrated.

7.1 Auditing in accordance with the BDEW white paper

In the course of an auditing procedure in accordance with the BDEW white paper through a German transport network operator (TNO), the software development also focussed on the implementation of the necessary security functions as per the middle of 2012. The first step included analysis of the actual status in comparison to the requirements of the BDEW white paper, both with regard to the installed SCADA system components and the telecontrol components. Initially, the emphasis was on device and communication security.

To increase the security device was also tested in addition to the timeliness of the software components used, if relevant vulnerabilities were known. If necessary, components were updated or the affected functions were deactivated if they were not required for operation. Whereas system hardening on the Windows-based SCADA components was comparatively easy thanks to given and manually expanded system profiles and already existing tools, it required significantly more effort on the embedded telecontrol components. On both systems, services that were no longer required were deactivated, and all unused user accesses were checked and – wherever possible – removed. To reduce communication capabilities, firewalls were used both for the SCADA and the telecontrol system components. For the firewall on the RTUs, a static configuration was used initially because this method could be implemented without major interventions into the telecontrol software and the configuration tool.

To archive communication security, a VPN solution was favoured to protect access to service and diagnostic interfaces; this solution realizes protection independently of the current application and thereby renders modifications of the existing software systems unnecessary. Furthermore, the secure VPN tunnel enables the simultaneous protection of several communication links. The VPN solution was also favoured for communication links for the exchange of process data because the use of an external VPN component also ensures backward compatibility with already existing systems.

With regard to data security, the existing integrity check designed for the detection of errors during the transmission and storage of configuration data was expanded by a secure authenticity and integrity check. Even though the device configuration could be viewed via the plain text, it was possible to clearly detect any unauthorised modifications.
In the course of further product development of the telecontrol components, the static configuration of the firewall was replaced by a dynamic configuration in 2013; with this new configuration, the firewall rules were matched exactly to the actual communication relationships of the respective devices. Furthermore, protection of the device configuration was expanded to ensure confidentiality. In this context, the initial operation process had to be expanded by a secure initial configuration in order to enable the secure installation of key material on RTUs.

7.2 Public key infrastructure

During the implementation of the various security functions for the auditing of SCADA and telecontrol components, it quickly became clear that the use of cryptographic certification material was an unavoidable necessity. Although it is true that several protocols provide mechanisms for the authentication of communication partners without certification material, they require, on the whole, more costs and effort for the administration and storage of authentication information. Moreover, it is possible to archive a number of security requirements for data security on the basis of certificates.
Therefore – and despite the complexity of certificate-based systems – it was decided to prefer the aforementioned authentication approaches. For this purpose, X.509 was selected as a suitable certification standard because it is supported by several authentication methods (e.g. HTTPS, IPsec/IKE, OpenVPN, TLS) and because there are commercial providers for certificates and the necessary administration software.
Unfortunately, an analysis of existing providers for X.509 certificates has shown that the certificates offered by them are not suitable for telecontrol systems. Apart from the costs, the main point of criticism is the short validity period of a public X.509 certificate. This period covers only a few years and is in conflict with the planned product lifecycle of telecontrol systems. Whereas an exchange of the existing certification material every 24 months might be acceptable for central control system components, this is absolutely not feasible with regard to distributed RTUs, both with regard to time and costs.
An alternative would be to use of certificates provided by a self-operated certificate authority or to choose a special certificate provider who offers suitable certification material with a sufficiently long validity period. The operation of one's own certification infrastructure, however, causes considerable problems, particularly for the owners of small-scale telecontrol systems.

8 Summary

The above actions and moderate cost system security in several layers can be significantly increased (Fig. 2).

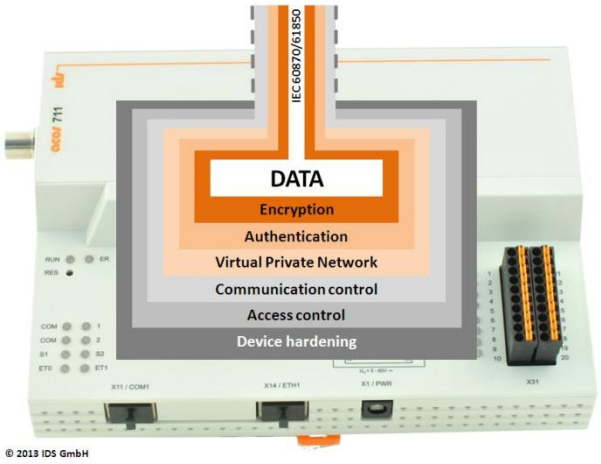

Figure 2 Layers of security for secure communication

In particular, the main tasks of device security and communications security could be implemented with standardized and available methods. There are open questions in the field of data security, since no common standards are available and questions about the provability of process actions (e.g. command output to switchgear) are to be expected in the future.

9 References

[1] White Paper "Requirements for Secure Control and Telecommunication Systems", BDEW - Federal Association of Energy and Water Industries, Berlin, 06/2008

[2] ISO / IEC TR 27019 - Information technology - Security techniques - Information security management guidelines based on ISO / IEC 27002 for process control systems specific to the energy industry (DRAFT), Geneva / Switzerland: Bureau Central de la Commission International Electrotechnical

[3] Execution instructions on use of the BDEW White Papers "requirements for safe control and telecommunication systems" in the field of protection and control systems, Dortmund: Amprion GmbH, 2010

[4] Testing Guide for BDEW white paper "requirements for safe control and telecommunication systems" in the field of protection and control systems, Dortmund: Amprion GmbH, 08/2010

[5] RFC 4301 - "Security Architecture for the Internet Protocol", IETF, 12/2005

[6] RFC 5246 - "The Transport Layer Security (TLS) Protocol Version 1.2", IETF, 08/2008

[7] ISO / IEC TS 62351:2007 - Power systems management and associated information exchange – Data and communications security, Geneva / Switzerland: Bureau Central de la Commission International Electrotechnical