White paper

Cyber Security

Declaration of Conformity BDEW

PHOENIX CONTACT

Introduction

This Declaration of Conformity describes the conformity to the document "Whitepaper: Requirements for Secure Control and Telecommunications Systems" by Oesterreichs Energie and the Bundesverband der Energie- und Wasserwirtschaft e.V. (referred to as BDEW white paper hereinafter). This applies to the following products:

- DIGICOM version 7.0.0 or higher
- KOMBISAVE for firmware version 3.00 and higher
- KOMBISAVE+ RN, RF, RQ, and RL for firmware version 3.00 and higher
- POWERSAVE RN and RF for firmware version 2.00 and higher

The following sections have the same structure as Section 4 of the BDEW white paper. The section number and the original text from the BDEW white paper are each quoted first. This is followed by the Declaration of Conformity from NSE AG, which is part of the Phoenix Contact Group.

Contents

1 Security requirements

Secure system architecture

BDEW 4.1.1

ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1

The individual components and overall system must be designed and developed for secure operation. Secure system design principles include:

Security by design:
The entire system and its individual components are designed on the basis of and with a focus on security. Deliberate attacks and unauthorised actions are explicitly taken into account while any repercussions arising from a security event are minimised by the system's inherent design.

Minimal need-to-know principle:
Each component and each user is only assigned the rights they need to execute a desired action. Applications and network services, for examples, are not run under administrator privileges, but only with the bare minimum of required system access rights.

Defence-in-depth principle:
Security risks are not tackled via single protection measures, but limited through the implementation of staggered, multi-level and complementary security measures.

Redundancy principle:
The entire system is designed to ensure that the failure of individual components does not impair security-related functions. The system's design lowers the likelihood and impact of issues caused by unrestricted requests for system resources such as e.g. main memory (RAM) or network bandwidth (so-called resource consumption or DoS attacks).

Phoenix Contact Group

SAVE protective devices and the DIGICOM operating program make it possible to design systems that can be operated securely. Please also refer to the explanations in the Function Manual, Section 50, Cyber Security.

Patching and patch management

BDEW 4.1.2	**ISO/IEC 27002:2013 / 27019:2017:12.6.1**
	All system components shall be patchable. The supplier shall support a patch management process for both the individual components and the entire system, designed to enable the control and management of security patch testing, installation and documentation. The operator himself resp. the assigned service provider shall be able to install the security patches and updates. Patch installations resp. uninstalls shall be authorised by the operator and shall not occur automatically. Any installation resp. uninstall shall be recorded in a transparent and tamper-proof way within the system. The integrity of security patches and updates shall be verifiable using a cryptographic mechanism.
Phoenix Contact Group	Updates for all system components can be installed by the operator. All installation procedures are logged in the security messages. Only update packages signed by NSE are allowed to be installed.

Provision of security patches for all system components

BDEW 4.1.3	**ISO/IEC 27002:2013 / 27019:2017:12.5.1, 12.6.1**
	The supplier shall ensure that security updates are available for all system components throughout the entire contractually stipulated operating timeframe. The contractor shall obtain, test and – where necessary – forward updates from the respective manufacturers for basic components that were not developed by the contractor himself such as the operating system, libraries or database management systems. All update testing, approval and delivery shall take place within an adequate, contractually stipulated timeframe.
Phoenix Contact Group	Security updates are reviewed internally, released, and posted on the website. The client is responsible for performing the installation. The standard duration of the contract is two years, but it can also be agreed upon individually with the client. The duration of the contract is stored on the devices in the maintenance file. For details on the maintenance file, please also refer to the Function Manual, Section 50, Cyber Security.

Support for deployed system components

BDEW 4.1.4	**ISO/IEC 27002:2013 / 27019:2017:12.6.1, 14.2.7**
	The supplier shall ensure that within the planned and contractually stipulated operating timeframe, manufacturer support and security updates are available for system components developed by both the supplier and third-parties (e. g. operating system, database management system etc.). A binding agreement should cover the discontinuation procedure as well as relevant minimum terms like e. g. last customer shipping and end of support.
Phoenix Contact Group	Security updates and related information are posted on the website. Discontinuation procedures, last-client-shipping, and end-of-support are defined and specified.

Encryption of sensitive data

BDEW 4.1.5	**ISO/IEC 27002:2013 / 27019:2017:10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4** Confidential data shall only be stored resp. transmitted encrypted.
Phoenix Contact Group	Confidential data is stored in encrypted form. Communication via the Ethernet interfaces is encrypted. Communication via USB or RS-485 is unencrypted. Please also refer to the explanations in the Function Manual, Section 50, Cyber Security.

Cryptographic mechanisms

BDEW 4.1.6	**ISO/IEC 27002:2013 / 27019:2017:10.1.1, 10.1.2, 13.1.4 ENR, 18.1.5** When selecting cryptographic mechanisms, national legislation shall be taken into account. Only approved mechanisms and minimum key sizes shall be used that are considered secure for the foreseeable future according to state-of-the-art technological knowledge. The supplier shall not use custom cryptographic algorithms.
Phoenix Contact Group	The selection of the cryptographic methods and keys used is based on the recommendations of the German Federal Office for Information Security (BSI).

Secure standard configuration

BDEW 4.1.7	**ISO/IEC 27002:2013 / 27019:2017:9.4.4, 12.5.1, 14.3.1** After initial installation, resp. at start-up or restart, the entire system shall be configured for a secure operating state. This defined basic configuration shall be documented. Services and functions as well as data that are only needed for development or testing shall be removed demonstrably resp. permanently deactivated before delivery resp. before the switch to live operations.
Phoenix Contact Group	The basic configuration only allows communication via the control panel or with a USB interface. All other communication interfaces (Ethernet, RS-485) are disabled by default.

Integrity testing

BDEW 4.1.8	**ISO/IEC 27002:2013 / 27019:2017:12.5.1, 14.2.1, 14.2.4** It shall be possible to check system files, applications, configuration files and application parameters for integrity, for example through cryptographic checksums.
Phoenix Contact Group	The integrity of system files and applications is secured using cryptographic methods. The integrity of the configuration files and application parameters is secured using checksums.

Use of cloud services

BDEW 4.1.9	**ISO/IEC 27002:2013 / 27019:2017: 15.1.1, 15.1.2, 15.2.1**
	Where cloud services are used, the following requirements apply: a) Agreements shall be made with the cloud service provider about security-related processes for cloud infrastructure operations. b) Functions for the control of Critical Infrastructures, where manipulations could threaten the energy supply, shall not be realised in external cloud services. c) Downtime of a cloud service resp. access to this service shall not lead to significant restrictions of the system's defined basic function. Cloud service disruptions or outages shall also be considered in the emergency concept and restoration plans (see 4.8.2).
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity, as no cloud services are used.

Documentation requirements

BDEW 4.1.10	**ISO/IEC 27002:2013 / 27019:2017:7.2.2, 12.1.1, 14.1.1, 14.2.7**
	At the latest, the client shall receive project-specific documentation at the system's handover. For individual components and entire systems, the documentation shall cover a description of all security-related system settings and parameters as well as their standard values. Furthermore, the documentation shall list and briefly describe security-specific implementation details (like the employed cryptographic mechanisms). The documentation shall also comprise additional information on the entire system's system architecture. This includes the system's basic and fundamental structure as well as interactions between all involved components. In particular, this part of the documentation shall highlight security-related or sensitive system components as well as their mutual dependencies and interactions.
Phoenix Contact Group	Documentation is provided in the form of device manuals and function manuals.

2 Project organization

Contacts

BDEW 4.2.1	**ISO/IEC 27002:2013 / 27019:2017:6.1.1, 6.1.5, 15.1.2** The supplier shall define a contact who is responsible for IT security during the tender process and the system development phase as well as throughout the planned operations and maintenance timeframe.
Phoenix Contact Group	The contact person for the IT security sector and this person's representative are members of the R&D department at NSE AG.

Security and acceptance testing

BDEW 4.2.2	**ISO/IEC 27002:2013 / 27019:2017:14.2.7, 14.2.8, 14.2.9, 15.2.1** Prior to delivery, the entire system's components and key functions shall be subjected to security and stress testing by the contractor – in a representative configuration and by an organisational unit independent of the development team. The actual procedure shall be discussed and agreed in coordination with the client. The results of these tests as well as the associated documentation (software versions, test configuration etc.) shall be made available to the client. In addition, the client shall have the right to undertake these tests himself or to have them carried out by an external service provider. The type and scope of the acceptance tests shall be defined by the client. For these tests, the client resp. the assigned service provider shall be given system access with a maximum of technologically possible access rights.
Phoenix Contact Group	The individual system components and the essential functions of the overall system are tested according to defined specifications before delivery.

Secure data storage and transmission

BDEW 4.2.3	**ISO/IEC 27002:2013 / 27019:2017:6.2.1, 8.3.3, 10.1.1, 13.2.2, 13.2.3, 13.2.4, 14.3.1** Confidential client data that is required or processed during the development and maintenance process shall be encrypted during transmission via insecure connections. When saved on mobile storage media or systems, such data shall only be stored encrypted. The amount and duration of data storage shall be limited to a contractually specified minimum.
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity, as there is no direct client submitting confidential data.

Delivery of project-specific modifications

BDEW 4.2.4	**ISO/IEC 27002:2013 / 27019:2017:14.2.7** For custom projects and project- resp. client-specific expansions, adjustments and engineering services, all project-specific parameterisations, changes and adaptations shall be comprehensively documented and supplied to the client in full.
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity.

3 Basic system

System hardening

BDEW 4.3.1	**ISO/IEC 27002:2013 / 27019:2017:9.4.4, 12.6.2, 13.1.2, 14.2.4, 14.2.10 ENR** All components of the base system shall be permanently hardened according to recognised best practice guidelines and the latest service packs and security patches shall be installed. Unnecessary users, default users, software, network protocols and services shall be uninstalled or – where an uninstall isn't possible – permanently deactivated and protected from accidental reactivation. The entire system's secure basic configuration shall be reviewed and documented.
Phoenix Contact Group	All components of the basic system are hardened, in accordance with the statements on the general requirements (Section 4.1 BDEW) and as described in the Functional Manual, Section 50, Cyber Security.

Malware protection

BDEW 4.3.2	**ISO/IEC 27002:2013 / 27019:2017:12.2.1** All networked systems shall be equipped with malware protection at the appropriate location. Alternatively to malware protection provided on all system components, the supplier can submit a comprehensive malware protection concept that provides equal protection. Where the use of a pattern-based solution is intended, these pattern files shall be updateable in a timely and automated manner. Such updates shall not take place via direct connection to update servers on external networks like the internet. For terminal systems, the time of updates needs to be configurable.
Phoenix Contact Group	The use of anti-virus software is not required, as only complete and signed update packages can be installed. This prevents malware from being installed and run on the device.

Autonomous user authentication

BDEW 4.3.3	**ISO/IEC 27002:2013 / 27019:2017:9.2.1, 9.2.2, 9.4.2**
	Data required for user identification and authentication shall not be obtained exclusively from outside the process network.
Phoenix Contact Group	Currently, the data for user identification and authentication is stored in the device. When a user logs in, no data is obtained from outside the process network. This requirement is thus met.

Virtualisation technologies

BDEW 4.3.4 **ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1**

The following requirements govern the use of virtualisation technologies:

a) Virtualised components assigned to different security or trust zones (e. g. internal components and DMZ components) shall not be operated on the same virtualisation servers. It shall not be possible to bypass the network segmentation of segregated security zones via virtualisation servers.

b) Networks used for management and administration services as well as data storage of the virtualisation infrastructure shall be segregated from other networks by firewalls with only the minimum of required network services enabled in a restrictive manner. Access to the management and administration services and the above-mentioned networks shall be restricted to administrators only.

c) The virtualisation layer, the management and administration interfaces as well as the associated infrastructure shall be configured, secured and hardened identically and according to manufacturer recommendations. They shall also be included in the patch management and backup concept.

d) The virtualisation servers shall have sufficient resources for operating all of the virtualised components they are running. This is especially important for high-load operating situations.

e) Any outage of virtualisation servers or of other components of the virtualisation infrastructure shall have no negative impact on the defined availability requirements. Disruptions and outages of the virtualisation environment shall also be covered and considered in the emergency concept and restoration plans (see 4.8.2).

Phoenix Contact Group This requirement is not relevant for this Declaration of Conformity, as no virtualization technologies are used.

4 Network and communication

Used protocols and technologies

BDEW 4.4.1	**ISO/IEC 27002:2013 / 27019:2017:9.4.1, 9.4.2, 10.1.1, 10.1.2, 12.9.1 ENR, 13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR** a) In general, only secure communication standards and protocols that include integrity protection, authentication and, if applicable, encryption shall be used if and where the technology allows. This is a non-negotiable requirement for any protocols used for remote administration and parameterisation and shall also be taken into account where non-standard resp. proprietary protocols are used. b) It shall be possible to integrate the entire system and any associated network components into the overall company's network concept. Central administration for relevant network configuration parameters like IP addresses shall be possible. For administration and monitoring secure protocols that ensure integrity protection, authentication and encryption shall be used. Network components shall be hardened, unnecessary services and protocols deactivated and management interfaces protected via ACLs. c) Network components provided by the supplier shall be capable of integrating into a central inventory and patch management. d) Where the technology allows it, WAN connections shall use the IP protocol and unencrypted application protocols shall be secured by encryption on the lower network layers (e. g. via TLS encryption or encrypted VPN technology). e) Where network infrastructure components are shared (e. g. by the use of VLAN or MPLS technologies), the network with the highest protection requirement level shall indicate the respective hardware and parameterisation requirements. The shared use of network components shall only be shared in case of different protection requirements when this shared use can in no way decrease the protection level or availability.
Phoenix Contact Group	The security of the available communication standards and protocols is ensured, in accordance with the statements on the general requirements (Section 4.1 BDEW) and as described in the Functional Manual, Section 50, Cyber Security. For IEC 61850, no additional security measures in accordance with IEC 62351 are currently implemented.

Secure network structure

BDEW 4.4.2	**ISO/IEC 27002:2013 / 27019:2017:9.4.1, 12.9.1 ENR,13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR, 13.1.5 ENR** a) Vertical network segmentation: Where applicable and technologically feasible, the system's underlying network structure shall be divided into zones with different functions and protection requirements. Where the technology allows it, these network zones shall be separated by firewalls, filtering routers or gateways. Communications with other networks shall only occur via the communication protocols approved by the client and in compliance with the applicable security guidelines. b) Horizontal network segmentation: Where applicable and technically feasible, the system's underlying network structure shall also be subdivided horizontally, into independent zones (e. g. according to sites) that are also separated by firewalls, filtering routers or gateways.
Phoenix Contact Group	The client is responsible for this requirement. It is therefore not relevant to this Declaration of Conformity.

Documentation of network structure and configuration

BDEW 4.4.3	**ISO/IEC 27002:2013 / 27019:2017:8.1.1** The following shall be documented: network design and configuration; all physical, virtual and logical network connections and the employed protocols, IP addresses and ports; and any network perimeters that are part of the system or interact with it. Any changes, e. g. via updates, shall be included in the documentation as part of the overall change management. This documentation shall also cover information on normal and maximum expected data transmission rates, to allow for limiting data transmission rates on the network components to prioritize traffic and prevent DoS issues, where necessary.
Phoenix Contact Group	The client is responsible for this requirement. It is therefore not relevant to this Declaration of Conformity.

Secure remote access

BDEW 4.4.4	**ISO/IEC 27002:2013 / 27019:2017:9.1.2, 9.4.1, 9.4.2**
	a) It shall be possible to administrate, maintain and configure all components via an out-of-band network, e. g. via local access, a serial port, a network or direct control of the input devices (KVM). b) Any remote access shall take place via centrally administrated access servers that are under control of the system operator. These access servers shall be operated within a DMZ and ensure isolation of the process network. Here, two factor authentication is mandatory. c) Strictly no direct dial in access to terminal devices. d) Any remote access shall be logged centrally; recurring failed attempts shall be reported. e) All remote access options shall be documented.
Phoenix Contact Group	The client is responsible for this requirement. It is therefore not relevant to this Declaration of Conformity.

Wireless technologies

BDEW 4.4.5	**ISO/IEC 27002:2013 / 27019:2017:10.1.1, 13.1.1, 13.1.2, 13.1.3**
	Short-range wireless technologies (e. g. Wi-Fi, Bluetooth, ZigBee, RFID etc.) shall only be used after assessment of the related risks, under consideration of the following minimum-security measures and after consultation with and approval by the client: • Wireless transmission technology shall to be secured with state-of-the-art measures. • Wi-Fi technology shall only be operated in dedicated network segments that are separated by firewalls and application proxies. • Wi-Fi networks shall be configured in a way that ensures that existing Wi-Fi networks are not affected, disrupted or impaired.
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity, as no short-range wireless technologies are used.

5 Application

Role concepts

BDEW 4.5.1	**ISO/IEC 27002:2013 / 27019:2017:6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1**
	The entire system shall support granular access control to data and resources. To this end, it shall support user concept that covers at least the following user roles: • Administrator: user who installs, maintains and manages the system. Among others, this gives the administrator the right to change security and system configurations. • User: User who operates the system according to the intended usage scenario, including the right to change operationally relevant settings. • Read-only user: User permitted to access the system status and pre-defined operating data without the right to make any changes. The standard access rights shall reflect a secure system configuration. Only the administrator role shall be able to read and change security-related system settings and configuration values. Regular system use shall only require user or read-only user rights. It shall be possible to deactivate user accounts individually without having to remove them from the system.
Phoenix Contact Group	The role concept has been implemented as required. Its implementation is described in the Functional Manual, Section 50, Cyber Security.

User authentication and login

BDEW 4.5.2 **ISO/IEC 27002:2013 / 27019:2017:9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3, 12.4.1**

The application shall use personal users to identify and authenticate each individual user; group accounts require special permission by the client and shall only be used in narrowly defined exceptional cases.

a) Without successful user authentication, the system shall only allow a range of narrowly defined actions.
b) The system shall support a state-of-the-art password policy.
c) Where technologically possible, strong two factor authentication shall be employed, e. g. via tokens or smart cards.
d) Data required for user identification and authentication shall not be obtained exclusively from outside the process network (see also 4.3.3).
e) Any successful or failed login attempts shall be centrally logged. It shall also be possible to centrally alarm in case of unsuccessful login attempts.

Phoenix Contact Group

The requirements for user identification and authentication were implemented as required. This implementation is described in the Functional Manual, Section 50, Cyber Security, especially in the sections “Security messages” and “Failed login attempts”.

Role-based access rights for secure workflows

Authorization of actions at the user and system level

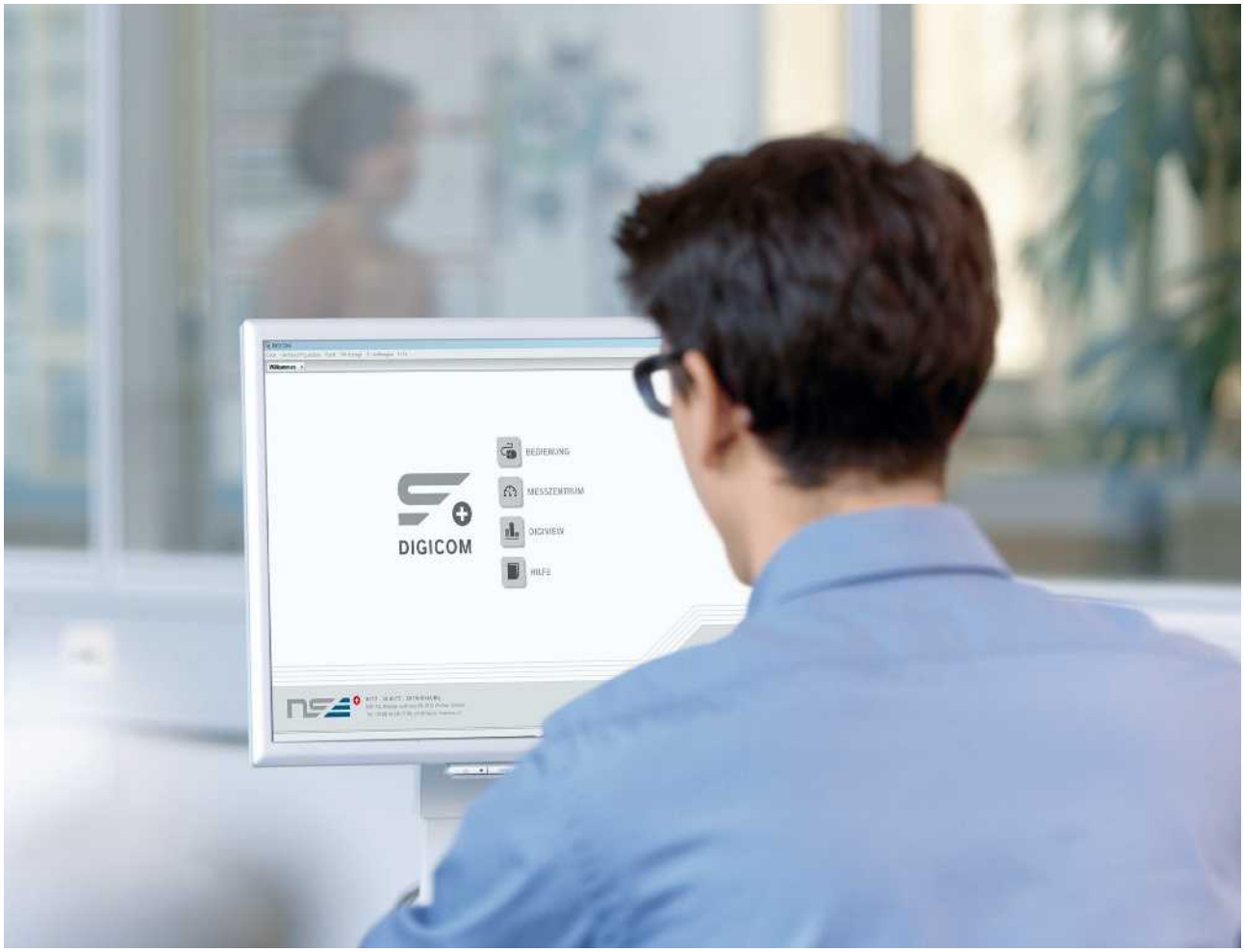
BDEW 4.5.3	**ISO/IEC 27002:2013 / 27019:2017:9.4.1, 9.4.4**
	Certain security-related or safety-critical actions shall require prior authorisation of the requesting user resp. the requesting system component. Such actions might also include a read-out of process data points or configuration parameters. **Additional information and notes** The security-related or safety-critical actions need to be specified by the client/system operator. The respective actions then require central logging, including the stated user ID. • Secondary, automation and telecontrol technologies: Not usually required for protection and substation control technology; potential use should be reviewed by the client/operator.
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity.

Web applications and web services

BDEW 4.5.4	**ISO/IEC 27002:2013 / 27019:2017:14.2.5**
	For web applications, web interfaces and web services, the recommendations of the OWASP TOP 10 and OWASP Application Security Verification Standard projects as well as the BSI Guideline on the Development of Secure Web Applications shall be applied. Any deviations from these guidelines require justification and prior approval by the client.
Phoenix Contact Group	This requirement is not relevant for this Declaration of Conformity, as no web applications or web services are used.

Integrity testing

BDEW 4.5.5	**ISO/IEC 27002:2013 / 27019:2017:14.2.5** The integrity of data processed as part of security-related activities shall be verified prior to processing (e. g. checked for plausibility, correct syntax and value range).
Phoenix Contact Group	The plausibility and the value range are checked in both the configuration tool and the device. The integrity of the data transfer to the device is ensured. In addition, the integrity of the data is checked on the device in regular cycles.



Logging

BDEW 4.5.6	**ISO/IEC 27002:2013 / 27019:2017:12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3**
	a) The entire system shall have a uniform system time as well as an option for synchronising this system time with an external secure time source. b) The system shall log user actions as well as security-related actions, events and errors in a format that is suitable for later and central processing. For a configurable minimum time period, these logs shall record date and time, the users and systems involved as well as the actual event and result. c) Log files shall be stored centrally at a freely configurable location. A mechanism for the automated transfer of the log file to central components shall be available. d) The log file shall be protected from subsequent modification. e) Older entries shall be overwritten on the log file overflow. The system shall send an alert before the log storage runs out of space. f) It shall be possible to include security-related log messages in a pre-existing alarm management.
Phoenix Contact Group	Time synchronization is possible via the NTP, for example. Security-relevant events are logged in the security messages. It is not possible to configure a minimum period for the security messages. Instead, if the memory space for the security messages is exceeded, older entries are overwritten. However, as soon as more than 80% of the memory for the security messages is filled with entries that have not yet been read out, a warning can be issued using the binary status signal ASECBUF. It is not possible to manipulate the security messages on the device. The list of security messages read out using DIGICOM is currently not protected against later modification.

6 Development

Secure development standards, quality management and approval processes

BDEW 4.6.1 **ISO/IEC 27002:2013 / 27019:2017:9.4.5, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1**

a) The system shall be developed by reliable and professionally trained employees. Where the development or parts thereof are subcontracted to a third party, this requires written permission by the client.
The subcontractor shall meet at least the same security requirements as the supplier.

b) The supplier shall develop the system in line with recognised development standards and quality management/assurance processes. As part of the development process, the following security-related development steps require special attention:
   - Definition of the security requirements
   - Threat modelling and risk analysis
   - Deduction of requirements for system design and implementation
   - Secure programming
   - Requirement testing
   - Security checks before commissioning

c) Testing shall be subject to the dual control principle: Development and testing shall be carried out by different people. Testing plans and procedures as well as expected and actual test results shall to be documented and comprehensible. It shall be ensured that they can be reviewed by the client as needed.

d) The supplier shall have a documented development security process in place that covers physical, organisational and personal security and protects the system's integrity and confidentiality. The effectiveness of the above-stated process may be verified by an external audit.

e) The supplier shall have a programming guideline in place that explicitly covers security-related requirements, e.g. avoiding insecure programming techniques and functions or the verification of input data to avoid buffer overflow errors. Where possible, security-enhancing compiler options and libraries shall be used.

f) The approval of the system resp. of updates/security patches needs to follow a specified and documented approval process.

Phoenix Contact Group

SAVE protective devices and the DIGICOM operating program are developed by reliable, trained employees who have been made aware of the security issues. Development is performed internally in accordance with a development process and a programming guideline. Tests are conducted based on the two-person rule and are performed by different individuals.

Secure development and testing systems, integrity testing

BDEW 4.6.2 **ISO/IEC 27002:2013 / 27019:2017:9.4.5, 12.1.4, 14.2.7, 14.3.1**

a) Development shall take place on secure systems; the development environment, source code and binary data all shall be protected from external access. All development systems shall be hardened according to recognised state-of-the-art and best practice specifications. Up-to-date malware protection shall be employed on the systems and all the latest security patches shall be installed.
b) Development and testing of the system, updates, extensions and security patches shall take place in a testing environment that is separated from the productive system.
c) No source code (except for interpreted scripting languages) shall be stored on productive systems.
d) It shall be possible to check the integrity of source code and binary data for unauthorised changes, for example via secure checksums.
e) A version history that tracks any changes to the software shall be kept for all employed software.

Phoenix Contact Group

The listed requirements for secure development and test systems and for integrity checks are met in their entirety.
Development is performed on secure systems. Development environments, source codes, and binary files are secured against unauthorized access in accordance with the current state of the art. Version management software is used to document the version history in a traceable manner.

7 Maintenance

Maintenance process requirements

BDEW 4.7.1	**ISO/IEC 27002:2013 / 27019:2017:9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2**
	a) Any remote and on-site access shall only be carried out by a predefined and properly trained group of people and only originating from secured systems. Access systems and IT infrastructures used for remote and on-site access need to be hardened according to recognised state-of-the-art standards and best practice specifications. Up-to-date malware protection shall be employed and all the latest security patches shall be installed. b) A pre-defined maintenance process shall be established to ensure that maintenance personnel only receives access to the systems, services and data as well as the respective physical premises that are actually required to carry out the related maintenance activities. c) Interactive remote access shall occur via personalised accounts and using two factor authentication. Special user IDs shall be established for automated processes – these shall only be able to execute specific functions and not have interactive access. d) Technical measures shall ensure that remote access is only possible if and where the responsible operator has explicitly approved this access. Each remote access session by external service providers shall require individual approval and disconnection. Sessions shall automatically disconnect after a reasonable amount of time. Access systems used for remote access, in particular, shall be logically or physically isolated from other networks during remote access. Here, a physical separation is preferable to logical uncoupling.
Phoenix Contact Group	This requirement is in the client's area of responsibility. It is therefore not relevant to this Declaration of Conformity.

Secure update processes

BDEW 4.7.2	**ISO/IEC 27002:2013 / 27019:2017:12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9** The provision and installation of updates, extensions and patches needs to occur according to a defined process and in coordination with the client.
Phoenix Contact Group	The process for providing update packages is defined.

Configuration and change management, rollback

BDEW 4.7.3	**ISO/IEC 27002:2013 / 27019:2017:12.1.2, 12.5.1, 12.6.2, 12.9.1 ENR, 14.2.2, 14.2.9** a) The system shall be developed and operated with a configuration and change management in place. b) The system shall support rollback to a pre-defined number of configuration states.
Phoenix Contact Group	Configurations can be stored via the operating program. A rollback to previous firmware versions, and therefore to previous configurations, is possible. The rollback option is available for all firmware versions ever since measures to implement cyber security were introduced (to see the firmware versions, refer to the Introduction). The client/operator is responsible for archiving older configuration versions. Previous firmware versions can be obtained from the website or upon request. It is ensured that older configuration versions can also be edited with newer versions of the operating software.

Handling of vulnerabilities

BDEW 4.7.4	**ISO/IEC 27002:2013 / 27019:2017:12.6.1, 16.1.2, 16.1.3**
	The supplier shall have a documented vulnerability handling process in place. Within this process, all concerned – including external parties – shall be able to report actual or potential vulnerabilities. In addition, the supplier shall stay up-to-date on current security issues that might affect the system or individual components. The vulnerability handling process defines how and in what timeframe a known or reported vulnerability shall be reviewed, classified, remedied and reported to all affected clients, including respective recommended measures. When the supplier finds out about a vulnerability, he shall inform the client in a timely manner and under consideration of the necessary confidentially restrictions, even when no patch to fix the issue is available yet.
Phoenix Contact Group	The assessment and handling of security vulnerabilities is performed in accordance with a documented process and is the responsibility of the contact person for IT security and their representative (see the section “Contacts”). Outside persons are able to report security vulnerabilities.

8 Data backup and contingency plan

Back-up: Concept, method, documentation, testing

BDEW 4.8.1	**ISO/IEC 27002:2013 / 27019:2017:12.1.1, 12.3.1** Documented and tested procedures for data back-up and recovery of the individual components resp. the entire system and the respective configurations shall exist. There shall be the possibility for central back-up of the configuration parameters of distributed components. After relevant system updates, the documentation and procedures shall be updated and retested accordingly.
Phoenix Contact Group	The client can use the DIGICOM operating program to create backups of the configuration versions. Furthermore, the NSE website provides an archive with various firmware versions.

Emergency concept and recovery plans

BDEW 4.8.2	**ISO/IEC 27002:2013 / 27019:2017:17.1.1, 17.2.1** The supplier shall provide documented and tested procedures and recovery plans – including expected restoration times – for relevant emergency and crisis scenarios. After relevant system updates, this documentation and these procedures shall be updated and retested as part of the approval process for release changes.
Phoenix Contact Group	This requirement is in the client's area of responsibility. It is therefore not relevant to this Declaration of Conformity.

VMM02-21.000.L3