Release of VHPready 4.0

Virtual Power Plant

Communication Path between Control Center
and Distributed Energy Resource

WHAT WE DO

With the VHPready 4.0 specification a field-tested solution is being further developed. In close cooperation of several experts from quite different areas of energy production, energy transport and distribution, energy trade as well as automation and communication technology the foundation for a standardized network of decentralized energy systems is being defined.

Regarding communications and security VHPready is based on public key infrastructure (PKI) secured Internet technologies with TLS encryption and the well-established IEC protocols 60870 and 61850. VHPready is not going to reinvent the wheel but is defining operating conditions, systems behaviour and performance as well as interfaces and data points in an exact and explicit way. By doing so distributed energy systems can be integrated into a VHPready network without any additional engineering effort.

Security in data communications as well as in systems operation is a significant part of the currently developed standard. VHPready is providing the basis for existing and future market models in the energy sector and contributes to a stable and reliable energy supply in Germany, Europe and worldwide.

VHPready 4.0

This is a standard under Industry Alliance VHPready e.V. (02/2017).

Virtual Power Plant (VPP)

Communication path between control center (CC) and distributed energy resource (DER)

Total of 32 pages

Industry Alliance VHPready e.V.

About Industry Alliance VHPready e.V.

The Industry Alliance VHPready e.V. develops the industry standard to encourage the networking of decentralized

energy systems, the certification program as well as the appropriate testing tools.

Supporting web links:

Publications:	https://www.vhpready.com/documents/
Contact:	https://www.vhpready.de/kontakt/

Entry into force

The VHPready technical regulation will apply as of 2015-11-01.

Content

Photos

Tables

Preamble

1. The Industry Alliance VHPready e.V. develops the industry standard to encourage the networking of decentralized energy systems, the certification program as well as the appropriate testing tools. The organization does this on the basis of international standards and as such enables the development of technical solutions that meet national and international requirements.
2. Formal resolutions on technical matters reflect the consensus of the participating industrial experts.
3. Publications by the Industry Alliance VHPready e.V. represent a recommendation for international use. Although every precaution is taken to guarantee accuracy, the Industry Alliance VHPready e.V. is responsible neither for how the standard is used, nor for incorrect interpretations of its content by its users.
4. In the medium term, the Industry Alliance VHPready e.V. aims to embed the standard in the national and international regulatory framework.
5. The Industry Alliance VHPready e.V. does not itself verify the conformity with standards. Independent test organizations offer such services.
6. All users are responsible for working with the applicable version of the standard.
7. Industry Alliance VHPready e.V., its managers, employees, contractors and representatives, incl. experts and members of technical committees, are not (neither directly nor indirectly) responsible for bodily injuries, property damage or damage of any other nature, nor for costs of any kind resulting from the publication, use of or reliance on this or any other publication of Industry Alliance VHPready e.V.
8. Normative references in this publication need to be observed as they are indispensable for its correct application.
9. It is to be noted that some elements of this document might affect patent rights. Industry Alliance VHPready e.V. is not responsible for the identification of any or all related patent rights.

This document was created by Industry Alliance VHPready e.V. working group on the further development of VHPready and declared valid in accordance with the rules of the organization.

It replaces version 3.0 of the standard which previously applied.

Overview

VHPready scope of application

The VHPready standard applies to the communication path between a control center (CC) and a distributed energy resource (DER) or technical unit (TU). The VHPready standard should create security and interoperability for the connection of technical units. The objective is to minimize the effort/cost for the integration of new technical units. Changing a technical unit from one control center to another, for instance in case of a marketer switch, should become very simple.

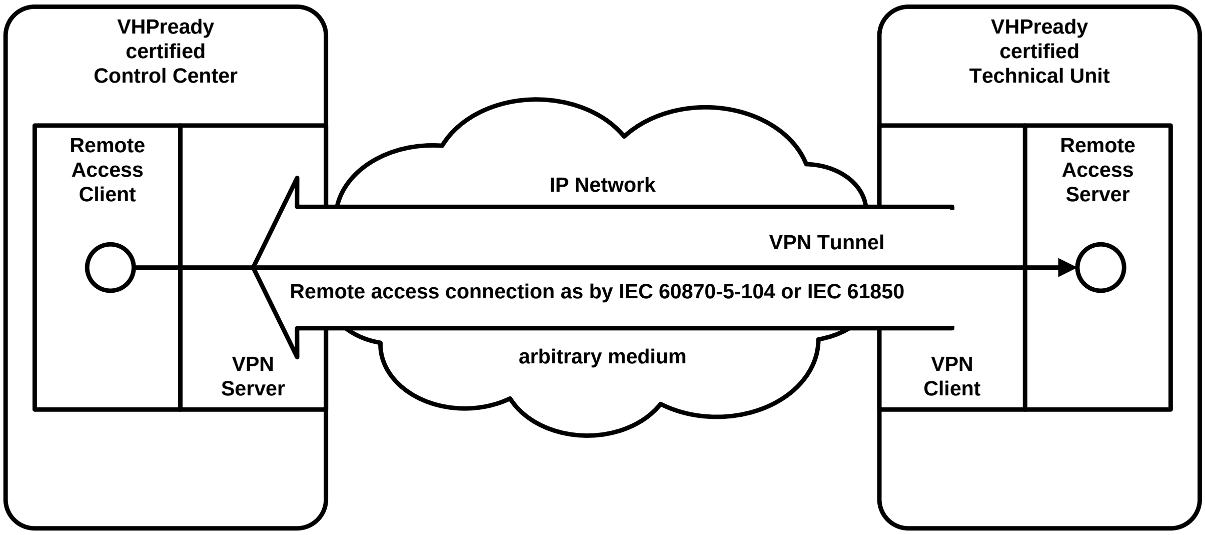
VHPready certified Control Center
VHPready certified Technical Unit
Remote Access Client
Remote Access Server
IP Network
VPN Tunnel
Remote access connection as by IEC 60870-5-104 or IEC 61850
arbitrary medium
VPN Server
VPN Client

Figure 1 Schematic description of the VHPready 4.0 scope

If a control center meets the VHPready specifications, it is called a VHPready-compliant control center. If a technical unit meets the VHPready specifications, it is called a VHPready-compliant technical unit. After successful certification, the technical unit or control center becomes VHPready-certified.

The VHPready compliance is based on three preconditions that have to be met by the control center and technical unit:

1. Communications between control center and technical unit use a Virtual Private Network (VPN) that follows the VHPready specifications. The technical unit creates a VPN connection to the control center. The VPN connection is IP-based. Which medium is used to transmit IP packages between the technical unit and the control center is not part of the VHP standard's scope and can be chosen freely.
2. The remote access connection between control center and technical unit has to be realized with one of the remote control protocols allowed for VHPready. Data have to be transmitted by TCP/IP within the VPN. The remote access connection from the control center to the technical unit is created.
3. The data points of the remote access connection between control center and technical unit have to follow the VHPready specification. The defined response behaviour also has to be observed.

During the VHPready certification process, all requirements are verified by an independent third party and a VHPready certificate is issued if these are all met.

The response characteristics with regard to the generation or consumption of electricity as well as the actual responses for other energy carriers are explicitly excluded from the VHPready specification. The VHPready specification exclusively concerns the specification of communications behaviour.

Normative references

IEC 60870-5-104	"Telecontrol installations and systems - Part 5-104: Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles" General transmission protocol between dispatching systems and energy-technical installations. The telegrams are transmitted via TCP/IP internet protocol. The protocol has general functionalities in the scope of SCADA applications;
IEC 61850-7-420	"Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes " Communications system for the decentralized generation of energy - defines object models for specific information that can be exchanged between distributed energy resources and corresponding monitoring and control systems.
IEC 61850-7-4	"Communication networks and systems for power utility automation - Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes" This part of the IEC 61850 standard specifies the information models of the devices and functions that are traditionally used in energy supply automation. The information models of devices and function-related applications in substations are also covered. It particularly specifies compatible names for logical nodes and data objects to communicate between so-called 'intelligent electronic devices' (IED).
TCP/IP	"Transmission Control Protocol / Internet Protocol" The Transmission Control Protocol (TCP) is provided for use as a highly available host-to-host protocol in package-connected computer communication networks and other meshed systems part of such networks. The internet protocol was developed for use in meshed systems within package-connected computer communication networks.
TLS	"The Transport Layer Security Protocol" The TLS protocol provides online communication security. This protocol allows client/server applications to communicate in such a way that wire-tapping, manipulation and forgery of information is prevented.
SNTP/NTP	"Simple Network Time Protocol/ Network Time Protocol Version" The Simple Network Time Protocol (SNTP) is a subset of the Network Time Protocol (NTP) and is used to synchronize computer clocks online. SNTP is applied when the full service capacity of the NTP is not required nor justifiable. The Network Time Protocol (NTP) is usually applied to synchronize computer clocks online.
UDP	"User Datagram Protocol" The User Datagram Protocol (UDP) was defined to make the datagram operating mode available for package-connected computer communication networks within meshed computer networks. This protocol requires that the internet protocol is also available.
ISO IEC 7498-1:1994	"Information technology - Open Systems Interconnection - Part 1: Basic Reference Model: The Basic Model" The purpose of the Basic Reference Model for Open Systems Interconnection (OSI) is the availability of a common basis to coordinate the development of standards for interconnected systems. It therefore allows building a relation between existing standards and the reference model.
ITU-T X.509	"Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks" Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines a framework for public-key and attribute certificates. The public-key and attribute certificate framework is the

basic specification for public-key certificates, the different components belonging to public-key infrastructure (PKI), for the validation procedures and the recall of public-key certificates, etc. The attribute certificate framework is the basic specification for attribute certificates and the different components belonging to a privilege management infrastructure (PMI). These frameworks can be used by standardization organizations to design their application according to PKI or PMI profiles.

Communication protocols

Communication between the technical unit and the control center is encrypted and takes place via IP networks, either based on standard IEC 60870-5-104 or the series of standards IEC 61850 (in particular IEC 61850-7-420). Time synchronization takes place via SNTP/NTP. The following protocols are used for communications:

- either IEC 60870-5-104 or IEC 61850-7-420
- TCP/IP
- TLS
- SNTP/NTP

IEC 60870-5-104

Communications take place on the basis of the application-relevant standard for remote control tasks in IP networks (IEC 60870-5-104). In this case, the control center assumes the role of 'master' whereas the VHPready-compliant technical unit assumes the role of 'slave'.

The connection is permanently kept open to allow the control center and technical unit to transmit messages or control commands over the connection without needing to establish it first.

The list of data points describes the general fields and functions as a basis for VHPready-compliant communications in accordance with IEC 60870-5-104. It also describes the specific classification of control commands or message information.

IEC 61850-7-420

As an alternative to communication based on standard IEC 60870-5-104, communications can also take place based on standard IEC 61850-7-420 or the series of standards IEC 61850.

The series of standards IEC 61850 meets all general requirements for substation automation (communication networks and systems in substations). Contrary to IEC 60870-5-104, which is based on a signal-oriented data model, the data model of the IEC 61850 interface is object-oriented.

For decentralized energy generation, the expansion of IEC 61850-7-420 provides object models for specific information that can be exchanged between distributed energy producers and corresponding monitoring and control systems.

With regard to protocol IEC 61850, the used excerpt from the object model is described. It also lists the specific objects to be introduced (logical devices, logical nodes and data objects) for all information in the command and monitoring direction.

TCP/IP

Communication via IEC 60870-5-104 or IEC 61850-7-420 uses an existing IP connection. Depending on the type of connection used by the control center, it is automatically established when creating the connection as per IEC 60870-5-104 or IEC 61850, or is permanently established independently of these.

The allocation of IP addresses to VHPready-compliant technical units as well as the transfer of the necessary IP information for the control center takes place when the connection with the control center is established.

Parameter setting for communication protocols used in VHPready

Protocol IEC 60870-5-104

Compatibility list IEC 60870-5-104

In order to design remote control systems, the standard IEC 60870-5-104 specifies sets of parameters and their alternatives. Specific solutions consist of subsets thereof. Some of the parameters mutually exclude each other, such as the choice of “structured” and “unstructured” address fields of the ASDU information object. In a given system only one single parameter setting is appropriate. Other parameters enable the definition of overall respectively subsets feasible for given applications. An example is the listed set of various process information to be sent either in command or in monitoring direction.

The compatibility list is defined identically to IEC 60870-5-101. It is extended with parameters used in the recent document. The descriptions of parameters prohibited in the recent document are marked accordingly.

REMARK:

The complete definition of a system may require the individual selection of specific parameters for individual parts of it. An example is the individual selection of scaling factors for individually addressable measurement values.

The selected parameters are marked as follows in the monitoring fields:

-	function or ASDU not used
X	function or ASDU used as per the standard (preferred value)
R	function or ASDU used in reverse mode
B	function or ASDU used in regular and reverse mode
Z	use of function prohibited

The available selection (-, X, R, B or Z) is defined for each section or parameter

System or device

(system-related parameter; the distinction of system or device shall be indicated by marking one of the following monitoring fields with “X”)

-	Controlling station
X	Controlled station

Application layer

Transfer mode of application data

The recent standard solely uses MODE 1 of IEC 60870-5-4 (least significant octet first).

Common address of ASDU (system-related parameter)

-	Single Octet
X	Double Octet

Information object address (system-related parameter)

-	Single Octet
-	Double Octet
X	Triple Octet

APDU length (system-related parameter; the APDU length shall be defined once per system)

253	Maximum APDU length per system

Selection of standard ASDU

Process information in monitoring direction (station-related parameter)

X	<30>	:=	Single message with time tag CP56Time2a	M_SP_TB_1
X	<36>	:=	Measurement value, short floating point number with time tag CP56Time2a	M_ME_TF_1

Process information in control direction (station-related parameter)

X	<45>	:=	Single Command	C_SC_NA_1
X	<64>	:=	Bit pattern of 32 bit time tag	C_BO_TA_1
X	<50>	:=	Nominal value, short floating point number	C_SE_NC_1

System information in control direction (station-related parameter)

X	<100>	:=	General query	C_IC_NA_1

Basic application functions (station-related parameter)

X	Station initialization
X	Cyclic Data Transmission
X	Station Query Global
X	Spontaneous Transmission

Command Transmission (object-related parameter)

X	Direct Command Transmission
X	No additional definition
X	Short Command Execution Duration
-	Long Command Execution Duration
X	Continuous Command

Special Definitions

Definitions for time control

Parameter	Remarks	Assigned Value
T0	time control for connection establishment	30s
T1	time control for sent APDU	15s
T2	time control for acknowledgement	10s
T3	time control for sent test telegrams in case of long idle states	1200s

Maximum range of time control values T0-T2: 1 sec - 255 sec, precision 1 sec

Maximum range of time control value T3: 0 sec - 48 h, precision 1 sec

Maximum number k of non-acknowledged APDU and latest APDU acknowledgement (w)

Parameter	Remarks	Assigned Value
k	Maximum difference between Receipt Sequence Number and Sender Sequence Number	12 APDU
w	Latest acknowledgement after receipt of w APDU in I format	8 APDU

Maximum value range k:	1 to 32767 APDU, precision 1 APDU
Maximum value range w:	1 - 32767 APDU, precision1 APDU (recommendation: w should not exceed k by more than 2/3 of k)

Port number

Parameter	Remarks	Value
Port number	In all cases	2404

Functional Description

Addressing a VHPready Connection

IOA3 data point (12 bit)												IOA2 number (4 bit)				IOA1 device type (8 bit)							
100												3				5							
0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	1
MSB												410373											LSB

The structure of the object addresses is defined in the data point lists.

It is possible to connect multiple technical units to the control station via a single gateway. To achieve this, the component type (IOA1) is coded in the addressing along with the sequence number of a given component (IOA2).

This coding allows the assignment of semantically differing data points (IOA3) to a technical unit and hence their parallel control over a range of technical units.

The assignment of individual bits to IOA 1-3 is as follows:

- IOA1: 8 bits (device type)
- IOA2: 4 bits (device number)
- IOA3: 12 bits (semantic meaning)

To answer a common schedule, to react to a call for balancing power etc. by establishing the control of multiple technical units (and not just by calling the same box) they are addressed as “System / Park” (IOA1=0) providing the sum of the measurement results. This “System” receives a common schedule / call for all involved technical units. At least in the case of balancing power calls the individual technical units need to provide their individually measured values as well to ensure traceability.

The common control in the sense of distribution to multiple technical units may be established either in the gateway or in a control unit located behind it. There is no definition of a given design by VHPready.

Time stamp

All transmitted time stamps refer to the UTC time zone. This applies to schedule entries provided by the control station as well as to any measurement value delivered by a technical unit to the control station.

Operation modes

Any technical unit is in one of three different operation modes. As long as the technical unit is not externally controlled it remains in the autonomous mode. As soon as the control station takes over control, the technical unit transits into either the scheduled mode or the power setpoint mode. The individual operation modes are described below in more detail.

Autonomous mode

In autonomous mode the technical unit has no external control impetus. The system operates as defined by the system control.

Scheduled mode

In scheduled mode the technical unit follows the schedule transmitted from the control station to the gateway. A future schedule may be transferred to and stored in the gateway at any time. Parts of or the full schedule may be deleted from the gateway or overwritten there. The information is contained in the information objects “working point schedule transmission part 1 and 2 for absolute schedule values”.

Power setpoint mode

In power setpoint mode the control station provides a nominal power setpoint to be delivered by the technical unit. This nominal setpoint describes an actual demand value. Due to this it is not possible to transmit upfront any future setpoint differing from the recent nominal power value. The information is contained in the information object “power setpoint determining an absolute value”.

Switching processes

Switching between the three operation modes using absolute values is triggered by two bit signals transmitted from the control center to the gateway. The bit signals concerned are “WorkingPointScheduleOperation active” and “PowerSetpoint active”. If both bits are inactive (FALSE) the technical unit is in autonomous mode. The precondition for setting a nominal power value by the control station is signalling of readiness by the technical unit (READY TRUE). Should the state of readiness cease during an active call the unit will drop back into autonomous operation mode.

If the control station sets the bit “workpoint scheduled mode active” to “active” (TRUE) and the technical unit is ready for the provision of external power, the technical unit changes from autonomous operation mode to the scheduled mode controlled by the control station. The bit “power setpoint active” serves as a switch between scheduled mode and power setpoint mode. If the bits “PowerSetpoint active” and “WorkingPointScheduleOperation active” are set to active (TRUE) the technical unit is in power setpoint operation mode. In case the bit “PowerSetpoint active” is set to active and the “WorkingPointScheduleOperation active” to inactive the technical unit is in autonomous operation mode.

Call for balancing power

Calls for relative balancing power are independent of the actual operation mode. They are transmitted as relative values and accordingly they become valid either immediately (SRL – “Secondary Control Power”) or in line with the schedule (MRL – “Minute Reserve”).

Should the state of readiness of the unit cease during an active call (for example caused by a disturbance) the technical unit will by definition independently drop back into autonomous operation mode.

Loss of connectivity

In case the technical unit loses connection to the control station during scheduled operation mode, the scheduled operation mode remains active. In case of a connection loss during power setpoint operation mode, the technical unit drops back into scheduled operation mode. The technical unit remains in the scheduled operation mode defined by the control station as long as there is a valid schedule. Should there be no (more) valid schedule, the technical unit drops back into autonomous operation mode.

Table 1 shows the data points to be reset, for example in the case of a connection loss.

Data point	Behaviour at connection loss	Remark
x-x-100	Reset	
x-x-101	Reset	
x-x-102	---	no valid schedule => autonomous mode
x-x-103..105	---	no valid schedule => autonomous mode
x-x-110 [kW]	Reset	
x-x-111..113 [%]	---	no valid schedule => => relative value = 0,0
x-x-120 active	Set state of 121	approve primary control power if connection to control station active
x-x-121 active	---	approve primary control power if connection to control station lost
x-x-122..129 [%/Hz]	---	active depending on connection state and x-x-120 and x-x-121

Table 1 Resetting data points at connection loss

The technical unit shall buffer the measurement values for at least 24 hours and send them to the control station after re-establishment of the signal connection.

Status diagrams switching processes

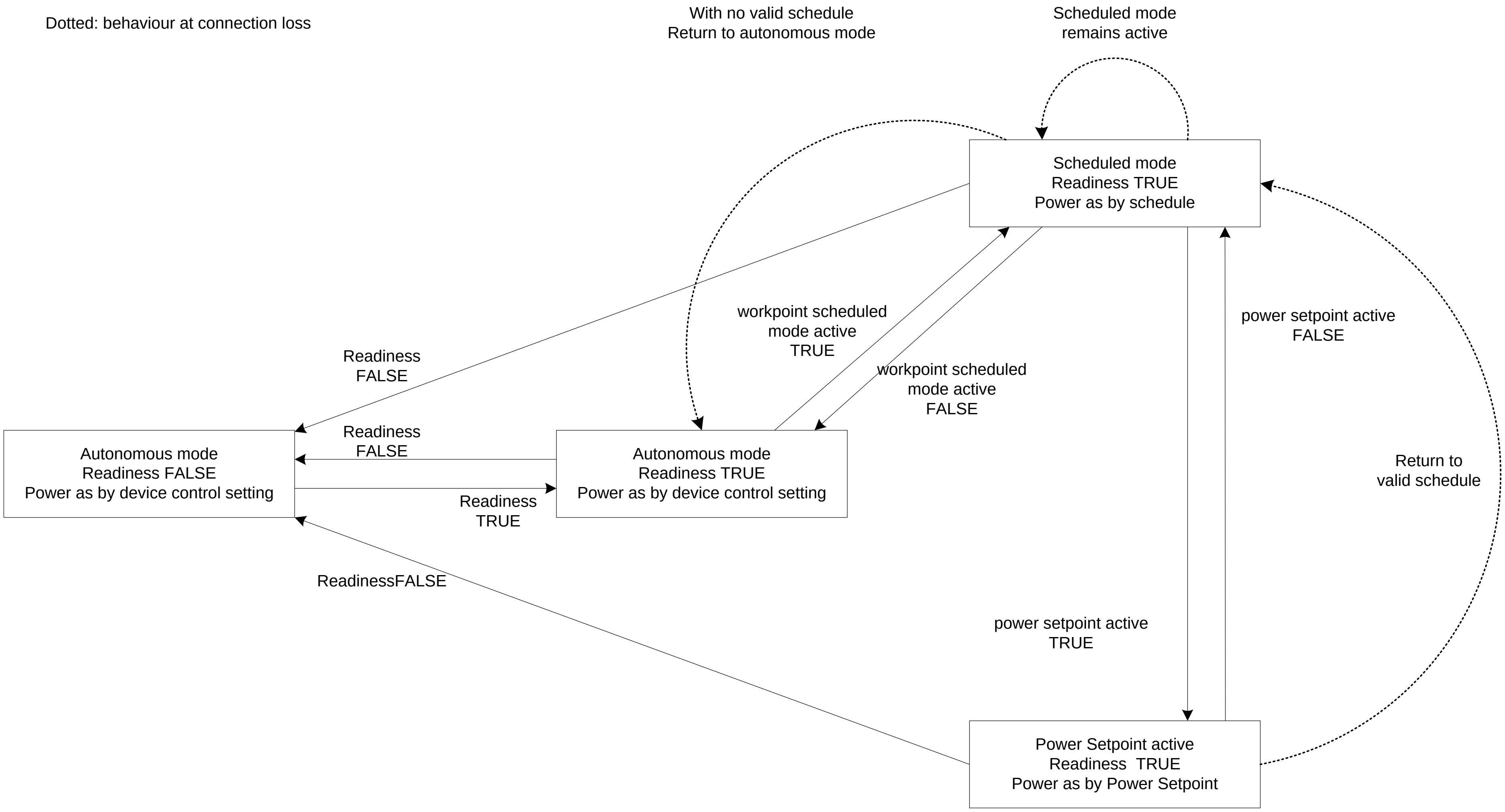

Figure 2 Switching processes for absolute values

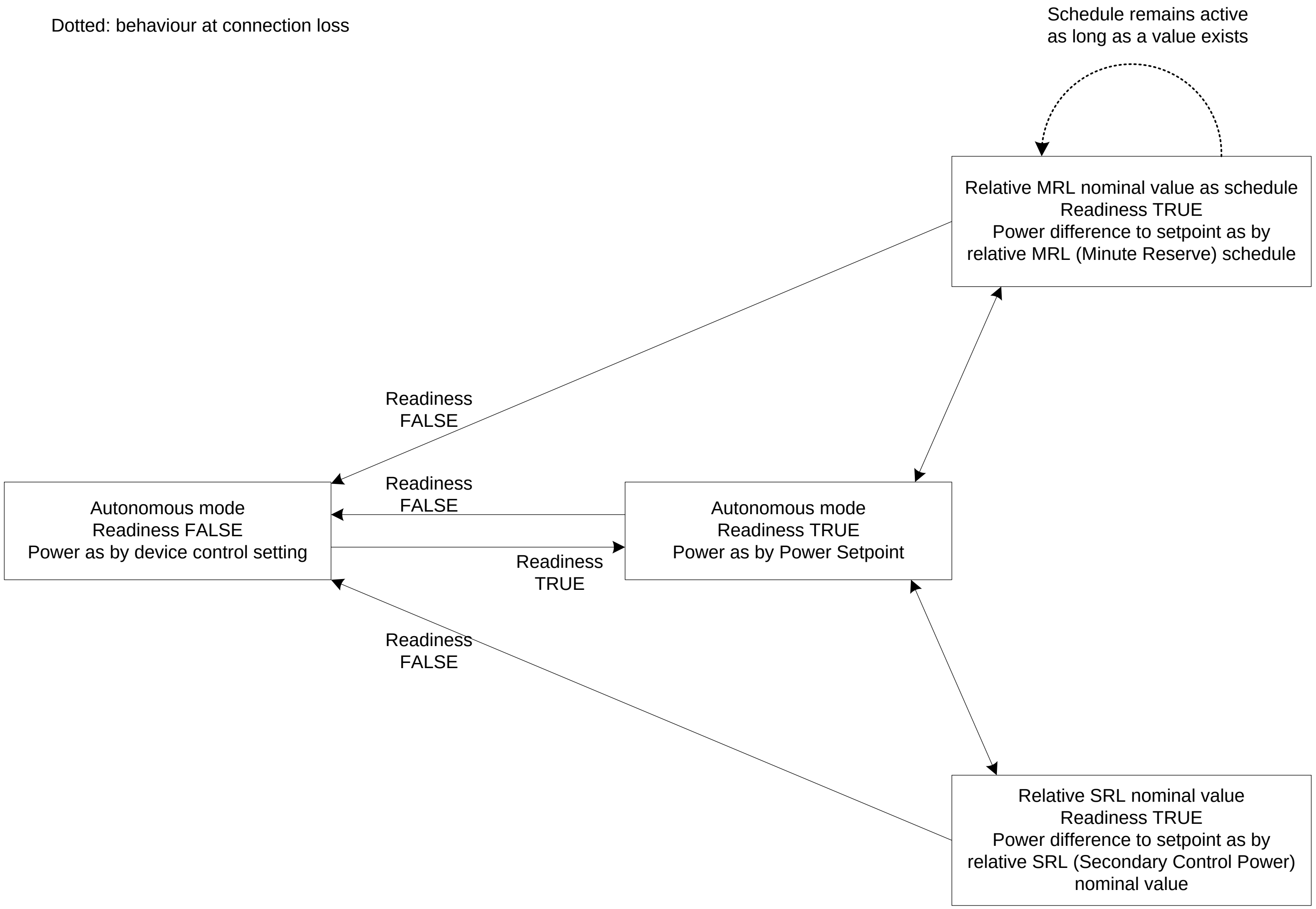
Dotted: behaviour at connection loss
Schedule remains active as long as a value exists
Relative MRL nominal value as schedule
Readiness TRUE
Power difference to setpoint as by relative MRL (Minute Reserve) schedule
Readiness FALSE
Readiness FALSE
Autonomous mode
Readiness FALSE
Power as by device control setting
Autonomous mode
Readiness TRUE
Power as by Power Setpoint
Readiness TRUE
Readiness FALSE
Relative SRL nominal value
Readiness TRUE
Power difference to setpoint as by relative SRL (Secondary Control Power) nominal value

Figure 3 Switching processes for relative values

Frequency of measurement value transmission - configuration

The frequency of transmitting measurement values by the VHPready interface is remotely configured through multiple data points.

It is possible to configure a cycle for power measurement values different from other measurement values. It is further possible to define a percentage minimum value deviation triggering a re-transmission of the measurement value even before the end of a cycle for power measurement values as well as other measurement values.

Data point list

The list of data points is contained in a separate document.

Establishing and terminating the schedule transmission

The start time of transmitted schedule entries may lie in the past as long as its duration reaches into the future.

In case the start time lies more than 43 200 minutes (= 30 days) in the past, it shall be assumed that the schedule refers to the following year.

Any received schedule entry must be confirmed by means of the third Information object. This also holds true for unchanged schedule entries received.

Schedule transmission

1. Information object (C_BO_TA_1)

bit	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
meaning	Del	Duration in minutes (0-2047 min)											Start time in minutes of the year (0-527040 min)																			LSB

2. Information object (C_BO_TA_1)

bit	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
meaning	CRC16 of the 1st information object																/	Vz	Schedule set point in percentage													LSB

3. Information object (MC_BO_TB_1)

bit	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
meaning	reserved																CRC16 of the 2nd information object															LSB

1st Information object	**Encoding the time of start and termination in minutes. Furthermore, it is possible to delete specific parts of or even the whole schedule.**	
	Start time in minutes of the year	Defines the start time of the schedule entry in minutes of a year (beware of leap years).
	Duration in minutes	Defines the duration of a sent schedule entry (max. 2047 minutes / >34 hours)
	Del	Delete-Bit TRUE -> if existing – delete the time range of the schedule with the start and end time. All 32 bits TRUE -> delete all schedule entries

2nd Information object	**Contains a CRC16 check sum to confirm the correct assignment of the transmitted power setpoint to the start and end time**	
	CRC check result of the 1st information object	This CRC check allows the gateway to assign the power setpoint to the correct start and end time.
	Setpoint with signed range	14 bits serve the transmission of the power setpoint (0-10000 -> 0,00-100,00%) and bit 15 the transmission of the sign (True -> - | False -> +)

3rd Information object	**Control object for the controlled station**	
	CRC check result of the 2nd information object	The CRC check of the 2nd information object offers the Virtual Power Plant a direct way to confirm the correct interpretation of the schedule.

Information on calculating CRC16

Verification polynomial	16#A001
Initial value of shift register	16#FFFF
Reverse In and Reverse Out	

Schedule - example

Example:	
Start time of the schedule entry	11.05.2015 11:55 UTC
Call Duration	15 minutes
Power setpoint	88.33%

1st information object	bit	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	1	1	0	1	1	1	1	0	0	0	0	0	1	0	1	1
	meaning	Del	15 minutes											Start time in minutes of the year (1879015 minutes)																			
	Hex: 00F2DE0B																																

2nd information object	bit	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1
	meaning	CRC16 of the 1st information object																/	Schedule set point 88.33%														
	Hex: B0B92281																																

3rd information object	bit	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	1	0	1	1	1	1
	meaning	reserved																CRC16 of the 2nd information object															
	Hex: 0000C12F																																

Calculation requirements for the determination of actual setpoints

Calculation VHPready Setpoint Values [x1__ and r1__ refer to the points x1__ = BOOL, r1__ = REAL of the VHPready Data Point List]
rSW[1] = absolute base value; rSW[2] = relative setpoint value; rSW[3] = MRL setpoint value; rSW[4] = PRL setpoint value;

x_100	Power setpoint active	BOOL	45 [C_SC_NA_1]
r_101	Power setpoint [working point]	REAL	50 [C_SE_NC_1] kW
x_102	Working point – scheduled operation active	BOOL	45 [C_SC_NA_1]
d_103	Working point – schedule transmission part 1	DWORD	64 [C_BO_TA_1] bit mask
d_104	Working point – schedule transmission part 2	DWORD	64 [C_BO_TA_1] bit mask
d_105	Working point – schedule transmission response	DWORD	33 [M_BO_TB_1] bit mask
r_110	Relative SRL target value	REAL	50 [C_SE_NC_1] kW
d_111	Relative MRL target value as schedule part 1	DWORD	64 [C_BO_TA_1] bit mask
d_112	Relative MRL target value as schedule part 2	DWORD	64 [C_BO_TA_1] bit mask
d_113	Relative MRL target value as schedule response	DWORD	33 [M_BO_TB_1] bit mask
x_120	PRL active	BOOL	45 [C_SC_NA_1]
x_121	PRL backup active	BOOL	45 [C_SC_NA_1]
r_122	Positive PRL for demand call	REAL	50 [C_SE_NC_1] kW
r_123	Negative PRL for demand call	REAL	50 [C_SE_NC_1] kW
r_124	Approved overdelivery of positive PRL	REAL	50 [C_SE_NC_1] %
r_125	Approved overdelivery of negative PR	REAL	50 [C_SE_NC_1] %
r_126	Positive power gradient at PRL delivery	REAL	50 [C_SE_NC_1] kW/s
r_127	Negative power gradient at PRL delivery	REAL	50 [C_SE_NC_1] kW/s
r_128	Approved charging power in dead band	REAL	50 [C_SE_NC_1] kW
r_129	Approved discharging power in dead band	REAL	50 [C_SE_NC_1] kW

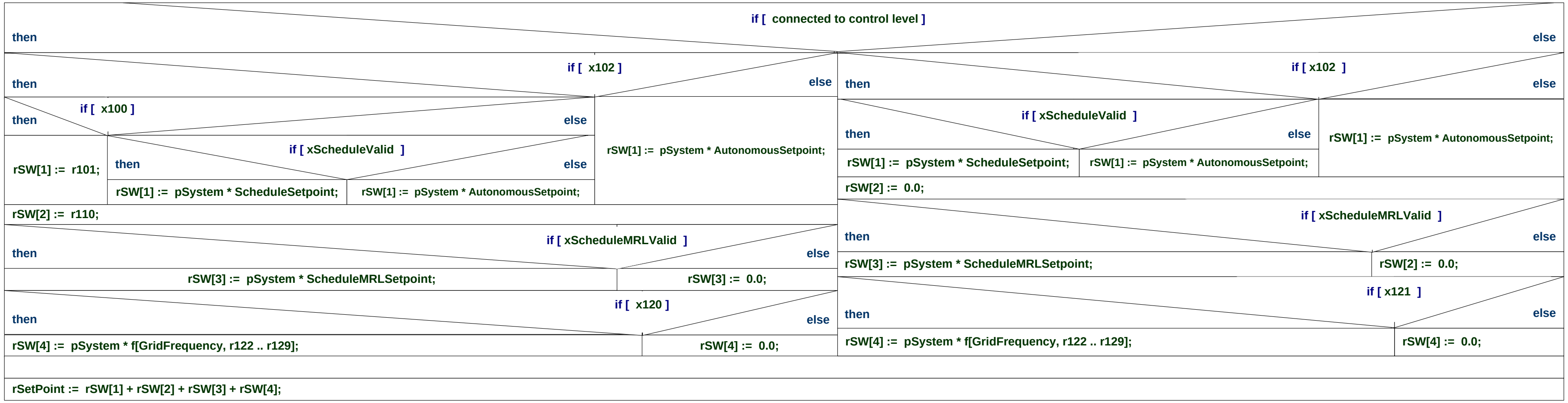
if [connected to control level]
then
else
if [x102]
then
else
if [x100]
then
else
rSW[1] := r101;
if [xScheduleValid]
then
else
rSW[1] := pSystem * ScheduleSetpoint;
rSW[1] := pSystem * AutonomousSetpoint;
rSW[1] := pSystem * AutonomousSetpoint;
rSW[2] := r110;
if [xScheduleMRLValid]
then
else
rSW[3] := pSystem * ScheduleMRLSetpoint;
rSW[3] := 0.0;
if [x120]
then
else
rSW[4] := pSystem * f[GridFrequency, r122 .. r129];
rSW[4] := 0.0;
if [x102]
then
else
if [xScheduleValid]
then
else
rSW[1] := pSystem * ScheduleSetpoint;
rSW[1] := pSystem * AutonomousSetpoint;
rSW[1] := pSystem * AutonomousSetpoint;
rSW[2] := 0.0;
if [xScheduleMRLValid]
then
else
rSW[3] := pSystem * ScheduleMRLSetpoint;
rSW[2] := 0.0;
if [x121]
then
else
rSW[4] := pSystem * f[GridFrequency, r122 .. r129];
rSW[4] := 0.0;
rSetPoint := rSW[1] + rSW[2] + rSW[3] + rSW[4];

Figure 4 Calculation of actual setpoints

Figure 4 describes the calculation of actual setpoints for the technical unit.

Determination of heat storage capacity

The available thermal storage capacity is calculated as a function of maximum generated temperature, actual return temperature, recent measured temperature at top and bottom of the storage device and its volume as follows:

$$Q = m \times c_P \times \left[(T_{VL} - T_{RL}) - \left(T_{Speicher,oben} - T_{Speicher,unten} \right) \right]$$

c_P…specific heat capacity

The resulting available electrical storage capacity is:

$$W = Q \times \sigma$$

σ...CHP coefficient

It is possible to split the overall volume into sub-volumes with individual temperature measurements.

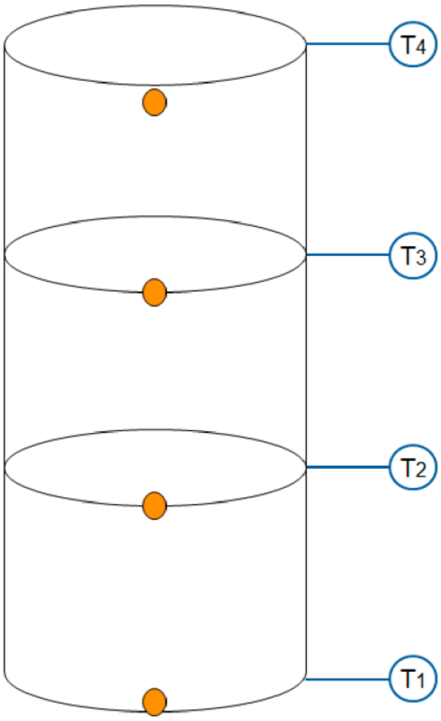

Figure 5 Partial volumes with multiple temperature measurements

The available storage capacity may be calculated from measurement values either in a distributed way at the system or centrally at the control station.

Secure communication

This chapter explains the requirements for secure communication between VHPready-compliant technical units (TU) and their assigned control center.

Introduction

The communication between the VHPready-compliant TUs and the control center has to be secured in view of the following criteria:

Guaranteed security during transmission of information with regard to

- Confidentiality
- Integrity (incl. authenticity)
- Availability

Furthermore, the availability of services required for secure communication also needs to be guaranteed.

To meet the IT security requirements, cryptographic procedures such as electronic signatures, encryption and certificate-based authentication in particular are qualified.

Implementation

To ensure secure communications, the implementation of the following requirements is necessary.

- The communication partners have to provide each other with authentication.
- During VHPready communication, the user data have to be encrypted.
- State-of-the-art[1] cryptographic algorithms have to be used.
- Protocols to realize secure communication have to secure all underlying protocol levels up to and including the data link layer as determined by the OSI model[2] during transmission.
- Already when establishing the connection, all session data (e.g. the keys during key exchange) that need to be protected can only be transmitted if encrypted.
- We have to determine how often the session keys for transmission encryption need to be replaced.
- Procedures have to be implemented for the generation of keys that can guarantee that the generated keys cannot be simply guessed or calculated (e.g. by using random numbers).

---

[1] BSI TR-02102-1 or RFC 3766 or NIST 800-131A

[2] ISO IEC 7498

Procedure to safeguard communications

For VHPready-compliant secure communication, a VPN has to be used that is based on TLS.

VPN makes it possible to guarantee the confidentiality of information when transmitting during the encryption procedure. Furthermore, the communication partners can be authenticated unambiguously during the establishment of the connection.

For VHPready-compliance, both the encryption procedure and authentication procedure need to be implemented.

The following specifications need to be followed when choosing the VPN technology:

- The most recent version of TLS has to be used (version 1.2 and higher[3]) to realize end-to-end encryption on the same communication line between the control center and the VHPready-compliant TU.
- The encryption has to be realized directly within the communication unit of the VHPready-compliant TU.
- The server has to be authenticated.
- For the authentication as well as for the key exchange, X.50[4] certificates have to be used.
- To guarantee the security of communications in the long term, Perfect Forward Secrecy has to be used. This requires the use of a Diffie-Hellman parameter on the server.
- The application of the UDP protocol has to be enabled by means of VPN technology so that the loss of performance as a result of the TCP protocol's flow control can be avoided.
- It has to be possible to configure the interval for the renewal of the session key. Intervals that are too short have to be avoided for the sake of practicality, especially when transmitting via mobile phone networks. Intervals that are too long also need to be avoided as this reduces the security of the session keys.

---

[3] RFC 5246

[4] X.509v3

Implementation guidelines

VPN

The VPN is created using open source software OpenVPN.

This can be integrated in the firmware of the corresponding bay control units for automation applications and realizes VPN connections, as required, by means of TLS-encrypted tunnels. For VHPready, version 1.2 or higher of TLS has to be used.

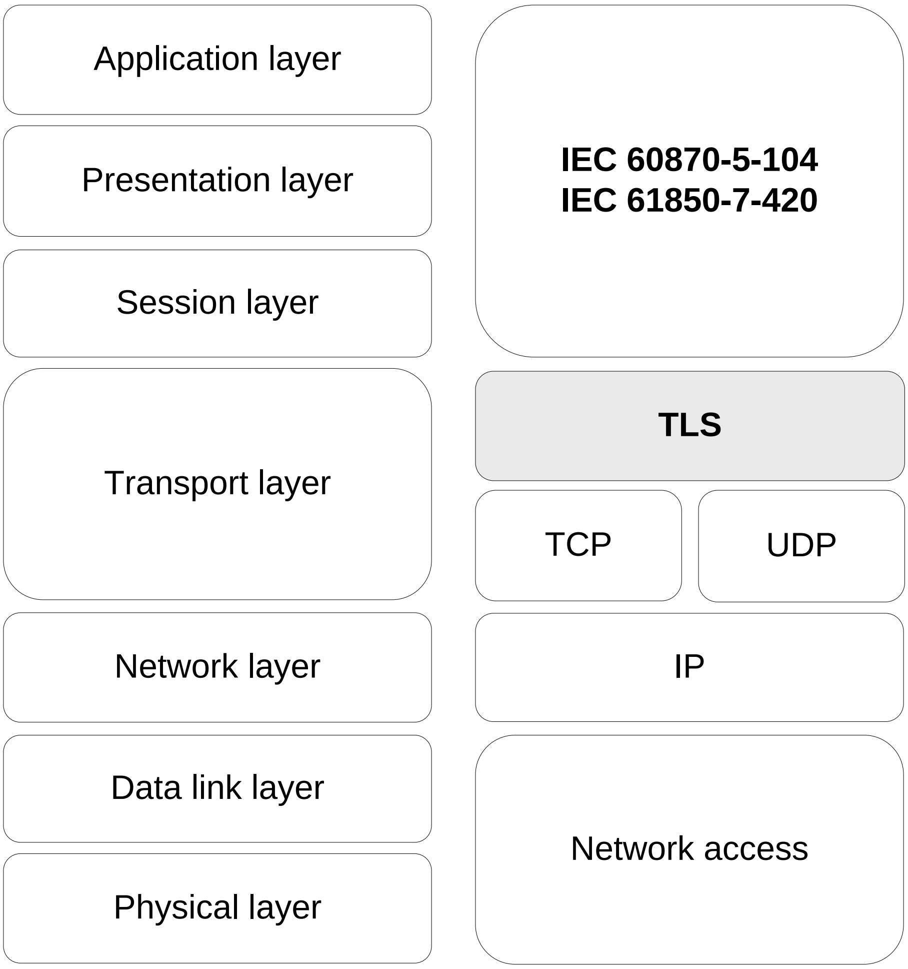

Figure 6 OpenVPN expands the transport layer by TLS

To configure the OpenVPN parameters, the following settings have been established.

Parameter	setting	Description
tls-version-min	1.2	Establishes the accepted minimum version for TLS. This ensures that no outdated TLS version is used, even if the communication partner requests this.
resolv-retry	infinite	Continuous verification of the server name Advisable in environments with unstable connections.
nobind		If this parameter is part of the OpenVPN configuration, no fixed port is reserved locally.
mute-replay-warnings		If this parameter is included in the OpenVPN configuration, no duplicate package warnings are generated. This is advisable in environments with wireless connections, as many duplicates occur in such environments.
remote-cert-eku [OID|STR] remote-cert-tls [OID|STR] tls-remote name (=CN) tls-verify cmd ns-cert-type [client|server]		All indicated parameters reduce the risk of man-in-the-middle attacks. One of these procedures has to be used.
tls-auth key file [0|1]	1	This is intended to protect against Denial of Service (DoS) attacks, as each package of the control channel is signed and packages without a valid signature are refused immediately without extensive verification of the client certificate.
cipher algorithm	AES-256-CBC	Defines the algorithm used for the symmetric encryption of the user data.
auth algorithm	SHA512	Indicates an algorithm used to sign all packages on the data channel.[5]

Table 2 The security parameters for the OpenVPN client configuration

VPN infrastructure design

An OpenVPN server is operated in the VHPready control center. All decentralized installations work as OpenVPN clients. Both the OpenVPN server and the OpenVPN clients in the installations use a certificate that was specifically issued to them, originating from a public key infrastructure (PKI).

The reciprocal authentication of the communication partners by verifying the certificate header is optional in OpenVPN. In VHPready, however, at least the server authentication is absolutely required. The authentication of the client is advisable.

The relevant client certificate with the corresponding private key, the certificate of the trusted certification office as well as the target address and the target port which can be used to reach the OpenVPN server are permanently stored in the configuration data of a VHPready-compliant installation. In the case of a private key, a secure storage location also needs to be provided.

---

[5] BSI TR-02102-1

Data needed for the OpenVPN connection have to be exchanged by authorized personnel. This mainly concerns, but is not limited to, the client key, the client certificate, the root certificate, the tls-auth key (and possibly other required certificates from the PKI), as well as the address and the port of the OpenVPN server.

Security characteristics and requirements

Certificates are issued per device. It is therefore not possible to undermine the security of all devices by breaching the security of a single one.

If a loss of integrity is suspected for a VHPready-compliant device, its certificate has to be blocked. As a result, the device is then no longer able to communicate with the control center. This procedure does not influence the functionality of other devices.

All certificates are issued for a limited time. After this term has ended, they automatically become invalid. For the VHPready-compliant devices, a service life of 2 years should not be exceeded to ensure that they are always state of the art[6].

A concept has to be developed for the key management of key generation with regard to key distribution and the use of the keys up to and including key suppression.

Apart from the data required for the tunnel structure, no communication should be possible between the VHPready-compliant devices and the control center unless it takes place via the tunnel.

The connection of a VHPready-compliant TU to its assigned control center should be used exclusively for VHPready-specific communication.

Direct communication between VHPready-compliant devices (clients) should be avoided.

All involved components need to have a synchronized time.

Patching has to be possible for the communication unit of a VHPready-compliant TU so that the software can be adjusted to recent developments.

Procedures and methods that make it possible to monitor the communications network and determine interruptions of availability and integrity, are developed and documented.

Access to the devices that are involved in the communication has to be logged with regard to successful and failed logins as well as configuration changes.

Interruptions of communication (intentionally or unintentionally) have to be logged and regularly analysed.

Robustness and possible effects of communication interruptions should be taken into account when designing the communication architecture.

---

[6] BSI TR-02102-1 or RFC 3766 or NIST 800-131A (see footnote 1)

Annexes

Annexe A (for informational purposes)

Organization of the documents of the VHPready 4.0 standard

The image below shows how the individual documents are interrelated within the VHPready 4.0 standard. It also shows which of the documents have a normative character.

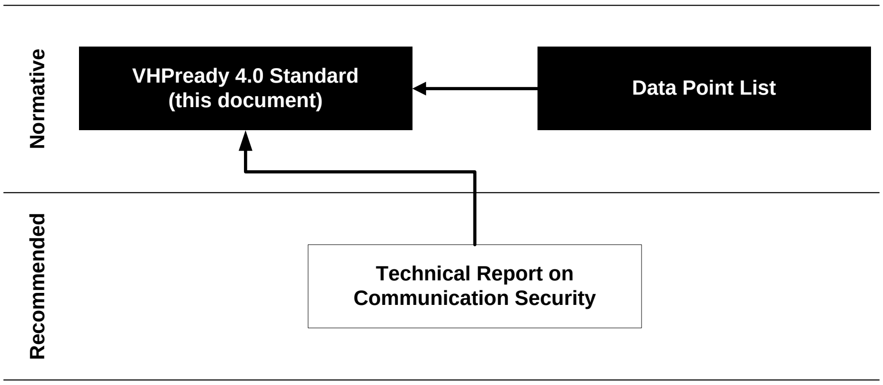
Normative
VHPready 4.0 Standard (this document)
Data Point List
Recommended
Technical Report on Communication Security

Figure 7 Interrelation of VHPready 4.0 documents

Data point list

The data points for remote access connections based on IEC 60870-5-104- or IEC 61850-7-420 are specified in the document "Datenpunkte V0.99999.ods".

Bibliography

[1] DIN EN 60870-5-104:2007-09. Telecontrol installations and systems - Part 5-104: Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles.

[2] DIN EN 61850-7-420:2009-10. Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes. English version EN 61850-7-420:2009.

[3] Minimum requirements for the supplier's information technology for the provision of automatic Frequency Recovery Reserve (aFRR). Version of 28/11/2014. 50Hertz, Amprion, Tennet, Transnet BW. (last consulted on 29/08/2015)

[4] Requirements for closed user groups to provide control power. Version of 12/05/2015. 50Hertz, Amprion, Tennet, Transnet BW. https://www.regelleistung.net/ext/download/itSrlPlatzhalter (last consulted on 29/08/2015)

[5] Website of open source software OpenVPN: (last consulted on 29/08/2015)

[6] IETF RFC-5246 "The Transport Layer Security (TLS) Protocol Version 1.2"; website of the IETF on TLS 1.2: (last consulted on 29/08/2015)

[7] IETF RFC-5905 "Network Time Protocol Version 4: Protocol and Algorithms Specification"; website of the IETF on NTP Version 4: (last consulted on 29/08/2015)

[8] Website of the IETF on SNTP (RFC-4330, see also RFC-5905): (last consulted on 29/08/2015)

Industry Alliance VHPready e.V.

EUREF-Campus 13
10829 Berlin
Germany
info@vhpready.de
www.vhpready.de

Contact:

VHPready Services GmbH
Franziska Schuth
Chief Executive Officer
Phone: +49 30 3988 4445
franziska.schuth@vhpready.de