CROSSWIND

HOLLANDSE KUST NOORD SITE V

SCADA INFORMATION – EXTRACT FOR BLPH

DOCUMENT NUMBER: CWHKN-INN-INP-SPC-00005



Revision	Date	Description	Prepared	Reviewed	Approved
1	28/08/2023	Issued For Information	DS	DS	DS

2 System Overview

2.1 Introduction

The SCADA system shall be based on the Copa-Data Zenon Energy edition platform that has a proven track record in HV system applications.

The SCADA system is designed to operate continuously without loss of function and that all components can be replaced, modified, or configured without loss of overall system functionality.

The SCADA system is designed to run on a dual redundant Virtual platform such that no fault in any hardware, network device, connection or software component shall jeopardise SCADA operability, safety, or plant availability.

The SCADA system will run virtually on a VMWare Cluster with no physical HMI machine workstation provided either offshore or onshore.

The SCADA system will be accessible via a Remote connection to a Windows Terminal Server using Microsoft Remote Desktop (RDP) with licensing to support up to 10 off users to access the SCADA displays at the same time, with independent sessions.

A separate Engineering Workstation VM is provided to support changes, modifications and commissioning.

2.2 Functionality

The SCADA system will have the following core functionality:

- Real-time supervision
- Control functionality
- Alarms and Events
- Historical data management
- Reporting
- Email alerts

2.3 Interfaces and Protocols

The SCADA system will be supplied with the following industry standard Ethernet based interface protocols for data exchange. Additional protocols can be added later to suit system expansion.

- IEC 61850 Client Edition 2
- IEC 60870-5-104 Client
- Modbus TCP/IP Client
- Siemens S7 TCP32 – to S7-1500

- OPC-UA Client
- OPC-UA Server

The SCADA system will provide interface to the following connected systems:

Interface	Protocol	Direction	Max Tags	Notes
Revenue Metering	IEC 60870-5-104	Remote => HV SCADA	1,000	24 x meters (8 IGRIDs each with 3 meters)
Power Quality (PQM)	Modbus TCP	Remote => HV SCADA	200	4 x PQM meters
DTS	Modbus TCP or IEC 60870-5-104	HV SCADA ⇔ Remote	TBA	
ICCP SCADA Server	TBA	HV SCADA ⇔ Remote	140	70 x locations Note 1
SCMS	TBA	HV SCADA ⇔ Remote	200	100 Input, 100 Output Note 1
O&M (Breeze)	OPC-UA server	HV SCADA => Remote	N/A	Access to tag database from Breeze. Note 1
O&M (Pi)	OPC-UA server	HV SCADA => Remote	N/A	Assess to tag database from OSIPi Connector. Note 1
O&M (Mail Alerts)	SMTP	Remote => HV SCADA	500	All alarms to trigger mail alarm
SGRE WPS	OPC-UA server	Remote => HV SCADA	1,125	69 x WTG Note 1
SGRE PPC	IEC 61850	HV SCADA ⇔ Remote	150	
SGRE AVI Navi	IEC 60870-5-104	Remote => HV SCADA	TBA	
SGRE Switchgear	IEC 61850	HV SCADA ⇔ Remote	2,277	2070 Input, 207 output
TSO LHVS curtailment & Info, Feedback setpoints	IEC 61850 Ed 2	HV SCADA ⇔ Remote	338	308 Input, 30 output
TSO OHVS Protection IED	IEC 61850 Ed 2	Remote => HV SCADA	TBA	12x relays
OHVS PLC Controllers A/B	Siemens S7	HV SCADA ⇔ PLC	50 / PLC controller	
LHVS PLC Controllers A/B	Siemens S7	HV SCADA ⇔ PLC	50 / PLC controller	
Innovation package	Future			

Table 2-a, SCADA System Interfaces

Notes:

1. Protocol TBC

3 SCADA Software Hosting

3.1 Introduction

The SCADA system will be based on the will be hosted on a number of VMs that will be supplied by CrossWind and configred by Proeon in accordance with this document.

3.2 Architecture

The SCADA system will be hosted on a number of VMs with the following system architecture:

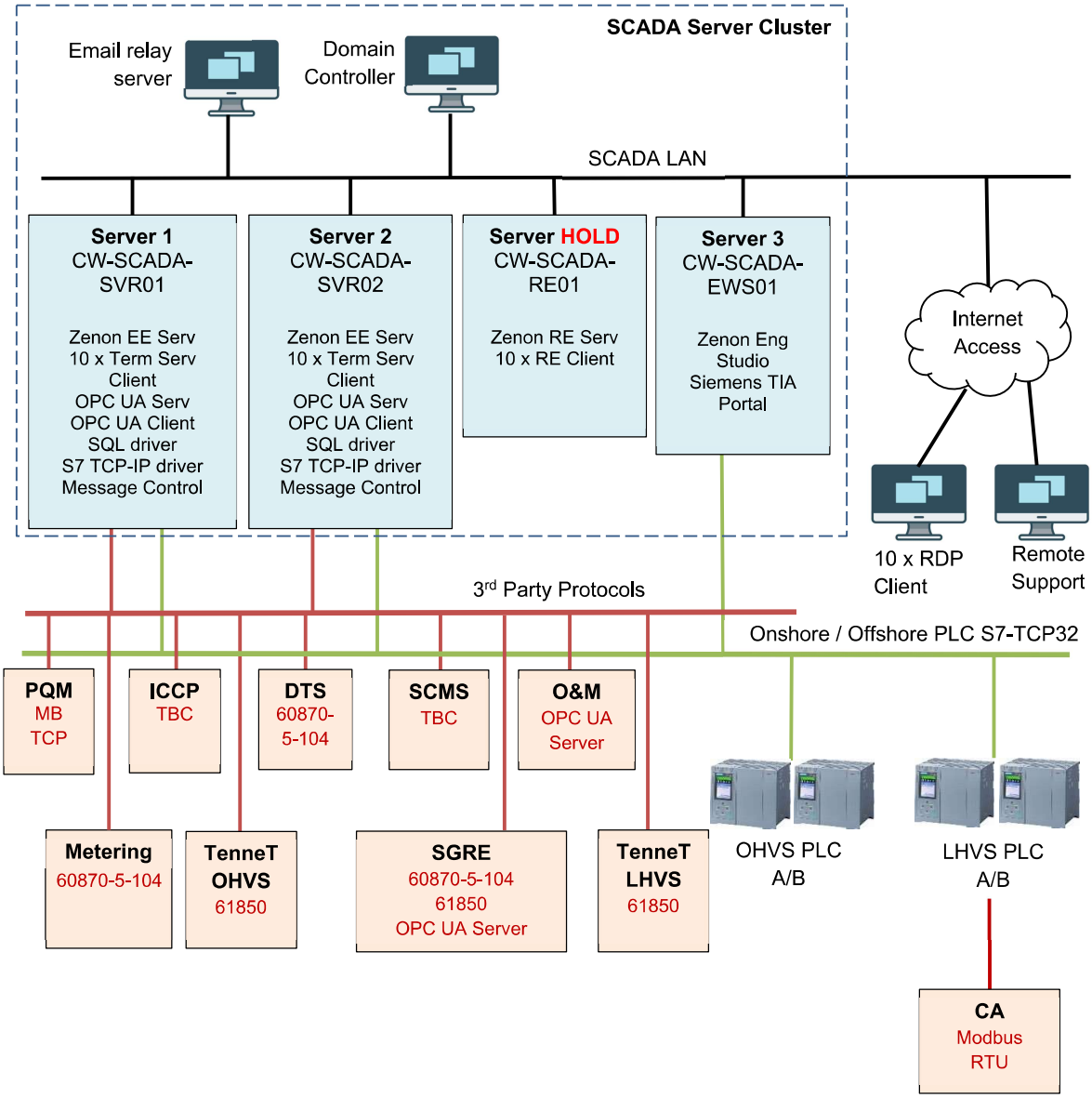


Figure 1, SCADA System Architecture

Notes:

1. Innovation package – future
2. Terminal services client shared between server A and B
3. Separate VM(s) may be configured to host test software

3.3 SCADA VMs and Licences

The following VMs and software licences will be deployed within the SCADA system:

Host VM	Licence	Qty	Functionality	Notes
CW-SCADA-SVR01 / CW-SCADA-SVR02	ZEE10-SRVUNLMTD	2	Server Licence - Unlimited tags	
	ZEE10-CLITERMS-10	1	Zenon EE Terminal server client - 10 User	
	ZS10-GWOPCUA	2	OPC UA Server	
	ZS10-DRVSQLDRV	2	SQL driver	
	ZS10-DRVS7TCP	2	S7 TCP-IP driver	
	ZS10-DRVOPCUA	2	OPC UA Client	
	ZS10-MC	2	Message Control	
CW-SCADA-RE01	ZRE10-SRV	1	Zenon RE Server	
	ZRE10-CLI-10	1	Zenon RE 10 Clients	
	MSSQLUSER-CAL	10	Microsoft SQL Server 2019 Standard Ed. User CAL	
CW-SCADA-EWS01	ZEE10-EDSA	1	Energy Edition Editor - Standalone version	
	TBA	1	Siemens TIA Version 16	

Table 3-a, Software Licences

Software licences for the SCADA system will be installed on each VM.

3.4 Server Hardware

All SCADA server hardware and associated power supplies are supplied and managed by CrossWind.

3.5 Network Architecture

All network LAN switches and firewalls and the like are designed, supplied and managed by CrossWind.

3.6 Operating Systems

All SCADA VMs will run on the Windows Server 2022 edition.

3.7 Domain Controllers

All Domain Controllers are designed, supplied and managed by CrossWind.

3.8 Email Relay Server

All Email Relay Servers are designed, supplied and managed by CrossWind.

3.9 Group Policy Management

HOLD – To be agreed with CrossWind.

3.10 Backup

All system / software backups will be the responsibility of CrossWind.

3.11 Licences

3.12 Time Synchronisation

The RTC on each of the SCADA system servers shall be synchronised to the CrossWind Domain Controller.

3.13 Redundancy Management

The SCADA software is configured for redundant operation with seamless redundancy. This means that no data is lost, even in the time period between the breakdown of one processor and the take over by the back-up.

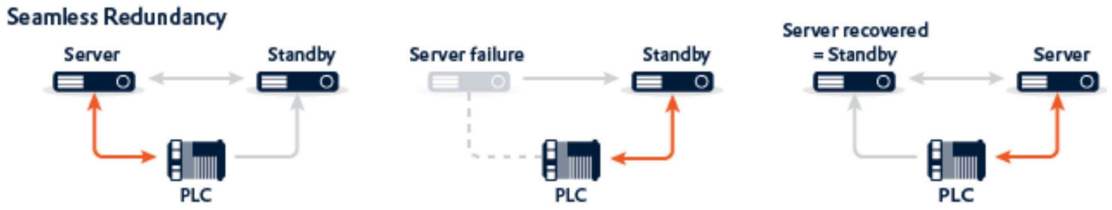


Figure 2, SCADA Redundancy

The redundancy configuration has the following basic operation:

- A server and a standby-server configured in Software redundancy mode.
- The standby server operates as a client. It receives data from the server and keeps its own autonomous buffer. In contrast to a normal client, the standby server records all historical data such as alarms, CEL and archives. Recipes, users, etc. are also synchronized.
- If the server fails, the standby server is promoted to server and takes over all tasks.
- All linked clients are informed of the server breakdown and connect fully automatically to the new server.
- Once the original server is back online, it connects to the newly promoted server as a standby server, ready to be promoted to server in the event of the newly promoted server failing.

4 Security

4.1 Two Factor Authentication

Two Factor Authentication (2FA) is not used within the SCADA system design.

4.2 Passwords

4.2.1 Policy

The following Password policy settings will be implemented:

Policy Settings		
Enforce password history	Complexity requirements are enforced when passwords are changed or created. These requirements include that the password cannot contain the user's account name, parts of the user's full name that exceed two consecutive characters, or a certain length of time that is exceeded before a similar password can be used.	10 - before the same password can be used again
Maximum password age	Security setting that determines the length of time before a password needs to be changed. Best practice is for password to expire 30…90 days to help prevent attacks.	365
Minimum password age	Minimum password age must be less than the maximum password age. For example, if the maximum password age is 1…999 the minimum password age can be up to 998 days.	0
Minimum password length	Security setting that determines the least number of characters for a password. Typically, the value of characters is set between 1…14. Zero characters if no password is required.	8 characters
Passwords must meet complexity requirements	Security setting determines the minimum requirements to meet complexity requirements. For example, some uppercase or lowercase characters, base 10 digits (0…9), or non-alphabetical characters.	Enabled
Store passwords using reversible encryption	Reversible encryption is used for password authentication. Microsoft recommends that this protocol be disabled because it's the same as storing plain text versions of the passwords. Microsoft states to use this policy only if 'application requirements outweigh the need to protect password information'.	Disabled

Table 4-a, Password Policy

4.2.2 Password construction

User password construction shall be at least 8 characters in length, and contain at least one character from each of the following:

- Alpha – Uppercase (A – Z)
- Alpha – Lowercase (a – z)
- Numeric (0 – 9) or special characters (!, $, #, %...)

The user will be asked to change their default password at first login.