Base Load Power Hub (BLPH)

Cybersecurity Workshop Preparation

Document Number: 1724000594-IN-RE-00041

Supplier Document Number: E366772C00-CWP

ROSETTI MARINO	
1	NO COMMENTS - APPROVED - WORK MAY PROCEED
2	MINOR COMMENTS - REVISE AND RESUBMIT - WORK MAY PROCEED
3	MAJOR COMMENTS – REJECTED – DO NOT PROCEED
4	APPROVAL NOT REQUIRED
NOTE: Approval doesn't relieve the supplier from mandatory compliance with contractual documents and specifications. Comments made do not imply acceptance of any cost or delivery impact.	
Sign	Date
	12/07/2024

Document Class: 3

00	04/06/2024	Issue for information	AB	AB	SC
Rev.	Date	Description	Prepared	Reviewed	Approved

YOKOGAWA Co-innovating tomorrow™

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Revision / Change Log

Rev.	Description
00	Issue for Information (IFI)

HOLDS LIST

No.	Description
1	
2	
3	
4	

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Table of contents

1 INTRODUCTION 5

1.1 PROJECT OVERVIEW 5

1.1.1 Project Location 5

1.1.2 Project Concept 6

2 DOCUMENT SCOPE 8

2.1 REFERENCES 8

2.2 DEFINITIONS AND ABBREVIATIONS 8

2.3 IEC 62443 standard 9

3 RISK ASSESSMENT PROCESS 10

3.1 input collection 10

3.2 Initial risk assessment 10

3.3 Detailed risk assessment 10

3.4 Gap analysis 11

4 TERMS OF REFERENCE 12

5 WORKSHOP AGENDA 13

6 CYBERSECURITY REPORT Table of contents 14

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

List of Figures

Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map 5
Figure 2 - Wind Park Details 6
Figure 3 – BLPH Concept 6

List of tables

Table 1 - Reference Documents 8
Table 2 - Definitions and Abbreviations 8

List of Attachments

ATTACHMENT-1 Proposed Cybersecurity Risk Matrix 16

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

1 INTRODUCTION

1.1 PROJECT OVERVIEW

Crosswind, a Shell and Eneco joint venture, was awarded the tender to develop the offshore Hollandse Kust Noord (HKN) wind farm, located 18.5km off the coast of Netherlands near the town of Egmond aan Zee. The consortium plans to have HKN operational in 2023 with an installed capacity of 759MW generating at least 3.3TWh per year. This is sufficient renewable power to supply more than 1 million Dutch households with green electricity.

Offshore wind farms produce intermittent electricity and balancing these dips and peaks and integrating this electricity into the national energy system requires new technologies. For this reason, the offshore wind farm will include several new technologies that could be implemented at full-scale in the future. The new technologies being explored include a floating solar park, a short-duration battery storage as well as long-term storage via green hydrogen produced by water electrolysis and subsequently consumed in a fuel cell. The combination of these individual measures, herein referred to as the Base Load Power Hub (BLPH) will ensure a continuous power supply regardless of the wind situation.

1.1.1 Project Location

The Hollandse Kust Noord (HKN) wind farm is located 18.5km off the coast of the Netherlands near the town of Egmond aan Zee.

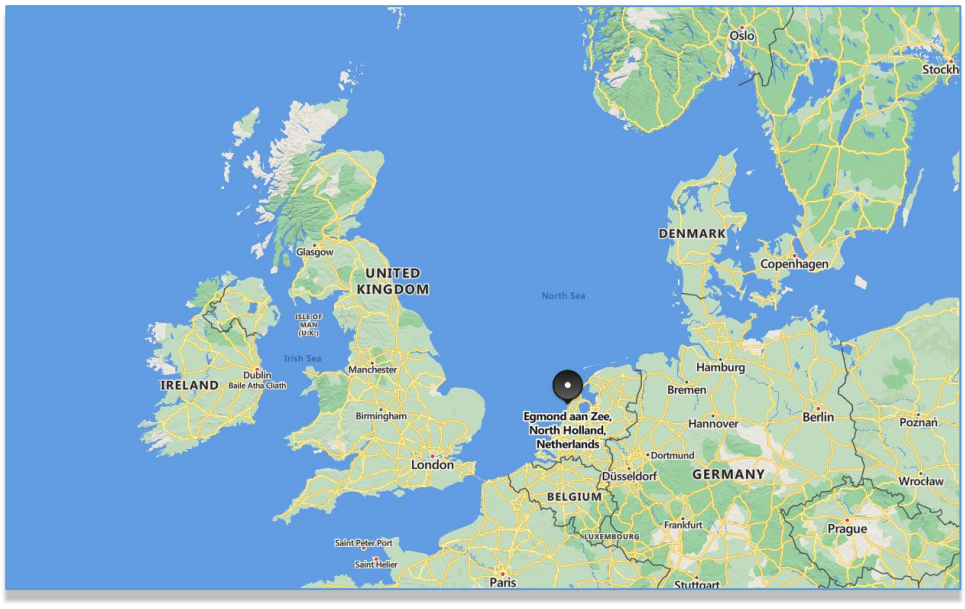


Figure 1 HOLLANDSE KUST NOORD WIND PARK Location Map



Figure 2 - Wind Park Details

The wind farm will consist of No. 69 x 11.5MW wind turbine generators each to be installed on a dedicated monopile structure. A 70th monopile located on coordinates E 590719.1, N 5841602.3 is reserved for installing the platform accommodating the BLPH. The monopile structure was designed and installed by Van Oord Offshore Wind (VooW) and therefore not part of the BLPH scope.

1.1.2 Project Concept

All components included in the BLPH will be integrated onshore on a topsides and installed in an offshore location within the boundaries of the HKN wind farm. At its simplest, the BLPH will store energy during periods of high electricity generation from renewable sources (a wind turbine generator and the floating solar PV farm) and release it during periods of low generation. In practice. It is expected that the energy stored will supplement generation from renewable sources to ensure that at least 1.0MW of power is exported to the electrical grid regardless of wind/solar availability.

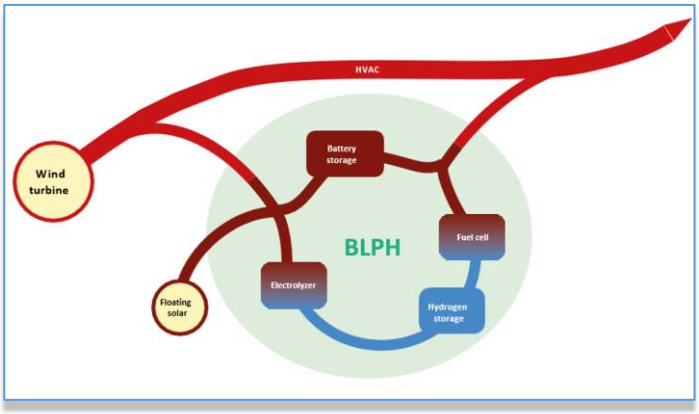


Figure 3 – BLPH Concept

Electricity in the BLPH will be stored in the form of electrons in a battery energy storage system (BESS) as well as converted into green hydrogen via water electrolysis. When the power output from the connecting wind turbine drops to below 1 MWe, the BLPH will return its stored energy to supplement the remaining power output. This will be by discharging the BESS, while stored hydrogen will be converted back into electricity using a fuel cell to extend the discharge duration.

The purpose of the BLPH s to function as a testbed for the integration of energy storage technologies with renewable generation. It is expected that equipment installed on the BLPH will operate as Normally Unmanned Installation for at least two (2) years with no or minimal maintenance and it will have its own independent control room with the ability to communicate with Crosswind's control room.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

2 DOCUMENT SCOPE

Scope of this document is to provide information about Cybersecurity Risk Matrix and ToC to be used for the Cybersecurity Workshop activity. This activity will be performed by Yokogawa, EPC and COMPANY.

2.1 REFERENCES

Doc. No.	Description
DEP 32.01.20.12-Gen.	DEP SPECIFICATION IACS SECURITY (February 2021).
CWHKN-PMT-PJA-PLN-00009	SYSTEM SECURITY REQUIREMENTS (Revision 1.0)
K559-2254-IC-REP-003	Cyber Security Assessment (Revision 0)
1724000594-IN-DD-00015	Yokogawa System Architecture (Revision 1)
123A90-DDL-IN-RE-40023	Cyber Security Design Philosophy (Revision 0).

Table 1 - Reference Documents

2.2 DEFINITIONS AND ABBREVIATIONS

COMPANY	Crosswind
EPC	ROSETTI MARINO S.p.A.
PROJECT	HOLLANDSE KUST NOORD WIND PARK Project
IACS	Industrial Automation and Control Systems
SUC	System under consideration
SL-T	Security Level - Target
ISA	International Society of Automation
OT	Operational Technology

Table 2 - Definitions and Abbreviations

2.3 IEC 62443 STANDARD

The standard used as reference for the Cybersecurity Risk assessment is IEC62443.

ISA/IEC62443 is in fact a series of standards and technical report. This series addresses the Cybersecurity of Industrial Automation and Control Systems (IACS) throughout their lifecycle. These standards and technical reports were initially developed for the industrial process sector but have proven useful, and thus applied, in different fields.

Initially, ISA developed this standard by considering "traditional" IT standards and practices. Then, it was considered that IACS has peculiar requirements. This is because the consequences of a cyberattack on a IACS system could be very different from IT systems. In fact, cyberattacks to OT system can result in loss of life, damage to the environment and productivity.

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to develop this standard for cybersecurity of IACS. The ISA99 Committee and the IEC Technical Committee 65/Working Group 10 continuously improve and publish the ISA/IEC 62443 Series. The focus is to detail a methodical engineered approach to addressing the cybersecurity of IACS.

In the end, the benefits of using a standards-based approach include reducing the likelihood of a successful cyberattack, the use of a common standard among stakeholders and security throughout the lifecycle.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

3 RISK ASSESSMENT PROCESS

According to IEC62443, the Risk Assessment workflow is composed of 4 phases:

- Input collection
- Initial risk assessment
- Detailed risk assessment
- Gap analysis

The activities of each phases are illustrated in the subsequent paragraphs.

3.1 INPUT COLLECTION

During input collection phase, the necessary input information is collected. This requires the cooperation of COMPANY and EPC.

Usually, since the acceptance of the residual risk is responsibility of the management of the COMPANY, Yokogawa expects to receive a risk matrix from the COMPANY.

In this specific project, Yokogawa proposes a Risk Matrix (Appendix 1), in order for COMPANY to comment and approve it.

Without an approved risk matrix, the activity cannot proceed.

Also, System architecture (doc. 1724000594-IN-DD-00015) is a fundamental document, that will be used as reference for the workshop.

A kick-off meeting is usually performed during this phase.

3.2 INITIAL RISK ASSESSMENT

During the initial risk assessment, a high level risk assessment is performed, with the task of executing an initial evaluation of risk. The result of this activity allows to understand if the initial risk is tolerable and helps in the subsequent activity of defining zones and conduits. In the end, an initial SL-T is defined.

In the end, a High Level Risk Assessment report can be generated.

3.3 DETAILED RISK ASSESSMENT

A detailed level cyber security risk assessment is intended to identify both the consequences and the likelihood of cyber-attack scenarios that are identified during the work process. This process requires knowledge of the (proposed) design, policies, and procedures to support the technical measures included in the design as well as of its system architecture.

In the end, a residual cybersecurity risk and SL-T for each zone and conduit will be determined.

3.4 GAP ANALYSIS

In case of changes impacting Cybersecurity, a Gap Analysis should be performed, and an analysis report should be prepared.

4 TERMS OF REFERENCE

The subsequent Terms of Reference list has been proposed to Crosswind for the Cybersecurity Workshop.

- CSRA / project CS objectives definition;
- Responsibilities & Governance / Battery Limits definition (es. CPI);
  - Stakeholders identification;
  - Involved sites and ownership identification;
  - Other assumptions / considerations;
- Project cyber lifecycle phases / Iterative Risk Assessment phases;
  - Safety-related considerations and integrations;
  - Design / Implement / Validation & Testing / Commissioning;
- Documentation review / vendor documentation Plan;
  - Specific contractual cyber-related deliverable milestones;
  - IP addressing plan (networks, subnetting & VLAN, company integration);
- Risk scoring / Threat Landscape / Threat Identification methodologies;
  - SuC / Criticality assessment;
  - Identification of Essential Functions;
  - Identification / analysis of major security conduits / zones;
  - Planned Yokogawa countermeasures;
- 62443 Compliance gap / praise metrics and reporting outcomes;
- Follow-up considerations / Risk monitoring;
  - Risk management plan and review cycles;

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

5 WORKSHOP AGENDA

The Cybersecurity Workshop is expected to last for 3 days. Yokogawa proposes the subsequent agenda.

Day1:

- CSRA / project CS objectives definition;
- Responsibilities & Governance / Battery Limits definition (es. CPI);
  - Stakeholders identification;
  - Involved sites and ownership identification;
  - Other assumptions / considerations;
- Project cyber lifecycle phases / Iterative Risk Assessment phases;
  - Safety-related considerations and integrations;
  - Design / Implement / Validation & Testing / Commissioning;
- Documentation review / vendor documentation Plan;
  - Specific contractual cyber-related deliverable milestones;
  - Network specific documents

Day2:

- Risk scoring / Threat Landscape / Threat Identification methodologies;
  - SuC / Criticality assessment;
  - Identification of Essential Functions;
  - Identification / analysis of major security zones and conduits;
  - Planned Yokogawa countermeasures;

Day3:

- 62443 Compliance gap / praise metrics and reporting outcomes;
- Follow-up considerations / Risk monitoring;
  - Risk management plan and review cycles;

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

6 CYBERSECURITY REPORT TABLE OF CONTENTS

After the activity, Yokogawa will produce a report with the subsequent table of contents

1. Introduction
1.1 Background
1.2 Project Overview
1.3 Purpose of This Document
1.4 Scope of the Document
1.5 Reference Documents
1.5.1 Project Specifications Documents
1.5.2 Customer Reference Documents
1.6 Definitions and Abbreviations
1.6.1 Definitions
1.6.2 Abbreviations
1.7 Hold List
2. Risk Assessment
2.1 Project RA Scope
2.2 Risk Assessment Schedule
2.3 HLRA Participant Details
2.4 DRA Participant Details
3. Risk Assessment Process
3.1 High Level Risk Assessment
3.2 Detailed Risk Assessment
4. Assessment Methodology
4.1 Preparation Phase
4.2 Gap Analysis Phase
4.3 Report Creation Phase
5. High Level Risk Assessment
5.1 HLRA Process
5.2 Zones in SuC
5.3 Worst-Case Threat Scenarios
5.4 Consequence
5.5 Likelihood
5.6 Risk Assessment Matrix
5.7 Calculating the Risk
5.7.1 SL & SL-T
5.7.2 CRRF
5.8 HLRA Workshop
6. Detailed Risk Assessment
6.1 Risk Levels (from HLRA)
6.2 Threats and Vulnerabilities
6.3 Countermeasures
6.4 DRA Workshop
7. Base Line Determintion

8. Gap Analysis
9. Assessment Findings
10. Foundational and Security Requirements
10.1.1 FR1 Identification and Authentication Control
10.1.2 FR2 Use Control
10.1.3 FR3 System Integrity
10.1.4 FR4 Data Confidentiality
10.1.5 FR5 Restricted Data Flow
10.1.6 FR6 Timely Response to Events
10.1.7 FR7 Resource Availability
11. Appendix
11.1 Appendix-1 : High Level Risk Assessment Sheet
11.2 Appendix-2 : Detailed Risk Assessment Sheet
11.3 Appendix-3 : Security Requirements Compliance Sheet

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy