Base Load Power Hub (BLPH)

Cyber Security Risk Assessment Report

Document Number: 1724000594-IN-RE-00035

Supplier Document Number: E366772C00-CSRA

Document Class: 2

02	12/Mar/2025	Accepted for Construction (AFC)	N S Rao	Alessandro Berra	Sonia Corradi
01	25/Sep/2024	Issue for Review (IFR)	N S Rao	Alessandro Berra	Sonia Corradi
00	05/July/2024	Issue for Review (IFR)	N S Rao	Alessandro Berra	Sonia Corradi
Rev.	Date	Description	Prepared	Reviewed	Approved

YOKOGAWA Co-innovating tomorrow™

Revision / Change Log

Rev.	Description
0	Issue for Review (IFR)
1	Issue for Review (IFR)
2	Accepted for Construction (AFC)

HOLDS LIST

No.	Description
1	Section 10 Gap Analysis
2	Section 11 Assessment Findings

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 6
1.1 PROJECT OVERVIEW 6
1.1.1 PROJECT LOCATION 6
1.1.2 PROJECT CONCEPT 7
2. DOCUMENT SCOPE 8
2.1 REFERENCE DOCUMENTS 8
2.2 DEFINITIONS AND ABBREVIATIONS 8
3. APPLICABLE CODES STANDARDS AND REGULATION 10
3.1 APPLICABLE DESIGN ENGINEERING PRACTICES 10
3.1.1 FULLY APPLICABLE DEP 10
3.2 APPLICABLE CROSSWIND SECURITY REQUIREMENTS 10
4. RISK ASSESSMENT 10
4.1 PROJECT RA SCOPE 10
4.2 RISK ASSESSMENT SCHEDULE 10
4.3 HLRA/DRA PARTICIPANT DETAILS 10
5. RISK ASSESSMENT PROCESS 11
5.1 HIGH LEVEL RISK ASSESSMENT 11
5.2 DETAILED RISK ASSESSMENT 11
6. ASSESSMENT METHODOLOGY 11
6.1 PREPARATION PHASE 12
6.2 GAP ANALYSIS PHASE 13
6.3 REPORT CREATION PHASE 13
7. HIGH LEVEL RISK ASSESSMENT 14
7.1 HLRA PROCESS 14
7.2 ZONES IN SuC 15
7.3 WORST-CASE THREAT SCENARIOS 15
7.4 CONSEQUENCE 16
7.5 LIKELIHOOD 16
7.6 RISK ASSESSMENT MATRIX 18
7.7 CALCULATING THE RISK 19

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

7.7.1 SL & SL-T 19
7.7.2 CRRF 19
7.8 HLRA WORKSHOP 20
8. DETAILED RISK ASSESSMEN T 21
8.1 THREATS AND VULNERABILITIES 22
8.2 COUNTERMEASURES 23
8.3 DRA WORKSHOP 24
9. BASE LINE DETERMINATION 25
10. GAP ANALYSIS 25
10.1 EXCEPTIONS 26
11. ASSESSMENT FINDINGS 26
11.1 CVE 27
12. APPENDIX 27
Appendix-1: High Level Risk Assessment Sheet 27
Appendix-2: Detailed Risk Assessment Sheet 27
Appendix-3: Security Requirements Compliance Sheet 27

List of Figures

Figure 1 - HOLLANDSE KUST NOORD WIND PARK Location Map 6
Figure 2 - Wind Park Details 7
Figure 3 – BLPH Concept 7
Figure 4 – Assessment Methodology 12
Figure 5 – HLRA Steps 14
Figure 6 – DRA Steps 21

List of Tables

Table 1 - Reference Documents 8
Table 2 - Definitions and Abbreviations 9
Table 3 – Applicable Document(s) 10
Table 4 – Applicable Document(s) 10
Table 5 - Schedule 10

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

Table 6 - Participant Details 11
Table 7 - Input Documents 12
Table 8 - List of Subsystems 12
Table 9 - Reference Documents for RA 13
Table 10 - Zone List 15
Table 11 - Worst Case Scenarios 16
Table 12 - Consequence 16
Table 13 - Risk Assessment Matrix 16
Table 14 - Risk Assessment Matrix 18
Table 15 - Risk and SL 18
Table 16 - Risk Assessment Matrix 20
Table 17 - Risk Assessment Matrix 21
Table 18 - Threats and Vulnerabilities 23
Table 19 - Mitigated Risk and SL 25
Table 20 - CVE Links 27

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.

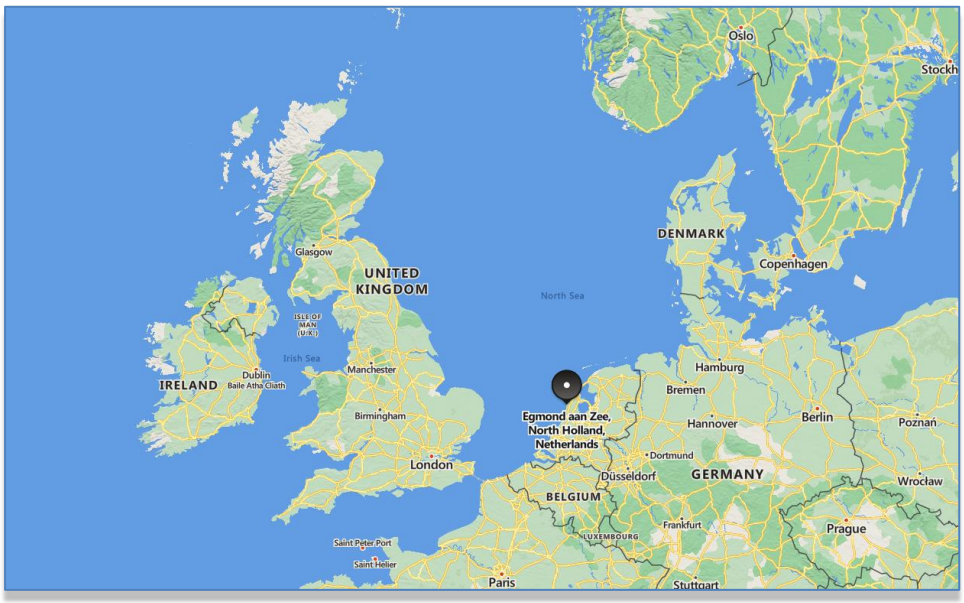


Figure 1 - HOLLANDSE KUST NOORD WIND PARK Location Map

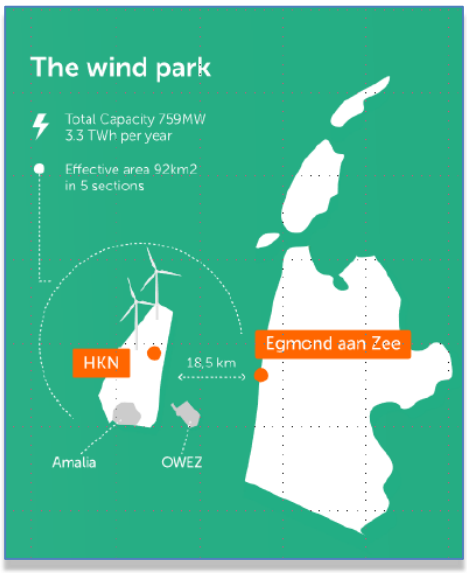


Figure 2 - Wind Park Details

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 topside 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.

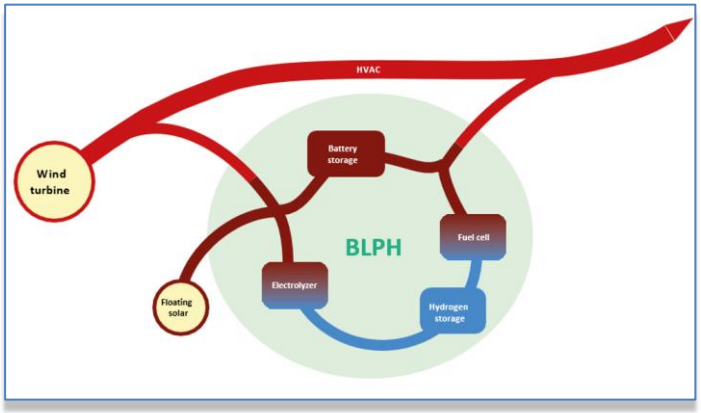


Figure 3 – BLPH Concept

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.

2. DOCUMENT SCOPE

The purpose of this document is to provide the ICSS Security Risk Assessment Report containing the zone details, security level information, Gap if any between baseline and system design requirements specifications and security countermeasures.

The intended audience for this document is the asset owners, system integrators, product and service suppliers to perform and ensure the compliance of the security requirement during the engineering and implementation phase and subsequently throughout the project lifecycle ensuring the adherence of CSMS process.

2.1 REFERENCE DOCUMENTS

REF	Document Title	Description
[1]	Design Engineering Practice (DEP)	32.01.20.12-Gen
[2]	Risk Assessment Matrix (Cybersecurity Workshop Preparation)	1724000594-IN-RE-00041
[3]	Cyber Security Assessment	K559-2254-IC-REP-003
[4]	Control System Philosophy	K559-2254-IC-PHI-001
[5]	System specification for Main Automation Contractor	K559-2254-IC-SPE-001
[6]	PCS and SAFETY SYSTEMS Software Functional Design Specification (FDS-SW)	1724000594-IN-SP-00018
[7]	Crosswind - System Security Requirements	CWHKN-PMT-PJA-PLN-00009

Table 1 - Reference Documents

2.2 DEFINITIONS AND ABBREVIATIONS

AD	Active Directory
BESS	Battery Energy Storage System
BLPH	Base Load Power Hub
BRS	Backup and Recovery System
CI Server	Collaborative Information Server
COMPANY	Crosswind
CRRF	Cyber Risk Reduction Factor
CSMS	Control Security Management System
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control System

DEP	Design and Engineering Practice
DRA	Detailed Risk Assessment
EMCS	Electrical Monitoring and Control System
EPC	Engineering Procurement Construction
EWS	Engineering Workstation
FDS	Functional Design Specification
FDS-SW	Software Functional Design Specification
GPO	Group Policies Objects
HIS	Host Integration Server
HKN	Hollandse Kust Noord
HLRA	High Level Rish Assessment
HMI	Human Machine Interface
IACS	Industrial Automation and Control Systems
ICSS	Integrated Control and Safety System
IEC	International Electrotechnical Commission
MAC	Main Automation Contractor
NMS	Network Management System
OD	Office Domain
OT	Operational Technology
PCS	Process Control System
PRM	Plant Resource Manager
RA	Risk Assessment
RAM	Risk Assessment Matrix
SHALL	An absolute requirement.
SL	Security Levels
SL-T	Security Level Target
SuC	System Under Consideration
UCP	Unit Control System
UPS	Uninterrupted Power Supply
WSUS	Windows Server Update Services

Table 2 - Definitions and Abbreviations

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

3. APPLICABLE CODES STANDARDS AND REGULATION

3.1 APPLICABLE DESIGN ENGINEERING PRACTICES

Design Engineering Practices (DEP) have a limited rollout on BLPH.

3.1.1 FULLY APPLICABLE DEP

The following DEP are identified as being fully applicable to the project.

Document Name	Document Title
DEP 32.01.20.12	Industrial Automation and Control Systems (IACS) Security

Table 3 – Applicable Document(s)

DEP 32.01.20.12 shall be applied to the project in full, in conjunction with IEC 62443, for the cybersecurity design.

3.2 APPLICABLE CROSSWIND SECURITY REQUIREMENTS

The following CW Documents are applicable to the project.

Document Name	Document Title
CWHKN-PMT-PJA-PLN-00009	Crosswind - System Security Requirements

Table 4 – Applicable Document(s)

4. RISK ASSESSMENT

4.1 PROJECT RA SCOPE

In Crosswind Project, the scope for Risk Assessment is Yokogawa MAC Supplied IACS component, including Interface of 3rd Party System (Until barrier).

4.2 RISK ASSESSMENT SCHEDULE

The assessment has been conducted based on the following schedule.

Sr. No	Activity	Date	Location
[1]	High Level Risk Assessment	17^{h} to 18th June'2024	Online
[2]	Detailed Risk Assessment	21st to 22nd August'2024	Online

Table 5 - Schedule

4.3 HLRA/DRA PARTICIPANT DETAILS

Sr. No	Risk Assessment team	Name	Organization
[1]	Facilitator for Risk Assessment	Mr. Sambasiva Rao	Yokogawa
[2]	Scribe - To take notes (Coordinator)	Mr. Alessandro	Yokogawa
[3]	Automation Control Engineer	Mr. Kamalnabh	Yokogawa
[4]	Network Security Solution Lead	Ms. Bhoomika	Yokogawa
[5]	EPC-Project Engineering Manager	Dossena Mauro	Rosetti Marino
[6]	EPC-IT Specialist	Piva Francesco	Rosetti Marino
[7]	COMPANY-IT	Edwin Klom	Crosswind

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

[8]	COMPANY-Instrumentation	Philip Robinson	Crosswind
[9]	COMPANY-Project engineer	Marta Iacopetti:	Crosswind

Table 6 - Participant Details

5. RISK ASSESSMENT PROCESS

The Risk Assessment is conducted in accordance with IEC 62443-3-2 standard. The process contains 2 key steps.

I. High Level Risk Assessment (HLRA)

II. Detailed Risk Assessment (DRA)

5.1 HIGH LEVEL RISK ASSESSMENT

The High-Level Cybersecurity Risk Assessment is the first step in assessment process which includes the following.

- Identifying Zones and Conduits
- List the Worst-Case Scenarios
- Determine the Unmitigated Risk for each zone

5.2 DETAILED RISK ASSESSMENT

A Detailed Cybersecurity risk assessment is to identify the risk associated with threat scenarios that will be influenced by the vulnerabilities that are present in the OT environment. The DRA includes

- Identify Threats, Vulnerabilities
- Determine Consequences and Impact (Severity)
- Estimate Likelihood of occurrence
- Consider Countermeasures
- Calculate Residual Risk
- HAZOP – RAM, Physical barriers

6. ASSESSMENT METHODOLOGY

The methodology to perform risk assessment is in phases, which includes HLRA, DRA, Gap Analysis, Reporting.

HLRA is used to determine the business and HSE impact in the event of system compromise or failure. The purpose of this initial risk assessment is to identify the worst-case unmitigated risk to the SuC. While this task is the first step of a risk assessment, it is NOT a detailed vulnerability or threat assessment.

HLRA result is the main inputs to conduct Detailed Risk assessment. Detailed Risk assessment shall be conducted during project execute phase.

A detailed risk assessment focuses on individual ICSS network devices and considers a detailed technical threats and vulnerabilities of these assets and the effectiveness of countermeasures.

Threat scenarios and the likelihood of the threat materializing based on industry experience determines the impact and helps to explain what happens with the system when the threat materializes. =The risk associated with a certain threat scenario will be influenced by the vulnerabilities that are present in the OT environment.

For this risk assessment, the risk target will be expressed as a tolerable risk value specified (by company) during the workshop. Any risk that scores lower than the risk target is considered acceptable, and any risk above the target risk is considered not acceptable.

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

In addition to assessing the unmitigated, the assessment will also aim to identify countermeasures that would reduce the risk for the scenarios that introduce a risk that exceeds the risk target. The scenario will then be reassessed with the hypothetical countermeasures in place to determine if these countermeasures can mitigate the risk.

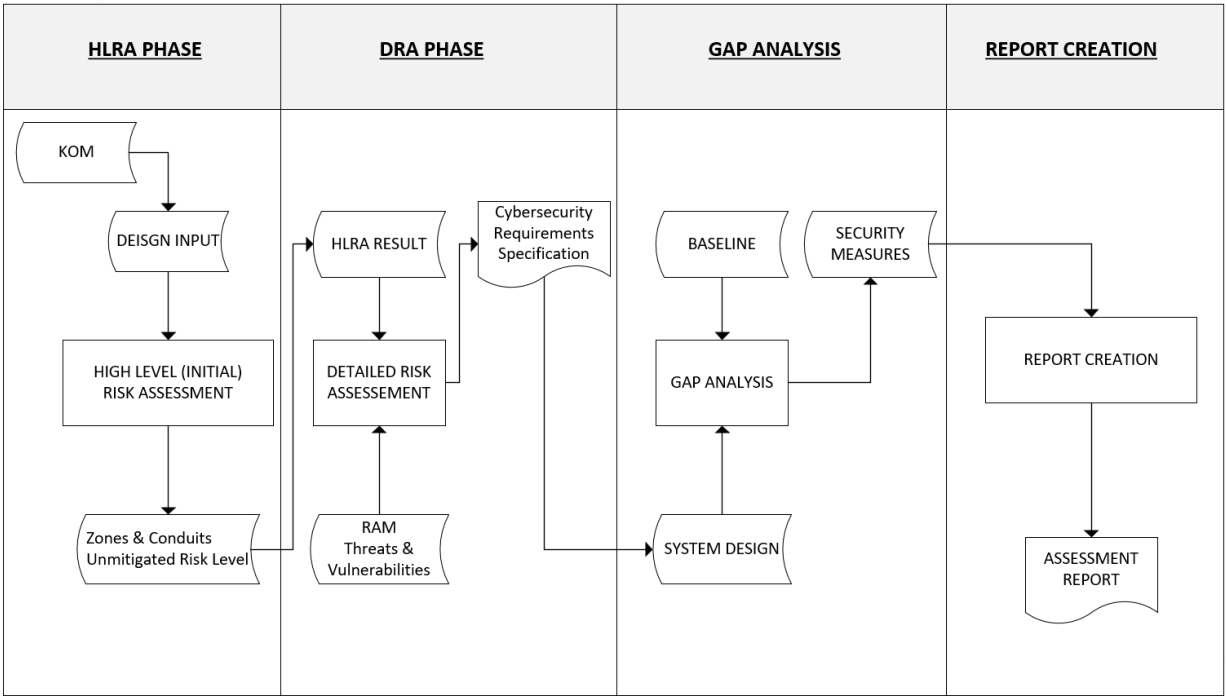


Figure 4 – Assessment Methodology.

6.1 PREPARATION PHASE

In Preparation Phase, System under Consideration (SuC) is defined to determine the scope and boundaries of the system that are to be assessed. Inputs document with revision number, list of subsystems is identified.

High Level Risk Assessment is done in this phase.

The Following are the input documents, subsystems identified for risk assessment of this project.

Sr. No	System	Document Name	Document Number
[1]	ICSS System	System Architecture	1724000594-IN-DD-00015

Table 7 - Input Documents

Sr. No	List of Subsystems
[1]	Water Treatment UCP
[2]	LV Switchgear
[3]	HVAC
[4]	UPS
[5]	Instrument Air UCP
[6]	Nitrogen UCP
[7]	EMCS

Table 8 - List of Subsystems

Sr. No	Document Name	Document Number	Revision
[1]	Design Engineering Practice	32.01.20.12-Gen	--
[2]	Risk Assessment Matrix ((Cybersecurity Workshop Preparation)	1724000594-IN-RE-00041	0
[3]	Cyber Security Assessment	K559-2254-IC-REP-003	0
[4]	Control System Philosophy	K559-2254-IC-PHI-001	1
[5]	System specification for Main Automation Contractor	K559-2254-IC-SPE-001	0
[6]	PCS and SAFETY SYSTEMS Software Functional Design Specification (FDS-SW)	1724000594-IN-SP-00018	0
[7]	Crosswind - System Security Requirements	CWHKN-PMT-PJA-PLN-00009	1.0

Table 9 - Reference Documents for RA

6.2 GAP ANALYSIS PHASE

The next phase in RA process comprises of Baseline Determination, Detailed Risk Assessment Workshop and Determine the Security measures required and Identifying the Gap in System Design.

6.3 REPORT CREATION PHASE

In this phase, upon DRA workshop and subsequent gap analysis a Detailed Assessment Report to be prepared. This report can be the baseline for future CSMS process.
The report to comprise the evidence of Security Solution implemented in the project.

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

7. HIGH LEVEL RISK ASSESSMENT

HLRA is the process of identifying and assessing the priority of risks.

The process involves the following key steps.

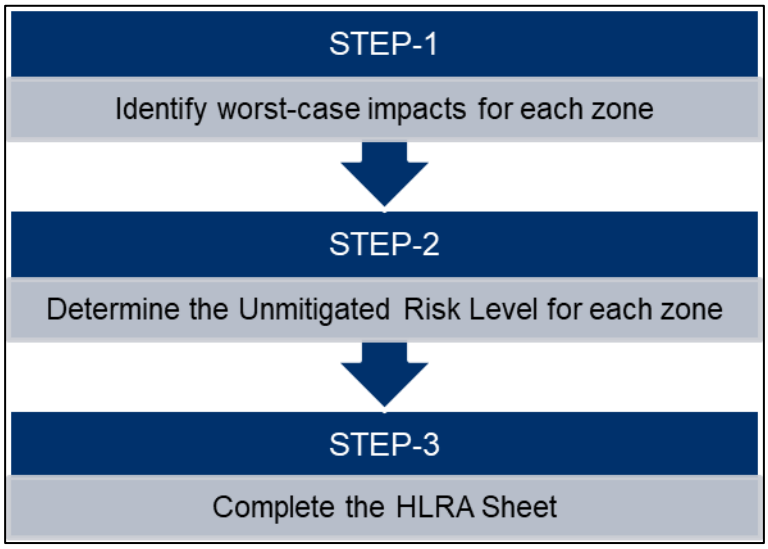


Figure 5 – HLRA Steps

Step -1: Worst case scenarios are listed. The likelihood and consequence(impact) of each with respective People, Asset, Community, Environment in accordance with the Risk Assessment Matrix (RAM) was determined.

This determination of likelihood and consequence was done based on the RAM provided by the COMPANY.

Step -2: The Unmitigated Risk by combining the Highest Impact rating and Unmitigated Likelihood to be arrived.

Unmitigated Risk = Highest Impact * Unmitigated Likelihood

The value for Unmitigated Likelihood is set to "Maximum" i.e. 5, as this is evaluated on a worst-case scenario, where no countermeasures are in place.

Step-3: Based on HLRA, Consequence / Impact, Unmitigated Risk values are populated.

7.1 HLRA PROCESS

High Level Risk Assessment involves identifying the cyber risks (Worst-case Scenario) associated for each zone. The impact, likelihood and the unmitigated risks are to be identified using RAM (Risk Assessment Matrix).

Risk = Threat x Vulnerability x Consequence

'Threat x Vulnerability' is Likelihood.

Consequence is the undesirable result of an incident, usually described in terms of health and safety effects, environmental impacts, loss of property, and business interruption costs result that occurs from a particular incident.

Impact measures of the ultimate loss or harm associated with a consequence. Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss, and recovery costs.

7.2 ZONES IN SuC

Partition of the SuC to zones and conduits have been identified during the HLRA, in accordance with

IEC 62443 process. The following were the Zones identified during workshop for HLRA from SuC.

Sr. No	ZONE	CONDUITS
[1]	PCS Control Zone	Vnet IP L2 Switch, Vnet IP Firewall
[2]	Safety Control Zone	Vnet IP L2 Switch, Vnet IP Firewall
[3]	PCS Zone	PIN Switch, OPC UA Switch, Sub-system Switch, Sub-system Firewall, PIN Firewall
[4]	Application Server Facility Zone	PIN Switch, PIN Firewall, Crosswind Firewall
[5]	Security Management Zone-1	PIN Switch, PIN Firewall
[6]	Security Management Zone-2	PIN Switch, PIN Firewall
[7]	Demilitarized Zone	PIN Switch, PIN Firewall, DMZ Switch
[8]	Crosswind Zone	PIN Switch, PIN Firewall
[9]	Third Party System Zone	Modbus Switch, Profinet Switch, Sub-system Firewall

Table 10 - Zone List

7.3 WORST-CASE THREAT SCENARIOS

The worst-case threat scenarios are listed to assess the impact/consequence to the process plant on the financial, health, safety and environment aspects, if the ICSS has been compromised.

Sr. No	Zone	Worst-Case Threat Scenario
[1]	PCS Control Zone	1) Communication loss. (Both Bus-Bus-2 Fail). Communication interruption. 2) Software: Controller malfunction. (Centum VP)
[2]	Safety Control Zone	1) Communication loss. (Both Bus-1 and Bus-2 Fail). Communication interruption. 2) Software: Controller malfunction. (Prosafe-RS) 3) Failure to detect process leak, toxic gas and fire leading a failure to alert Operation.
[3]	PCS Zone	1) Non-availability of DCS Engineering function due to malware. 2) Database integrity compromised. 3) Manipulated operation and logic changes (Via DCS Eng) Eg: Offline Download. HMI Compromised. 4) Malicious event causes all HIS/HMI stations to be encrypted, not available or responding, even after a reboot. 5) Manipulated operation via HIS/CI Server
[4]	Application Server Facility Zone	1) The adversary is trying to get into ICSS environment by breaching the solutions, to run code or manipulate system functions, parameters and data in an unauthorized way.
[5]	Security Management Zone-1	1) AD User can compromise the system. (through e.g.: DCS EWS) by creating an Unauthorized access.

Sr. No	Zone	Worst-Case Threat Scenario
[6]	Security Management Zone-2	1) Potential of someone gaining unauthorized or manipulative access to a cyber security solution.
[7]	Demilitarized Zone	1) Potential of someone gaining unauthorized or manipulative access to a cyber security solution, can compromise the system by creating an Unauthorized access.
[8]	Crosswind Zone	1) Potential of someone gaining unauthorized or manipulative access to a cyber security solution, can compromise the system.
[9]	Service Centre Zone	1) Potential of someone gaining unauthorized or manipulative access to a cyber security solution, can compromise the system.
[10]	Application Server Facility Zone-OD	1) The adversary is trying to get into ICSS environment by breaching the system, to run code or manipulate system functions, parameters and data in an unauthorized way.
[11]	Third Party System Zone	1) Database integrity compromised. 2) Non-availability of system or engineering function due to malware.

Table 11 - Worst Case Scenarios

7.4 CONSEQUENCE

The following are the categories of consequence considered as available in project RAM for the risk assessment.

Sr. No	Consequence
[1]	Safety
[2]	Environment
[3]	Assets
[4]	Data Integrity
[5]	Confidentiality
[6]	Operations
[7]	Financial
[8]	Reputation

Table 12 - Consequence

The impact rating of each category for each threat scenario is ranked as 1~5.

Only the highest-ranking category for a threat scenario are considered, since HLRA's primary objective is to determine impact for worst case scenario.

Impact/Likelihood determination can consider Independent Protection Layers (IPLs) such as mechanical safeguards (e.g., relief valve), physical security that are in place to mitigate the threat.

7.5 LIKELIHOOD

The likelihood is probability that the threat will be realized. The likelihood is categorized as 1 to 5 namely,

Sr. No	Likelihood
[1]	Rare
[2]	Unlikely
[3]	Possible
[4]	Likely
[5]	Almost Certain

Table 13 - Risk Assessment Matrix

The measure of likelihood is typically qualitative and is determined using a likelihood scale that is defined by the COMPANY as part of the Risk Assessment System.

For HRLA, Likelihood is considered as '5' as countermeasures are still not in consideration.

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

7.6 RISK ASSESSMENT MATRIX

Below is the Risk Assessment Matrix provided by the COMPANY. The Risk matrix is categorized into different Risk Rating Levels i.e., Level 1(Green), Level 2(Blue), Level 3(Yellow), Level 4(Red). This is not the Security Level (SL).

						PROPOSED CYBERSECURITY RISK MATRIX									
										Mitigation control	Highly effective controls in place, regularly updated.	Effective controls in place but may need updates.	Controls in place but may have some gaps or weaknesses.	Controls are partially effective, with significant gaps.	Ineffective or missing controls.
										Grade of outcome	Very low probability of successful attack.	Low probability of success.	Moderate probability of success.	High probability of success.	Very high probability of success.
										Attack complexity	Very high complexity requiring advanced skills and resources.	High complexity, requiring specialized tools and expertise.	Moderate complexity, requiring common tools and skills.	Low complexity, easily executed with available tools.	Very low complexity, easily executed with minimal effort.
										Seen Before	Never seen before: No known occurrences in the industry or location. (< 0.00001 per year)	Rarely seen in industry or location: Very few occurrences; highly unusual. (0.0001 to 0.00001 per year)	Occasionally seen in industry or location: Some occurrences; infrequent but known. (0.001 to 0.0001 per year)	Commonly seen in industry or location: Regularly occurs; recognized as a potential threat.(0.1 to 0.001 per year)	Frequently seen in industry or location: Occurs often; high awareness and preparedness (>0.1 per year)
											Rare	Unlikely	Possible	Likely	Almost certain
IMPACT	Safety	Environment	Assets	Data Integrity	Confidential	Operations	Financial	Reputation			1	2	3	4	5
	Slight injury or health effects;	None or low environmen	Minor impact; non-	Slight data integrity issues; minor recovery;	Minor impact on	Slight impact;	< 100K$	No impact on reputation;	Trivial	1	1	1	2	2	2
	Minor injury or health effects;	Temporary envirmental	Limited impact;	Minor data integrity issues; partial	Limited impact on	Limited impact;	< 1M$	Minor reputational	Minor	2	1	2	2	3	3
	Moderate injury or health	Minor environmen	Significant impact;	Moderate data integrity issues; full	Significant impact on	Significant impact;	< 10M$	Limited reputational	Moderate	3	2	2	3	3	4
	Major injury or significant	Major environmen	Major impact;	Major data integrity issues or partially	Major impact on	Major impact;	< 100M$	Significant reputational	Major	4	2	3	3	4	4
	Life-threatening impact or	Disaster, major	Complete loss;	Total data corruption or destroyed; full system	Complete loss of	Complete loss; total	> 100M$	Major reputational	Critical	5	3	3	4	4	4

Table 14 - Risk Assessment Matrix

Risk	5	10	15	20	25
SL	0	1	2	3	4

Table 15 - Risk and SL

7.7 CALCULATING THE RISK

The worst-case threat scenarios to be evaluated for the consequence, the resultant Impact and likelihood, based on which the unmitigated risk to be arrived for each zone.
This will be required to determine the Security Level Target. (SL-T)

7.7.1 SL & SL-T

Security level (SL) is a measure of confidence that the industrial automation and control system is free from vulnerabilities and functions in the intended manner.

SL-T is the desired level of Security for a particular system. A security level target for each security zone to be arrived.

SL-T is dependent upon the CRRF, which is a measure of the degree of risk reduction required to achieve tolerable risk.

7.7.2 CRRF

CRRF (Cyber Risk Reduction Factor) is the ratio that is determined by dividing unmitigated risk by tolerable risk.

The Tolerable Risk is the level of risk that an organization willing to take while optimizing the cost for the associated security measures.

$$\text{CRRF} = \text{Unmitigated Risk}/\text{Tolerable Risk}$$

During the Detailed Risk Assessment (DRA), the Tolerable Risk to be discussed and subsequently the Security Level i.e. SL-T for the project to be deduced.

In this project Tolerable Risk is considered as 10.

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

Tolerable Risk		10
RISK	CRRF	SL-T (0-4)
0	0	0
1	0.1	0
2	0.2	0
3	0.3	1
4	0.4	1
5	0.5	1
6	0.6	1
7	0.7	1
8	0.8	2
9	0.9	2
10	1	2
11	1.1	2
12	1.2	2
13	1.3	3
14	1.4	3
15	1.5	3
16	1.6	3
17	1.7	3
18	1.8	3
19	1.9	3
20	2	3
21	2.1	4
22	2.2	4
23	2.3	4
24	2.4	4
25	2.5	4

Table 16 - Risk Assessment Matrix

7.8 HLRA WORKSHOP

High Level Risk Assessment workshop was conducted, for the SuC.
Refer Section 2.3 (HLRA/DRA PARTICIPANT DETAILS)

The Worst-case Scenario, consequence/impact, likelihood, the unmitigated risks, RAM (Risk Assessment Matrix), mentioned in the previous sections of this document were used in conducting the workshop.

Risk Assessment was done considering no countermeasures being in place, i.e. the Likelihood is considered as maximum, along with the maximum value among the Impact categories as per the project RAM.

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

High-Level Risk Assessment			
Sr. No	Process Zones	Consequence (Max Value among the impact categories)	Likelihood (Unmitigated) Max Value
1	PCS Control Zone	5	5
2	Safety Control Zone	5	5
3	PCS Zone	5	5
4	Application Server Facility Zone	5	5
5	Security Management Zone-1	5	5
6	Security Management Zone-2	5	5
7	Demilitarized Zone	5	5
8	Crosswind Zone	3	5
9	Service Centre Zone	5	5
10	Application Server Facility Zone-OD	2	5
11	Third Party System Zone	4	5

Table 17 - Risk Assessment Matrix

For full HLRA's sheet Refer Appendix-1: High Level Risk Assessment Sheet

8. DETAILED RISK ASSESSMEN T

DRA process involves the following steps.

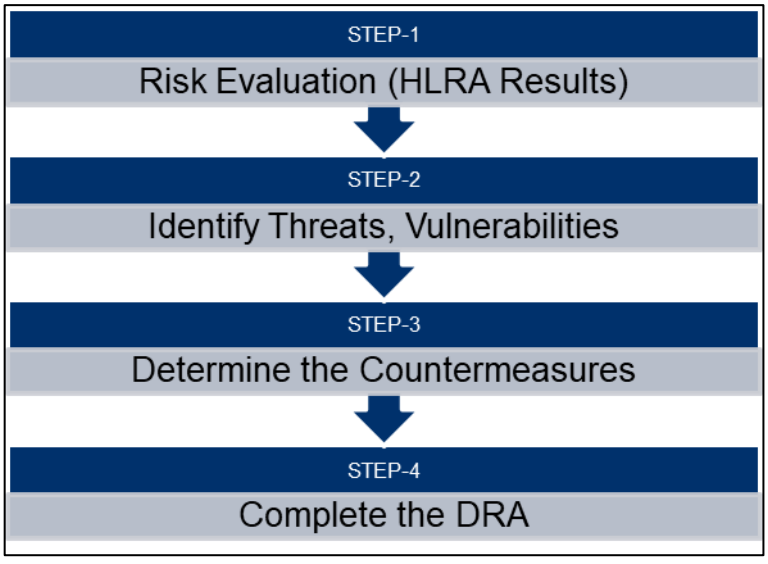


Figure 6 – DRA Steps

Step -1: Review and evaluate the risk of each zone determined during HLRA.

Step -2: Threats and Vulnerabilities to be listed.

Step -3: For each Zone, depending on the threat, vulnerabilities and impact, the security countermeasures to be planned. Assess the residual risk and check if any further countermeasures are required.

Step -4: Based on DRA, MTL (Mitigated Threat Likelihood), Mitigated Risk, Residual Risk values are populated, countermeasures are recorded.

8.1 THREATS AND VULNERABILITIES

The context of security risk is based on the concepts of threats, vulnerabilities, and countermeasures. Threats and Vulnerabilities relevant to the ICSS system to be identified.

The following Threat events and vulnerabilities were identified for the DRA.

Sr. No	Threat Event	Vulnerability
1	Authentication attacks	1.No security perimeter defined 2.Poor configurations are used 3.Logs are not maintained 4.Lack of integrity checking for communications 5.Lack of adequate authentication policy 6. Vendor default passwords are used
2	Authorization attacks	1.Lack of adequate access control policy 2.Inadequate security policy for OT 3. Inadequate access controls applied
3	Communications attacks	1. Standard, well-documented communication protocols are used in plaintext 2. Use of unsecure OT protocols 3. Lack of integrity checking for communications
4	Denial of Service/Denial of control attack	1. Poor configurations are used 2. Non-availability of the patches. 3. Firewalls are nonexistent or improperly configured
5	Worms, viruses & malicious code	1. Malware protection is not installed or up to date 2. Malware protection implemented without sufficient testing 3. Unsecured physical ports
6	Misconfiguration	1. Lack of configuration management policy 2. Poor configurations are used
7	Loss or misuse [of access cards, devices etc.]	1. Inadequate security policy for OT
8	Behavioral	1. Lack of administrative mechanisms for security policy enforcement 2. Inadequate security policy for OT
9	Unauthorized access to / deletion / modification of devices / data etc.	1. Lack of administrative mechanisms for security policy enforcement 2. Unauthorized personnel have physical access to equipment 3. Unsecured physical ports 4. Lack of backup power

Sr. No	Threat Event	Vulnerability
10	Software exploitation	1. Improper data validation 2. Installed security capabilities are not enabled by default 3. Inadequate authentication, privileges, and access control in software
11	Supplier compromise	1. Non-availability of the patches. 2. Use of unsecure OT protocols
12	Process failure	1. Inadequate incident detection and response plan and procedures 2. Inadequate management of change that allows insecure architecture to evolve
13	Technology failure	1. Improper data validation 2. Lack of redundancy for critical components
14	Social engineering	1. Inadequate OT security training and awareness program 2. No security perimeter defined 3. Control networks used for non-control traffic 4. Poor remote access controls
15	Reconnaissance/information gathering	1. Lack of administrative mechanisms for security policy enforcement 2. Lack of adequate access control policy 3. Lack of adequate authentication policy
16	Information leakage	1. Lack of administrative mechanisms for security policy enforcement 2. Lack of adequate access control policy 3. Lack of adequate authentication policy

Table 18 - Threats and Vulnerabilities

8.2 COUNTERMEASURES

Countermeasures are the mitigations considered or provisions made for the purpose of reducing risk to an acceptable level or to meet security policies.
Based on each Zones threats and vulnerabilities and the impending security risks, various countermeasures to be considered.
The following are the essential countermeasures considered in Crosswind Project.

- Active Directory:
  System Hardening to be done through GPO, to prevent unauthorized access to sensitive data.
  Role based access to all systems and devices will be achieved through Active Directory.
  Account Management, Segregation of duties and password management will be achieved through AD

- Anti-Virus:
  Anti-virus software shall be configured to scan files accessed by the system and logs, notify detection of malware infected files.

- OS Patch Management:

Software Update Management and maintenance to be achieved through patch management
Patch Installation, testing and verification can be achieved through OS Patch management

- Backup Recovery:
  Systems will be regularly backed- up at intervals to meet the data restore recovery objectives and business requirements. Operating System Files, application, Database files, Log files to be backed up.

- Network Management System:
  Log Monitoring and Log forwarding shall be available.
  Security Logs will be collected, retained and sent to a centralized Security information and event Monitoring (SIEM) tool (If required).

- Firewall:
  Network Segregation and Network Management shall be achieved through Firewalls.
  Network Segmentation and intercommunication through Firewall.

Additionally, the following Measures to be done.

- Up-to- date Firmware and Patches.
- Disable unsecure Protocols.
- Proper Management of Change method.
- Enforcement of Policies and Procedures.
- Confidential information (System Drawing, Configuration, IP address) protection.
- Periodical Security Awareness Training.
- Physical Security.

For more details, refer to - 1724000594-IN-RE-00043-Cyber Security Settings.

8.3 DRA WORKSHOP

A workshop was conducted to perform Detailed Risk Assessment.

For each zone. the impact on Safety, Environment, Assets, Data Integrity, Confidential, Operation, Financial, Reputation due to the Threat and Vulnerabilities along with the unmitigated likelihood (without any countermeasures) was determined (considered HLRA worst case values) to obtain the unmitigated Risk.

To mitigate the risk countermeasures are to be applied.

For each Zone, level of risk (after countermeasure/mitigation) shall be taken for consideration to obtain Zone SL-T. The mitigated threat likelihood is considered as 3 (MTL), based on the RAM provided.

This DRA is being done at design phase of the project, the mitigated likelihood of occurrence was taken as 'possible' i.e. '3', considering that no countermeasures are in place presently and shall be implemented.

Subsequent risk assessments as part of CSMS can further reduce the mitigated possibility.

The below table comprises of mitigated SL-T's of each Zone.

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

Sr. No	Zones	Mitigated		
		Risk	SL-T	Residual Risk
1	PCS Control Zone	15	2	5
2	Safety Control Zone	15	2	5
3	PCS Zone	15	2	5
4	Application Server Facility Zone	15	2	5
5	Security Management Zone-1	15	2	5
6	Security Management Zone-2	15	2	5
7	Demilitarized Zone	15	2	5
8	Crosswind Zone	9	1	0
9	Service Network Zone	15	2	5
10	Application Server Facility Zone-OD	12	2	2
11	Third Party System Zone	12	2	2

Table 19 - Mitigated Risk and SL

For full DRA's sheet Refer Appendix-2: Detailed Risk Assessment Sheet

9. BASE LINE DETERMINATION

Baseline is the required security requirements for the system. The baseline is determined by the security level target (SL-T).

Oftentimes the security of a zone or conduits is dependent upon factors outside of the zone or conduit such as clean and additional layers of physical and mechanical security. These assumptions and interdependencies are also considered during the baseline risk assessment.

In this project for cyber security risk determination the mechanical barriers, safeguarding barriers are considered being still intact. The unmitigated risk was considered on cybersecurity failure only.

Crosswind - System Security Requirements (CWHKN-PMT-PJA-PLN-00009) in accordance with the Security Level requirements from RA, have been considered as a base line for the project security solutions.

Compliance was made for this CW security requirements and the SL-T based on IEC requirements has been mapped.

Refer Appendix-3: Security Requirements Compliance Sheet

10. GAP ANALYSIS

Further to the DRA done, Risk Assessor will assess compliance status by analyzing the gaps between baseline security requirements and the system design. For example, if the system doesn't have anti-virus software, a security requirement regarding malware protection will not comply.

The security design document describes security requirements to protect Operational Technology (OT) against unauthorized access or modification and to ensure availability of operational processes. It defines, provides core practices implementing controls and requirements in the OT environment.

This security requirements are based on the ISA / IEC 62443 (formerly known as ISA - 99) Series of Standards for Industrial Automation and Control Systems (IACS) Security

The system design can achieve the SL-T if all the below key recommended security countermeasures are implemented.

Prevent

- Access Control
- Network Segmentation
- Asset and Patch Management
- System Hardening

Detect

- Logging And Monitoring

React

- Backup & Restore
- Incident Management

The verification activity of these required security solutions is to be done when system is Staged.

Refer HOLD -1 in Hold List.

10.1 EXCEPTIONS

During the gap analysis done at DRA workshop, with respect to Crosswind - System Security Requirements (CWHKN-PMT-PJA-PLN-00009) the following exceptions were identified.

- System Hardening:

Physical and logical access to diagnostic and configuration ports that shall be protected - No Physical Locks provided.

- Network Scanning:

When technically feasible, technology should be deployed to detect unauthorized connections or unauthorized software installed on the system - Fortinet clients are not used in our configurations.

- Penetration testing:

Penetration test shall be performed to assess security of network entry points to the OT network - Not preferred by Yokogawa.

External penetration tests shall simulate the threat of external attackers to identify potential gaps in external connections - Not preferred by Yokogawa.

11. ASSESSMENT FINDINGS

The following are some of the findings during Risk Assessment Process.

a) The design has Remote Access for Operation and Monitoring of the Plant Control System. This connectivity is to be a Secure Connection (Ex: Using a VPN from outside to DMZ.)

b) The Control Room location, usage and connectivity is to yet to be confirmed.

c) To achieve the SL that was obtained from the Detailed Risk Assessment, the compliance with CW Security requirements is to be implemented. The supporting documentation, settings, configuration details to be provided to analyze system security.

d) Post FAT/SAT stage, upon handover to Operations, System Security should be regularly analyzed and as a CSMS Process there should be a 'Tabletop Exercise' yearly on the network and security

solutions and have an assessment of the SL, biannually (Once in Two Years) to strengthen the security further.

Complete Gap Analysis results will be published post FAT. Refer HOLD-2 Hold List.

11.1 CVE

CVE stands for Common Vulnerabilities and Exposures. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.

For details, refer to CVE - CVE (mitre.org).

For the system present in this project, the following are the links can guide on the latest CVV information.

Sr. No	Application	CVE Links
1	Centum VP	Yokogawa: Products and vulnerabilities, CVEs (cvedetails.com)
2	Prosafe-RS	
3	PRM	
4	CI Server	
5	Antivirus/Application Whitelisting	Trellix: Products and vulnerabilities, CVEs (cvedetails.com)
6	WSUS	Microsoft: Products and vulnerabilities, CVEs (cvedetails.com)
7	BRS (Veeam)	Veeam: Products and vulnerabilities, CVEs (cvedetails.com)
8	NMS (Whats Up Gold)	Progress Whatsup Gold versions and number of CVEs, vulnerabilities (cvedetails.com)

Table 20 - CVE Links

12. APPENDIX

Appendix-1: High Level Risk Assessment Sheet

Appendix-2: Detailed Risk Assessment Sheet

Appendix-3: Security Requirements Compliance Sheet