National College of Ireland

An Effective Cybersecurity Risk Assessment Framework for a Public Sector Gas Production/Distribution Company

M.Sc. Industry Internship
M.Sc. Cybersecurity

Meraz Hussain
Student ID: X21138290

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Meraz Hussain
Student ID:	21138290
Programme:	M.Sc. Cybersecurity **Year:** 2022-2023
Module:	Industry Internship
Supervisor:	Prof. Vikas Sahni
Submission Due Date:	06/01/2022
Project Title:	An Effective Cybersecurity Risk Assessment Framework for a Public Sector Gas Production/Distribution Company
Word Count:	…5842…… **Page Count:** …22……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature	Meraz Hussain
Date	05/01/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

An effective Cybersecurity Risk Assessment Framework for a Public Sector Gas Production/Distribution Company

Meraz Hussain
x21138290

ABSTRACT

Computer systems developed specifically for use in critical infrastructure sectors (energy, water, etc. fall under the umbrella term "operational technology" (OT). The field of operational technology that deals with systems for keeping tabs on and regulating factories inner workings is known as "Industrial Control System" (ICS). These systems are the foundation of every nation's critical infrastructure (CNI) such as the gas, water, electricity, transportation. However, in recent years, a significant number of cyberattacks have been directed against Industrial Control Systems (ICS) because Information technology (IT) and operational technology (OT) areas are gradually becoming more intertwined.

This research presents a novel approach to define, implement and test a cyber security risk assessment methodology for a public sector natural gas producer and distributor with complex control system environments by leveraging the international cybersecurity standards and consequently measure as well as recommend remediation for threats and vulnerabilities to its OT infrastructure. The use of multiple cybersecurity frameworks aids to assess the risks, measure the recommendations and efficiently reduce risks. This research developed a realistic Risk Assessment approach to analyze a critical infrastructure energy sector organization's critical assets and cyber maturity. The organization was able to use this methodology to assess its existing cyber controls and plan cybersecurity program improvements. The result of the methodology shows the gap in the maturity of the current organization per NIST CSF Tiers with that of target state organization's stakeholders aim to reach which was level 3 (Repeatable).

Keywords: Industrial control systems (ICS), Operational Technology (OT), Critical Network Infrastructure (CNI), Distributed control systems (DCS), IT-OT Convergence

1. INTRODUCTION

Industrial control system (ICS) is a broad term for industrial automation and control systems. It mostly refers to supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system equipment and components like programmable logic controllers (PLC). Their function is to provide the expected outcomes, which in the case of an industrial result, often requires keeping a certain phase constant or doing some other prescribed action. Sensing devices gather information about the physical environment on their behalf. In order to keep processes in the desired states or finish tasks, PLC compare this information with desired set points, compute and execute command functions, and then use final control components such control valves to make the necessary adjustments.[1]

There was a long period of time when industrial systems were isolated from the rest of the world, ran only on proprietary protocols and software, and required human intervention for management and monitoring. Since of this, cybercriminals did not put much effort into targeting them because there was no networked interface to exploit and hackers stood to gain neither anything nor lose anything by doing so. Obtaining physical access to a terminal was required to infiltrate these

[1] Industrial Control Systems (ICS): System Types & Examples | Study.com

systems, which was a challenging task in. However, as more industrial systems are connected to the internet in the modern day to give big data and smart analytics as well as to embrace new capabilities and efficiency via technological linkages, the landscape has drastically changed.

IT and OT convergence provides businesses with a unified picture of their industrial systems and with process management solutions that guarantee timely, accurate data delivery to all relevant stakeholders in a manner that best suits their needs.(Maleh, 2021) The main components of an ICS design are theoretically divided into six zones, each of which contains both IT and OT systems, according to a model known as the Purdue reference model, as shown below.[2] When properly implemented, it aids in creating an "air gap" between ICS/OT and IT systems, separating them so that a company may implement efficient access restrictions.

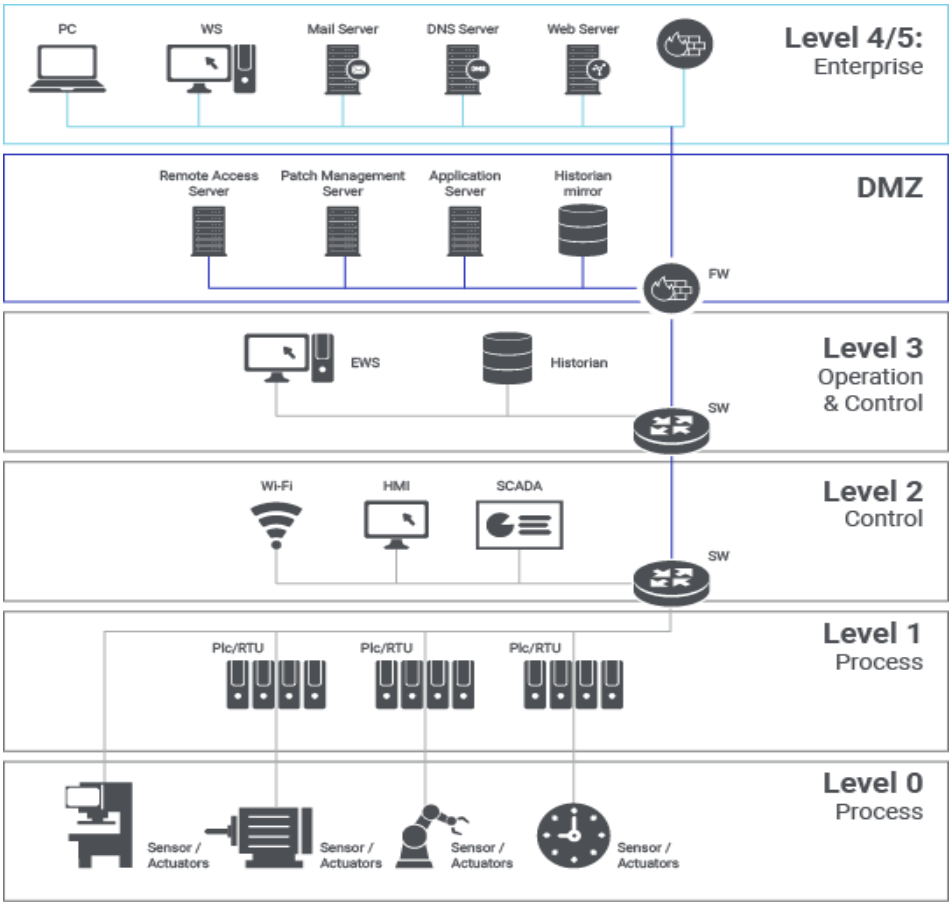

Figure 1: ICS Purdue Reference Model [1]

As seen in Figure 1, Level 0 comprises of the physical components required to build goods and includes field instruments and physical devices such as process equipment such as actuators, pumps, sensors, and valves. Systems at Level 1 monitors and provide instructions to level 0 equipment. Examples include intelligent electronic devices (IEDs), Remote Terminal units (RTUs) and Programable Logic Controllers (PLCs). Industrial automation and control systems are used at Level 2 to monitor and visualize a plant operation using a Human-Machine interface (HMI), operate process equipment, manage people, and analyze data, hence, devices at level 2 govern the overall operations of the system. HMIs and SCADA software, for example, allow plant operators to monitor and control the process. [3]
Production workflow management is supported at Level 3. Customized systems based on various

[2] https://www.researchgate.net/publication/349195440_A_Survey_on_Industrial_Control_System_Testbeds_and_Datasets_for_Security_Research/download

[3] Introduction to ICS Security Part 2 | SANS Institute

operating system like Windows are used to manage batches, gather data on operations and plant performance, and regulate the overall quality of the product. Manufacturing operations management/manufacturing execution systems (MOMS/MES), batch management, and data historians are some examples. The DMZ, which is Level 3.5, separates the OT networks from the IT networks. Jump boxes and similar devices may restrict access to ICS systems from IT environments, but this segmentation can also stop cyber-attacks in the IT environment from propagating to OT systems, and vice versa. Level 4 of the ICS segmentation architecture is made up of enterprise business systems, such as enterprise resource planning (ERP) systems, which are located on the corporate IT network and supervise management of all operational of the company's processes. Even though it's not an ICS setting, this aids in collecting data from ICS systems for use in making business decisions.

It is important to note that as a result of making the shift from closed to open systems, a whole new set of security concerns has arisen. Industrial control systems are increasingly susceptible to vulnerabilities because of their increased connectivity. The enormous cost of industrial equipment and the destruction that a cyber-attack may do to communities and economies are important considerations for businesses wanting to safeguard their industrial networks and avoid legal, financial and reputational implications.[4]

Attacks on major utilities can have a devastating effect on large populations, as demonstrated by a cyberattack in 2015 that targeted three energy distribution companies in Ukraine. As a result of this attack, the electricity supply was temporarily disrupted for more than three hours for over 200,000 customers during the winter.[5] Similarly, the biggest U.S. gasoline pipeline, the Colonial Pipeline, was shut down in May 2021 after a ransomware attack. About 45 percent of the United States' East Coast's demand for gasoline and jet fuel is met by this pipeline at a rate of 2.5 million barrels per day. This resulted in a shortage of gasoline and other refined goods throughout the East Coast since the colonial pipeline business had to suspend operations to stop the spread of ransomware.[6]

Research Question: How can a natural gas producer and distributor company with complex control system environments leverage the international cybersecurity standards to measure and remediate threats and vulnerabilities to its OT infrastructure that is mandated by law? Moreover, how can a Gas operator be proactively prepared to control and recover from the harm caused by any incident(s) causing interruption to the plant's operation, while also ensuring that it is prepared for high service availability?

2. Related Work

Not only in the business of information technology, but also in the field of academic study, the idea of Industrial Control System (ICS) Security has been a critical topic for a very long time. Because of this, a few publications on the body of knowledge about security of operators of essential and critical services have been published. Despite this, the number of papers focused specifically on ICS and OT security is limited.

(Jazri & Jat, 2016) presented a cybersecurity framework that utilizes ISO/IEC 27001:2013 and the NIST Cybersecurity Framework was proposed, to improve the cybersecurity of critical infrastructure. Researchers formulated an indication of the integrity of a cybersecurity system, based on the cybersecurity framework that has been presented. Researchers identified nine

[4] https://www.fortinet.com/blog/industry-trends/as-ot-systems-become-more-connected-ot-security-becomes-more-challenging
[5] https://www.cbsnews.com/news/colonial-pipeline-cyberattack-shut-down/
[6] 2015 Ukraine power grid hack - Wikipedia

critical organizations in Windhoek, Namibia, and approached them via nine unique facilitator groups to enable flexibility and ease of implementation. The facilitator's ensured that the proposed simplified framework and template for implementing it was followed by the participating organizations. The whole exercise was completed in less than a day, when all the necessary artefacts were made available. The dependability of the outcome is contingent upon the precision of the control's implementation status supplied by each critical organization. Researchers did not establish validation criteria for each of the controls, making it difficult to assess the correctness of the results as the validation process becomes more detailed.

Another study (Oliveira and Santos, 2022) proposed a strategy for improving ICS security and maturity by establishing a framework for real-time analysis and monitoring that periodically assesses ICS systems. This framework, developed on the basis of ISA 62443, served as a model for assessing and certifying the cybersecurity of real-time ICS operations. Following the Plan-Do-Check-Act methodology, researchers developed a cycle that begins with a description of the appropriate scopes of analysis, such as the establishment of systems, security zones, and conduits. After determining what security controls and requirements were needed to effectively lessen the risks and vulnerabilities of the systems under review, a multistage risk assessment was carried out using IEC 62443-2-1. Following this, researchers selected the assessment criteria using the 62443-3-3 framework based on the amount of security required for each Zone and conduit.

(Malatji, 2022) conducted research where the aim was to define the fundamental cyber hygiene measures required to prevent cyber-attacks against connected IT- OT environment. This paper reviews the history of research on industrial control system (ICS) security over the last decade (2012 – 2022). Eight "Basic ICS Cyber Hygiene Practices" were found to be common among all of the papers: frequent password reviews and changes, careful handling of storage and media devices like USBs, active management of user Identity, authentication and authorization of users, and physical separation of the ICS network and devices. Researchers also identified that those 8 fundamental cyber hygiene techniques necessary to prevent unauthorized cyber activity in interconnected ICS environments were not in place.

Additionally, it was also discovered that the rising convergence of the IT and OT domains multiplies and complicates the risks of connected ICS infrastructures. According to the study's key findings, many critical infrastructure operators fail to properly enforce password and access control policies for local and remote network access, fail to update and patch their systems when necessary, fail to effectively restrict, segregate, and/or separate access to ICS networks and systems, and fail to conduct cybersecurity awareness training as frequently as they should. The researchers did not conduct an exhaustive, systematic review of the literature (SLR). To incorporate more literature, other combinations of additional relevant keywords and search terms might have been utilized, and an SLR technique could have improved the results.

(Curtis and Mehravari, 2015) assessed and built a Cyber Security Capability Maturity Model (C2M2) and a modified version of the model called Cybersecurity Capability Maturity Model for the Oil & Natural Gas industry. The C2M2 model was developed by researchers to be used as a tool for self-evaluation. The purpose of the study was to assist natural gas critical infrastructures in effectively and consistently evaluating and benchmarking their cybersecurity capabilities, to enable organizations to prioritize actions and investments to improve their cybersecurity posture and to share knowledge, methodologies, and relevant references amongst one another in an effort to improve cybersecurity. The model was built using 10 distinct domains. Each domain represented a separate logical classification of various cybersecurity strategies. The activities that comprise a domain are classified into categories based on the domain's aims and objectives. The practices within each purpose are structured in a hierarchy established by the Maturity Indicator

Levels. The model's 10 domains each included a set of organized cybersecurity procedures. The actions an organization may take to create and develop capacity in the domain were represented by each set of practices. This model developed four maturity indicator levels, MILO to MIL3, which apply to each domain in the model individually. The MILs defined two stages of maturity: the approach stage and the institutionalization stage. Approach was a way to talk about how complete, thorough, or far along an activity in a domain was. As an organization moves from one MIL to the next, its core activities are required to be implemented in a more complete or advanced way. The degree to which a control activity was integrated into the day-to-day workings of an organization is referred to as its "institutionalization. Following 2 diagram represents the structure of Model and Maturity Level definition and specifications summary:

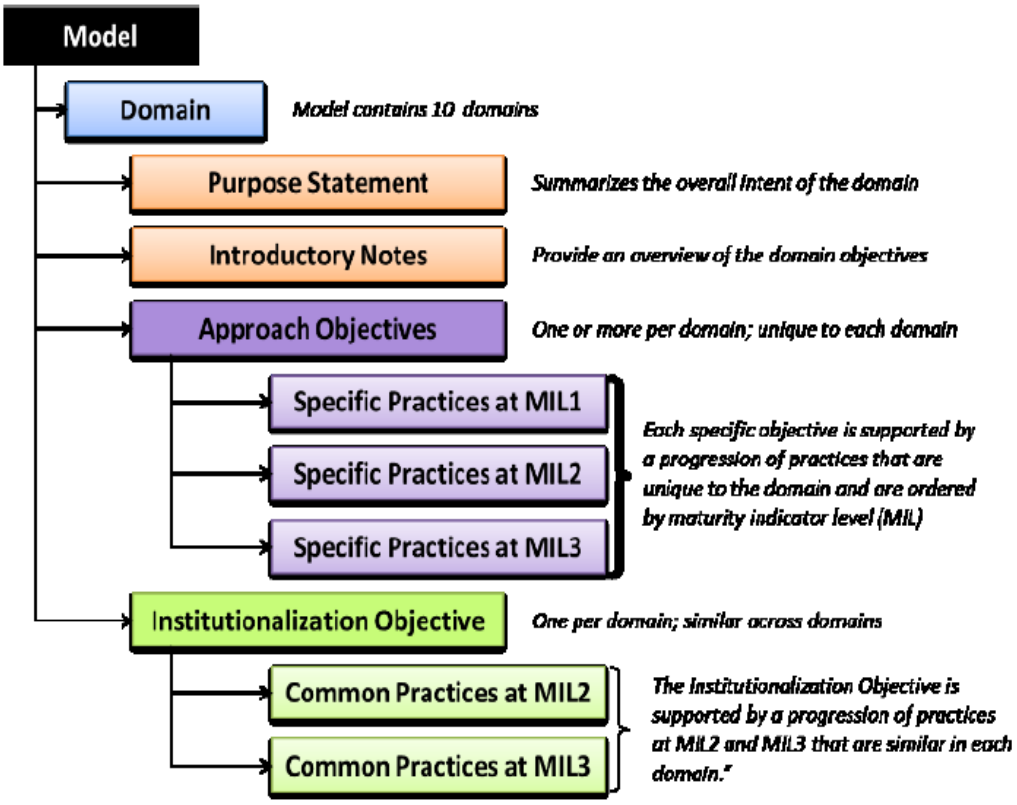

Figure 2 - Structure of Model (Curtis and Mehravari, 2015)

Level	Name	Description
MIL0	Not Performed	MIL1 has not been achieved in the domain
MIL1	Initiated	Initial practices are performed, but may be ad hoc
MIL2	Performed	**Institutionalization characteristics:** • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation **Approach characteristic:** • Practices are more complete or advanced than at MIL1

MIL3	Managed	**Institutionalization characteristics:** • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge **Approach characteristic:** • Practices are more complete or advanced than at MIL2

Figure 3 - Maturity Level Indicator specification (Curtis and Mehravari, 2015)

(Kanamaru, 2021) proposed a security risk assessment for the purpose of studying, devising countermeasures, and assessing security risks pertaining to Industrial Automation and Control Systems (IACS) from the viewpoint of IT/OT convergence. To conduct a security risk assessment that included IT and OT, safety and security, cyber and physical, as a series of sequences, researcher had presented an extended risk assessment form to encompass all of these aspects. Cyber and physical security were found to be intertwined in the analysis of safety and security. The table below illustrates the conceptual links between safety and security, as well as between cyber and physical security. Researchers said that separate risk assessments were conducted on each of them since attributes were analyzed using differing methods.

	Safety	**Security**
Cyber	Functional safety (IEC 61508 etc.) - safety instrument system - safety control system	Cyber security (IEC 62443) - access control - authentication - firewall, IDS
Physical	Physical protection (IEC 12100 etc.) - guard, fence	Physical security (ISO 27001 Annex A) - security gate, CCTV

Figure 4 - Cyber-physical security and safety relationship (Kanamaru, 2021)

The approach for the extended risk assessment was developed by including different risk mitigation methods, such as engineering, safety, and security, as well as risk re-evaluating for the measures that were established.

3. RESEARCH METHODOLOGY

This section provides a description of the approach taken in the proposed model, which explains the step-by-step procedure for building a Risk Assessment Framework methodology. The main idea was to comprehensively define, implement, and test a proposed cyber security risk assessment for a facility of a public sector natural gas producer and distributor firm called Gas Networks Ireland in Lougshinny, Ireland. This was accomplished by combining the NIST Cybersecurity Framework and the IEC 62443 standards developed by the International Electrotechnical Commission (IEC). By combining the NIST Cybersecurity Framework with the IEC 62443 framework, organizations can evaluate risks, quantify suggestions, and effectively mitigate threats posed to OT/ICS network. By applying the NIST Cybersecurity Framework Methodology and offering suggestions for discovered gaps with the aid of the IEC 62443 standards ensure measurable improvements in cyber security and compliance.

The research method for the project is broken up into many stages or steps. The first step is to identify the assets and systems that are consideration, and then to conduct an impact assessment on the identified assets by following the instructions in the IEC 62443-2-1 standard. The assets are identified by site/facility level for purposes of this research. The ISA/IEC 62443-2-1 standard outlines the procedure for performing a cybersecurity risk assessment as a first step in risk assessment and understanding the existing degree of risk within Industrial Automation and Control Systems (IACS).[7] The second step is to perform a comprehensive risk assessment based on the results of step 1 and evaluate the current maturity state of the company in terms of how mature its cyber practices and controls are. This is done by identifying and evaluating risks in the IT/OT/Operations controls for each of the subcategories in the five NIST functions. The next step is to compare the present maturity ratings of five NIST functions to the target cyber maturity level. The last stage is to build a Remediation/Action plan to bridge the gap between the present maturity state and the target maturity level. This involves leveraging the guidance from the security requirements established by the IEC 62443-3-3 and some security requirement from 62443-2-1 standards, to mitigate the risks that have been determined. Therefore, the workflow below summarizes the stages for achieving the planned approach for the proposed method:

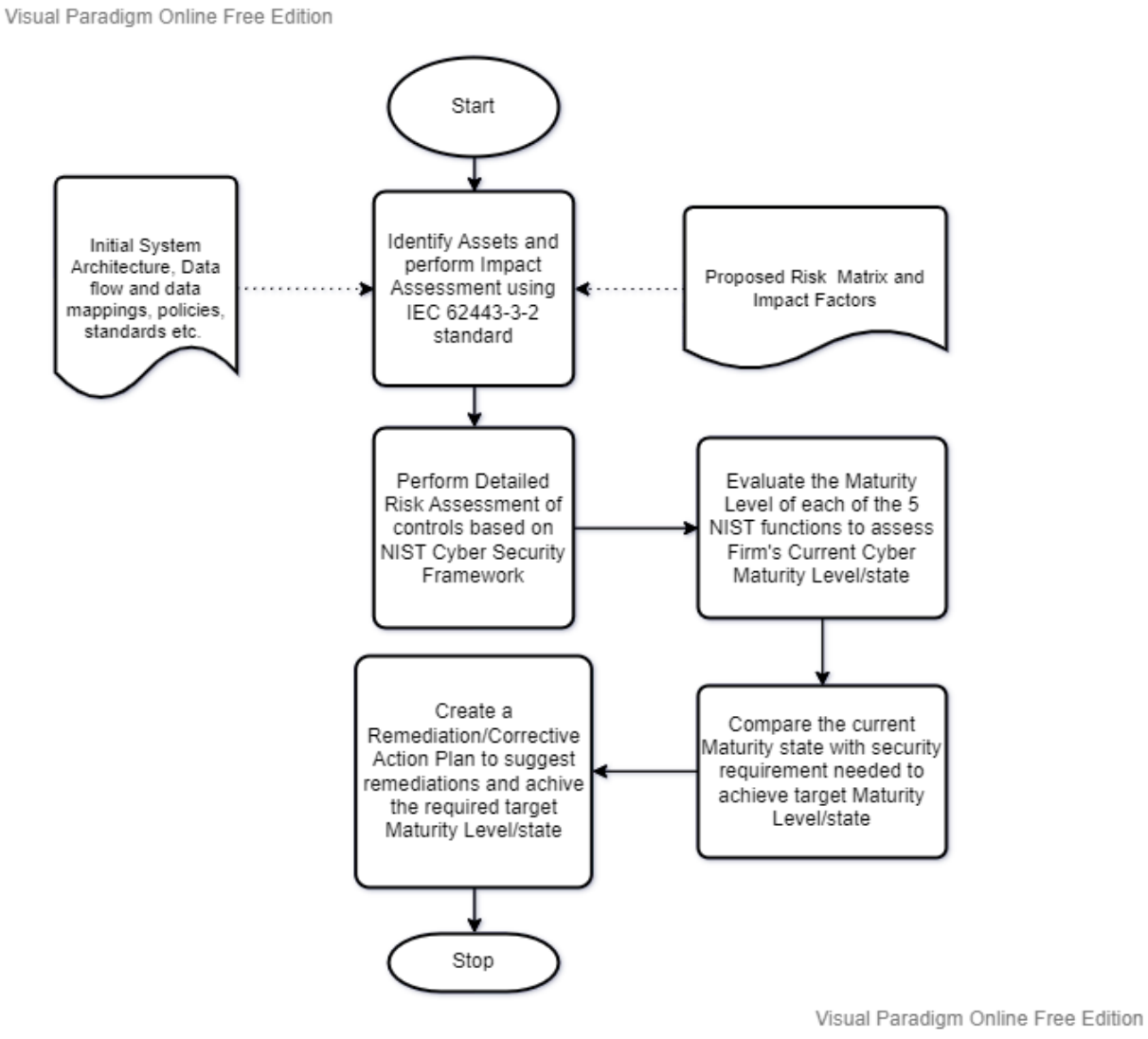

Figure 5 - Proposed Risk Assessment Methodology

[7] https://www.exida.com/Blog/iec-62443-levels-levels-and-more-levels

4. DESIGN SPECIFICATION

4.1Identify Assets and perform Impact Assessment on identified Assets

To begin the process, it is essential to identify and compile an inventory of all physical and logical assets within the risk assessment's scope. An information asset is any relevant information or asset that contributes to a company's ability to operate and serve the business. It might be a physical or electronic file, tape backup, SCADA devices, an external hard drive, Active Directory server etc. The first stage is to identify who inside the company oversees those assets, hence the steps involve reaching out to the asset owner(s)/individual(s)/team(s) in the facility under scope and then requesting to fill the details about the assets that are functioning and are available to support the IT, OT and operational functions. The next step is to use the asset inventory list as the basis for drawing a network architecture diagram, which shows the connections and data flow between assets, processes, and entry points in the network. Once the Asset register is populated with asset's details, a risk analysis is performed that involves assessing the probability or likelihood of an attack on each asset and assess the potential impact on that asset if the risk were to be exploited. The Risk is measured by calculating the impact of threats on six different impact factors: Safety, Environment, Financial, Quality, Business Continuity and Reputation & License. Moreover, a 5 x 5 risk matrix is also used to assign a numerical value from 1-5, to each of the above six impact factors if threat were to occur. The risk measurement criteria for each of the six impact factors and their description are shown in the Figure below:

	Impact Factors						
	Safety	**Environment**	**Financial**	**Quality**	**Business Continuity**	**Reputation & License**	**Impact**
I M P A C T	Minor Injury Loss if Visibility/Control to an Individual Site	Small Release of Gas	Equivalent to an annual economic profit impact up to Euro 100,000	Will not affect end of product/service or assurance of quality	Loss of service capacity between 1-4 working hours for one essential business process or Loss of service capacity for less than 1/2 hour for one critical business process	No Regulator Involvement	1 Trivial
	Minor Injury Requiring Outpatient treatment	Medium Release of Gas	Equivalent to an annual economic profit impact up to Euro 100,000 to Euro 500,000	Has potential to impact quality of product/service	Loss of service capacity between 1/2 to 2 days for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Customer Complaint	2 Minor
	Loss Time Incident	Medium to Large Release of gas	Equivalent to an annual economic profit impact up to Euro 0.5 million to Euro 3.5 million	Direclty affects quality of product/service	Loss of service capacity between 2 to 7 days for one essential business process or Loss of service capacity for more than 1 hour for one critical business process	Informal Regulator Involvement	3 Moderate
	Single Fatality orf Serious Injury	Lasting but localised damage	Equivalent to an annual economic profit impact up to Euro 3.5 million to Euro 7.5 million	Seriously affects quality of product	Loss of service capacity between 1 to 4 weeks for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Investigation from Regulators & Possible Sanctions	4 Major
	Multiple Facilities Loss of visibility and control to all Sites	Lasting but Widespread damage	Equivalent to an annual economic profit impact above Euro 7.5 million	Failure to meet even basic intended standards for product/service	Loss of service capacity more than 4 weeks for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Possible loss of license	5 Critical

Likelihood →				
Inconceivable.May never Happen. Only in exceptional Circumstances	Possible but conisdered unlikey	Possible- Circumstances be envisaged for it to occur	Likely to happen	Will happen or highely likely to happen
1 Improbable	2 Rare	3 Unlikely	4 Possible	5 Likely
1	2	3	4	5
2	4	6	8	10
3	6	9	12	15
4	8	12	16	20
5	10	15	20	25

Figure 7 – Description of 6 Impact factors and corresponding Risk Matrix

Next step is creation Impact assessment template which was created using the above designed risk matrix. The template included assessing and documenting the Threat action(s) of malicious threat actor(s)/source(s), vulnerability/vulnerabilities and the consequence or impact on the asset if threat agent exploited the vulnerability. This is followed by assigning impact values (from 1-5) for six different impact factors: Safety (S), Environment (E), Financial (F), Quality (Q), Business Continuity (BC) and Reputation & License (RL).

Inherent likelihood value, which depicts probability of the threat actor acting on the vulnerability without considering any existing countermeasure(s), is then assigned for each threat sources. This is followed by calculating Inherent Risk which is measured as:

Inherent Risk = Impact x Inherent Likelihood

Last step in the impact assessment process involves identifying and documenting existing technical/operation controls to produce Residual Likelihood and from there on measuring Residual Risk, which is calculated as:

Residual Risk = Impact x Residual Likelihood

Following Figure shows proposed Impact Assessment template:

					Impact											
Asset Name and Type	Threat Action	Vulnerabilities	Impact Description	Threat Source	S	E	F	Q	BC	R & L	Max	Inherent Likelihood	Inherent Risk	Exisiting Countermeasure(s)	Residual Likelihood	Residual Risk

Figure 8 - Proposed Impact Assessment Sample Template

After completing the impact assessment, a Network Diagram is created for the site showing critical assets with same residual risk scores are placed into same area called Zones. The diagram

also shows data flow, internal and external connections and various interfaces for the in-scope site.

4.2Detailed Risk Assessment by assessing the NIST CSF controls, identify gaps in controls and evaluate organization's current Cyber Maturity state

The National Institute of Standards and Technology (NIST) created a Framework for Improving Critical Infrastructure Cybersecurity which is called Cybers Security Framework (CSF). There are three parts to the NIST CSF: the framework core components, the implementation tiers, and the profiles. The CSF framework core relates to the activities and results of adopting cyber security best practices which can be broken down into five functions: Identify, Protect, Detect, Respond, and Recover. An organization's framework Profile consists of the outcomes it has selected from the various categories and subcategories considering its business requirements and risk tolerance. The level to which an organization has implemented the CSF controls is indicated by its placement in one of four implementation tiers.[8]

In this model, each of the 108 CSF controls/subcategories are evaluated for a Natural Gas production site based on the Assessment of below 4 proposed Objectives:

a) Operational objective of the controls and cybersecurity processes
b) Design objective of the controls and cybersecurity processes
c) Implementation objective of controls and cybersecurity processes
d) Review frequency of the controls

Each of the four objectives are assessed based on following requirements and metrics:

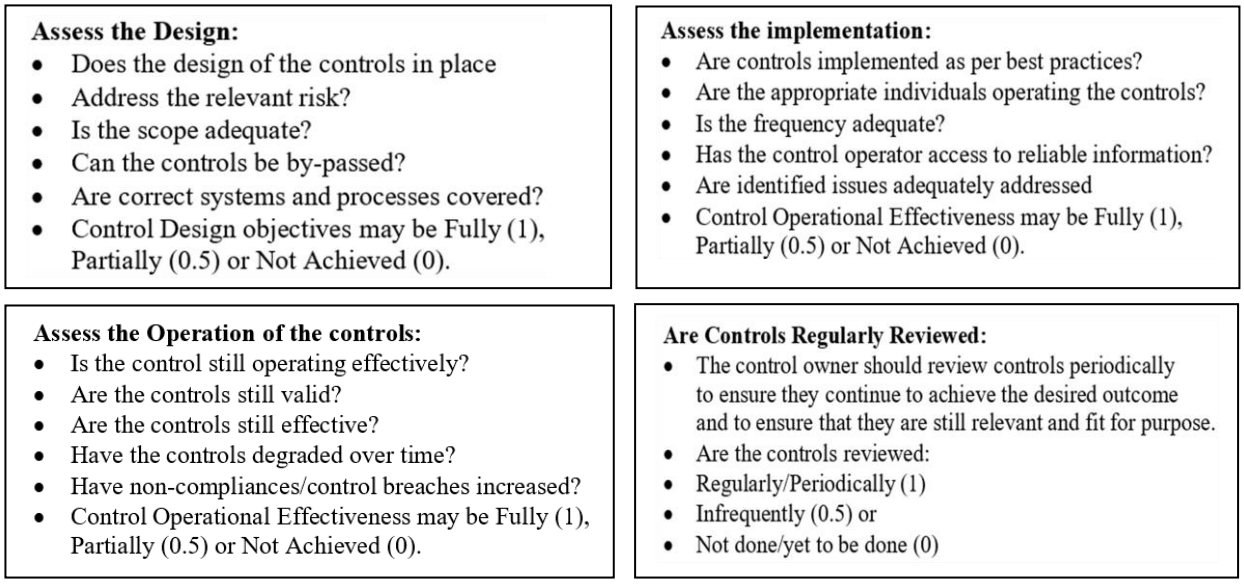

Figure 9 - NIST CSF Proposed Objectives

Once the organization's controls pertaining to Information security and related practices are assessed against NIST CSF controls, next phase is to determine the maturity score of each of the five CSF functions. This is calculated in two additional steps, as described below:

a) To start, all the CSF categories/controls are assigned a score of 0, 0.5 or 1 based on their

[8] https://www.nist.gov/cyberframework/online-learning/components-framework

alignment with the proposed objectives described in Figure 9.

- 1 signifies control objective is Fully Achieved
- 0.5 signifies control objective is Partially Achieved
- 0 signifies control objective is Not Achieved/ /Yet to be done

Identify (29 Subcategories/Controls) Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities								
Category	**Subcategory**	**Controls in place**	**Control Owner**	**Design Assessment**	**Operational Assessment**	**Operational Assessment**	**Control Review**	**Gaps in the controls**

Figure 10 - Proposed Detailed Risk Assessment Proposed Sample Template

b) Next step is to measure the overall score of individual subcategories and then, calculate their average to create individual category's score i.e.

Individual Subcategory Score = (Design Assessment + Implementation Assessment + Operation Assessment + Control Review)
Operation and Control Review)

Individual Category Score = $\frac{\text{Individual Subcategory Score}}{\text{Count of Subcategories}}$

To support the understanding of above calculations, a use case from the Risk assessment template is shown below:

Category	**Subcategory**	**Design Assessment**	**Implementation Assessment**	**Operational Assessment**	**Control Review**	**Score**	**Average**
Identify							
Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	0.5	0.5	0.5	0	1.5	1.67
	ID.AM-2: Software platforms and applications within the organization are inventoried	0.5	0.5	0.5	0	1.5	
	ID.AM-3: Organizational communication and data flows are mapped	0.5	0.5	0.5	0	1.5	
	ID.AM-4: External information systems are catalogued	0.5	0.5	0.5	0	1.5	

Figure 11 – Cyber Maturity Assessment Sample Template

4.3Compare against Target Cyber Maturity state

An average score for each Function is determined by performing the methods outlined in the section above and applying them across all the subcategories and categories. The scores of each function are then compared to the Target Cyber Maturity score specified by the company for each function in the "To Be" stage. Organizations are asked to select in advance what degree of Cyber-Security Framework (CSF) compliance maturity they prefer, with 1 being the lowest level of maturity and 4 representing the greatest level of maturity. By comparing the current cybersecurity practices, processes and controls with the intended target level, gaps in controls and/or processes are identified and documented for each subcategory. There are 4 levels/tiers

defined by NIST CSF as show in the below Figure:

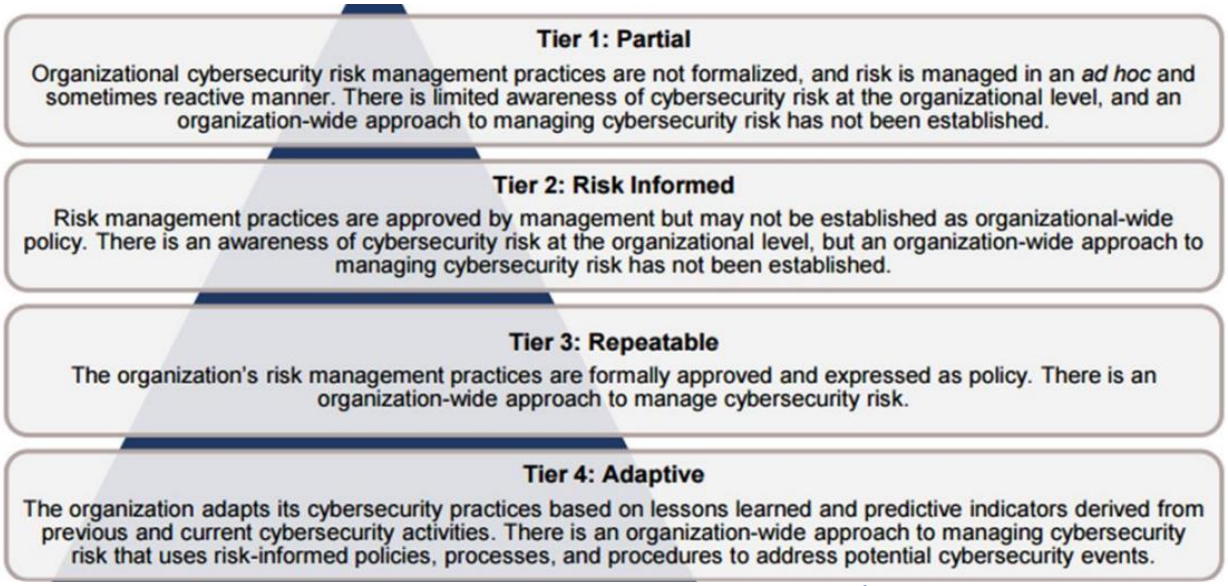

Figure 12 - NIST CSF Implementation Levels/Tiers[9]

4.4 Create Remediation/ Corrective Action Plan and assign risks to Risk/Control Owners

The final step is to assign control owner for each of the gaps identified in previous step. Once the control owners are identified, a Remediation or Corrective Action plan is created to bridge the gap between organizations current cyber maturity state to target state. For an IACS facility, there could be multiple controls owners from company or vendor's side as well. Moreover, the remediation plan takes guidance from IEC 62443-2-1 standard for suggestion of secure design of controls and security requirement of an IACS infrastructure.

5. IMPLEMENTATION

This section of the report describes the implementation of the Risk assessment approach outlined in the Methodology and Design Specification sections for a Landfall gas pipeline site located in Lougshinny, Ireland. The Lougshinny Landfall facility serves as a logistical connection between the Northern Ireland Unified Gas Transport System and the Gas Network Ireland (GNI) Pipelines. Natural gas gets here by pipeline from Northern Ireland and is prepared at a compressor plant at the site before entering the Gas Network Ireland Pipeline system.

5.1 Asset Identification and Impact Assessment

As described in design section, all the assets are identified as first step which is then followed by determining various threat scenarios that can disrupt daily function of the gas pipeline operation. The impact is calculated on six factors by assigning an impact value to each asset. The likelihood of the threat actor exploiting the vulnerability is assigned based on discussion with internal and external stakeholders, guidance given by various internal standards and industry best practices. By factoring the impact and likelihood, Inherent risk is calculated. In the end, GNI's current countermeasures are considered and evaluated for each scenario and risk is re-evaluated to

9 https://www.npstc.org/download.jsp?tableId=37&column=217&id=3806&file=DHS_OEC_SAFECOM_NIST_Cybersecurity_Framework_Presentation_v2.pdf

produce Residual risk for each scenario.
Below Figure depicts the screenshots of Impact Assessment conducted on some of the Assets (grouped in zones):

					Impact										
Asset Name/ Group/ Zone	Threat Action	Vulnerabilities	Impact Description	Threat Source	S	E	F	Q	BC	R & L	Max Impact	Inherent Likelihood	Inherent Risk	Exisiting Countermeasure(s)	Residual Likelihood	Residual Risk
SCADA Comms. Zone	User accesses the configuration interface of the wired (MPLS) SCADA router and applies an incorrect configuration.	•Routers physically accessible to all on site. •Web configuration interface not restricted to OoB management port. •Default credentials in use. •Admin passwords widely-known. •DHCP enabled on network.	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C&I technicians to site. •Recovery of configuration from backups. •Possible to run these sites "on paper"	Authorized Personnel					3		3	2	6	• Redundant SCADA routers (1 Wired, 1 GPRS/3G/4G installed on site. • TACAS used for authentication on configuration interfaces	2	6
				Authorized Personnel					3		3	3	9		2	6
				Authorized 3rd Party					3		3	2	6		2	6
				Unauthorized 3rd Party					3		3	3	9		2	6
	Malicious actor carries out DDOS attack on the WAN side of the SCADA routers.	No Denial of Service Attack protection mechanism used on routers	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C & I technicians to site.	Authorized Personnel					3		3	2	6	• Physical security on site, such as the external gate mitigates this somewhat • Local SCADA on site can be used for comparison • Private connection supplied by the ISP	2	6
				Authorized Personnel					3		3	2	6		2	6
				Authorized 3rd Party					3		3	2	6		2	6
				Unauthorized 3rd Party					3		3	4	12		3	9
DMZ	Malware Infection (e.g. ransomware) becomes active on the network	•Device patching is unmaintained, resulting in systems with known vulnerabilities. •Lack of network segmentation.	•Downtime due to restoring from known good, offsite backups. •Loss of confidentiality on documentation, data, network layouts	Malware	5	5	5		5	4	5	4	20	Antivirus installed on networked Windows devices	3	15
	User disrupts power to DMZ PCs	•PCs easily accessible by all on site. •No UPS Installed.	•Remote access to EWS via Jump-Box disrupted. •Loss of emissions monitoring. •IACS nodes got receiving WSUS/AV signature updates meaning they are more exposed in the event of further attack on the network.	Authorized Personnel					3		3	3	9	•UPS on sites powering these machines •Backup generator onsite for automatic failover	1	3
				Unauthorized Personnel					3		3	2	6		1	3
				Authorized 3rd Party					3		3	3	9		1	3
				Unauthorized 3rd Party					3		3	3	9		1	3

Figure 13 - Impact Assessment on Few Grouped Assets

5.2Evaluation of NIST CSF controls for the in-scope facility, identifying gaps in controls and measurement of current Cyber Maturity

After the assets are identified and the impact assessment is performed, next step involves assessing GNI's technical, non-technical and operational controls at the site as well as organization wide policies and procedures in respect with the 108 NIST CSF controls. The controls are evaluated based on 4 objectives as described comprehensively in Design specification section above. For illustration purposes, below Figure showcases control testing performed on some of the controls in the Identify function:

Identify (29 Subcategories/Controls) Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities								
Category	**Subcategory**	**Controls in place**	**Control Owner**	**Design Assessment**	**Implementation Assessment**	**Operational Assessment**	**Control Review**	**Gaps in the controls**
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed	**ID.AM-1:** Physical devices and systems within the organization are inventoried	BCP Framework Refresh -Consolidation of Group, EBS and GNI materials. Review of scenarios, to be prioritised in order of business impact/criticality, development plans to be put in place for high priority response plans (Cyber, Security of Supply, Single Source Supplier etc.) 2022 Business Continuity Exercise Programme - Co-ordination of our annual business continuity exercise plan in line with our business continuity framework guidelines. (2022 exercise plan available upon request).	Security & Operations Technology Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	An informal check of the Core Asset register is performed quarterly but this is not under any governed control. Also, no formal Control Monitoring policy in place.

Figure 14 - Risk Assessment for few Identify subcategories

Below is the Network diagram created based on the impact assessment conducted in section 5.1:

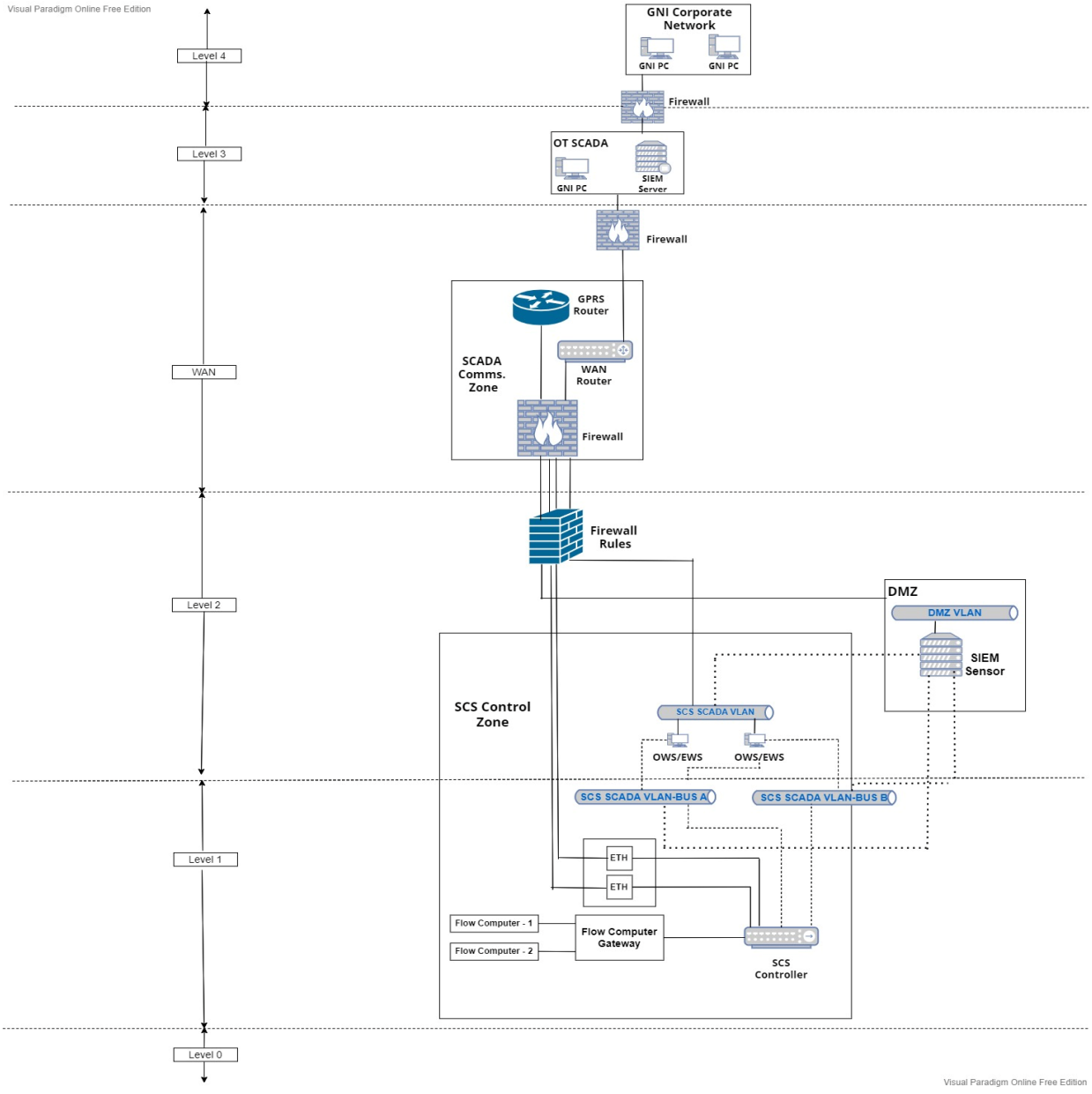

Figure 15 - Lougshinny Site High Level Network Diagram based on Impact Assessment

5.3Evaluation of Company's Current vs Target Cyber Maturity Level/Tier

The preceding step evaluated GNI's risk management capability across the five NIST functions. Next phase involves first determining company's current Target maturity score agreed by the management and relevant stakeholders and then comparing the results of NIST CSF controls scores with the target score. GNI's Information Security Team chose the third (i.e. Repeatable) NIST maturity level for the last quarter of 2022, to serve as the baseline for each function's results. As show in the Figure below, scores for each subcategory are listed against the target score set by the management:

Category	Subcategory	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Score	Average
Identify							
Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	0.5	0.5	0.5	0	1.5	1.67
	ID.AM-2: Software platforms and applications within the organization are inventoried	0.5	0.5	0.5	0	1.5	
	ID.AM-3: Organizational communication and data flows are mapped	0.5	0.5	0.5	0	1.5	
	ID.AM-4: External information systems are catalogued	0.5	0.5	0.5	0	1.5	
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	0.5	0.5	0.5	0	1.5	
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	0.5	0.5	0.5	1	2.5	
Business Environment (ID.BE)	ID.BE-1: The organization's role in the supply chain is identified and comamunicated	0.5	0.5	0.5	1	2.5	
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	0.5	0.5	0.5	0	1.5	

Figure 16 – Calculation of NIST CSF's Categories individual and average scores

Above Figure shows calculation of 3 categories from Identify function. Similarly, all the Categories are assigned assessment scores and average is calculated discussed in "Evaluation" section.

		Target Score (Q4-2022)	GNI Current Score (Q4-2022)
	Overall	**3.00**	**2.33**
Identify	Asset Management (ID.AM)	3.00	1.67
	Business Environment (ID.BE)	3.00	2.50
	Governance (ID.GV)	3.00	4.00
	Risk Assessment (ID.RA)	3.00	2.00
	Risk Management Strategy (ID.RM)	3.00	4.00
	Supply Chain Risk Management (ID.SC)	3.00	2.50
Protect	Identity Management and Access Control (PR.AC)	3.00	2.29
	Awareness and Training (PR.AT)	3.00	3.20
	Data Security (PR.DS)	3.00	1.50
	Information Protection Processes and Procedures (PR.IP)	3.00	2.63
	Maintenance (PR.MA)	3.00	2.25
	Protective Technology (PR.PT)	3.00	2.20
Detect	Anomalies and Events (DE.AE)	3.00	1.90
	Security Continuous Monitoring (DE.CM)	3.00	2.63
	Detection Processes (DE.DP)	3.00	2.80
Respond	Response Planning (RS.RP)	3.00	1.50
	Communications (RS.CO)	3.00	2.60
	Analysis (RS.AN)	3.00	2.30
	Mitigation (RS.MI)	3.00	2.17
	Improvements (RS.IM)	3.00	1.50
Recover	Recovery Planning (RC.RP)	3.00	1.50
	Improvements (RC.IM)	3.00	1.50
	Communications (RC.CO)	3.00	2.50

Figure 17 – GNI's Current vs Target NIST CSF Function's scores

5.4 Preparing Corrective Action Plans to meet Target Cyber Maturity level/Tier

In this step, remediation or corrective action plan is created for the gaps identified during the control testing of NIST controls. The IEC 62443-3-3 and some security requirement stated by 62443-2-1 standards are used in the remediation plan as recommendations for secure control design and security requirements for each of the identified gaps. It is to be noted that even though the assessment conducted was for a single facility/site of GNI, some of the controls are applied company wide and hence, it is up to GNI's management to allocate Risk Owner(s) for the risks/gaps. Moreover, from discussion with GNI management, it was also established control owners may or may not be risk owners. Following figure shows the screenshot of the template used for document Corrective Action plan with two Identity use cases/examples:

Corrective Action Plan					
Identify					
Category	Controls in Place/Current Profile	Gaps/ Residual Risk Identified	Risk Rating (H/M/L)	Risk Owner Assigned	Remediation Activity/ Project/Timeline
Asset Management (ID.AM)					
ID.AM-1: Physical devices and systems within the organization are inventoried	BCP Framework Refresh -Consolidation of Group, EBS and GNI materials. Review of scenarios, to be prioritised in order of business impact/criticality, development plans to be put in place for high priority response plans (Cyber, Security of Supply, Single Source Supplier etc.) 2022 Business Continuity Exercise Programme - Co-ordination of our annual business continuity exercise plan in line with our business continuity framework guidelines. (2022 exercise plan available upon request).	An informal check of the Core Asset register is performed quarterly but this is not under any governed control No formal Control Monitoring - Policies and Procedures to be developed to formally govern the management, maintenance and monitoring of controls — to ensure inventory controls operate as intended. GNI must install an appliance in the Enterprise and O.T. Core to discover/report on equipment installed on the site network The Operational impact of loss of availability of systems should be categorised. Details of all high impact systems are captured Automated discovery/detection tools should be used to collect inventory data.	Medium		
ID.AM-2: Software platforms and applications within the organization are inventoried	For Core Assets there is an up to date software inventory in place through the application landsweeper. A copy of the latest software inventory can be provided upon request. It lists the following : Asset Name, Software, Version, Publisher, OS, Domain, Install Date OT Core utilize WSUS (Windows Update Pogram), Ansible (Red Hat), Oracle Enterprise Manager and VMware vCentre discovery components for managing hardware and software implementations. Cyber security site surveys have been completed and assesment on three sites have taken place. The detailed design is ongoing with the plan to implement IEC 62443. The recommendation to install an appliance in the O.T. Core to discover/report on equipment installed on the site network e.g. Claroty, or similar will be addressed through the GNI OT Security program.	An up to date record of Software inventory which underpins each Critical Activity should be maintained The inventory should capture details such as: Business Owner, L'CenCes, Warranty, EoL For OT/ICS assets the inventory captures information such as: Model, Type, Firmware revision The inventory captures details of software maintained by a 3rd party Software licences are managed. Hardware and Software inventories are integrated.	High		

Figure 18 – Corrective Action Plan Screenshot

6. EVALUATION

This section of the study report describes the evaluation carried out and the outcomes attained after the use of the suggested approach. Controls for each function are assessed and maturity scores are measured. The maturity scores are represented first for each function and then for overall company.

6.1Company's individual Function NIST Maturity Level/Tier

Following Radar/Spider charts are leveraged to visualize the maturity scores measured for each function:

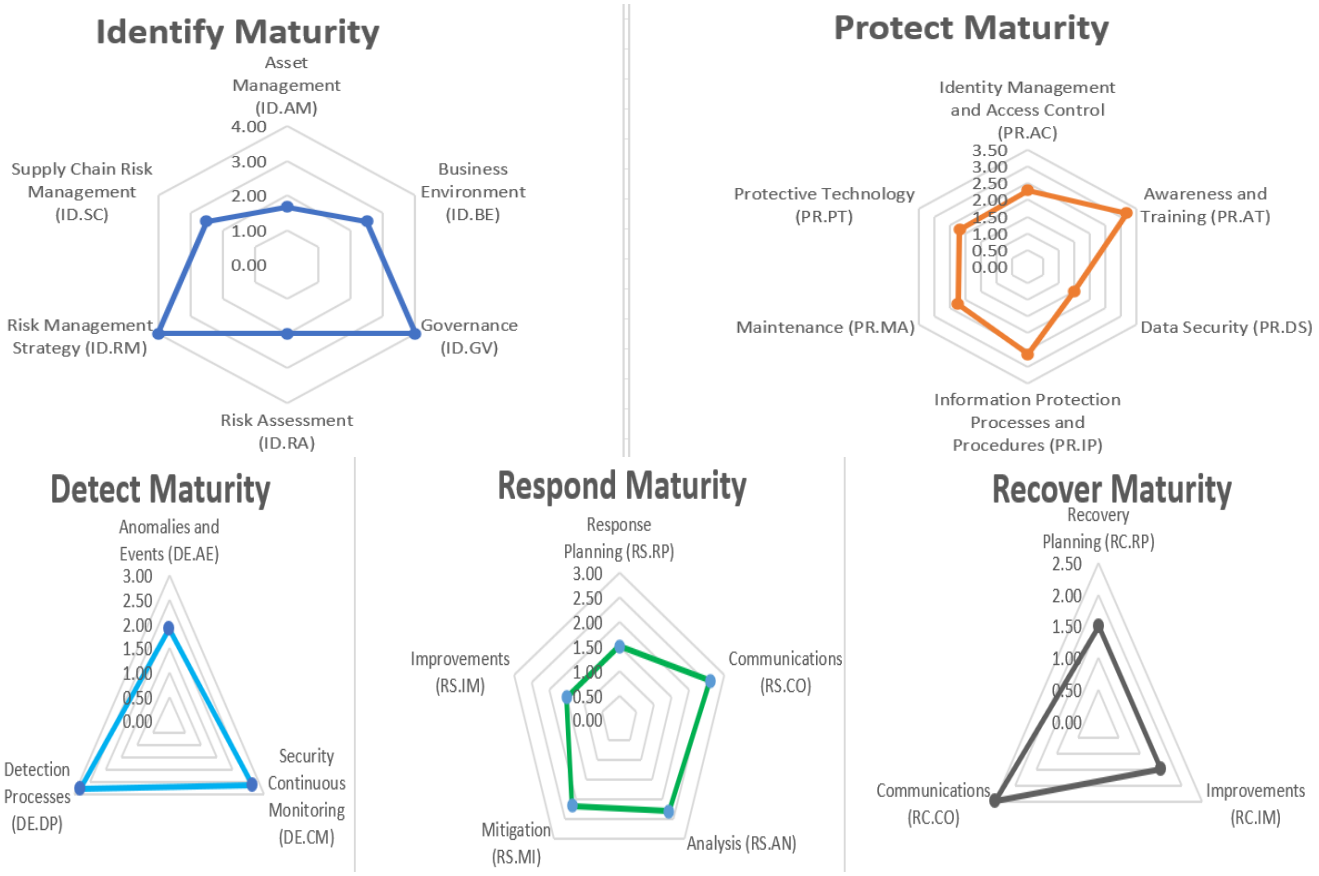

Figure 19 – GNI's Individual Functions NIST CSF Current Maturity vs Target scores

6.2Company's overall NIST Maturity Level/Tier

Following Radar/Spider charts are used to visualize the company's overall maturity score:

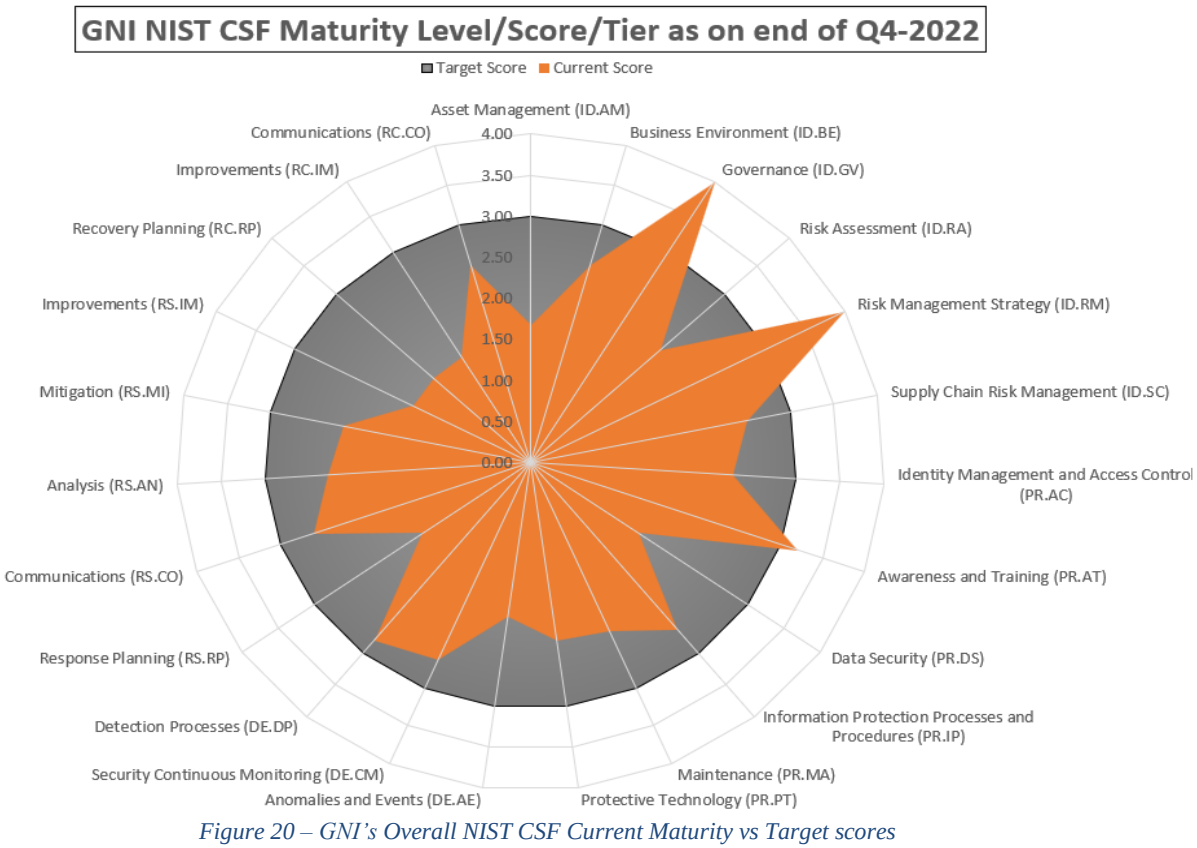

Figure 20 – GNI's Overall NIST CSF Current Maturity vs Target scores

6.3 Discussion

From the graphs above, we can observe following:

- From Identify function, it is observed that Governance and Risk Management Categories are meeting and exceeding the company's target maturity level, indicating that GNI Information Security policies, procedures, and processes are established and understood in accordance with business objectives to manage and monitor its regulatory, legal, risk, environmental, and operational needs. Additionally, it reveals that GNI's risk management program is administered and overseen by knowledgeable firm personnel. Asset Management, Business Environment, Risk Assessment, and Supply Chain Risk Management need improved rules, procedures, technological controls, and operational controls.

- From Protect Function, Awareness and Training category meet the target level denoting that the people and stakeholders of the business get training on cybersecurity awareness and are appropriately educated to carry out their information security-related activities and obligations in a manner that is compatible with applicable company policies, procedures, and agreements. Other subcategories need improvement to meet the target level set by the company.

- None of the three subcategories for the Detect function are aligned with the objective, necessitating more continual improvement. The Anomalies and Events subcategory received a score of 1.9, which was the lowest. Better proactive detection capabilities are required to come closer to the target level.

- From Response function, company scored lowest for Response Planning and Response Improvements signifying lack of Incident response plan. Organization needs a clear and documented Incident Management and response plan and processes to execute response strategies consistently after an incident. In addition, this demonstrates that the organization does not periodically update its response tactics based on the gaps discovered during testing or past incidents. All the response subcategories also failed to meet the target score hence need further continuous improvement.

- The company's Recovery strategy, policies, procedures, and controls do not meet the requirements of the company's goal maturity level, as shown by the fact that all 3 of its subcategories under the Recover function scored below the target.

7. CONCLUSION AND FUTURE WORK

The objective of this paper was to provide a technique for assessing cybersecurity risks with the intention of preventing hostile cyber activities in settings using linked IACS. This is accomplished by using the NIST Cybersecurity Framework (CSF) as a baseline to determine the level of cybersecurity maturity at a gas distribution pipeline site in reference to IT, OT, and operational controls, and then providing recommendations based on IEC 62443 standards.

Initially, the proposed Impact Assessment was successfully carried out making use of the six different impact factors which is then followed by assessing NIST CSF 108 controls on the basis of Design efficiency, Implementation, Operation and Review frequency of the current controls. The method is also validated via assessment conducted at an operational gas pipeline site. The result of the methodology shows the gap in the maturity of the current organization per NIST

CSF Tiers with that of target state organization's stakeholders aim to reach which was 3 (Repeatable).

Finally, it is discovered that the rising convergence between the IT and OT domains results in a multiplication and complexity of the vulnerabilities that are present in linked ICS setups for which remediations/corrective action plan is developed.

The developed Risk Assessment approach is tested on just one IACS site due to time constraints and complexity of ICS/OT infrastructure at the site, hence the results are the reflection of technical and operational cybersecurity controls implemented and followed at that site with exception of some cybersecurity practices followed organization wide for all sites.

In future, Reporting Part of the assessment involving manual work can be Automated using Robotic Process Automation like Ui Path. Moreover, The Risk Assessment approach can be applied to Critical National Infrastructure and can be used as internal or self-assessment compliance framework that can aid an organization in proactively determining the cyber security measures of people, process and technologies and comply with host of various audit and compliance obligations and /or industry certifications such as NIS Directive[10], ISO 27001, ISO 22301 etc. This approach can also be combined with standards/frameworks like MITTRE ATT&CK[11] for ICS, ICS Cybersecurity Assessment Framework from BSI.[12]

8. REFERENCES

Jazri, H. and Jat, D. S. (2016) "A quick cybersecurity wellness evaluation framework for critical organizations," in 2016 International Conference on ICT in Business Industry & Government (ICTBIG). IEEE, pp. 1–5.

Oliveira, A. da S. and Santos, H. (2022) "Continuous industrial sector cybersecurity assessment paradigm: Proposed model of cybersecurity certification," in 2022 18th International Conference on the Design of Reliable Communication Networks (DRCN). IEEE, pp. 1–6.

Malatji, M. (2022) "Industrial control systems cybersecurity: Back to basic cyber hygiene practices," in 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET). IEEE, pp. 1–7.

Curtis, P. D. and Mehravari, N. (2015) "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," in 2015 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, pp. 1–6.

Kanamaru, H. (2021) "The extended risk assessment form for IT/OT convergence in IACS security," in 2021 60th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), pp. 1365–1370.

[10] NIS Directive & NIS Regulations | Redscan
[11] Your Guide to the MITRE ATT&CK Framework for ICS – How to Use It to Enhance Security (nozominetworks.com)
[12] ICS Cybersecurity Assessment Framework | BSI (bsigroup.com)

Turrin, M. C. D. D. (2021) A Survey on Industrial Control System Testbeds and Datasets for Security Research, pp.23–35

Segers, G. (2021) Cyberattack prompts major pipeline operator to halt operations. CBS News.

Wikipedia contributors. (2022) 2015 Ukraine power grid hack. Wikipedia, The Free Encyclopedia.

An introduction to the components of the Framework | NIST. (2018)

Medoff, M. (2018). IEC 62443: Levels, levels and more levels.

Industrial Control Systems (ICS): System Types & Examples. (2019, June 19)

Blades, E., Christopher, J. D., & ICS, S. (2021) Introduction to ICS Security Part 2.

Guide to industrial control systems (ICS) security NIST 800-82r2. (2022). REPLIL - Industrial Patch Management.

NIS directive & NIS regulations. (2019, November 8).

Peters, R. (2020, May 18). Security concerns when enabling IT/OT convergence. Fortinet Blog.

ICS cybersecurity assessment framework. (2021)

Yassine, M. (2021). IT/OT convergence and cybersecurity. Researchgate.net, 1–5.

Di Pinto, A. (2020, August 11). Your guide to the MITRE ATT&CK Framework for ICS. Nozomi Networks.