AA26 - Application of Operational Technology Cybersecurity in Alumina Refining

Giovanni Djotiko[1], Karthik Sitaraman[2] and Saif Bin Rahal[3]
1. DCS Safety Systems & Maintenance Engineer
2. Head of Industrial Solutions
3. Senior Superintendent – DCS
Emirates Global Aluminium (EGA) - Al Taweelah alumina refinery, Technical Department, Abu Dhabi, UAE
Corresponding author: gdjotiko@ega.ae

Abstract

Operational Technology (OT) Cybersecurity is one of the pivotal contributors to live EGA's value of innovation and continuous improvement and help fulfil EGA's purpose – Together, innovating aluminium to make modern life possible. As OT and Cybersecurity landscapes are changing faster than ever, proficiencies in this arena are rapidly evolving with constant developments in ways to control operations, increase efficiency, and streamline processes. With the constant risks of insider attacks, state actor threats and opportunistic attackers, the need for a 'Secure-by-Design' approach is critical when deploying tools to prevent and mitigate these types of attacks. Using a strategy of segregating Governance, Compliance and Assurance roles, EGA aims to establish a cybersecurity posture in line with industry-leading practices and standards such as ISO 27001, IEC 62443 and the NIST Cyber Security Framework.

Keywords: Cybersecurity, Operational Technology, Industrial Control Systems, Digital Transformation.

1. Introduction

To control the production process in Alumina refineries, Operational Technology (OT) systems, otherwise known as Industrial Control Systems (ICS), can be divided into the following main categories:

- Controllers: For control of machines and processes such as Regulatory Controllers, Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), etc.
- Applications: For data gathering and analysis such as Supervisory Control and Data Acquisition (SCADA) and Manufacturing Execution Systems (MES).
- Operating Systems (OS): For managing software and hardware in a computer such as Windows and Linux.

These critical parts of the OT systems are increasingly connected to environments outside the organization e.g., the internet, third parties and cloud which expose them to cyberattacks. Attackers could use this exposure to exploit vulnerabilities and gain control of the production process to ultimately cause physical damage, process disruption, or steal confidential information.

It is without a doubt that innovation is necessary for any successful organization. Taking carefully calculated risks by leveraging emerging technologies like Artificial Intelligence (AI), Machine Learning (ML) and Cloud Computing connected to OT systems will offer great benefits to safety, productivity, and cybersecurity. Any new vulnerabilities and threats that may arise from adopting these new methods and technologies must be managed accordingly.

This paper examines EGA's approach to exploring best-in-class tools and best-practices and designing and applying cybersecurity measures to the OT environment in Al Taweelah alumina

refinery. The adopted measures should adhere to the "Secure-by-Design" principles, which means that these measures should be developed such that they are at least susceptible to attack and as free of vulnerabilities as possible. Overlapping measures can be used to mitigate any gap that might exist in individual applications and procedures.

The final objective is to safeguard the OT environment against all cybersecurity threats using standards like IEC62443 [1, 2], ISO27001 [3], ISO27002 [4] and the NIST Framework [5, 6].

2. Differences Between Information Technology (IT) and OT Approach

Al Taweelah alumina refinery started production in 2019 and 3 years prior to its commissioning, the OT was being designed with the best technologies and practices available for alumina refineries. During that time, EGA had OT environments already established in its aluminium smelters, so it was also able to leverage those skills and infrastructure.

Similarly, the organization also leveraged its enterprise IT environment. Many tools were reused in the refinery and the IT stakeholders were involved in determining the design scope of the refinery's OT assets.

At the same time, monitoring and managing OT environments can be challenging when using security tools traditionally meant for IT networks and infrastructure. It is critical to understand the differences between these two environments prior to deploying any tool. The following section focuses on these differences.

3. Confidentiality, Integrity, Availability (CIA) to Availability, Integrity, Confidentiality (AIC)

A reprioritization within the CIA triad is required when we determine the importance applicable for OT environments. Confidentiality deserves more importance than the other goals when we apply the triad for EGA's Enterprise IT assets. Understandable, since a myriad of personal and corporate information about employee payroll, email communications, corporate transactions, etc. are to be treated as extremely confidential. Corporate data integrity and availability follow close behind.

When it comes to OT, a shift of importance is required since the goal of availability deserves more importance than the other goals.

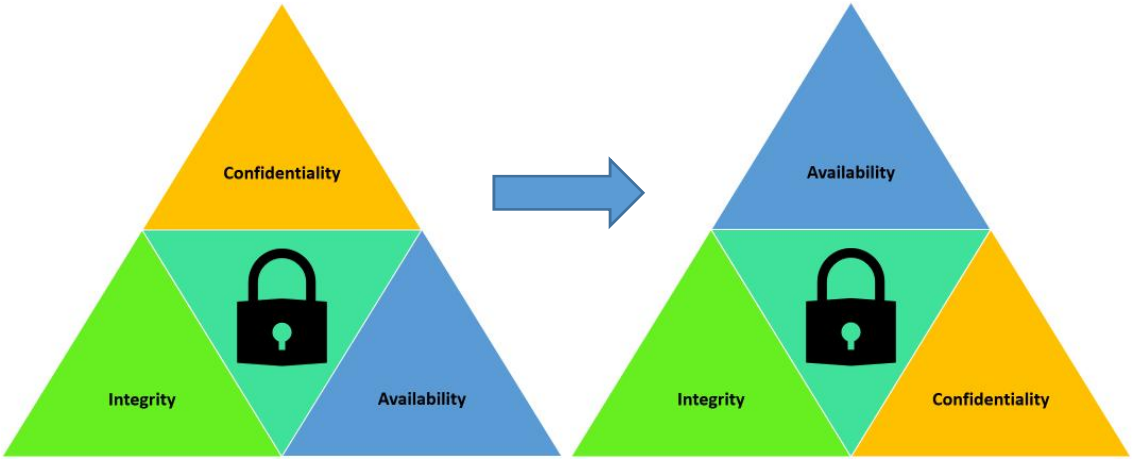

Figure 1. Availability as most important goal in AIC triad.

For manufacturing industries, a 30-minute interruption of email access or a 1-hour inability to apply for your vacation leave is not as detrimental as a 5-minute Loss of View (LoV) to the refinery process or any Loss of Control (LoC) of a Distributed Control System (DCS) or PLC.

3.1 Safety First, then Security

Traditionally, OT environments sacrifice security for more safety. The main objective of OT cybersecurity is to ensure safety of equipment, processes, environment and, especially, personnel. Any modern manufacturing facility will consider the safety and well-being of its employees as the most important objective. Several security measures are consciencely being compromised to enable greater safety. A common example are automatic wallpaper or lock screens that are widely used in enterprise IT workstations to assist the user in preventing unauthorized access. These types of automatic screen locking mechanisms are chosen to not be implemented on operator workstations in 24x7 control rooms to enable the operator to always have access and a view to the plant conditions and alarms.

3.2 Direct Impact

OT systems are often more critical to an organization's production operations than IT systems. IT systems typically store and process data and do not directly control physical processes. On the other hand, a compromised OT system could not only lead to production disruption, but potentially causing personal injury or death, damage to equipment and the environment. As a result of this difference, OT environments often require different security measures than IT systems.

4. OT Cybersecurity Tools and Procedures

It becomes clear that the application of OT cybersecurity tools must be done carefully by considering the differences between OT and IT environments, while still acknowledging which strong IT processes and procedures can be leveraged.

A combination of processes, procedures and applications can be selected to cover each core function in the NIST Framework, as illustrated below. In this chapter, we will try to create a better understanding of this selection.

Figure 2. Example of processes, procedures and applications applied at Al Taweelah alumina refinery.

4.1 Identify

"Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."

Figure 3. Example of activities related to the Identify function.

Asset and Risk Management are the most important categories addressed within this function. A conjunction of applications is used for automatic and on-demand asset discovery and all trusted assets are documented in an asset register. Figures 3 and 4 below show examples of how applications can be used to for asset management, particularly for automated asset discovery. The benefit of using such tools is that the discovery happens in real-time and could trigger alerts and reports to notify stakeholders.

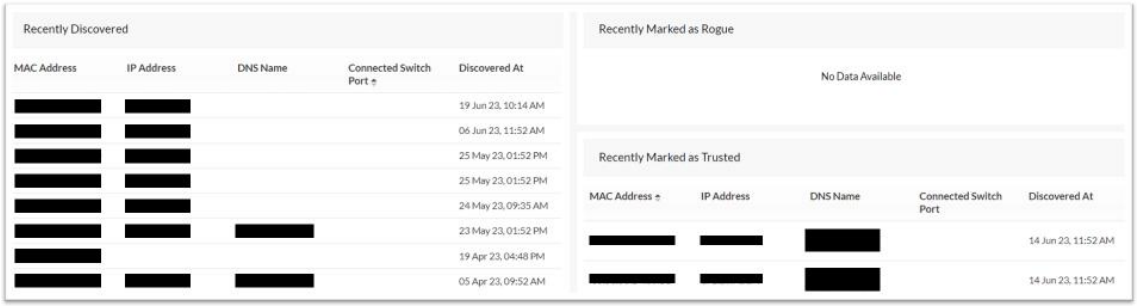

Figure 4. Asset discovery using a Network Management System (NMS).

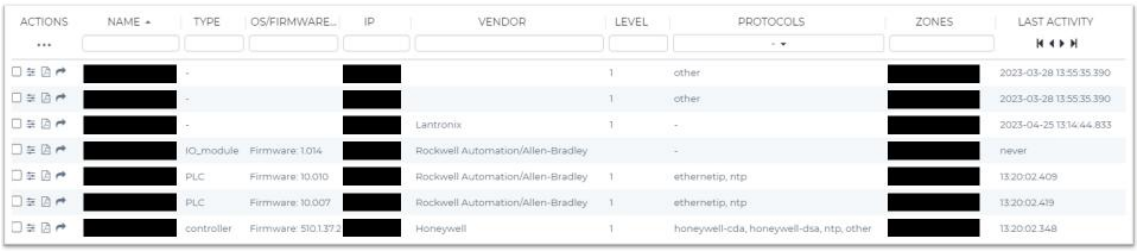

Figure 5. Asset management using an Intrusion Detection System (IDS).

The risks corresponding with every asset go through a risk assessment and are documented in a risk register. The asset and risk registers are included as part of the company-wide Information Security Management System (ISMS) in line with the ISO/IEC 27001 standard. The addition, removal and update of assets as well as the evaluation of existing and new risks is conducted as an interactive, ongoing process as part of normal operations.

4.2 Protect

"Develop and implement appropriate safeguards to ensure delivery of critical services."

Figure 6. Example of activities related to the protect function.

5. System, User and Data Access Management

The main objective of this function is to support the ability to limit or contain the impact of a potential cybersecurity event. Access management stands central in this function. To further elaborate on the activities related to managing access, we will divide these measures into 3 types:

- System (physical and logical) access;
- User (authenticated) access;
- Data (encrypted) access.

System access control is achieved by creating both physical and logical barriers. Physical barriers are measures put in place to limit unauthorized persons from reaching and accessing a system. Such physical restrictions must be implemented for all controller, servers, engineering stations, etc. in levels 1, 2 and 3 of the OT environment as per the Purdue model. The main reason being that these devices have direct or indirect control of the refinery process, which is why these levels together known as the control network. The physical restrictions include cabinets and rooms only accessible using keys, access cards and biometric scanners, or Air-Gapping systems and networks. Logical barriers are forms of systematic segregation of systems from each other using certain system or network configurations. An example of this is network zoning using Active Directory (AD) domains and subdomains.

Table 1. Overview of network zoning using AD.

Name	Domain	Purdue Level	Remarks
NA	NA	0	Transmitters, Sensors, etc.
NA	NA	1	Control Network: PLC, DCS, etc.
Peer DC	AD Domain 1 – Subdomain 1	2	Area 1 Supervisory Network
Root DC	AD Domain 1 – Subdomain 2	2	Area 2 Supervisory Network
Peer DC	AD Domain 1 – Subdomain 3	3	MES Network
DMZ DC	AD Domain 2	3.5	De-Militarized Zone (DMZ)
Enterprise DC	AD Domain 3	4	Corporate Network
Enterprise DC	Azure AD	5	Cloud

Other methods for establishing logical barriers include network segmentation are Virtual Local Area Networks (VLANs) and Internet Protocol (IP) Subnets.

Table 2. Overview of network segmentation using VLANs and Subnets.

Name	Purdue Level	Role Segregation	Remarks
NA	0	NA	Transmitters, Sensors, etc.
VLAN 11	1	Area 1 Control Network	DCS, PLCs, IEDs, etc.
VLAN 21	1	Area 2 Control Network	DCS, PLCs, IEDs, etc.
192.168.0.0/25	1	Area 3 Control Network	DCS, PLCs, IEDs, etc.
VLAN 12	2	Area 1 Supervisory Network	Servers, Engineering Stations, etc.
VLAN 22	2	Area 2 Supervisory Network	Servers, Engineering Stations, etc.
192.168.0.128/25	2	Area 3 Supervisory Network	Servers, Engineering Stations, etc.
VLAN 30	3	MES Network	Web and Application Servers

User access is most commonly achieved by implementing Windows AD and, more increasingly, Azure AD. Policies and (documented) procedures must be in place to properly manage user access to data, systems and resources. Real-time alerts and/or scheduled reports from AD auditing or managing tools can be utilized to notify concerned parties of (un)authorized modifications of the AD so they can be reviewed and acted upon, if required. The next figure shows a sample of such an alert.

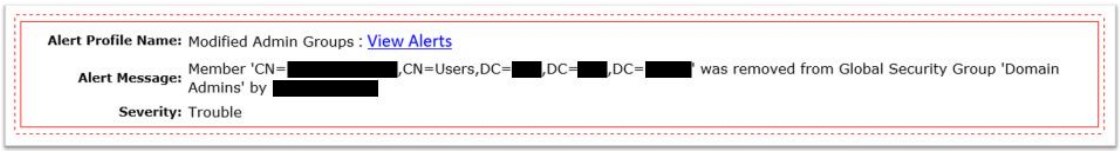

Figure 7. Email alert showing AD modifications in real-time.

Scheduled reports like the one shown in Figure 8 can also be used to ensure compliance to the policies and procedures. These reports must be routinely checked or audited by those granting the access, those approving the access requests, as well as other parties, e.g., different team members or internal and external auditors.

Data access is the last form of access management and is focused primarily on data protection and security. Company data must only be transferred over a private and encrypted network for example:

- **Application – Application communication**: The communication between applications must be executed over secured ports via Secure Sockets Layer (SSL) certificates to protect the data through encryption and authentication.
- **User – Website traffic**: Al Taweelah alumina refinery uses web applications as the user interface for most MES and other management/supervisory applications. Hypertext Transfer Protocol Secure (HTTPS) is used to send data between the user's web browser and the solution website. HTTPS is encrypted for security of data transfer from the user to the application and back.
- **User – Machine connection**: Through a combination of network zoning and segmentation rules and configuration, users can connect to machines in the OT environment from within. Certain connections outside the OT environment (meaning

everything above level 3.5 DMZ) must only be allowed vis SSL encrypted VPN connections.

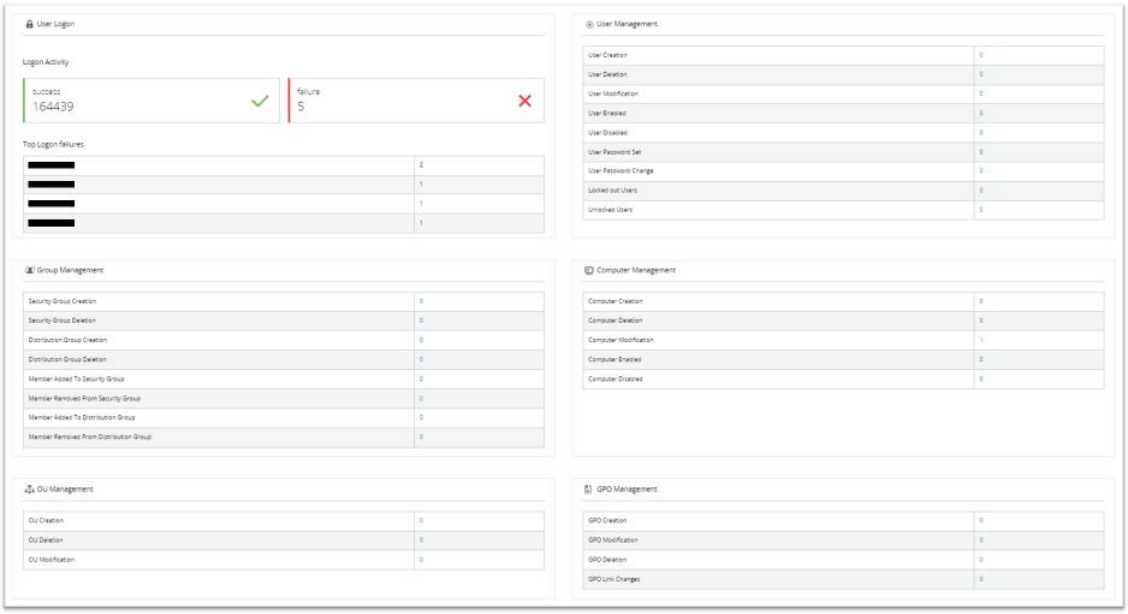

Figure 8. Scheduled report showing AD modifications during a specified period.

6. Software and Hardware Maintenance Procedures

The installation, replacement and maintenance of all items included in the asset registers must be documented in standard operating and maintenance procedures. These may be supported by user manuals and guides from the vendors.

7. Malware Protection

Several solutions have been used as malware protection (commonly referred to as anti-virus) to protect against malicious programs and exploits for decades. Malware protection adds an extra layer of security to your environment by constantly monitoring and periodically scanning your assets to identify, quarantine, and eliminate any malware to keep your systems functioning safely and securely. Important factors to consider when implementing a malware protection solution include:

- **Automatic actions and self-protection**: Client agent and consoles should have a proven track record of their ability to protect the client machine by stopping/killing malicious programs and processes, blocking/deleting/quarantining suspicious files, etc.
- **Automatic virus definition updates**: The virus definitions can be downloaded from upstream or enterprise hosted repositories, directly from the malware protection vendor, or from managed services.
- **Scheduled reports**: These can be configured and used for similar purposes as all previously mentioned scheduled reports, namely for ensuring compliance to the policies and procedures.
- **Alert and notifications**: Utilized to notify concerned parties of any suspicious detections so these can be investigated and acted upon, if needed. Figure 9 shows such a suspicious detection.

Time, 06/26/23 07:56:58 UTC
Host, [redacted]
IPAddress, [redacted]
OS, Server
ThreatName, ExP:Illegal API Use
EventDescription, An exploit was detected.
TargetFile, C:\WINDOWS\SYSTEM32\[redacted]
SourceProcess,
Severity, Critical
ActionTaken, Blocked
Handled, True
EventID, [redacted]

Figure 9. Email alert showing AD modifications in real-time.

7.1 Detect

"Develop and implement appropriate activities to identify the occurrence of a cybersecurity event."

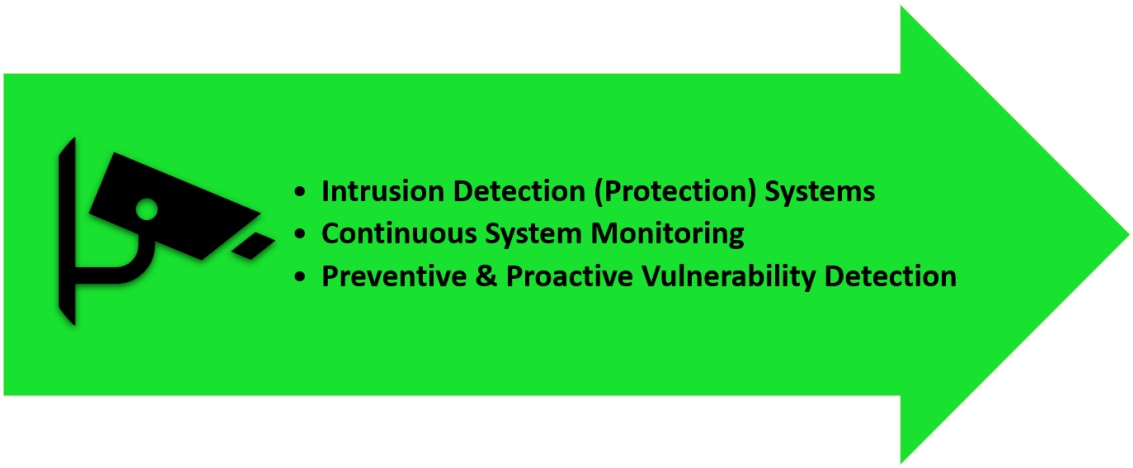

Figure 10. Example of activities related to the Detect function.

The activities and solutions mentioned so far as part of the Identify and Protect functions are also used for timely discovery of cybersecurity anomalies and events. As the threat landscape is a continuously changing one, so should the detection mechanisms constantly be adapted and improved. New, previously unidentified, vulnerabilities need to be located as soon as possible and processes and procedures must be reviewed and updated, as required.

Vulnerabilities can also be pro-actively detected by executing penetration tests and red team exercises.

Since OT systems typically run 24x7 industrial operations, the organization should also engage in continuous system monitoring of the environment. Establishing or including OT into a Security Operations Center (SOC) to continuously monitor anomalous events, will enhance the organization's ability to prevent, detect, and respond to cyber threats around the clock.

7.2 Respond

"Develop and implement appropriate activities to take action regarding a detected cybersecurity incident."

Figure 11. Example of activities related to the respond function.

The activities for this function are all about the ability to contain the impact of a potential cybersecurity incident. Most, if not all, organizations will have a Business Continuity Strategy (BCS) in place to standardize and facilitate the response to different types of incidents and events that can potentially interrupt critical business resources and functions. The activities related to this NIST core function should be in line with the objectives in this BCS.

For all the items in the asset register compiled as part of the Identify function, backup and recovery mechanisms must be established and included as part of Business Continuity Plans (BCP) or Disaster Recovery Procedures (DRP).
Important topics to consider in the BCP/DRP include, but are not limited to:

- Recovery strategy and objectives
- Roles and responsibilities
- Critical resources, dependencies, and communications
- Procedure activation guidelines
- Procedure testing and training requirements

The procedures and the systems referred to in the BCP and DRP are to be reviewed and tested on a routine basis to ensure relevance and effectiveness. Several exercises can be conducted to test the readiness of the organization to respond to cybersecurity incidents. Examples include disaster table-top exercises, cyber-attack drills and backup recovery activities.
These exercises can also be used to put into practice the various maintenance procedures mentioned in section 6. These activities help prepare the organization for the next NIST core function.

7.3 Recover

"Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

Figure 12. Example of activities related to the recover function.

The final core function helps to ensure that the organization can timely recover everything included in the asset register to normal or acceptable operations to reduce the impact or recover from a cybersecurity incident. The ability to source software and hardware spare parts through support contracts and Service Level Agreements (SLA) are a critical prerequisite for any recovery efforts.

Even after all the measures, processes and procedures that are put in place as part of the previous four NIST core functions, it is quite possible that systems were able to be compromised by malicious actors. The capability to be able to recover critical assets is the last line of defense.

8. Challenges in OT Environments

OT environments face a number of cybersecurity challenges, including:

- **Critical infrastructure:** Alumina refineries are critical infrastructure, which means that a cyberattack could cause significant damage to the safety, economy, or environment as mentioned in paragraph 3.2.
- **Complex systems (Heterogeneity):** Alumina refineries are complex systems consisting of a mix of different devices and systems from different vendors, which requires a tailor-made cybersecurity program to safeguard them from cyberattacks.
- **Isolation:** OT systems are often required to be physically isolated from IT systems to eliminate the risks originating from external systems. This can make it difficult to apply security patches and updates, and it can also make it more difficult to monitor them for security intrusions and threats.
- **Lack of awareness:** Although they might have plenty resources and experience to address IT security concerns, organizations may lack the knowledge and skills to identify and respond to cybersecurity threats typical to OT environments.
- **Increased connectivity:** With the Fourth Industrial Revolution (Industry 4.0), the increased mining of data to help solve business problems through advanced data analysis also expands the cyber-attack surface of the OT environment. Organizations will struggle to protect their assets if they do not establish the necessary people, processes, and tools to manage new threats and vulnerabilities, especially those specifically to exploit emerging technologies such as AI, ML, Edge Devices, Industrial Internet of Things (IIoT), and Cloud Computing. With the importance and availability of more data, the amount of consumers of OT data will also increase. More and more users of this data reside outside of the control network and even outside the organization's premises, e.g., cloud networks, governmental/regulatory authorities, vendors, and other third parties.

9. Recommendations and Opportunities

The design, implementation, and management of the integrated cybersecurity solution for the Al Taweelah alumina refinery have enriched the organization with several experiences and learnings that can be leveraged for future (greenfield, brownfield) projects. Some of these learnings are:

- **Reuse IT security tools:** There are a number of security tools originally meant for typical IT environments that are just as effective for OT environments. Reusing tools that your organization's IT professionals have a good knowledge and experience with can speed up the implementation of these tools for your OT network. This can also cause huge savings by enrolling into organization-wide (for IT and OT) support or procurement contracts.
- **Implement a zero-trust security model:** This model assumes that no user or device can be trusted by default and requires organizations to implement strong authentication and authorization controls for all users and devices that access their data and networks.
- **Defense-in-depth strategy:** This is the use of multiple layers of security controls to protect systems from cyberattacks. As explained in section 5, this includes physical security controls, network security controls, system/application security controls, and data security controls.
- **Train and educate employees:** Employees, especially those who use and interact with the OT systems, should be educated about cybersecurity threats and how to identify and report suspicious activity.
- **Vendor and managed services support:** OT vendors and companies providing cybersecurity services play a valuable role in helping organizations to secure their OT environments. Vendors can test and qualify security updates and provide training and other resources specifically for their products that can help organizations to protect their systems. Managed services can help monitor the system and execute/assist prevention, mitigation or recovery activities.
- **Stay up-to-date:** The threat landscape is constantly changing, so it is important to stay up-to-date on the latest threats and vulnerabilities. Organizations should subscribe to security newsletters and alerts, and they should participate in security forums and conferences to build a comprehensive threat intelligence.
- **Emerging technologies:** As was discussed in the earlier chapter, the increase of the use of AI, ML, Edge Devices, IIoT and Cloud Computing in OT environments create an additional threat vector and increase the OT attack surface. At the same time, these emerging technologies offer opportunities to enhance cybersecurity capabilities for example AI/ML powered Intrusion Detection/Prevention Systems (IDS/IPS) that build models to predict threats and incidents. A popular way to ensure that these emerging technologies become embedded in cybersecurity processes is the inclusion of cybersecurity in the organization's Digital Transformation journey.
- **Legacy systems:** Without proper managements of product lifecycles and roadmaps, many OT components may become outdated. Some components may become End of Life/Service/Support (EOL/EOS/EOSL) therefore no longer supported by the vendor and no longer receiving security updates making these components vulnerable to attacks. Some outdated products may just simply lack the security features required to operate in modern OT landscapes.
- **Continuous improvement**: Al Taweelah alumina refinery aims to comply with all the company mandated policies, procedures, rules, and regulations. It is also critical to check compliance to industry standards and adherence to best practices. Additionally, all available dashboards, alerts and reports mentioned in this document can be used by the cybersecurity team to engage in routine assurance exercises to give confidence in the

systems and processes in place. Finally, good governance is required by the organization's leadership to support and empower a strong cybersecurity culture.

10. Conclusion

Metals, mining, and manufacturing industries are reliant on OT systems making them vulnerable to cyberattacks. Organizations in these industries should adopt cybersecurity best practices, but also develop custom techniques and solutions to protect their OT environments from cyberattacks. Alumina refineries are no exception. By implementing the approach described in this paper, Al Taweelah alumina refinery has improved its OT cybersecurity posture to ensure its readiness to deal with cybersecurity events and incidents.

The application of cybersecurity measures, specifically in OT environments, is a complex and continuously evolving one. This demands organizations to adapt by continuously improving existing measures and utilizing new techniques and technologies.

11. References

1. *IEC/TC 62443-1-1*, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models.
2. *IEC 62443-3-3*, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
3. *ISO/IEC 27001*, Information security, cybersecurity and privacy protection — Information security management systems — Requirements
4. *ISO/IEC 27002*, Information security, cybersecurity and privacy protection — Information security controls
5. Framework for Improving Critical Infrastructure Cybersecurity, *National Institute of Standards and Technology Publication* NIST.CSWP.04162018, Ver. 1.1, 55 pages, 16 April 2018.
6. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, Guide to Industrial Control Systems (ICS) Security, *National Institute of Standards and Technology Special Publication* 800-82, Rev. 2, 247 pages, May 2015.