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.

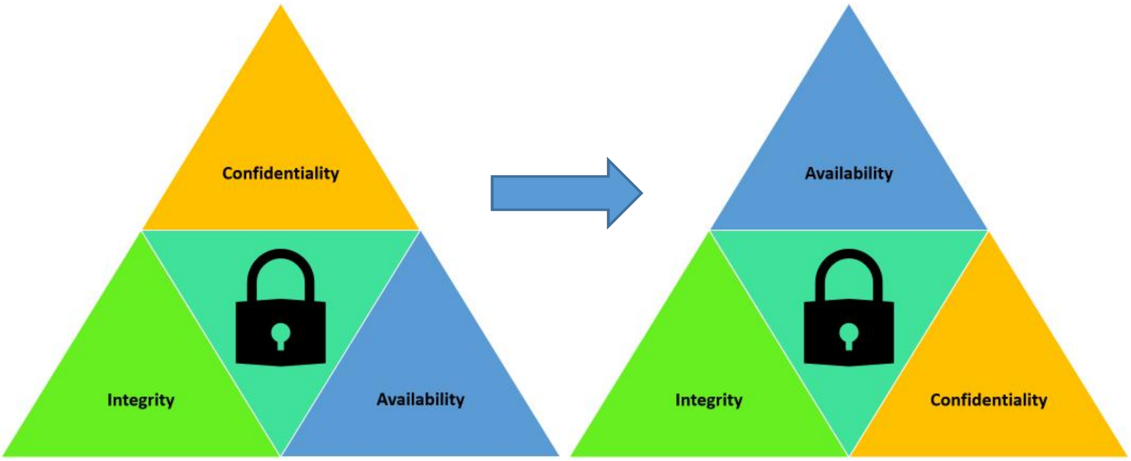

Figure 1. Availability as most important goal in AIC triad.

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.