Process Improvement for Enterprise OT Asset Intelligence & Lifecycle Management

Stephanie Guzmán Huertas
Master of Engineering in Manufacturing Engineering
Advisor: Carlos J. González, PhD
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2026

Abstract — *This design project aims to improve the Operational Technology (OT) asset management process by implementing a centralized infrastructure for managing and monitoring industrial automation assets across manufacturing facilities. The initiative focuses on optimizing OT asset inventory and lifecycle management processes to reduce inefficiencies, improve data accuracy, strengthen cybersecurity risk management, and drive standardization across the enterprise. The improvement initiative was conducted following the DMAIC (Define, Measure, Analyze, Improve, Control) methodology, ensuring a systematic and data-driven approach. Currently, OT asset inventory is maintained through offline lists that require manual updates whenever systems are upgraded or newly introduced to the manufacturing sites. This approach often leads to data inaccuracies, limited visibility, and delayed updates. By implementing a centralized system with automated network discovery, asset information will be continuously updated and validated in real time. This ensures greater data accuracy, improved lifecycle management, and enables faster, more effective responses to identified vulnerabilities, helping improve system reliability and overall cybersecurity.*

Keywords — *Assets, Cybersecurity Risk, Lifecycle, Operational Technology (OT).*

INTRODUCTION

The ABC Company is committed to serving patients with chronic diseases by ensuring the reliable and consistent production of high-quality products. The manufacturing process is divided into several stages, including raw material handling, weighing and dispensing, formulation filling, packaging, and inspection. These operations take place across multiple buildings, where processes are controlled through automation systems to maintain efficiency and consistency.

A key component of this automation is the use of a Programmable Logic Controller (PLC). PLCs are industrial control systems that monitor "inputs" such as temperature, pressure, and flow, and make real-time decisions to control "outputs" like motors, valves, and alarms. They execute programmed logic to ensure that each step of the process operates within defined parameters, whether controlling formulation mixing or managing packaging lines.

PLCs play a critical role across all manufacturing stages by ensuring processes remain stable, precise, and compliant with regulatory requirements. Due to their importance, maintaining full visibility of these assets is essential. An accurate inventory of PLCs enables better tracking of their location, configuration, firmware, and lifecycle status. This supports effective maintenance planning, timely system upgrades, and minimizing the risk of equipment obsolescence. Additionally, improved visibility strengthens cybersecurity by allowing faster identification and mitigation of potential vulnerabilities, helping protect operations and maintain a secure manufacturing environment.

PROBLEM STATEMENT

Operational Technology (OT) asset management across manufacturing buildings is limited by low visibility and the use of fragmented, manually maintained inventories, covering a total of 125 assets. This often leads to inaccurate data, poor lifecycle management and outdated systems remaining in use. The lack of real-time information increases operational risk, especially when identifying and responding quickly to cybersecurity vulnerabilities. Missing or incomplete data can delay mitigation actions and expose critical processes to threats. This project will follow DMAIC methodology to improve the current inventory structure by implementing a centralized, intelligent asset management system that increases visibility, strengthens cybersecurity response, and supports better lifecycle management.

RESEARCH DESCRIPTION

This project evaluates current OT asset management practices, focusing on visibility gaps, lifecycle control, and cybersecurity risks caused by manual inventories. It analyzes how limited, outdated information affects response time and operational reliability across manufacturing assets.

RESEARCH OBJECTIVES

The objective is to implement a centralized and intelligent asset management approach using the DMAIC methodology, leveraging Rockwell FactoryTalk AssetCentre, an OT infrastructure software to improve visibility, strengthen cybersecurity response, and enable effective lifecycle management.

RESEARCH CONTRIBUTIONS

This project improves OT asset visibility, lifecycle management, and cybersecurity risk mitigation by replacing manual and scattered inventories with one centralized, automated system. It increases data accuracy, standardization, and the speed of response to vulnerabilities, helping reduce operational risk. It also changes the way asset inventories are created. Instead of physically entering manufacturing areas to collect asset lists, teams can access an instant and automated inventory of all assets. This reduces time and effort while supporting more proactive, reliable, and secure asset management.

LITERATURE REVIEW

Operational Technology (OT) assets are critical components used to monitor, control and automate manufacturing processes. These assets include Programmable Logic Controllers (PLC), Human Machine Interface (HMI), network switches, sensors, drives, and other control system components. Among these, PLCs play a particularly important role because they execute the control logic that allows equipment, production lines, and process systems to operate safely and consistently. As manufacturing environments continue to incorporate greater levels of computerization, process control has become increasingly dependent on rapid feedback of operation quality data, allowing organizations to improve efficiency, consistency, and decision-making within the production environment [1].

Effective process control is essential because manufacturing performance can vary according to process conditions and operational changes. For this reason, maintaining records of process capability and monitoring significant variances of deterioration are critical practices within modern industrial operations [1]. OT assets support these objectives by providing real-time data, automation, and control functions that reduce human variability and improve product stability. In environments where conventional or partially manual processes are still used, proper worker training and operational oversight remain equally important to maintain production quality and reliability [1].

Since OT assets are directly connected to manufacturing operations, their lifecycle and maintenance are essential to ensure reliability, safety, performance, capacity, and continuity. Proper lifecycle management helps organizations track asset installation, support status, firmware versions, maintenance needs, upgrades, replacement timelines, and even predictive maintenance. Maintaining visibility of the OT assets is crucial for important maintenance, spare parts management, cybersecurity, and compliance activities.

With the importance of assets visibility, industry standards and best practices further reinforce the need of centralized management of OT systems. Standards such as ISA/IEC 62443 [2] and guides from the National Institute of Standards and Technology [3], highlight the importance of maintaining accurate asset inventory, enabling continuous asset monitoring. Additionally, the increasing adoption of Industrial Internet of Things (IIoT) technology has accelerated the need for IT and OT teams to centrally manage industrial systems.

However, despite the availability of these standards and technologies, many organizations face challenges when asset information is incomplete, outdated, or stored across different files. This decentralized system can create duplicate records, inconsistent data, manual effort, and delays when teams need accurate information. Without a standardized process, manufacturing areas may manage OT asset data differently, making enterprise visibility difficult. This practice can increase the risk of unexpected failures, production downtime, unsupported equipment, undetected cybersecurity vulnerabilities, and higher maintenance costs, demonstrating the need for a centralized enterprise-level and reliable OT asset management approach.

DMAIC Process Structure

DMAIC methodology is a structured approach used for problem-solving that forms part of the core methodologies of Six Sigma and continuous improvement. The acronym stands for Define, Measure, Analyze, Improve, and Control (See Figure 1). It is widely used in industries and organizations to improve process quality, reduce defects, increase efficiency, and solve operational problems systematically by using data instead of assumptions. It is mainly used when there is a potential Six Sigma project within existing processes that are not performing well and need improvement [4].

Figure 1
DMAIC Methodology

Each stage of this methodology provides a disciplined approach to identifying problems, understanding their causes, implementing improvements and sustaining results over time.

Define

In the Define stage the problem is clearly identified. The team determines what issue needs to be solved and why it is important to the organization. Key activities may include developing a project charter, identifying stakeholders, defining the voice of the customer, and mapping the high-level process. Project goals are set, the scope is outlined, and customer requirements are understood. This step ensures everyone agrees on what needs to be improved and why [4], [5].

Measure

Measure stage involves collecting data about the current process. Key performance indicators are identified, and baseline measurements are taken to understand how the process is being performed at the moment. Some of the tools used during this stage include SIPOC, a process mapping tool that identifies Suppliers, Inputs, Process, Outputs, and Customers of the process, and VOC, a method to capture the Voice of the Customer by understanding customer needs, expectations and requirements. Common activities include selecting appropriate metrics, validating measurements systems, gathering process data, and identifying current levels of defects, delays, variation, or inefficiency. This provides a factual starting point for analysis and to compare performance before and after improvements are made [4], [5].

Analyze

During Analyze stage the data is examined to find the root cause of the problem. Tools such as cause-and-effect diagrams (fishbone diagram), Pareto charts, and statistical analysis may be used to determine why the problem occurs. Teams look for patterns, identify potential causes, and verify which factors are actually driving defects or inefficiencies [4], [5].

Improve

The Improve stage focuses on developing, testing, and implementing solutions to address the root causes identified during the analysis. Potential improvements are evaluated based on feasibility, expected impact, cost, and risk. Teams may use techniques such as brainstorming, pilot testing, design of experiments, or process redesign to identify and refine the most effective solutions. After implementation, the improvements are monitored and adjusted as needed to ensure they successfully enhance process performance and achieve project objective [4], [5].

Control

The Control stage ensures that improvements are sustained over time by establishing monitoring systems and standardized procedures that prevent problems from recurring. This stage may involve the use of control charts, dashboards, standard operating procedures, training programs, audits, documentation updates, and response plans to maintain consistent performance. Control is essential because it transforms a temporary improvement into a stable, and long-term process outcome [4], [5].

PROJECT METHODOLOGY

The DMAIC methodology was selected for this project because it aligns well with the project objectives and nature of improvement needed. This structured approach supports a clear understanding of the current OT asset management gaps, including visibility, process inconsistencies and cybersecurity risks. Through systematic analysis and improvement, the project proposes the implementation of a centralized solution to enhance inventory accuracy, strengthen lifecycle management, and ensure sustainability control of asset data over time.

RESULTS AND DISCUSSION

This section presents the results obtained through the DMAIC methodology applied to the current OT Asset management.

Define

A project charter was prepared in the Define stage to support the OT asset management improvement, to outline the problem statement, goal, and metrics definition. See Table 1.

Table 1
Project Charter

Project Charter
Problem Statement: The OT asset management process relies on manual, segregated inventories, reducing visibility and accuracy across site buildings. This results in poor lifecycle control, slower response to cybersecurity risks, increased operational risk, and higher effort to maintain reliable records.
Goal: Implement a centralized OT asset management system to improve visibility of 125 assets, reduce manual effort, strengthen lifecycle and cybersecurity risk management, and prevent downtime and costly disruptions.
Metric Definition: OT asset inventory

The Define stage confirmed that the current OT asset management process lacks centralization, standardization, and real-time visibility. These gaps affect lifecycle management, cybersecurity response, and the reliability of asset data across manufacturing buildings. This results in inaccurate information, limited visibility and lack of standardization across buildings. These gaps make lifecycle management more difficult and delay the identification of assets affected by cybersecurity vulnerabilities. This current scenario shows the need for a centralized and standardized system to improve accuracy, visibility, consistency, and support for manufacturing operations.

Measure

Data collection was performed to capture the current condition of OT asset management across the different manufacturing buildings. Data was collected on the number of assets identified, the time required to create and update inventory records, the accuracy and completeness of existing asset information, and the ability to identify assets affected by lifecycle or cybersecurity concerns.

The baseline condition showed that the current inventory process depends on manual collection and validation of asset information. Asset records format may vary by building depending on the person responsible for maintaining the list, and the frequency of updates. Important fields such as firmware version, physical location, lifecycle status, support status, model, IP number, and system owner may not always be complete or standardized. As a result, additional time is required to confirm whether an asset is active, vulnerable, obsolete, or affected by a required update.

A SIPOC was developed during the Measure stage to provide a high-level view of the current OT asset management process, for a better understanding of the existing process, inputs and outputs, and the key areas where data was collected to establish a project baseline. See Table 2.

Table 2
SIPOC

Suppliers	Inputs	Process	Outputs	Customers
IT / OT teams	Current asset inventory	Asset data collection	Consolidated inventory	Cybersecurity IT / OT Teams
Engineering	Asset information (Brand, model, firmware version)	Asset information confirmation	Accurate asset information	
Vendors	Technical specifications	Data standardization	Centralized visualization	Operations
Current Systems (CMMS, Excel)	Historical registers	Centralized system integration	Asset reports	QA / Compliance
Cybersecurity	Security requirements	Updates and monitoring	Vulnerabilities identifications	Management

The SIPOC analysis describes the current OT management process, where multiple suppliers like IT/OT, engineering, third party vendors, and existing systems provide fragmented data (current inventory, technical specifications, and historical records). These inputs go through a process that includes the asset data inventory compilation, validation, standardization and integration of the information, having as a result the consolidated inventory and greater visibility of the asset. However, the SIPOC analysis evidence that the process depends heavily on manual sources, and non-integrated systems, which impact the accuracy, consistency, and availability of the information. This lack of centralization limits the capacity to react quickly to vulnerability alerts, increasing the operational risk, and requires a significant human effort to maintain data up to date, justifying the need for a centralized system to optimize management and decision making on these systems.

Based on the findings, the key needs of the clients were identified and are summarized in the following VOC (Voice of the Customer) table 3.

Table 3
VOC

Voice of the Customer	Key Customer Issues	Customer need
IT/OT Temas	Asset lists are manual, incomplete, and the process is different by building	Access to accurate, current and complete OT asset information
	Existing records may be outdated or inaccurate	Reliable information for maintenance and system updates
	Each building manages inventory differently	Standardized process across all buildings
	Information is segregated by building	Enterprise-level visibility of OT asset
Engineering	Information is not centralized and takes time to find	Easy access to asset details for troubleshooting and support
Cybersecurity	Missing information slows mitigation actions	Faster assessment of vulnerable or unsupported assets
Current systems	Inventory creation requires physical checks and manual updates	Reduced manual effort and less time spent building inventories

The Voice of the Customer shows that teams are facing common challenges with OT asset information. IT/OT teams are concerned that asset lists are manual, incomplete, and spread across different buildings, making it difficult to maintain accurate and current records. They also need a standardized process, and an enterprise level visibility across all OT assets. Engineering needs quick access to asset details to support troubleshooting and reduce delays caused by missing or hard-to-find information. Cybersecurity is concerned that missing asset data slows down risk assessment and the response to vulnerable or unsupported assets. Current systems also require physical checks and manual updates, which take time and increase effort. Overall, the main customer concerns are poor asset visibility, inconsistent data, manual processes, slow response to issues, and the need for reliable automated inventory system.

Analyze

The analyze stage showed that the main root causes of the problem are the manual management of asset inventories, the lack of a standardized process across buildings, and the absence of a centralized system for OT asset visibility. These conditions lead to inaccurate and outdated information, inconsistent practices between sites, and delays in identifying assets affected by cybersecurity vulnerabilities. As a result, the current process increases operational risk and limits effective lifecycle management.

The fishbone diagram (see figure 2) highlights the root causes contribution to the lack of visibility and inefficiencies in OT asset management, categorized across People, Process, Method, Data, Management, and Cybersecurity risk. From a people perspective, limited accountability, and inconsistent data ownership affect the reliability of asset information. Process related gaps, such as manual updates, lack of standardization, and fragmented workflows, further contribute to delays and errors. Method and data issues, including inconsistent formats, incomplete records, and absence of centralized systems, reduce data accuracy and usability. Additionally, management factors like lack of governance and prioritization limit sustained improvements, while cybersecurity risk concerns emphasize delayed vulnerability identification and response. Overall, the diagram illustrates that the problem is multifactorial, driven by both operational inefficiencies and systems gaps, reinforcing the need for a centralized, standardized approach to OT asset management.

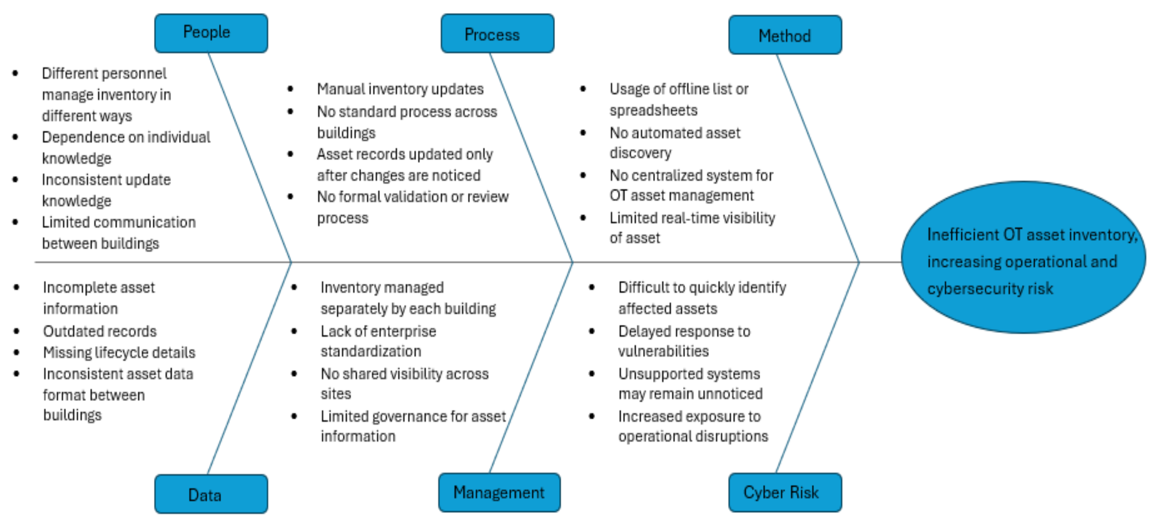

Figure 2
Fishbone Diagram

Improve

The improvement stage focuses on designing the future state solution for the centralized infrastructure OT asset management. A proposed architecture diagram was developed to show how asset information from each manufacturing area and building will be collected, standardized, and stored in one centralized system. This solution will replace manual and segregated inventories with an automated process that improves visibility, data accuracy, lifecycle tracking, and cybersecurity response. The improved design will also define standard asset data fields, user access needs, reporting capabilities, and potential integrations with cybersecurity and maintenance tools. A pilot implementation can be completed in one selected area to validate the solution, measure improvement, and confirm that the centralized system reduces manual effort and supports faster decision-making.

Figure 3 illustrates the proposed infrastructure architecture, showing how OT asset data will move from manufacturing areas into a centralized inventory platform through automated collection, standard data fields, and validation steps. This platform will serve as the single source of truth for IT/OT, Engineering and Cybersecurity teams, supporting lifecycle tracking, vulnerability identification and response, dashboards, reporting, and action tracking. The centralized system eliminates the need to physically enter manufacturing areas to collect asset information, replacing manual inventory checks with automated asset discovery and centralized reporting.

Figure 4 illustrates the proposed future-state process for OT asset management. Asset information is first collected through automated discovery and then validated using standardized data fields. Once validated, the information is stored in the centralized inventory platform, where dashboards and reports can be used by IT, OT, Engineering, and Cybersecurity teams. The data then supports lifecycle planning, vulnerability response, troubleshooting, and periodic review activities. This process creates a continuous cycle that helps maintain accurate and current asset information.

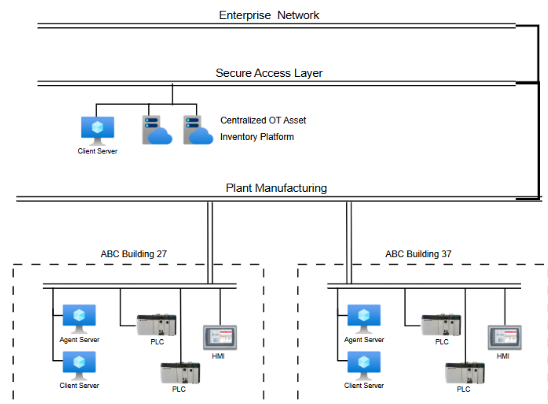

Figure 3
Infrastructure Architecture Diagram

Figure 4
Future State OT Asset Management Process Flow Diagram

This improvement directly addresses the concerns identified by providing accurate, current and complete asset information. It gives Engineering faster access to asset details for troubleshooting and support, while enabling Cybersecurity to identify vulnerable or unsupported assets more quickly. To evaluate the effectiveness of the proposed solution, key performance indicators should be monitored before and after implementation, including inventory accuracy, time required to update inventory records, percentage of assets with complete lifecycle data, and response time to cybersecurity vulnerability alerts.

Control

In the control stage, the focus is on sustaining the improvements achieved through the implementation of the centralized OT asset management system. This includes maintaining accurate, visible asset information, ensuring consistent use across buildings, and supporting lifecycle and cybersecurity risk management. Standard practices, defined responsibilities, and continuous monitoring are necessary to keep the process effective over time and preserve the process effective over time and preserve the benefits of the project.

To sustain the improvement, asset governance should be established through defined ownership, periodic reviews, and required data standards. Each manufacturing area should have an assigned responsible owner to validate asset information and ensure that changes are reflected in the centralized system. The system should include mandatory asset data fields such as asset name, location, IP address, model, firmware version, lifecycle status, support status, area owner, and cybersecurity risk status. These required fields help standardize the information collected across buildings and reduce incomplete or inconsistent records.

A periodic review process should also be implemented to verify the accuracy and completeness of the centralized inventory. Monthly or quarterly reviews can be used to identify missing fields, outdated lifecycle information, unsupported firmware, inactive assets, and assets exposed to cybersecurity vulnerabilities. These reviews should involve IT, OT, Engineering, and Cybersecurity teams to ensure that the inventory remains useful for maintenance planning, troubleshooting, vulnerability response, and lifecycle decision-making.

In addition, inventory updates should be connected to the site change management process. When new OT assets are installed, upgraded, replaced, or removed from service, the centralized inventory should be updated as part of the change documentation. This control prevents the system from becoming outdated and ensures that the asset inventory continues to reflect the actual manufacturing environment. Dashboards, reports, and automated alerts can also be used to monitor inventory completeness, lifecycle status, and cybersecurity exposure.

The control plan outlines how these improvements will be maintained, and defines the data used to verify that the centralized OT asset management process remains effective, consistent and sustainable across the site. See Table 4.

Table 4
Control Plan

CONTROL DATA	METRIC / MEASURE	MONITORING METHOD	FREQUENCY	RESPONSIBLE OWNER	OBJECTIVE
Asset Visibility	Percentage of OT assets visible in the centralized system	Review of system inventory records	Monthly	IT/OT Teams	Ensure complete asset visibility
Inventory Accuracy	Percentage of assets with correct and updated information	Validation of asset records against system changes	Quarterly	IT/OT Teams	Maintain reliable asset data
Standardization	Compliance with standardized asset data structure across all buildings	Review of required fields and naming consistency	Annually	IT Team	Ensure consistency across sites
Lifecycle Management	Percentage of assets with lifecycle status and version information available	Review of lifecycle-related records	Quarterly	IT/OT Teams	Support proactive lifecycle planning
Cybersecurity Risk / Manufacturing Support Response	Time required to identify assets for manufacturing support or affected by a vulnerability	Review of response records during support / cybersecurity events	Quarterly	Cybersecurity/ Engineering Teams	Improve mitigation response time
System Adoption	Number of buildings using the centralized system	Access and usage review	Monthly	IT Team	Confirm effective implementation
Process Sustainability	Compliance with update and review practices	Periodic audit of process execution	Quarterly	IT Team	Prevent returning to manual practices

CONCLUSION

In the investigation process, several gaps were identified in the current process for managing OT asset inventory and lifecycle information. These gaps included lack of centralized information, manual effort to build and maintain inventories, limited enterprise level visibility, and inconsistencies across buildings. It was also identified that customers need accurate, complete and reliable OT asset information to support maintenance activities, system upgrades, troubleshooting, cybersecurity vulnerability management, and lifecycle decisions. The problem definition, identification of customer needs, and the analysis of current gaps were all supported through the application of the DMAIC methodology.

Based on these findings, a centralized system is proposed as the main improvement to standardize the process across all buildings, provide easier access to asset information and reduce manual inventory efforts. This solution would improve data accuracy, increase enterprise visibility, support faster decision making, and reduce operational and cybersecurity risks.

REFERENCES

[1] J. M. Juran, A. B. Godfrey, R. E. Hoogstoel and E. G. Schillig, Eds., *Juran's Quality Handbook*, 5th ed. McGraw-Hill, New York, NY, 1999.

[2] International Society of Automation, ISA/IEC 62443-3-3: *System Security Requirements and Security Levels*, Research Triangle Park, NC, 2013.

[3] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security,* NIST Special Publication 800-82, Gaithersburg, MD, 2022.

[4] J. R. Evans, *Managing for Quality and Performance Excellence,* 12th ed. Cengage Learning, Boston, MA, 2024.

[5] M. L. George, J. Maxey, D. Rowlands, and M. Price, *The Lean Six Sigma Pocket Toolbook: A Quick Reference Guide to Nearly 100 Tools for Improving Process Quality and Speed,* First Edition, McGraw-Hill, New York, NY, 2004, pp. 1-72.