

**Enterprise Architecture of
Danforth Manufacturing Company**

Gabrielle Decker
Spencer Gilbert
Emily Ramirez
Kati Rosquist

OSU Institute of Technology
ITD-3453 Information Systems Architecture
Dr. Darren Waldrep
August 17, 2025

Table of Contents

Table of Contents.....	2
Introduction	3
Line of Business.....	3
EA Components.....	4
EA6 Level 1: Strategy and Goals.....	4
EA6 Level 2: Business Services and Processes	5
EA6 Level 3: Information and Data	7
EA6 Level 4: Systems and Applications	9
EA6 Level 5: Technology and Infrastructure	12
EA6 Level 6: Security and Privacy	14
Conclusion.....	15
References	17

Introduction

The following analysis offers a top-down description of the enterprise architecture for Danforth Manufacturing Company (DMC) using the Enterprise Architecture 6-level (EA6) framework, with a focus on the Manufacturing Operations line of business (LoB). EA6 consists of six levels that link business strategy and organizational objectives with the supporting processes, data, systems, and infrastructure (The Open Group, 2011). A recurring challenge within DMC, which involves multiple business areas requesting overlapping technology, serves as the motivation for adopting a structured EA approach. An organized repository of artifacts has been established to align requirements and solutions across the EA6 layers in order to improve planning and oversight. In addition, because the Manufacturing Operations LoB combines Information Technology (IT) with Operational Technology (OT) for shop-floor control and automation, recognized OT security practices have been considered alongside existing institutional policies to promote reliability and data protection (Stouffer, et al., 2023).

DMC manufactures photovoltaic storage cells for consumer, commercial, and aerospace customers, making Manufacturing Operations a primary value driver for the organization. The LoB must plan, schedule, execute, and verify production activity while capturing accurate shop-floor data that supports downstream functions such as Sales and Finance. A roadmap that connects current-state artifacts with target-state scenarios guides investment decisions and provides measurable outcomes aligned with business goals (The Open Group, 2011). Emphasis is placed on bridging legacy systems with advanced Industry 4.0 practices so that DMC can gain near real-time visibility into operations and analytics. Such visibility is essential to improving quoting accuracy, production throughput, cost control, and overall competitiveness under market pressures (Theunissen, 2021).

The overarching EA approach is designed to benefit both executives and operational teams by presenting architecture content according to the EA6 levels. Each level offers DMC-specific artifacts chosen to avoid unnecessary repetition while still clarifying how strategy, processes, data, systems, and technology must interoperate. Particular attention is also given to security and privacy requirements as outlined by institutional policies. Techniques from established frameworks, such as The Open Group Architecture Framework (TOGAF), serve to maintain coherence and consistency in how the enterprise architecture is defined and managed (The Open Group, 2011). By aligning these practices to DMC's manufacturing needs, resilience, safety, and data protection become integral goals of the architecture rather than novel or separate considerations.

Line of Business

Manufacturing Operations at DMC transforms engineered designs and raw material inputs into finished photovoltaic storage products that meet performance, quality, delivery, and cost objectives. This business unit is accountable for planning orders, sequencing production, verifying quality, and capturing historical data that informs downstream costing and sales commitments. A clear challenge is the lack of real-time visibility into production schedules and inventory availability, limiting Sales in providing accurate quotes. This information gap causes both customer-facing issues, such as order delays, and internal planning inefficiencies (Theunissen, 2021). A more unified information environment is expected to resolve these concerns by integrating Manufacturing, Sales, and Finance around shared data, standardized processes, and appropriately governed systems.

Two critical, vertical components reside under Manufacturing Operations leadership. The first, shop-floor automation and control, covers Supervisory Control and Data Acquisition (SCADA) and Human-Machine Interface (HMI) systems, Programmable Logic Controllers (PLCs), robotics, test stands, and process historians. These technologies ensure that machines operate with consistent throughput and traceability while adhering to safety standards. The second vertical component is the Manufacturing Execution System (MES), which manages work-in-progress (WIP) tracking, quality checks, labor and machine time capture, and nonconformance workflows. Both of these systems include both OT and IT elements, so they require strict control over interfaces and network access points, as examined in detail at the technology and security layers (Stouffer, et al., 2023).

Besides the vertical components, two cross-functional frameworks connect Manufacturing Operations with other LoBs to drive enterprise-wide value. One framework coordinates with a Sales and Inventory Tracking System (SITS) to supply accurate real-time availability, ensuring that sales representatives can provide immediate and valid quotes to customers. The other framework interfaces with Finance, offering standardized cost-accounting data that details labor, materials, inventories, and rework or scrap at a granular level. Through a consolidated EA approach, these solutions are planned to avoid duplication of effort and system integration overhead, leading to better return on investment and decision-making alignment across all functions (The Open Group, 2011).

Each of these architecture components is further mapped in the next sections of the EA6 framework. The final objective centers on ensuring that Production, Sales, and Finance have consistent and trustworthy operational data whenever they require it. By methodically aligning each LoB service, each data entity, and each technology investment with overarching corporate strategy, the enterprise can effectively eliminate the visibility gap that currently hinders competitiveness in the market (Bernard, 2020).

EA Components

DMC's approach to enterprise architecture, rooted in the EA6 method, begins at the strategy and goal level then proceeds through business services, information assets, software applications, and technology infrastructure. By uniting these layers, decision-makers and solution teams can spot overlaps in technology requests, align on capabilities, and enhance security controls without compromising plant performance (The Open Group, 2011). The EA repository, informed by content management principles from TOGAF, offers structure for storing artifacts and clarifies governance by showing how each architectural element relates to strategic objectives.

EA6 Level 1: Strategy and Goals

A central objective for Manufacturing Operations is to reduce lead times, increase quoting accuracy, and define the true cost-to-serve model for production activities. Achieving these objectives supports improved profitability, streamlined order fulfillment, and higher win rates by furnishing the Sales team with precise data on production schedules and available inventory (The Open Group, 2011). DMC's leadership has sanctioned a segmented EA program specifically for the production and finance domains, enabling a methodical approach to technology investments with minimal redundancy. As

initiatives progress, each proposed change is tied to the established strategic goals through an internal governance process that scrutinizes benefits, risk exposure, dependencies, and resource allocation.

A concise Gantt chart or similar roadmap can illustrate how initiatives are timed, demonstrating how earlier efforts (such as enabling visibility of WIP through the MES) provide inputs for downstream activities (like real-time quoting in SITS). Through outcome metrics, executive decision-making is better informed by measuring improvements in areas like on-time shipment rates, labor cost variances, and scrap percentages. Portfolio management can further use these metrics to refine capabilities and incorporate feedback from the shop floor or the finance department. By connecting strategy directly to funded initiatives, DMC ensures that the architecture aligns with genuine business value rather than merely technical expediency.

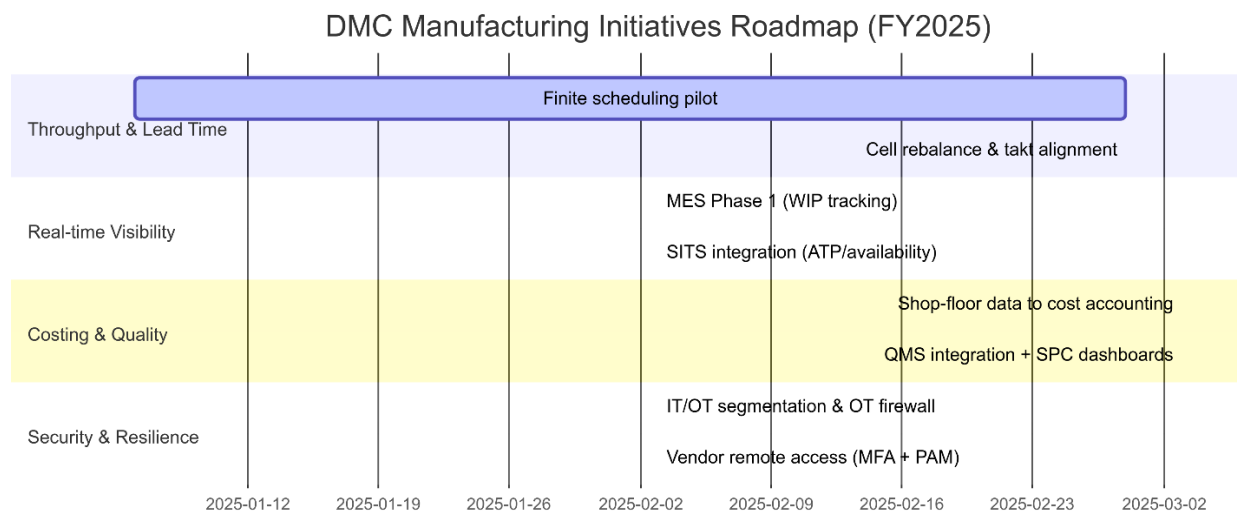


Figure 1 Artifact — Level 1: Gantt Chart (Initiative Roadmap). [View on Mermaid.js](#).

The Working Group's approach helps leadership see how recommended strategies play out under different market scenarios. Such planning provides a level of resilience in that resource reallocation or project reprioritization can occur if market conditions suddenly shift. Tying each strategic promise to business metrics and progressively reviewing results can also foster a culture of accountability. Overall, Level 1 in EA6 ensures that every subsequent architectural element remains firmly aligned with DMC's most critical goals (The Open Group, 2011).

EA6 Level 2: Business Services and Processes

Manufacturing Operations delivers capabilities like Production Planning, Finite Scheduling, and Quality Assurance that jointly translate demand into tangible products. At this level, each discrete service is documented with inputs, outputs, ownership, and functional goals (The Open Group, 2011). Production Planning rationalizes overall demand against available raw materials, workforce availability, and production lines. Finite Scheduling refines the plan for shorter intervals, considering real-time equipment status or other constraints. Quality Assurance imposes checks for incoming materials, outgoing products, and any nonconforming items that must be tracked or reworked.

Maintenance activities ensure that factory assets remain reliable and capable of meeting throughput targets. Materials Handling organizes stock movements, while Continuous Improvement employs data-driven insights for discovering process inefficiencies. Visualizing how these services interrelate through a unified taxonomy clarifies roles such as who is responsible for scheduling or how nonconformance data should flow to the right people. Many frameworks, including TOGAF, encourage establishing a shared business language that identifies consistent service categories, which aids in cross-LoB integration and fosters more robust security safeguards (The Open Group, 2011).

Diagrammatic representations, such as an overview of services in Unified Modeling Language (UML) format, often help clarify these processes for a broad audience. Managers and executives can quickly identify groups responsible for each process, as well as pinpoint critical dependencies or bottlenecks that might hinder lead-time reduction efforts (Theunissen, 2021). By refining business services first, the architecture ensures that each subsequent data, applications, and infrastructure decision aligns directly with operational goals. This approach provides a stable foundation that is less likely to be disrupted by vendor changes or internal reorganizations, since the business services remain the anchor for how work is done.

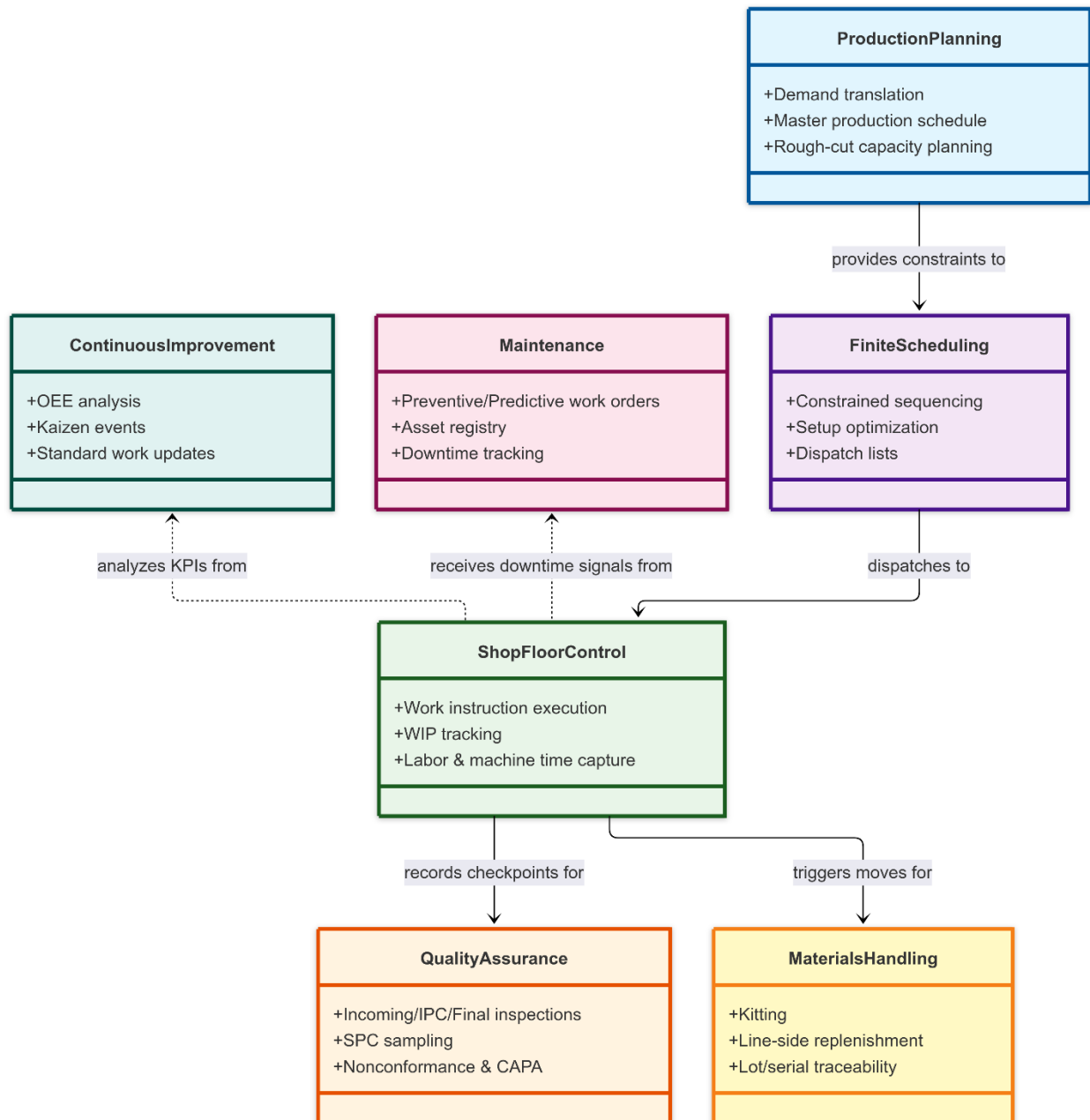


Figure 2 Artifact — Level 2: UML Class Diagram (Service Taxonomy and Relationships). View on [Mermaid.js](https://mermaid.js.org).

Articulating each service in detail both facilitates compliance with institutional policies and supports well-defined service-level objectives. For example, the process of capturing real-time WIP data has immediate implications for data classification and stewardship, which must be addressed at the infrastructure and security layers. Ultimately, a coherent set of business services and processes lays the groundwork for a resilient and efficient manufacturing organization (The Open Group, 2011).

EA6 Level 3: Information and Data

Information management is essential for coordinating accurate production schedules, cost accounting, and quality tracking across various LoBs. In Manufacturing Operations, critical entities

include Work Orders, Operations, and Inventory Lots, supported by the Bill of Materials and Routings that instruct how products move through the plant (The Open Group, 2011). Canonical definitions and naming conventions for these entities reduce integration friction, so Sales and Finance receive consistent data when calculating item availability and costing. Quality records and sensor readings must also be stored securely for traceability and improvement initiatives.

Entity-Relationship (ER) diagrams characterize how these information elements link to each other, making it easier for system owners to evaluate the impact of system or process changes. Supplementary artifacts, such as Data Flow Diagrams (DFDs), show how data travels among the MES, SITS, and cost-accounting modules via an integration broker that resides in the Industrial Demilitarized Zone (DMZ) (Stouffer, et al., 2023). In addition, metadata about data classification and lifecycle management clarifies who is authorized to access which data attributes. Policies on confidentiality, integrity, and availability provide the backdrop for these discussions, ensuring that privacy requirements are part of design considerations.

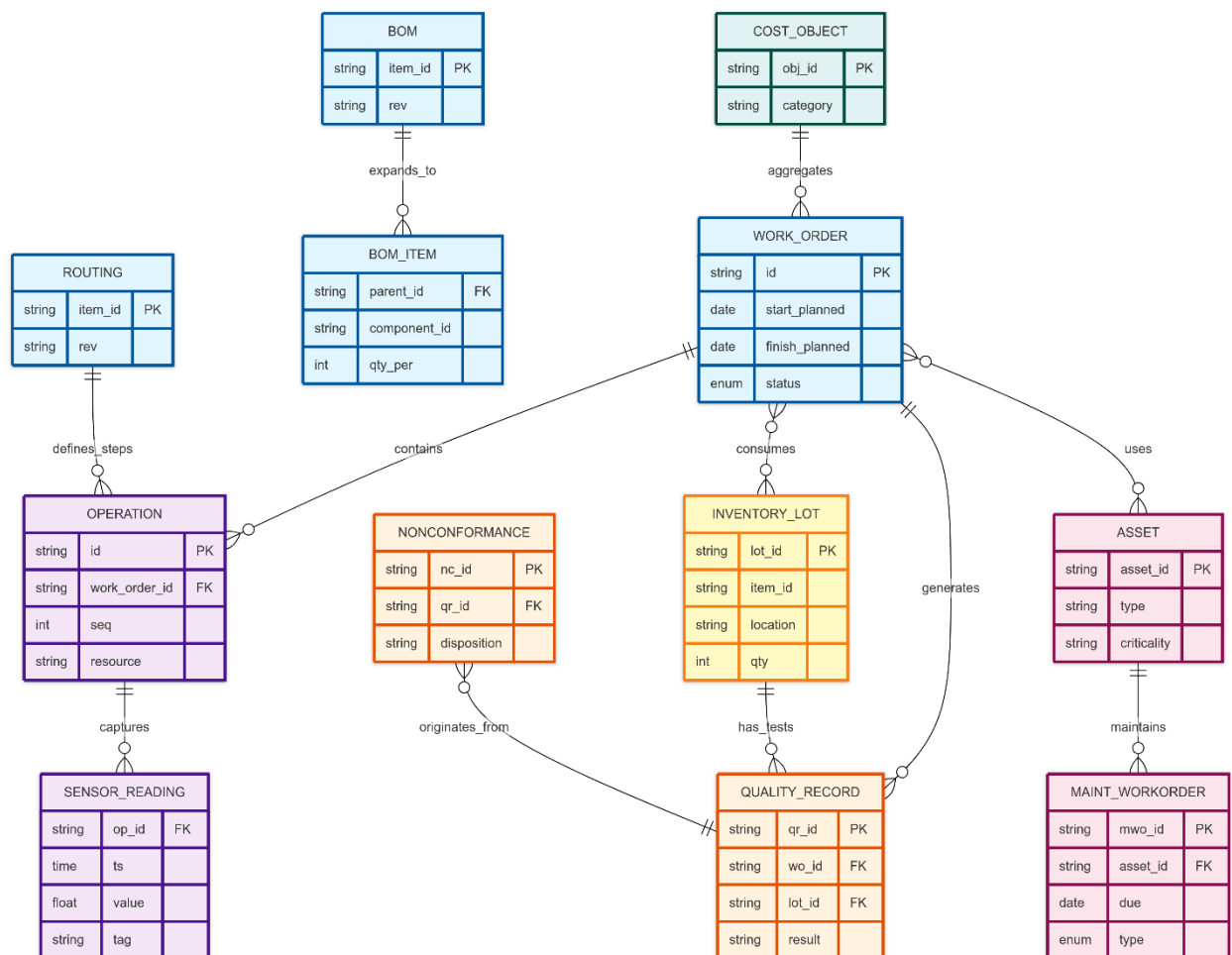


Figure 3 Artifact — Level 3: ER Diagram (Canonical Manufacturing Data). View on [Mermaid.js](#).

Where operational technology data moves into enterprise systems, the architecture employs constrained conduits—preferably with unidirectional gateways where data flows remain one-way—to

limit the risk of external threats compromising the factory environment (Stouffer, et al., 2023). The alignment of these data flows with the broader security posture helps protect both intellectual property and customer-driven information. This approach also supports compliance with internal data stewardship policies by clearly designating who manages each data entity through the entire lifecycle. By clarifying the data model and data flow, DMC stakeholders can design and manage solutions that are both precise and secure.

Statistical Process Control (SPC) readings, nonconformance logs, and any time-series data from factory sensors enrich the analytics capabilities for continuous improvement. These same data flows inform financial calculations and inventory adjustments, tying Level 3 directly to enterprise reporting. The result is a system of record that places data accuracy and timeliness at the forefront, fulfilling strategic objectives around traceability, improved quoting, and efficient cost management (Theunissen, 2021).

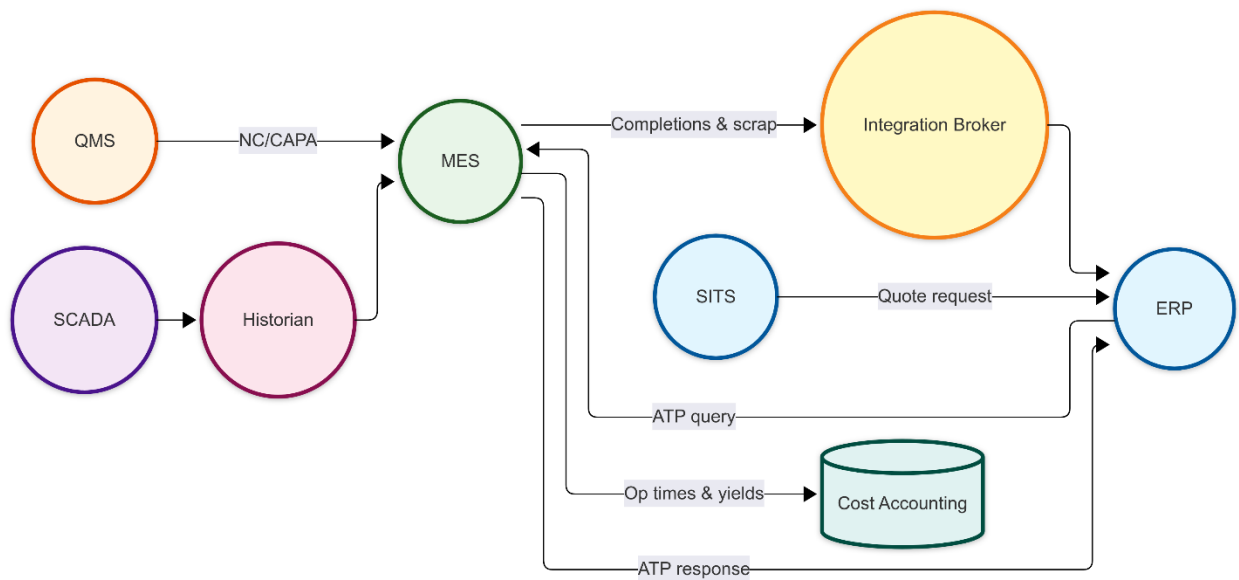


Figure 4 Data Flow Diagram. [View on Mermaid.js](#).

EA6 Level 4: Systems and Applications

Systems and applications serve as the functional engines of the enterprise architecture. DMC's Enterprise Resource Planning (ERP) solution manages order intake, inventory, and standard costing for Finance, while the MES focuses on work-in-progress, dispatching, and unique data feeds from the shop floor. A Quality Management System (QMS) handles nonconformance, corrective actions, and statistical charts, and a Computerized Maintenance Management System (CMMS) organizes preventive and predictive maintenance plans. The Sales and Inventory Tracking System (SITS) provides real-time quoting and visibility for external customers, relying on published data from MES and other relevant applications (Bernard, 2020).

Application interactions can be visualized with a C4 Container Diagram or a comparable representation, showing how each system stores, processes, and shares information (The Open Group,

2011). An event-driven integration broker coordinates data exchanges through approved application programming interfaces (APIs) or scheduled workflows, ensuring coherent transaction integrity. Key performance indicators (KPIs) are derived in specialized analytics layers that consolidate data from multiple sources, including the process historian, which collects sensor data from the OT environment.

Enterprise Architecture of Danforth Manufacturing Company

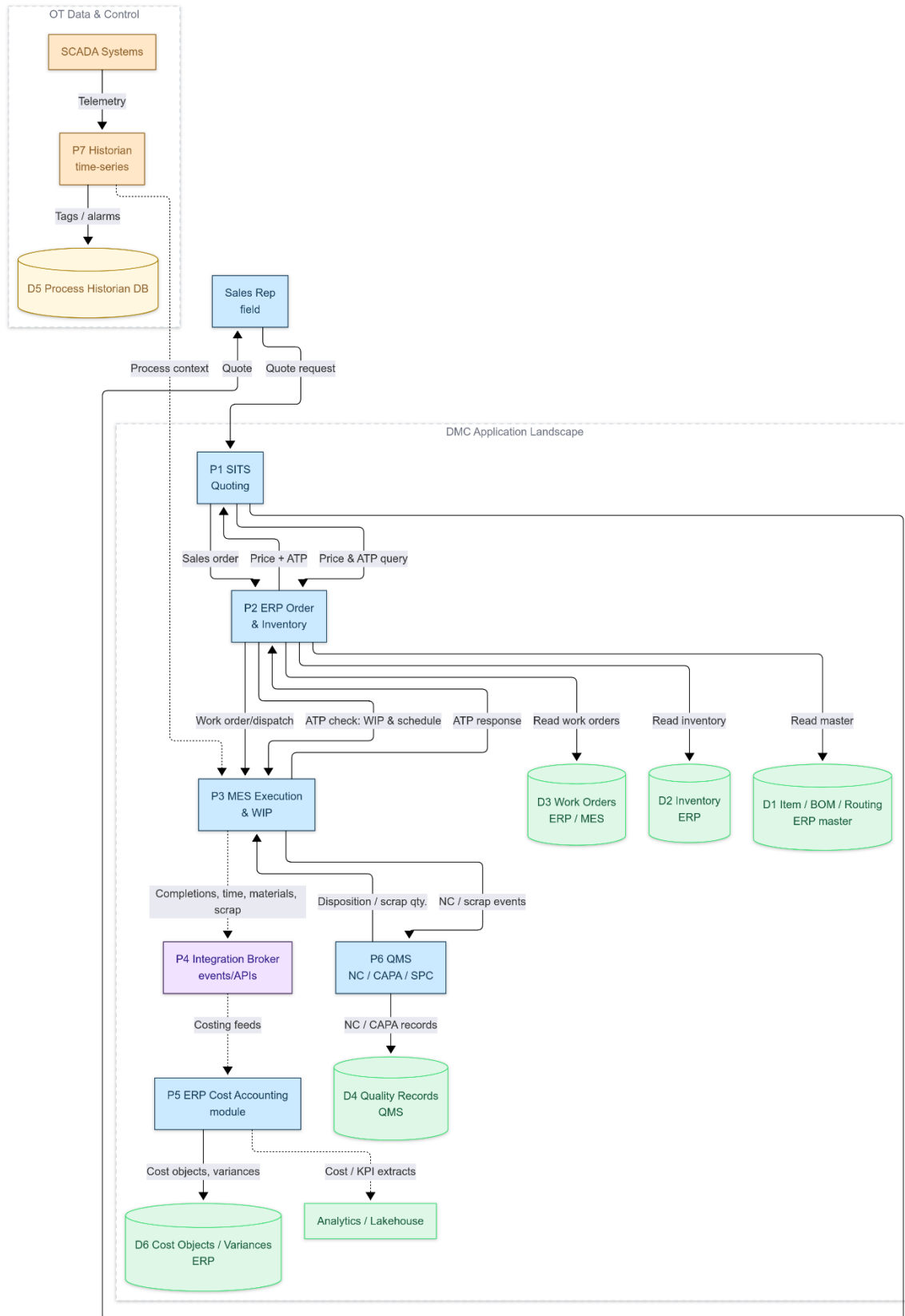


Figure 5 EA6 Level 4: Application Interaction Map (System Landscape). [View on Mermaid.js](#).

Ownership and access responsibilities for each system are clarified in a responsibility matrix, where primary custodians handle authoritative data updates, and secondary custodians rely on these updates to perform related tasks (OSU-IT, 2021). This approach avoids ambiguous ownership and simplifies tasks like provisioning or deprovisioning accounts, especially in high-impact systems such as SCADA/HMI gateways or historian servers (Stouffer, et al., 2023). Proper implementation of least-privilege and role-based access ensures that data integrity is maintained across tightly integrated domains.

System controls further incorporate separation of duties, multi-factor authentication (MFA) for privileged functions, and periodic logging and review of user activities. By applying these principles consistently, DMC balances usability with a robust security posture that safeguards both IT and OT assets. Furthermore, a comprehensive repository tracks each application's compliance status, facilitating audits and enabling incremental improvements whenever a new policy or standard is introduced (OSU-IT, 2021).

EA6 Level 5: Technology and Infrastructure

The final EA6 layer addresses the hardware and network environment required to support DMC's application portfolio. Office, manufacturing, and Industrial DMZ networks are segmented through firewalls that default to deny-all, thus limiting unauthorized east-west or north-south traffic (Stouffer, et al., 2023). The OT environment, containing PLCs, SCADA/HMI clusters, and testing racks, is further subdivided to prevent risks from proliferating across manufacturing cells. Intrusion detection systems (IDS) are placed at the boundary and in select internal segments to observe malicious or anomalous behavior in real time.

These technical controls reflect guidance in institutional policies that mandate firewall rules for device authorization, centralized logging, and the ability to quickly quarantine or remove non-compliant devices (OSU-IT, 2019). Additionally, the technology layer ensures that remote vendor access is carefully channeled through a jump host in the DMZ, requiring MFA, auditable sessions, and time-limited approvals. This approach respects the criticality of OT systems as they underpin production, thereby reducing potential disruptions to real-time control processes (Stouffer, et al., 2023).

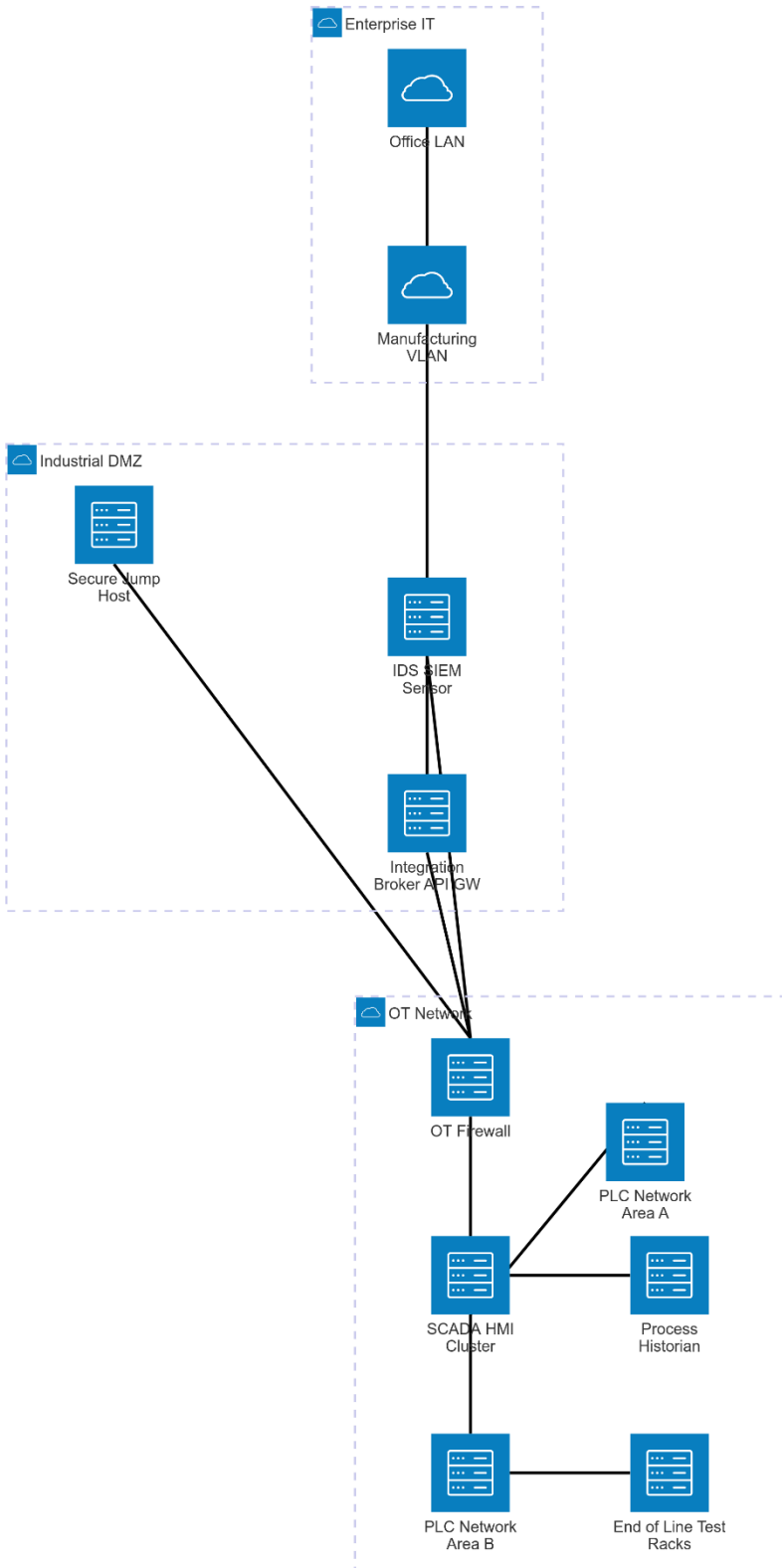


Figure 6 Artifact — Level 5: Architecture Diagram (IT/OT Segmentation and Controls). [View on Mermaid.js](#).

Centralized backups and patch management must accommodate OT-specific constraints by scheduling changes during maintenance windows and employing passive vulnerability scanning tools (OSU-IT, 2021). Active scanning may interfere with device operation, so scanning methods are adapted to avoid inadvertently halting production. Periodic tests of incident-response plans also confirm the environment's ability to detect and mitigate security intrusions without endangering employee safety or production continuity (Stouffer, et al., 2023).

Deploying these infrastructure components completes the link between strategy and execution, ensuring that the underlying technical environment can sustain DMC's goals for real-time visibility and cost transparency. By layering advanced security measures onto the infrastructure, the organization upholds a defense-in-depth model and meets high standards for availability and compliance.

EA6 Level 6: Security and Privacy

Security and privacy considerations receive special attention at each EA6 level. Institutional cyber resilience policies mandate an asset inventory, vulnerability remediation, segmentation of networks, and robust firewall controls (OSU-IT, 2021). These mandates dovetail with recognized guidance for Operational Technology, helping Manufacturing protect against malicious threats that could disrupt plant operations. Access control practices, including role-based permissions and multi-factor authentication, satisfy the institution's expectation that privileges remain aligned with the principle of least privilege and are re-evaluated upon employee transitions or departures (OSU-IT, 2020).

In the technology realm, segmented networks isolate office systems from more sensitive OT resources, mitigating the risk of lateral movement by malicious software (Stouffer, et al., 2023). Industrial DMZs shield critical PLC networks from direct internet exposure, and remote access must be approved and recorded to avoid unauthorized entry. Network security policies specify a deny-all default posture, requiring formal exceptions for data flows across the OT environment, which helps keep essential control processes stable and trustworthy (OSU-IT, 2019). Physical security measures cover locked enclosures for control devices and badge-only access to restricted areas.

Data stewardship policies require that information be classified according to its potential impact on confidentiality, integrity, and availability (OSU-IT, 2019). Manufacturing's operational data often involves real-time data from sensors, which is necessary for immediate process decisions, and customer-related data that must be protected from unauthorized disclosure. When integrated with business applications, these data sets are regulated by data custodians and subject to role-based constraints that limit exposure to sensitive material. Conformance with such policies ensures that investment in applications and technology aligns with both internal governance standards and external regulatory frameworks (OSU-IT, 2019).

Within the Manufacturing Operations environment, specialized OT adaptations include scheduling patch cycles carefully, employing passively monitored intrusion detection, and offering vendors only restricted remote support windows. These measures help ensure that essential systems keep functioning without risking performance or creating direct openings for intrusion. Security monitoring solutions are expanded at critical boundaries to detect device anomalies or traffic patterns

that raise potential concerns. By embedding these practices across every EA6 layer, DMC fosters a culture of resilience that anticipates threats and mitigates risks.

Policy-to-Control Traceability (selected examples)

In order to illustrate policy-to-control alignment, a traceability table links key policy mandates with the controls selected in DMC's enterprise architecture. For example, under the Cyber Resilience directive, DMC maintains a continuous asset inventory, performs vulnerability scans where feasible, and coordinates patching within a strict maintenance window (OSU-IT, 2021). The same policy enforces a deny-all-by-default firewall stance, so industrial DMZs and broker-mediated flows are deployed in the infrastructure design. Access Control Policy instructions guide the adoption of role-based groups in Active Directory and require immediate offboarding of separated staff, preventing unauthorized account retention (OSU-IT, 2020). These policies reflect recognized best practices for both IT and OT.

OSUIT Control Ref.	Key Requirement	Realization in DMC Architecture	Risk Addressed
Cyber Resilience 6-003	Asset inventories; vulnerability scanning; patch management	IT CMDB; passive OT discovery; maintenance window scans; documented patch orchestration	Unknown/unsupported assets; unpatched vulnerabilities
Cyber Resilience 6-003	Deny all by default firewalls; segmentation	Industrial DMZ; OT firewall rules; minimal conduits; broker mediated flows	Lateral movement into PLC networks
Access Control 6-015	Least privilege; separation of duties; provisioning/deprovisioning	Role based AD groups; JIT elevation; HR triggered offboarding	Excess privilege; orphaned accounts
Network Security 6-005	Central device authorization; monitoring; ability to disconnect	Approved network gear only; monitoring taps; disconnect playbook	Rogue/compromised devices in IT/OT

Figure 7 Policy-to-Control Traceability Matrix

Network Security guidelines ensure that only approved network equipment connects to the production environment and that advanced monitoring can detect and isolate anomalous traffic (OSU-IT, 2019). This approach limits the risk of a compromised device pivoting into high-value OT controllers or exposing sensitive production data. Aligning policies with functional controls thus reduces the possibility that critical security steps will be overlooked. Clearly documented traceability also improves audit readiness by providing direct evidence that DMC's architecture meets institutional, regulatory, and operational requirements (Stouffer, et al., 2023).

Conclusion

Applying the EA6 framework at DMC has created a structured enterprise architecture that spans strategy, business processes, data, systems, and infrastructure for the Manufacturing Operations line of business. By anchoring technical decisions in strategic objectives, the organization clarifies how automation systems, applications, and data structures must interact to address real-time quoting,

accurate costing, and continuous operational improvements (The Open Group, 2011). The vertical components of shop-floor automation and MES provide critical production data, while cross-functional integrations with Sales and Finance promote consistent insights and financial accountability.

Unique artifacts at each EA6 level illustrate the progression from top-level business goals to day-to-day operational workflows. At the same time, security and privacy are integrated into every layer, reflecting current institutional policies and recognized guidance for OT environments (Stouffer, et al., 2023). Firewalled network segments, regulated access privileges, and comprehensive data stewardship enforce defense-in-depth while ensuring that essential processes remain stable. Implementing these measures helps DMC maintain competitiveness in a rapidly evolving market, perform strategic investments in technology, and reduce costly inefficiencies tied to quoting errors or data silos.

By consolidating the efforts of diverse functional teams into a single architectural repository, the organization can track where investments overlap, identify potential system conflicts, and apply capital more effectively. The capital planning process benefits from clear linkages between proposed improvements and measurable outcomes, including reduced lead times, more reliable cost models, and better alignment between manufacturing capacity and customer demands (Theunissen, 2021).

References

- Bernard, S. A. (2020). *An Introduction to Holistic Enterprise Architecture* (4th ed.). Authorhouse.
- OSU-IT. (2019, December). *Data Stewardship Responsibilities, Guidelines, and Classification Policy (Policy 6-014)*. OSU Institute of Technology, Technology Services. Retrieved from OSU Institute Of Technology: osuit.edu/about/administration/files/6-014-data-stewardship-rev-dec-2019.pdf
- OSU-IT. (2019, December). *Network security (Policy No. 6-005)*. OSU Institute of Technology, Technology Services. Retrieved from osuit.edu/about/administration/files/6-005-network-security-rev-dec-2019.pdf
- OSU-IT. (2020, December). *Access control policy (Policy No. 6-015)*. OSU Institute of Technology, Technology Services. Retrieved from osuit.edu/about/administration/files/6-015-access-control-tech-services-12-2020.pdf
- OSU-IT. (2021, June). *Cyber Resilience (Policy No. 6-003)*. OSU Institute of Technology, Technology Services. Retrieved from osuit.edu/about/administration/files/6-003-osuit-cybersecurity-resilience-policy.pdf
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., . . . Thompson, M. (2023, September). Guide to Operational Technology (OT) Security (NIST Special Publication (SP) 800-82r3). doi:10.6028/NIST.SP.800-82r3
- The Open Group. (2011). *TOGAF Version 9.1. (Document G116)* (1st ed.). Zaltbommel: Van Haren Publishing.
- Theunissen, C. (2021). *Enterprise Architecture Within the Manufacturing Industry*. [Student thesis: Master's Thesis, Open University of the Netherlands]. Retrieved from research.ou.nl/en/studentTheses/enterprise-architecture-within-the-manufacturing-industry