Introduction

For this blog series, we use a fictious specialty manufacturing company called Alpha Nine Fabrication, Inc. (ANF) that fabricates parts for aircraft, heavy duty vehicles and industrial equipment. Job bid requests are received via email and when approved are passed through the fabrication design, specification, fabrication, Q/A, packaging and shipping processes. The process is largely automated though the use of CAD/CAM software that is run on locally hosted servers. Automated CNC machining equipment is used to turn raw materials into finished parts that are assembled into finished product. The basic process consists of the following steps:

1. **Design (CAD)**: A 3D model of the desired part is created using CAD software according to customer order specifications.

2. **Programming: Computer-Aided Manufacturing (CAM)**: CAD files are translated into G-code that contains instructions for the CNC machining in computer readable formats.

3. **Setup** – Raw material is selected, cutting tools are chosen and the tooling is calibrated.

4. **Manufacturing** – Using G-code, material is cut, shaped and formed to specification. Parts are assembled into final form and prepared for finishing and quality control.

5. **Finishing** – Product is sanded, polished, painted, powder-coated or plated to create finished product.

6. **Quality Control** - Throughout the process, checks are performed to ensure the part meets specifications and has the correct dimensions and tolerances.

7. **Packaging and Shipping -** The final product is packaged and sent to the customer.

In addition to the core manufacturing process, financial accounting software manages the invoicing, billing and payment processes. These processes are hosted on a cloud-based SAAS system in addition to corporate administration processes that include email, ERP/CRM and HR.

Cybersecurity compliance requirements

ANF recently received multiple US Department of War (DoW) contract awards for the production of military aircraft parts and specialized terrain vehicles. These contacts are conditional on receiving CMMC Cybersecurity certification to CMMC level 2 with expectations for follow on contracts will require CMMC level 3 certification. Core requirements are related to the handling of Controlled Unclassified Information (CUI) consisting of:

- Orders sent via email that contain specifications for parts production that contain CUI information
- Maintaining CUI data protection requirements throughout the design, manufacturing and shipping processes.
- Maintaining CUI data protection requirements for order processing, invoicing and accounting functions that process CUI information

In preparation for achieving the level 2 certification, ANF has prepared a comprehensive plan in the form of a System Security Plan (SSP) that encompasses all phases of CMMC CUI handling requirements. These include:

- Encryption of email correspondence from government sources that transmit CUI
- Secure storage and encryption of all product specifications and design documentation
- Encryption of all CAD/CAM files (including CAD/CAM drawings and specifications, manufacturing G-Code and related files
- Secure handling of CUI and related data throughout Alpha Nine's OIT (Operations Information Technology) operations that includes programming and DEVSECOPS processes
- Secure handling of CUI throughout the manufacturing process that spans shop floor, robotics, materials processing, finishing, packaging and delivery handling

A master CUI data flow diagram has been created that maps the transmission and processing of CUI information. This flow diagram is used as the basis to determine AN's network structure consisting of Process Control, CAD/CAM systems, manufacturing systems, cloud service provider interfaces, accounting and plant and administrative operations physical security. This includes the definition of security enclaves and DMZ structures.

Network Infrastructure

The ANF network is divided into six network zones all segregated by network firewalls.

- Secure Business (SECBUS)
- CAD/CAM (CADCAM)
- Shop Floor (SHOPFLOOR)
- Security Operations (SECOPS)
- Operations Information Technology (OIT)
- Corporate Business (CORP)

The CAD/CAM, Shop Floor, Secure Business and SECOPS networks are structured to meet CMMC CUI compliance data protection requirements. The network zones are interconnected through firewall network connections. Highlights of each network segment follow.

CAD/CAM (CADCAM)

The CAD/CAM network contains the systems used for CAD/CAM operations. Six Apple Mac Studio-based workstations (five user and one backup) are used for CAD/CAM applications consisting of parts design, modeling, specification and CAM code generation. A server is utilized to provide common file storage, deployment of encryption software, file transfer functions to the SHOPFLOOR network and utilities needed for managing the environment.

All CAD/CAM files are encrypted with 256-bit storage encryption and files are encrypted when in transit. The primary application used by CAD/CAM engineers is Autodesk Fusion 360 that executes locally on workstations. The core process used involves the receipt of job tickets generated in the SECBUS network that have attached specification files received from ANF customers.

When the product design is completed, generated G-code/M-code and associated files are securely transferred to the SHOPFLOOR network along with the updated job ticket for production purposes. An in-house program is used to transfer the job ticket and files to the SHOPFLOOR server and triggers a message to the SHOPFLOOR supervisor that alerts when a new job is ready. The transfer program uses secure FTP (to 256-bit encryption standard) and does not rely upon email. Microsoft Project is used for project management functions.

Secure Business (SECBUS)

The Secure Business network is used to handle secure communications with ANF customers and consists of secure email, order processing, job ticket generation and related accounting functions (invoicing, payment processing, general accounting). A secure email process that uses an internally hosted, hardened email server is used to receive email and attachments sent to the SECBUS zone. These are authenticated, cross checked upon receipt to verify for known sources and scanned for viruses. File attachments are also checksum verified if check sums are provided by the sender. Any suspicious email is immediately quarantined and flagged for investigation. Once the email receipt processing is completed, ANF order processing personnel prepare the order and generate a job ticket that is used to track the production process.

ANF uses the cloud-based Microsoft Dynamics Government 365 software for accounting and general business functions. All ANF access to the Microsoft Azure cloud-based services is supported via a secured gateway connection hosted in a separate demilitarized zone (DMZ) that interconnects to all of the ANF network zones.

Shop Floor Control (SHOPFLOOR)

The Shop Floor Control network zone is used to control the production process. A server stores job tickets and g-code CAM files that are used by CNC machines to produce product

components. CNC Technicians have software tools that are used to modify g-code files and update job tickets, as needed. A version control system is used to track G-code files as they are developed and modified. Shopfloor machine log files are stored locally for reference by Shop Floor technicians and forwarded to the central log server on the SECOPS network zone. A Shop Floor control workstation is used by Shop Floor technicians to access Shop Floor system applications. Each CNC machine has a control panel that is used to control machining functions. A locally developed custom software agent runs on the control panels that decrypts G-Code files as they are ingested and handles event log generation to the Shop Floor logging server.

Assembly line production and Q/A processes are largely manual-based due to the nature of the custom products that ANF produces. Microsoft-based workstations connected to the SHOP Floor server are utilized for job ticket tracking, event logging and record keeping purposes of the results of the assembly line process.

Security Operations (SECOPS)

The Security Operations network zone houses cybersecurity related systems including authentication, centralized event logging and management, intrusion detection / prevention (IDS/IPS) and Security Operations Center (SOC) functions. Microsoft Active Directory (AD/DS) is deployed on a centralized Microsoft server supports all local AD functions and supports a gateway link to the Microsoft Azure cloud service for cloud AD management purposes. Active Directory is deployed in a hybrid internal Cloud, cloud service provider-based structure. An internal Active Directory server deployed in the SECOPS network zone supports local authentication services to internal secured zones and interfaces to the Microsoft Azure cloud for cloud-based functions.

Utility security functions for physical access control and video surveillance are contained in the SECOPS network zone. Workstations are used by ANF security OIT personnel to manage the SECOPS environment.

Operations Information Technology (OIT)

The Operations Information Technology network zone supports operations and information technology functions of the organization. ANF management combines Operations Technology (OT) and Information Technology (IT) into one organization called OIT. The emphasis is on support for the core mission of the organization to fabricate and manufacture highly customized products for industry. The OIT zone supports DEVSECOPS functions, computer programming and system development functions for the organizations.

Included is a locally hosted GITHUB server that supports local software development. A set of workstations are deployed for software development purposes. The OIT group is responsible for developing and maintaining all system security functions including network

design, firewall configuration and rule sets, authentication functions (user management, roles, passwords, key management, etc.), encryption management, management of interfaces (internal and external) and management of all event logging functions (system security event logs, application event logs, etc.).

Corporate Business (CORP)

The above network zones are interconnected to a corporate network zone (CORP) that supports corporate management systems. This connection is made through a Demilitarized Zone (DMZ) that contains the necessary interconnection systems to allow secure interchange of corporate information. No Controlled Unclassified Information (CUI) is interchanged between secured zones and the corporate network zone. Any CUI data that is required by the CORP network is sanitized prior to transmission. Corporate applications include office automation (Microsoft 365 cloud-based), Enterprise Resource Management (ERP), Customer Relationship Management (CRM) and corporate accounting.

System Interconnections

SECBUS

connects to:

External Email Clients - to receive secure emails from government customers. Emails are received via secure internet connections and sent to the internal SECBUS email server.
CAD/CAM – to send job tickets created from external clients email
SHOPFLOOR – to receive updates to and completed job tickets
SECOPS – for authentication request processing and receipts of authorizations (interface to Microsoft Active Directory)
DMZ - for general Internet connections including access to Microsoft Azure Office 365 government cloud (via DMZ) for general business applications access (CRM/ERP)
CORP – to send accounting related records for corporate accounting

CAD/CAM

connects to:

SECBUS – to receive Job Tickets and product order specifications
SHOPFLOOR – to send G-Code CAM files and receive updated G-Code files for modifications, receives connections to CAD/CAM server for reference specification files
SECOPS – for authentication request processing and receipts of authorizations (interface to Microsoft Active Directory)
DMZ - for general Internet connections

SECOPS

connects to:

SECBUS – supports inbound connections for authentication and event log data collection
CAD/CAM – supports inbound connections for authentication and event log data collection
SHOPFLOOR – supports inbound connections for authentication and event log data collection
OIT – supports inbound connections for authentication and event log data collection
DMZ - for general Internet connections including access to Microsoft Azure Office 365 government cloud (via DMZ) for general business applications access (CRM/ERP)

OIT

Connects to:

SECOPS – for authentication request processing and receipts of authorizations (interface to Microsoft Active Directory)
CAD/CAM - for sending / receiving programming updates, software releases
SHOPFLOOR – for sending / receiving programming updates, software releases
SECBUS - for sending / receiving programming updates, software releases
DMZ - for general Internet connections, access to Azure Government cloud for Office 365

DMZ

Description:

VPN-based servers hosted on hardened Redhat Linux systems are used to connect the DMZ to the CORP network and to the Microsoft Azure Government cloud. The Microsoft cloud connection is made through use of Microsoft ExpressRoute for secure direct connection via Internet service provider Spectrum.

- **Encryption**: MACsec for Layer 2 encryption is used for end-to-end IP-level encryption.
- **Security controls**: Azure Firewall or Network Security Groups (NSGs) are used to filter traffic and enforce security policies.

Connects to:

All Internal network zones
Microsoft Asure cloud via Microsoft ExpressRoute
Internet for general access

Role-based Access Control

All access to ANF systems are controlled by tightly managed role-based access control. Users are assigned access rights to the minimum levels only necessary to perform job functions

Privileged access to administrative functions are controlled though superuser logons that are used only for duration necessary to complete job tasks

Policies and Procedures:

- Provide an overview of the organization's security policies and procedures that govern its cybersecurity practices.
- Reference applicable policies and procedures that are relevant to the controls being implemented.

Roles and Responsibilities:

ANF roles and responsibilities are mapped to the organizational structure of the corporation.

ANF has a functional-based, hierarchical structure to ensure clear communication and efficient operations. It is headed by executives and divided into specialized departments that manage everything from initial customer orders to final product delivery.

Executive leadership
Executive leadership sets the company's overall direction, long-term strategy, and corporate culture.

- **CEO:** Principal decision-maker responsible for the company's vision, financial performance, and all operational results.
  - **Name:** Herbert K. Bardwell
  - **Title**: Chief Executive Officer (CEO)
  - **Department**: Corporate Management
  - **Phone Number**: 555-630-3300
  - **Email**: HBardwell@anfinc.com
- **Chief Operating Officer (COO):** Oversees the company's day-to-day operations, ensuring that all departments are running smoothly and efficiently.
  - **Name:** Albert Johnson
  - **Title:** Chief Operating Officer (COO)
  - **Department:** Operations
  - **Phone Number**: 555-630-3301
  - **Email**: AJohnson@anfinc.com
- **Chief Financial Officer (CFO):** Manages all financial aspects of the company, including budgeting, financial reporting, and forecasting.
  - **Name:** Alice Ford
  - **Title:** Chief Financial Officer

    - **Department:** Finance
    - **Phone Number**: 555-630-3302
    - **Email**: AFord@anfinc.com
- **Vice President Operations Information Technology**: Responsible for Operations and Information Technology systems and assets. Functions as Chief Information Officer (CIO) and Information System Owner
    - **Name**: Samuel Gruenfeld
    - **Title**: VP OIT
    - **Department**: Operations Information Technology (OIT)
    - **Phone Number**: 555-630-3303
    - **Email**: SGruenfeld@anfinc.com

Operations and production departments
This core division is the backbone of the company, responsible for manufacturing products efficiently and to specification.

- **Operations Manager:** Oversees all manufacturing processes, including production scheduling, machine utilization, and workflow optimization.
- **CNC Programming and Engineering:** Develops the computer-aided manufacturing (CAM) programs that run the CNC machines. This team also handles process engineering to improve efficiency and reduce costs.
- **Production Supervisors:** Manage the day-to-day activities on the shop floor, overseeing CNC machine operators, addressing issues, and ensuring production schedules and goals are met.
- **CNC Machine Operators:** The frontline workforce responsible for setting up, running, and monitoring the CNC machines to produce parts.
- **Maintenance:** A specialized team of technicians who perform preventative and emergency maintenance to keep all equipment running smoothly and minimize downtime.

Support departments
These departments work in concert with operations to provide necessary materials, ensure quality, and manage customer relations.

- **Operations Information Technology (OIT)**: Responsible for implementing and supporting all Operations Information Technology. This includes procurement, installation, maintenance and support for all computer-based equipment. The OIT group also include support for computer programming and cybersecurity functions.
    - **OIT Manager**: Manages all OIT related projects and on-going functions. This includes management of programming and technology support groups.
    - **SECOPS Manager**: Implements the SECOPS function that has responsibility for cybersecurity functions including defining and implementing cybersecurity controls, cybersecurity compliance program (includes risk assessments, controls implementation and monitoring, and conducting self-

assessments in preparation for external party audits) and implementing cybersecurity throughout the organization.

- **Quality Control (QC):** Conducts inspections and tests to ensure that all finished products meet strict quality standards and customer specifications.
    - **QC Manager:** Oversees all quality assurance procedures and manages a team of inspectors.
    - **QC Inspectors:** Perform in-process and final inspections of machined parts.
- **Sales and Marketing:** Responsible for securing new business, maintaining customer relationships, and managing existing client accounts. This team is the primary link between the company and its customers.
    - **Sales Manager:** Leads the sales team and manages major client accounts.
    - **Sales Engineers:** Work with customers to translate technical requirements into manufacturable parts.
- **Supply Chain and Procurement:** Manages the flow of materials, from sourcing raw materials to managing inventory and shipping finished products.
    - **Purchasing Manager:** Handles the procurement of all raw materials, tools, and outsourced services.
    - **Logistics Coordinator:** Manages the shipping and receiving of all goods.
- **Human Resources (HR):** Manages all aspects of the workforce, including recruiting, hiring, training, and managing employee performance

MES software

ANF uses Manufacturing Execution Management (MES) software to manage the manufacturing production process. ANF uses the factorylogix software package by Aegis Corporation for MES software functions.

Core functions of MES software:

- **Production control and scheduling:**
  Manages production dispatch, sequencing, and work orders to optimize the use of resources and personnel.
- **Data acquisition:**
  Collects real-time data from machines, sensors, and operators on the factory floor.
- **Quality management:**
  Monitors and enforces quality standards throughout the production process and helps manage product specifications.
- **Traceability and genealogy:**
  Tracks and documents every product and batch from raw materials to finished goods, which is crucial for compliance and recalls.
- **Performance analysis:**
  Analyzes key performance indicators (KPIs) such as Overall Equipment Effectiveness (OEE) to identify areas for improvement.
- **Resource management:**

Tracks the status and availability of equipment, tools, and personnel to ensure they are used efficiently.

- **Inventory and WIP tracking:**
  Monitors and manages work-in-progress (WIP) inventory as it moves through various stages of production.
- **Document management:**
  Controls and distributes production-related documents, such as standard operating procedures and recipes, to ensure consistency.
- **Maintenance management:**
  Supports maintenance operations and helps track equipment health.