Digitally Enabling the Supply Chain

Integrating Existing Tools and Capabilities to Guide Application

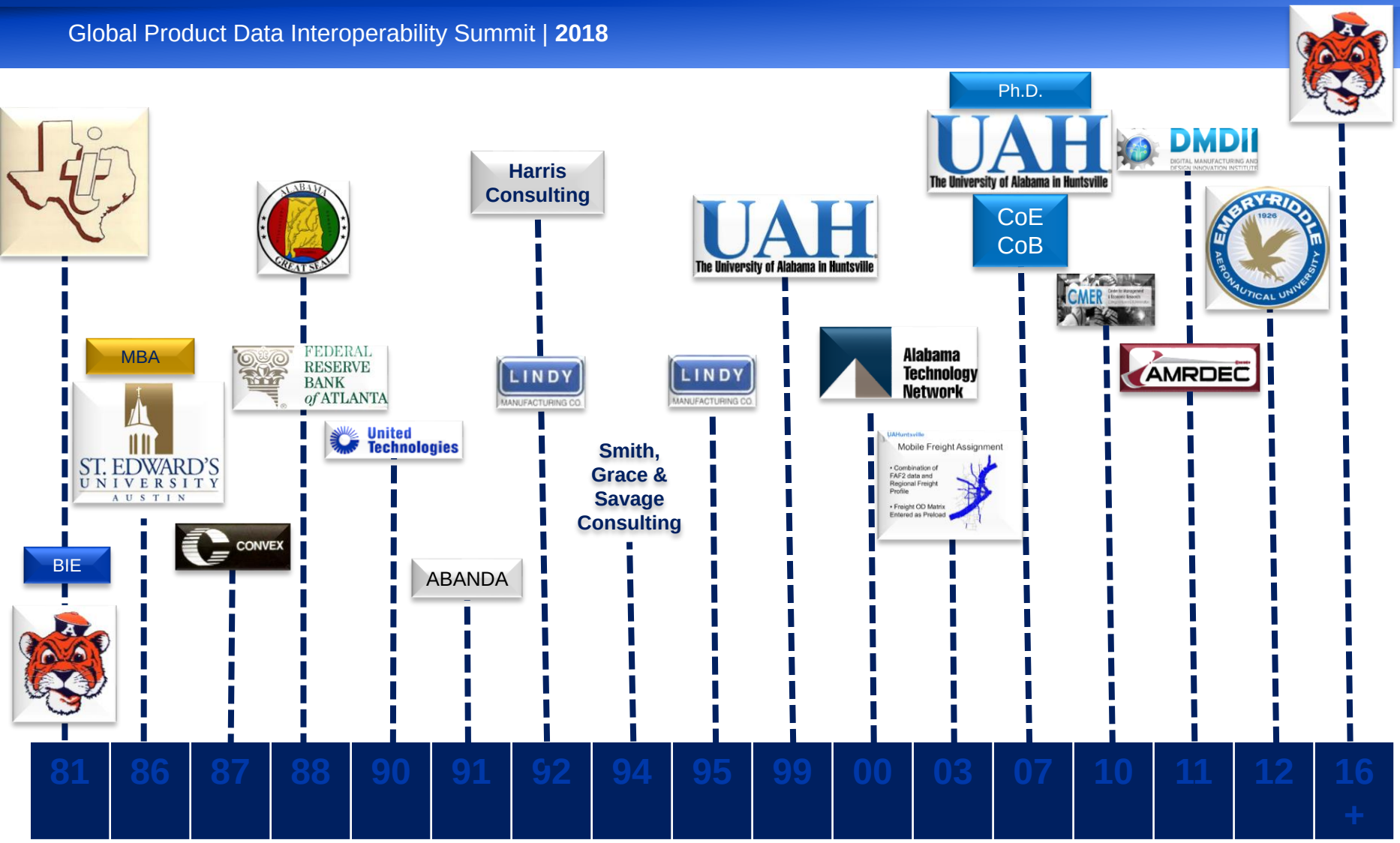
GLOBAL PRODUCT DATA INTEROPERABILITY

SUMMIT 2018

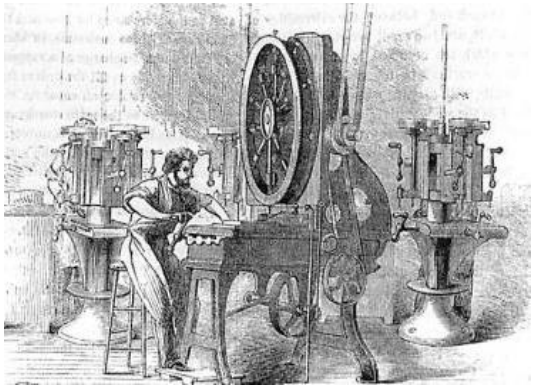
ELYSIUM Parker Aerospace NORTHROP GRUMMAN BOEING

My career timeline - Bio

Global Product Data Interoperability Summit | **2018**

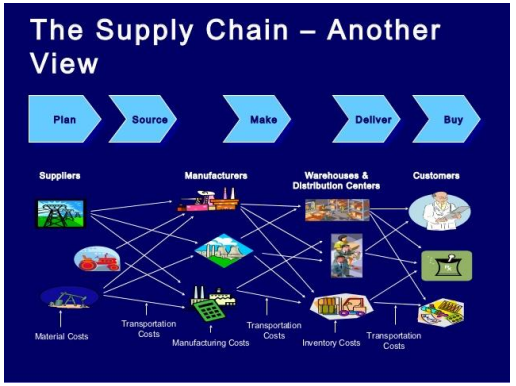


Manufacturing Data History



Antebellum Era of Manufacturing

Mass Production



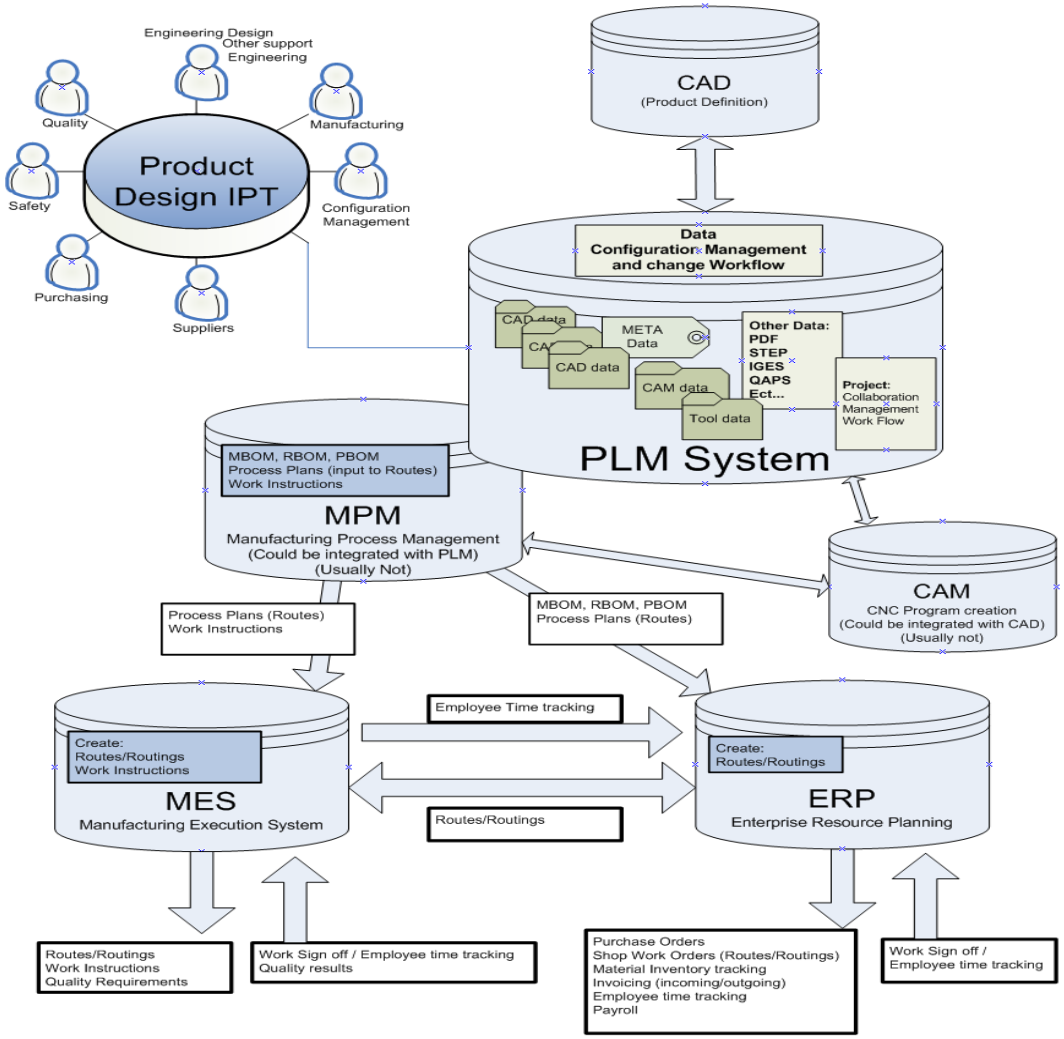
"One of the most noteworthy accomplishments in keeping the price of Ford products low is the gradual shortening of the production cycle. The longer an article is in the process of manufacture and the more it is moved about, the greater is its ultimate cost."

Henry Ford, 1926

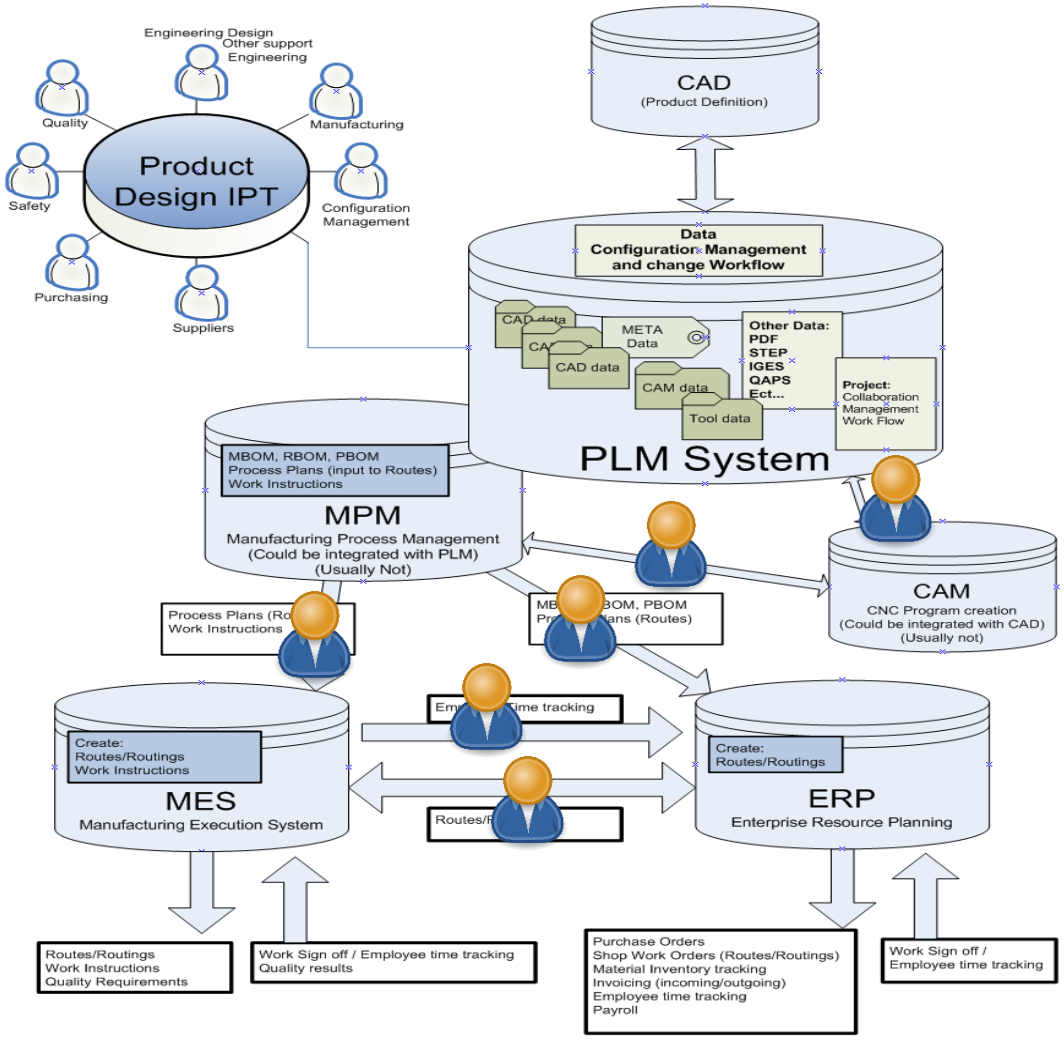
- Most engineering and manufacturing activities relied on 2 Dimensional (2D) drawings in hardcopy or digital form

- Today, it is possible to perform most engineering functions using data models

Manufacturing Networks – What we think we have



Manufacturing Networks – What we really have



The Cyber Security Problem

- Defense contractors throughout DoD's supply chain have been targeted by cyber criminals attempting to steal unclassified technical data.
- Protecting the operational systems of a manufacturing enterprise presents a new and different set of challenges. Technical data must be protected from theft, alteration, and impairment or denial of process control
  - These concerns are especially challenging for small and mid-size manufacturers.

- Manufacturing is consistently one of the most targeted sectors for cyber attack.
  - *"Attackers tend to go after systems that can be successfully compromised, and ICS [industrial control systems] have shown themselves to be a target-rich environment." McAfee 2012*
  - Over 70% of the attacks examined in 2012 were of low or moderate sophistication. As Verizon puts it, "Would you fire a guided missile at an unlocked screen door?"

NDIA, Cyber Security for Manufacturing, 2014

Manufacturing Needs and Priorities Differ from Business IT Systems

- Large companies are confident in their risk management posture but are concerned about suppliers.
  - Supplier vulnerabilities could become their vulnerabilities.

- Industrial Control Systems (ICS) that control these processes typically
  - Run specially designed operating systems and communications protocols
  - Handle real-time processing and synchronization needs
  - Have a lifetime on the order of 15-20 years
  - Are rarely rebooted or stopped to install patches
  - Depend on networked sensor feedback
  - Can have catastrophic physical safety consequences if they are compromised.
  - Outages may need to be scheduled weeks in advance.

- While cybersecurity is deeply ingrained in the IT culture, the Operations Technology (OT) culture is focused first and foremost on safety and availability of factory systems for production output.

- Technicians, including those from the original manufacturer, often have administrator privileges, and use them creatively to keep the machines running.

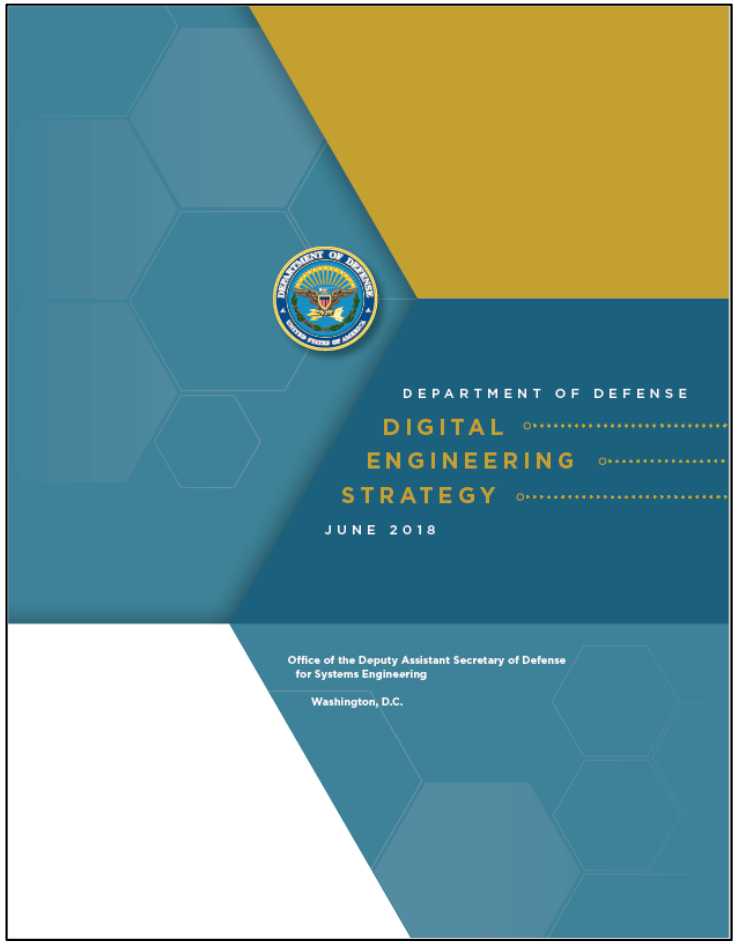
- Cybersecurity features were not a high priority when there was an air gap between ICS networks and other networks in the enterprise.

NDIA, Cyber Security for Manufacturing, 2014

DoD Digital Engineering Strategy

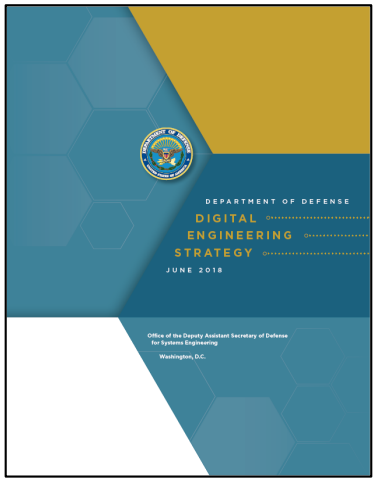
Global Product Data Interoperability Summit | **2018**

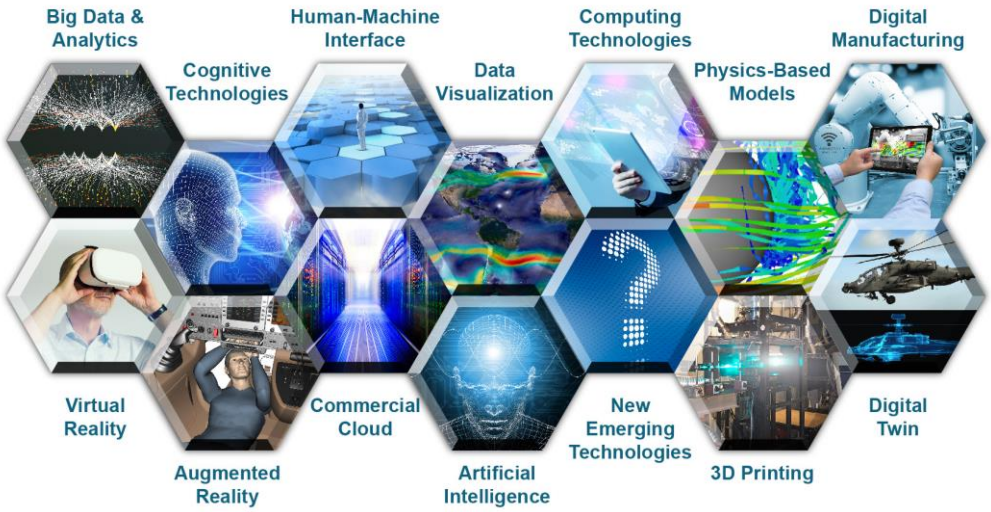
- To help ensure continued U.S. technological superiority, the Department is transforming its engineering practices to digital engineering, incorporating technological innovations into an integrated, digital, model-based approach.
- DoD defines digital engineering as an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.
- DoD's approach is to securely and safely connect people, processes, data, and capabilities across an end-to-end digital enterprise.

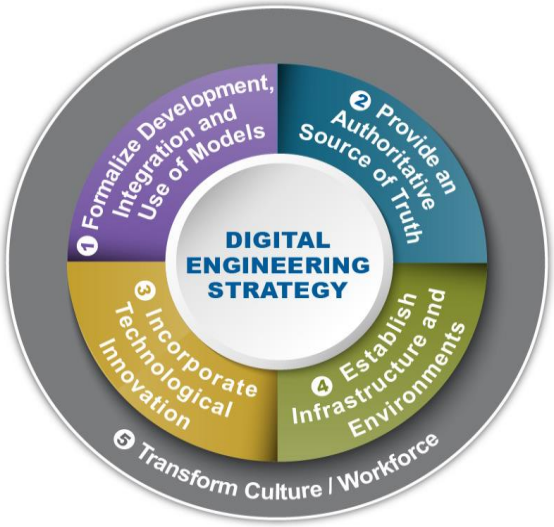


DoD Digital Engineering Strategy Goals

1. Formalize the development, integration, and use of models to inform enterprise and program decision making.
2. Provide an enduring, authoritative source of truth.
3. Incorporate technological innovation to improve the engineering practice.
4. Establish a supporting infrastructure and environments to perform activities, collaborate, and communicate across stakeholders.
5. Transform the culture and workforce to adopt and support digital engineering across the lifecycle.

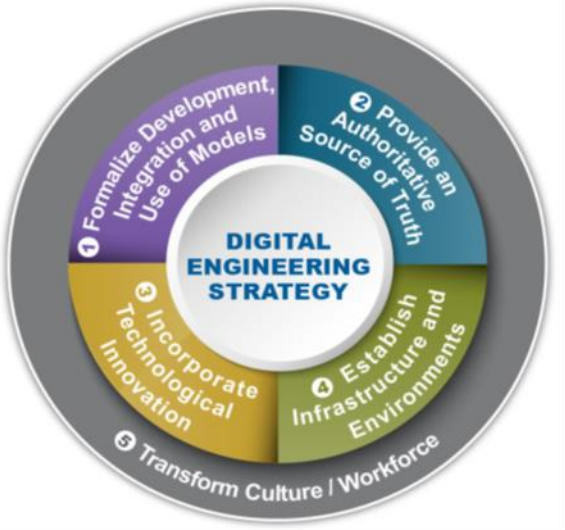






Office of the Deputy Assistant Secretary of Defense for Systems Engineering, June 2018

DoD Digital Engineering Strategy Goal Focus



1. This goal focuses on the formalized application of modeling to support all the system lifecycle phases from concept through disposal.

2. This goal provides the authoritative source of truth for stakeholders across organizations to access, manage, protect, and analyze the models and data.
   - The primary means for communication moves away from static and disconnected artifacts and shifts the paradigm to models and data serving as the basis for connecting traditionally siloed elements and providing an integrated information exchange throughout the lifecycle.

3. This goal is designed to enable DoD organizations to maintain technological superiority by innovating rapidly and providing access to and use of advanced technologies.
   - This goal infuses advancements in technology and practice to build an end-to-end digital enterprise.

4. This goal focuses on building digital engineering infrastructures and environments to support all of the digital engineering goals.
   - Current DoD IT infrastructures and environments do not fully support digital engineering stakeholder needs.

5. Takes a deliberate and systematic approach to planning, implementing, and supporting the DoD's digital engineering transformation.

Digitally Enabling the Supply Chain - Project Team

- DMDII (Digital Manufacturing Design & Innovation Institute) is a National Manufacturing Institute engaged in the digitalization of manufacturing.
- The project will create a roadmap and set of playbooks for Original Equipment Manufacturers (OEMs) and Small/Medium Manufacturers (SMMs) to guide the implementation of secure digitally-enabled supply chain practices and technologies.

Rockwell Collins

Raytheon

lucrum the group

NIST National Institute of Standards and Technology U.S. Department of Commerce

MBD 360

ITI International TechneGroup

The Problem

- Communications inefficiencies increase costs and time while stymying innovation.
- NIST research indicates that these challenges contribute to a $1 billion per year cost to the U.S. automotive supply chain.[1]
- Reduction in lead time and error rate have long been goals of manufacturers and a significant contributor to long lead times and increasing errors are interoperability problems between systems in the design, manufacture, deliver, and sustainment processes and is a significant source of pain, difficulty and increased costs.
- Even with a sustained effort by industry to become model centric, there is still a significant manual intervention in the supply chain to adapt to a Model Based Enterprise environment.
- Most collaborative exchanges around technical data are executed via unstructured communications and unstructured data does not easily allow for capture, analysis and re-use.

[1]*NIST Interoperability Cost Analysis of the U.S. Automotive Supply Chain*

Why Try?

- There is anecdotal evidence of the benefits of MBE and connecting within the digital thread.

- Areas in which there has been evidence of improvement include:
  - The elimination or reduction in the need to re-create downstream models,
  - Reduction in cycle time and costs,
  - Reduction in the risks of introducing downstream errors,
  - Increases in part yield,
  - Production of parts that meet customer requirements and expectations.

- There has not been a comprehensive effort to pull together and integrate the previous work performed by DoD, ManTech, NIST, DMDII and industry that produced tools and capabilities for providing a step by step approach to developing digital capability for supply chain engagement.

- There has never been a true implementation guide created and shared with all of industry, especially one that targets the SMMs.

- This project will weave together the good work that has been performed until now and create a picture of the digital thread in a manner designed to accelerate the depth and breadth of adoption.

Methodology

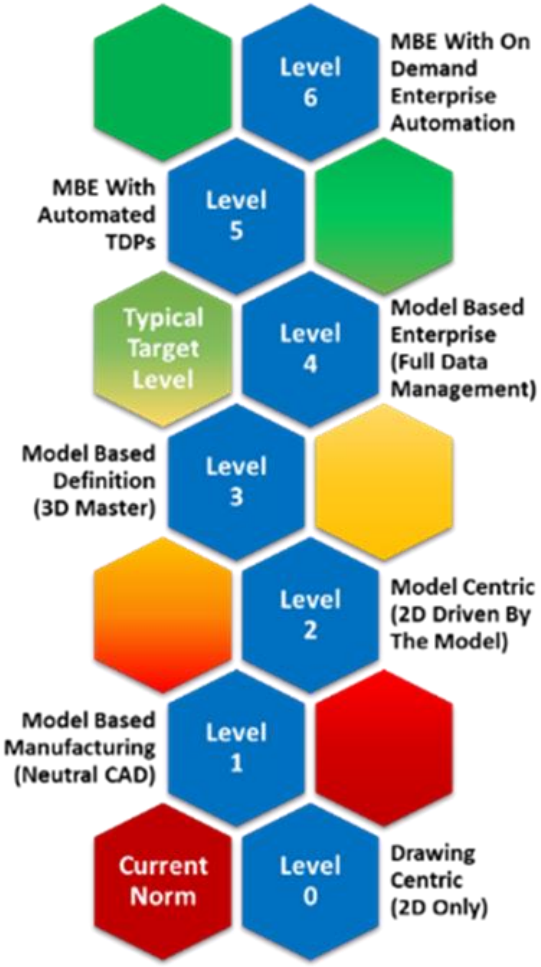
- Incorporate existing tools and technologies developed to create a roadmap and set of playbooks for Original Equipment Manufacturers (OEMs) and Small/Medium Manufacturers (SMMs) to guide the implementation of secure digitally-enabled supply chain practices and technologies.
- Examine and define the current and desired state of digitally-enabled supply chain practices and technologies in both commercial and defense supply chains.
- Document issues, pain points, current supply chain practices, identify critical information flows, and prioritize the gaps in technology that hinder the creation and adoption of a digitally enabled supply chain.
- Establish the business case and identify the corporate, individual and financial incentives to implement the guidance and adopt the frameworks and applications.
- Review the current state of model-based technology solutions and standards that affect how data is created, transferred and consumed within the supply chain.
- Address the supply chain for both new and legacy parts.

Major Issues Categories

- **Interoperability**
- **Data Reuse, Communication, and Archiving**
- **Advanced Manufacturing Vulnerabilities**
- **Analysis**
- **Infrastructure**

Future State of MBE Capability - (What is needed)

- More than just replacing drawing type information exchange to include design intent and context.
- Robust interoperability among disciplines and organizations.
- Responsive and adaptive to the changing market place and technology.
- Improved product life cycle time and costs.
- A building block for accelerating the maturation of the full MBD schema and communications across silos.



Summary

- DMDII 17-01 is a effort to develop as complete a picture as possible in the adoption and implementation of digital manufacturing capabilities in the commercial and defense supply chains.
- The team will pull in as many of the appropriate completed projects and technologies as possible in this project. Feel free to reach out and participate.
- It is my opinion that the efforts made here to remove inefficiencies and wastes from the flow of data and information in our product and system realization systems will be the next big productivity revolution in the US.

QUESTIONS?

Thank You!

Gregory A. Harris, Ph.D., P.E.
greg.harris@auburn.edu