Nathan W. Hartman, Ed.D.

SECURING DIGITAL PRODUCT DATA THROUGH THE SUPPLY CHAIN IN A PLM ENVIRONMENT

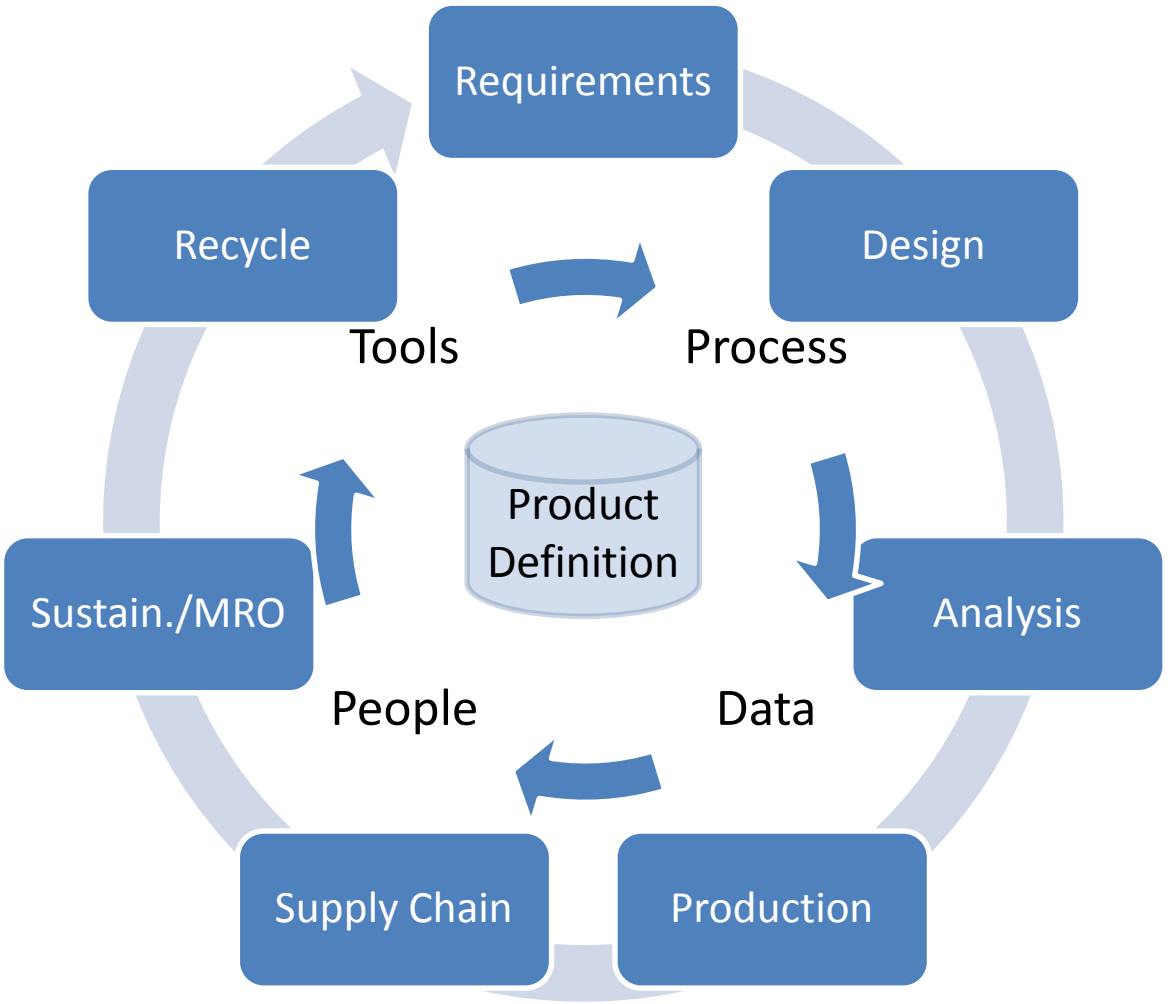
PURDUE
POLYTECHNIC

PLM
PURDUE
CENTER

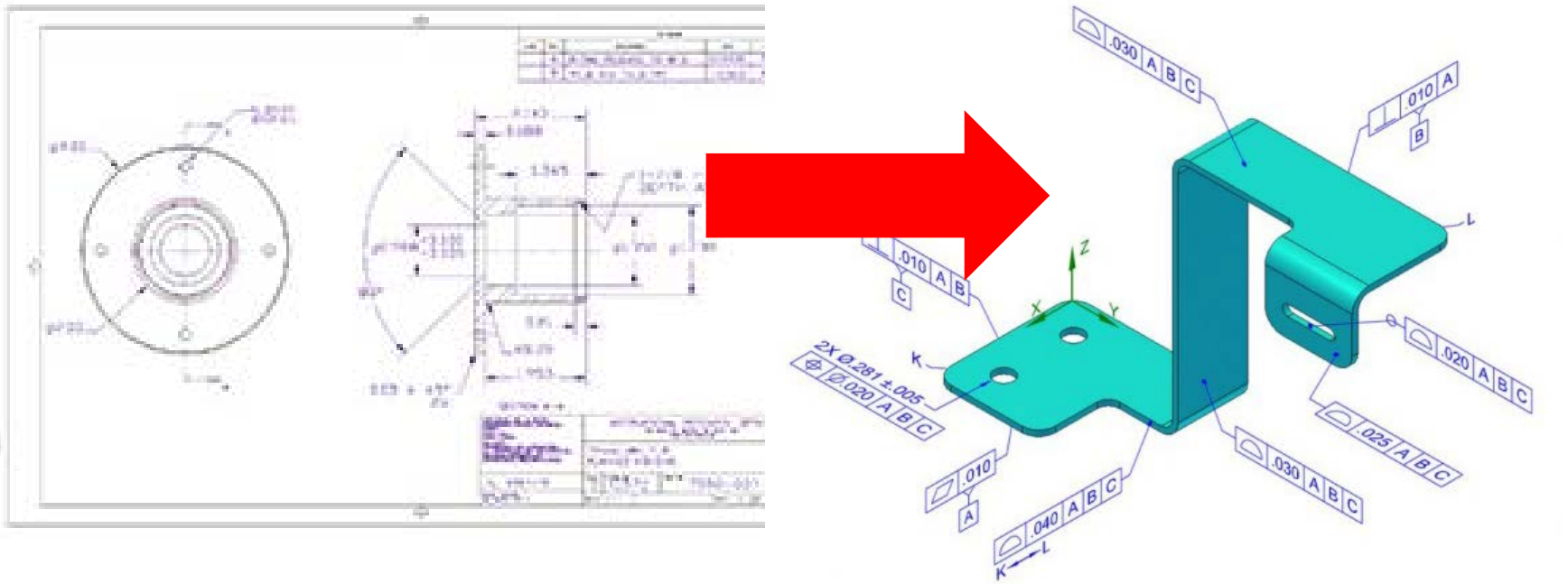
What is PLM?

The digital product definition forms the core of how product and process information is moved through an organization

- Business Metrics
- Communication
- Security
- Interoperability
- Behavior



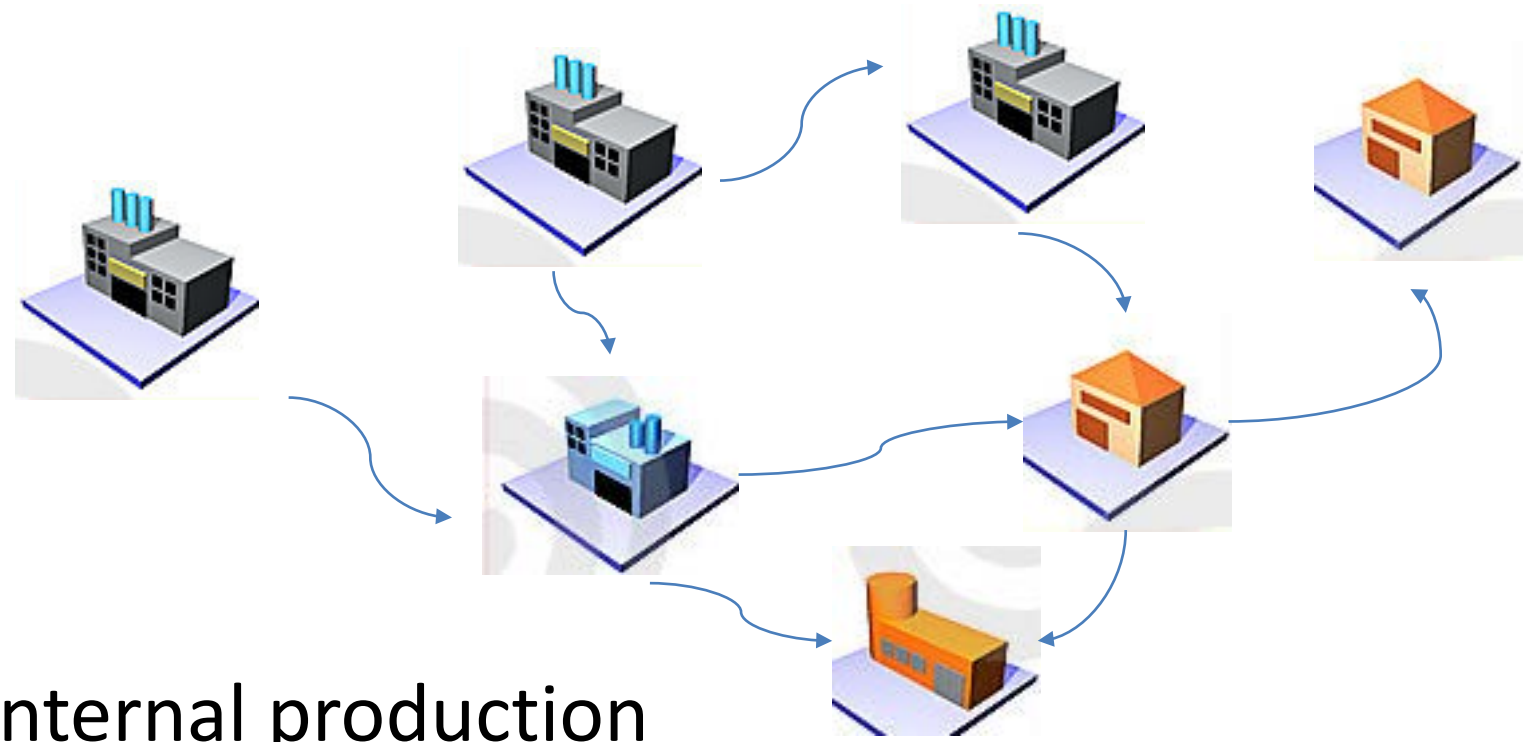
What does MBD mean?



For many people, it is a matter of whether they are an author or a consumer. MBD is fundamental to successful PLM, but it is more than a proxy for a drawing.

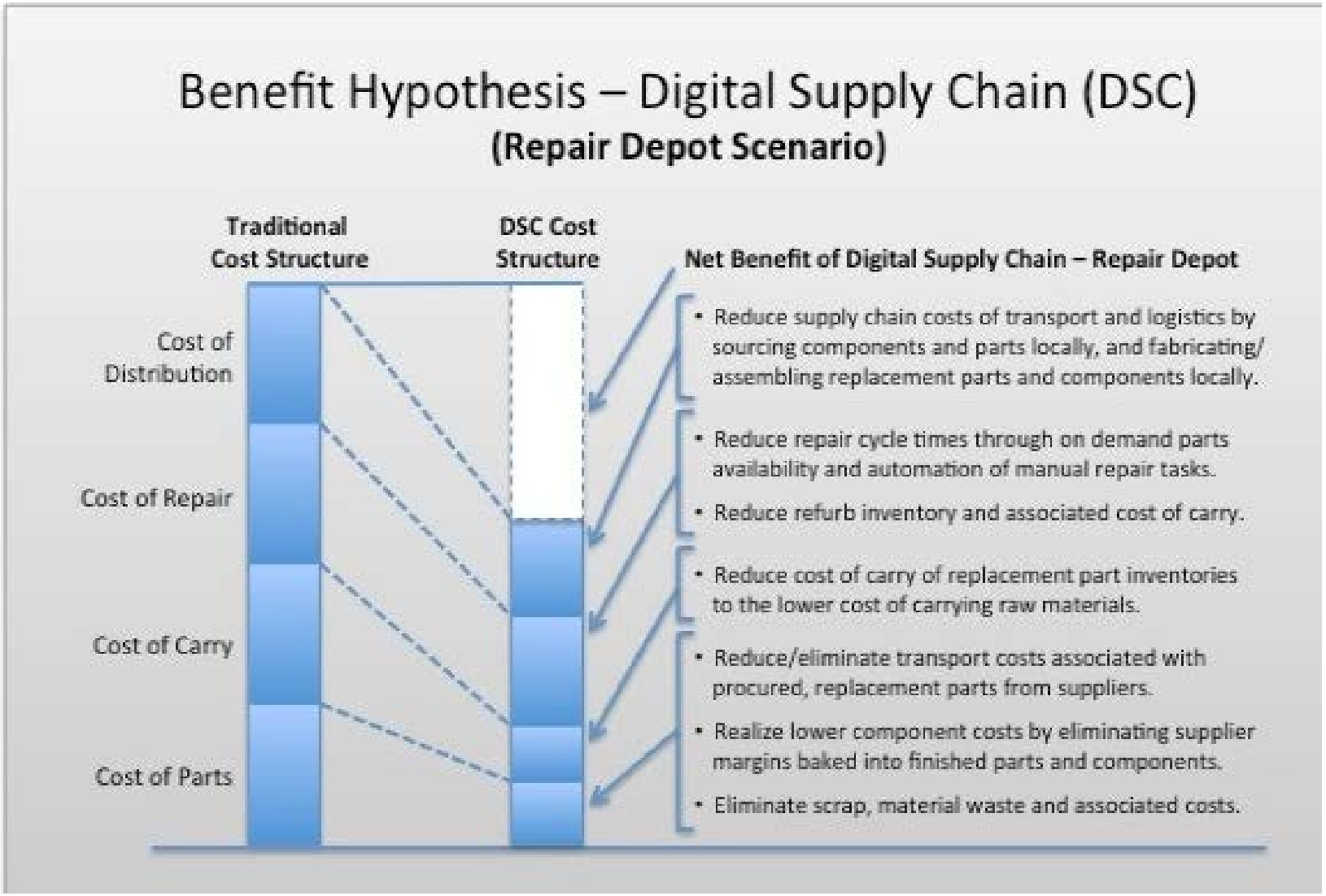
Integrating the supply chain

Production, Sustainment, Recycling



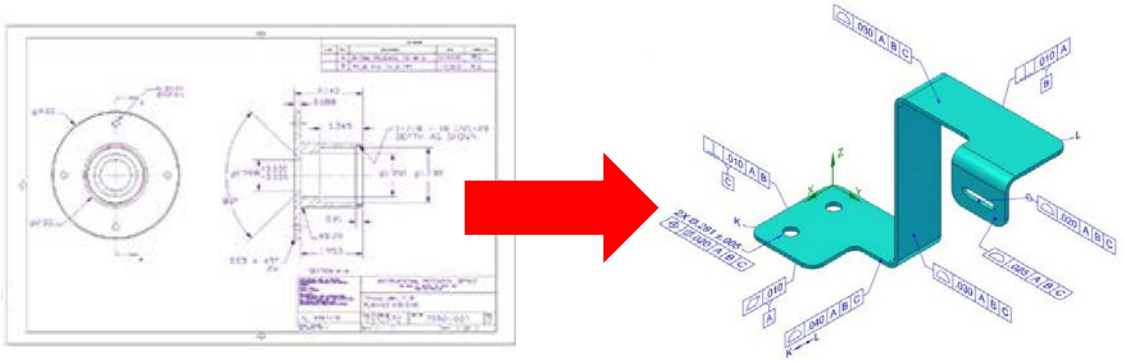
- Internal production
- Design-Make
- Make-to-model

Benefits of a digital supply chain

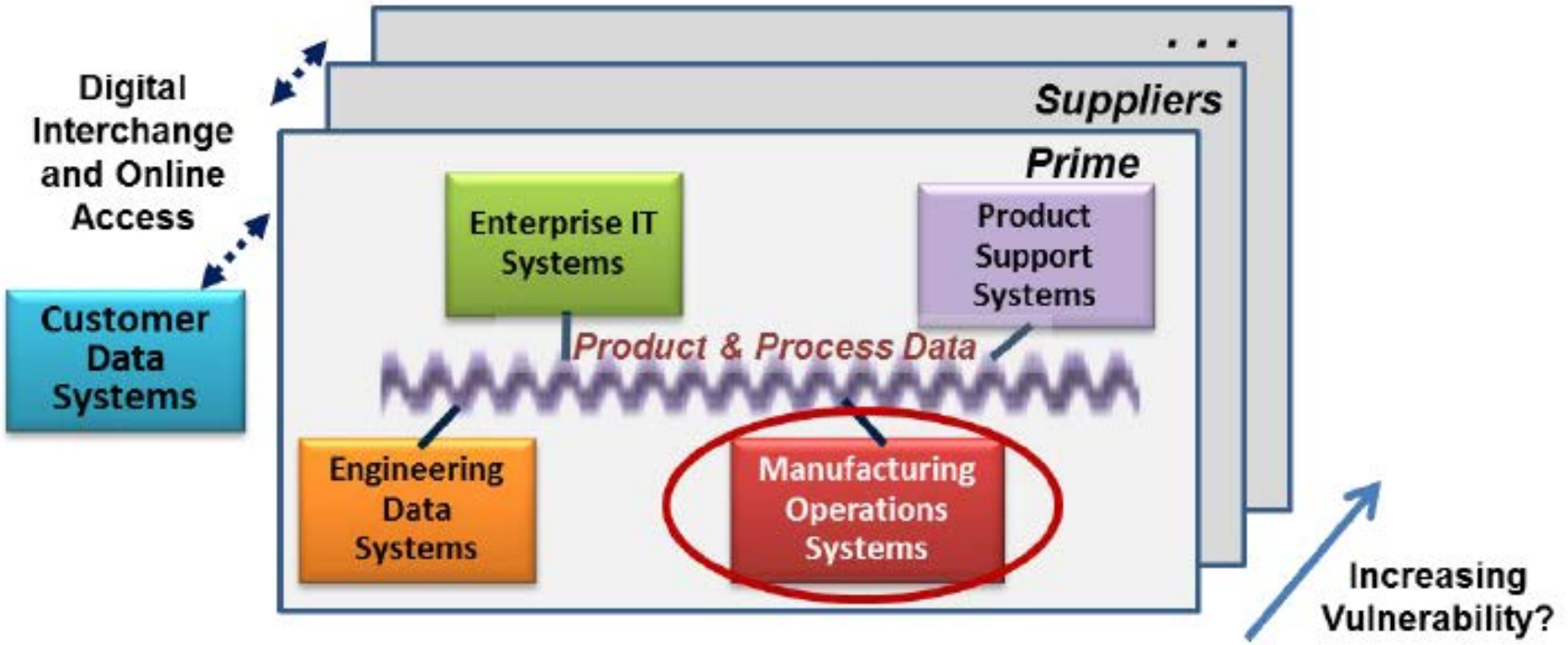


http://insights-on-business.com/electronics/3d-printing-transforming-the-supply-chain-part-2/

Protecting the digital thread



How does our security model change?



Cybersecurity for manufacturing, NDIA, May 2014

The threat to product data is real

- Theft of technical data, including critical national security information and valuable commercial intellectual property. *This is a Confidentiality concern.*
- Alteration of data, thereby altering processes and products. *This is an Integrity concern.*
- Impairment or denial of process control, thereby damaging or shutting down operations. *This is an Availability concern.*

ISA (2013), "NIST Cybersecurity Framework ISA99 Response to Request for Information," April 5, 2013, Research Triangle Park, NC: ISA, p3.

Some things to think about…

- Symantec reports that manufacturing was the most targeted sector in 2012, accounting for 24% of all targeted attacks.
- State-sponsored data breaches became the second most common variety of data breaches in 2012, following only organized crime, according to a study by Verizon.
- McAfee's 2012 Threat Predictions identifies industrial networks as the leading cybersecurity vulnerability
- Cyber spies, cyber criminals, cyber terrorists, disgruntled insiders and hacktivists can attack in very sophisticated ways. For example, the Washington Post (May 28, 2013) reported that a cyber espionage … exfiltrated technical design data on over two dozen US defense systems.
- Mandiant provided details on a class of sophisticated APTs that took most victim companies months to discover and mitigate – a long window during which sensitive intellectual property was being compromised.
- Stuxnet, the worm that attacked the Iranian uranium refinement capabilities, was a sophisticated attack targeted to specific machine controllers similar to those widely used in manufacturing operations.

ISA (2013), "NIST Cybersecurity Framework ISA99 Response to Request for Information," April 5, 2013, Research Triangle Park, NC: ISA, p3. (http://csrc.nist.gov/cyberframework/rfi_comments/040513_international_society_automation.pdf)
Symantec Internet Security Threat Report - 2013, p15 (www.symantec.com)
Verizon 2013 Data Breach Investigations Report, p21 (http://www.verizonenterprise.com/DBIR/2013/)
McAfee 2012 Threat Predictions, p3 (http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf)
Mandiant Intelligence Center APT1 report (http://intelreport.mandiant.com/)
Symantec W.32 Stuxnet Dossier (http://www.symantec.com)

How do we mitigate the risks?

Large companies tend to have the resources to address the challenges; however:

- Are confident in their risk management posture but are concerned about suppliers, especially small businesses, who lack the resources and knowledge to identify and mitigate cyber risks. Large companies are concerned that supplier vulnerabilities could become their vulnerabilities, and are willing to work with suppliers on improvements.
- Have not yet seen an upsurge in the threat to factory systems, but acknowledge the growing interconnections between factory systems and other systems, and the existence of targeted attack examples. They do not want manufacturing systems to be the weak link in the enterprise.
- View increased mandatory cyber protection requirements with concern unless they are accompanied by funding for implementation. They advocate use of voluntary commercial standards and practices where possible, and advocate a process of cost/risk tradeoffs to arrive at affordable solutions for cybersecurity in the DIB.

Cybersecurity for manufacturing, NDIA, May 2014

What will we discuss today?

- Today's program will include ideas to address product data security in the supply chain via:
  - Hardware and software technology
  - Process, practice, and the human interface
  - Policy and regulation

Our agenda

8:00 – 8:30 a.m.	**Continental Breakfast**
8:30 – 8:50 a.m.	**Welcome, Updates, and Meeting Theme** ***Nathan Hartman*** *– Professor, Computer Graphics Technology and PLM Center Director*
8:50 – 9:30 a.m.	**PLM Center Research Overview – Faculty Fellow Presentations** Supplier/Supply Chain Metrics: ***Thomas Brush*** *– Senior Associate Dean, Head, Department of Management, & Professor of Management (Strategic Management Area)* Model-based Definition: ***Nathan Hartman*** *–Professor, Computer Graphics Technology and PLM Center Director*
9:30 – 10:00 a.m.	**Invited Speaker** ***Eli Ribble*** – Chief Technology Officer, Authentise
10:00 – 10:30 a.m.	**Break & Networking**
10:15 – 11:15 a.m.	**PLM Center Research Overview – Faculty Fellow Presentations** Requirements: ***Dan DeLaurentis*** *– Professor, Aeronautics and Astronautics and Director, Purdue Center for Integrated Systems in Aerospace* PLM Data Curation: ***Michael Witt*** *– Associate Professor, University Libraries* Security: ***Elisa Bertino*** *– Professor, Computer Science; Research Director of CERIAS; Director of Cyber Center, Discovery Park*
11:15 a.m. – 11:45 p.m.	**Invited Speaker** ***John Wallrabenstein*** – Staff Research Scientist, Sypris Research Center, Sypris Electronics
11:45 – 1:45 p.m.	**Lunch and Keynote Presentations** ***Keng Lim*** – CEO, NextLabs, Inc. **Kristin Holzworth** – Deputy Director, Joint Advanced Manufacturing Region (SW), Space & Naval Warfare Center Pacific

Our agenda

1:45 – 2:45 p.m.	**Securing Product Data in the Supply Chain with PLM Panel** The panelists in this moderated session will provide their insights on securing product data within the supply chain using PLM tools and methods. The viewpoints from industry and government will be presented. ***Kristin Holzworth*** – Deputy Director, Joint Advanced Manufacturing Region (SW), Space & Naval Warfare Center Pacific ***John Irons*** – Director, Enterprise Technical Computing, Cummins ***Gary Mills*** – Director, Engineering and Factory Solutions, Rockwell Collins Engineering and Information Technology **John Wallbrenstein** – Staff Research Scientist, Sypris Research Center, Sypris Electronics ***Keng Lim*** – CEO, NextLabs, Inc. ***James Graham*** – Professor, University of Louisville
2:45 – 3:15 p.m.	**Break & Networking**
3:15 – 5:00 p.m.	**PLM Roadmapping Exercise – Strategic Doing** This facilitated, collaborative exercise involving all meeting attendees will work to develop the initial outline for Purdue's PLM Center PLM/product data security technology and research roadmap. ***Scott Hutcheson*** – *Senior Associate, Purdue Ctr for Regional Development (PCRD)* ***Ed Morrison*** – *Regional Economic Development Advisor, PCRD*

Thank you to our members…

TEXTRON

Gulfstream®

Rockwell Collins

P&G

BOEING®