Cybersecurity For
Advanced Manufacturing Forum

CFAM Manufacturing Environment Team

Dr. Marilyn Gaska, Lockheed Martin
Team Lead

Lockheed Martin
Global Vision Center
Arlington, VA

November 15, 2016

Manufacturing Environment Team (MET)

Sean Atkinson GLOBALFOUNDRIES	**Daryl Haegley** OASD (EI&E) IE	**Chris Peters** The Lucrum Group	**Andrew Watkins** DMDII
Dean Bartles ASME	**Larry John** Anser	**Haley Stevens** DMDII	**Mary Williams** MTEQ
Marilyn Gaska Lockheed Martin Corporation	**Karlton "Blade" Johnston** Alcoa	**Rebecca Taylor** Nat'l Center for Mfg. Sciences	**Fran Zenzen**
Bill Glynn Westar Energy	**Greg Larsen** Institute for Defense Analyses	**Dennis Thompson** DMDII	
Dan Green SPAWAR	**Sean Miles** Defense Intelligence Agency	**Irv Varkonyi** SCOPE	

Introduction:
MET Objective

Identify actions and activities that can have the greatest impact to improve cybersecurity in the manufacturing environment

Recommend implementation processes

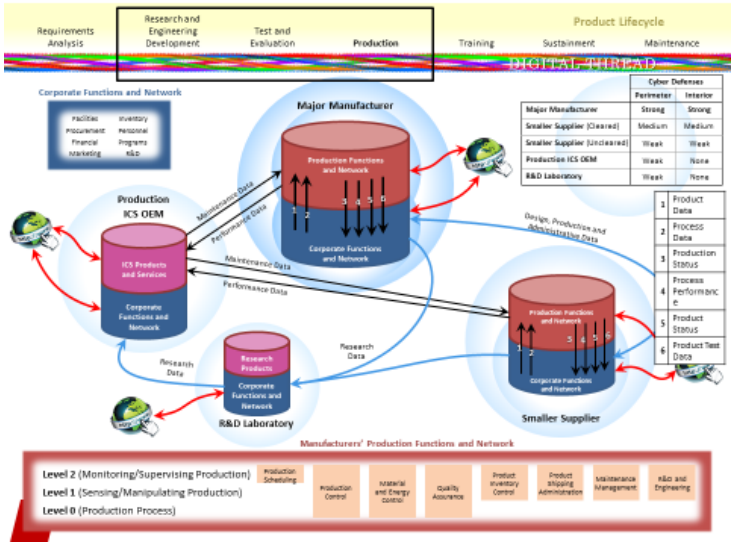
Focus on the operational environment to address scope and implementation challenges in terms of education and culture change

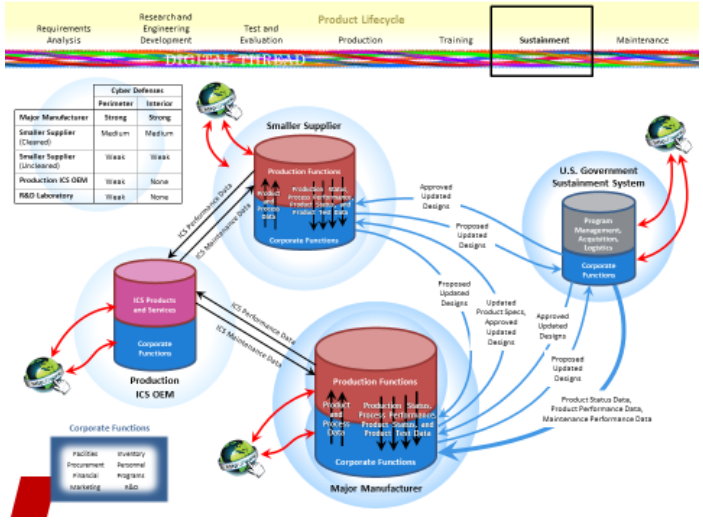
Manufacturing Environment Challenges

- Considering both manufacturing and sustainment
- Developing use cases that demonstrate risk / recommendations
- Simplifying ICS guidance for all sizes of organizations
- Addressing human factors incentivizing culture change
- Integrating cyber education into existing delivery network
- Leverage existing technology to mitigate immediate risks / create R&D projects for new technology solutions
- Determine balance of regulation with voluntary measures to achieve greatest benefit

Use Cases to Demonstrate Risk/Recommendations: CFAM Joint Team Collaboration

- **Confidentiality**
- **Integrity**
- **Availability**



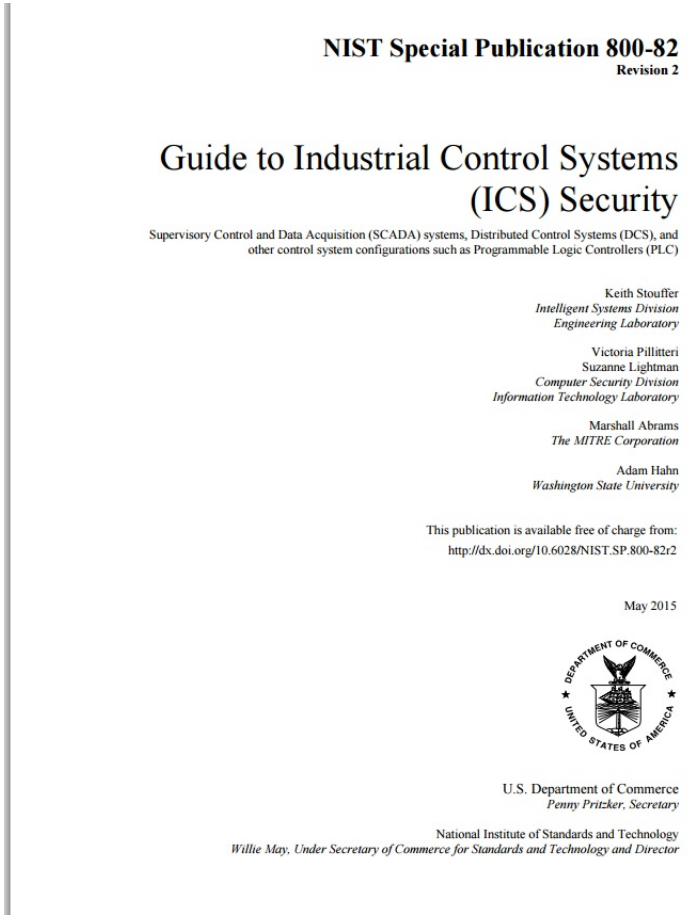


MET White Paper Deliverable Overview

Terms of Reference (TOR) Question	Status	Comments
Delineation of the manufacturing environments that are to be included in the CFAM effort.	✔	Scope diagram developed using ISA-95 model with all-team concurrence
What defines a manufacturing environment for the defense industrial base?	✔	Diagrams completed including data flows (See Larry John presentation)
What are the cybersecurity threats, vulnerabilities, and consequences? How can the cybersecurity risks in manufacturing environments be identified and mitigated?	✔	Risk Working Group MET White Paper Section on Risk leveraging NIST 800-82 R2 (Larry John lead)
What conditions and practices contribute to cybersecurity or increase cyber risks? What actions and activities can improve cybersecurity in the manufacturing environment? What are the activities with the potential to have the greatest near-term impact? How can cultural and behavior change contribute to increased cybersecurity?	✔	Culture / Human Factors Working Group MET White Paper Section (Chris Peters lead)
What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership?	✔	Education Working Group Collaboration with DMDII / NIST MEP Effort and Forward Plan (Haley Stevens / Dennis Thompson DMDII)

NIST SP 800-82
Keith Stouffer, NIST POC/CFAM MET Member

- **Guide to Industrial Control Systems Security**
  - Provides guidance for establishing secure ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- **Initial draft - September 2006**
- **Revision 1 - May 2013**
- **Revision 2 - May 2015**
- [+ Draft Cybersecurity Framework (CSF) Manufacturing Profile]



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

CFAM MET Risk Recommendations Leverage NIST ICS 800-82r2 Per CFAM 2014 Recommendation

Recommendations: Culture, Organization, and Education

2014 Recommendations for USD (AT&L)

- Create common business interface expectations among DoD, prime contractors and suppliers for cybersecurity controls in manufacturing systems.

2016 Recommendations for USD (AT&L)

- **Leverage NIST ICS efforts. Fund DoD participation in effort/research to establish common interfaces across commercial, DoD, and critical infrastructure industrial control systems to leverage commonality across sectors.**

Cultural/Behavioral Hurdles / Desired Outcomes

- **Adoption Hurdles**
  - Human Factors – People don't want to:
    - Change
    - Do any more work than needed or take longer than necessary on any task
    - Stand out from the peer group
  - Organizational Factors: - Organizations don't want to:
    - Impact production (reaching key metrics, getting paid, or keeping jobs)
    - Lessen their competitive stance (quality or lose money)
    - Regulatory compliance
- **Driving Adoption**
  - Articulate the case - learn about CFAM
  - Make it personal – education to include importance to livelihood
  - Make it required – employee and supply chain contracts
  - Offer help – leverage NIST MEP network
  - Offer rewards – appreciation certificates

DMDII Cybersecurity Projects In Process

- DMDII-15-01-91 Assessing, Remediating, and Enhancing DFARS Cybersecurity Compliance in Factory Infrastructure
- DMDII-15-13 Cyber Security for Intelligent Machines
- Continue to leverage deliverables as available

Recommendations: Culture, Organization, and Education

2014 Recommendations

- Develop programs to facilitate manufacturing system cybersecurity in defense supply chains
  - Work with the NIST Manufacturing Extension Partnership network and other delivery channels to develop and deliver training to small and mid-size manufacturers and assist them in implementing cybersecurity principles, standards, and practices to meet the needs of DoD and DIB trading partners.

2016 Recommendations

- **Collaborate with MEP to extend cybersecurity pilot program to include issues in OT and manufacturing networks.**
- **Include a simplified awareness campaign in social and mass media channels like "Loose Lips Sink Ships" model from WWII to raise awareness.**
- **Simplify the message by crafting and delivering simple messages for target audiences developed by communications professionals.**

Recommendations: Culture, Organization, and Education

2014 Recommendations for USD (AT&L)

- Evaluate the core standards, practices and concepts of the NIST Framework as a starting point for improving Industrial Control System (ICS) security in manufacturing applications, with DIB sector-specific extensions as needed. Use a common vocabulary and aim for compatibility with commercial solutions wherever possible, while meeting national security needs. Collaboration with DHS established and DoD managed DIB Sector Critical Infrastructure Protection Program may prove fruitful for this effort.

2016 Recommendations for USD/AT&L, DoD/CIO and OASD(L&MR)

- **Should jointly <u>establish specific training:</u>**
  - **Vulnerability assessment, risk identification and management, content of relevant NIST Special Publications and Frameworks, identification and implementation of appropriate controls, and cybersecurity incident management for industrial cybersecurity, especially manufacturing.**
  - **Use most effective combination of :**
    - **military or civilian personnel from either or both the Active Duty or Reserve components,**
    - **programs affiliated with other government entities and programs (National Initiative for Cyber Education (NICE), NIST Manufacturing Extension Program (MEP)**
    - **commercial providers (with DoD subsidizing costs as needed, possibly under authorities granted to the Office of Economic Adjustment)**

Recommendations: Culture, Organization, and Education

2014 Recommendations

- Develop Defense Acquisition University training modules to familiarize the DoD acquisition workforce with cost-effective cybersecurity risk management practices and to provide training in appropriate application of contract requirements for safeguarding unclassified controlled technical information, including in manufacturing systems.

2016 Recommendations

- **Establish certification program to provide incentive for people to become more engaged in preventing CFAM attacks. Track certification metrics to measure effectiveness.**
- **Recommend/update modules that address CFAM scope for inclusion in DAU training tailored to specific stakeholder groups. Explore exporting DAU module to other venues.**

Recommendations:
Culture, Organization, and Education

2014 Recommendations

- Provide incentives and, where justified, investment assistance for capital investments to upgrade and strengthen ICS systems and networks.

2016 Recommendations

- **Provide additional motivation to drive desired behavior, such as:**
  - **Succinct and readily understood regulations.**
  - **Financial incentives / tax abatements**
  - **Additional support from DoD / Government vulnerability assessment red teams**

Education / Assessment Resources Back Up

- MEP – Manufacturing Extension Partnership leveraging NIST efforts
- NICE – National Initiative for Cybersecurity Education
- DAU – Defense Acquisition University
- GICSP - Global Industrial Cyber Security Professional
- ICS-CERT – Industrial Control Systems – Cyber Emergency Response Team
- ISA IACS – ISA Industrial Automation and Control System (IACS) assessment
- InfraGard - partnership between the FBI and the private sector for information sharing, including Defense Industrial Base Sector

Questions and Discussion

Leverage for Cyber Education Integration: IMEC/DMDII/MEP Award

IMEC, DMDII Awarded $1.2 Million to Fund Advanced Manufacturing Workforce Initiative

September 22, 2016 - Chicago, Illinois - The Illinois Manufacturing Excellence Center (IMEC), Purdue Manufacturing Extension Partnership (Purdue MEP), and the Digital Manufacturing and Design Innovation Institute (DMDII) were named recipients of a $1.2 million award by the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Hollings Manufacturing Extension Partnership (MEP).

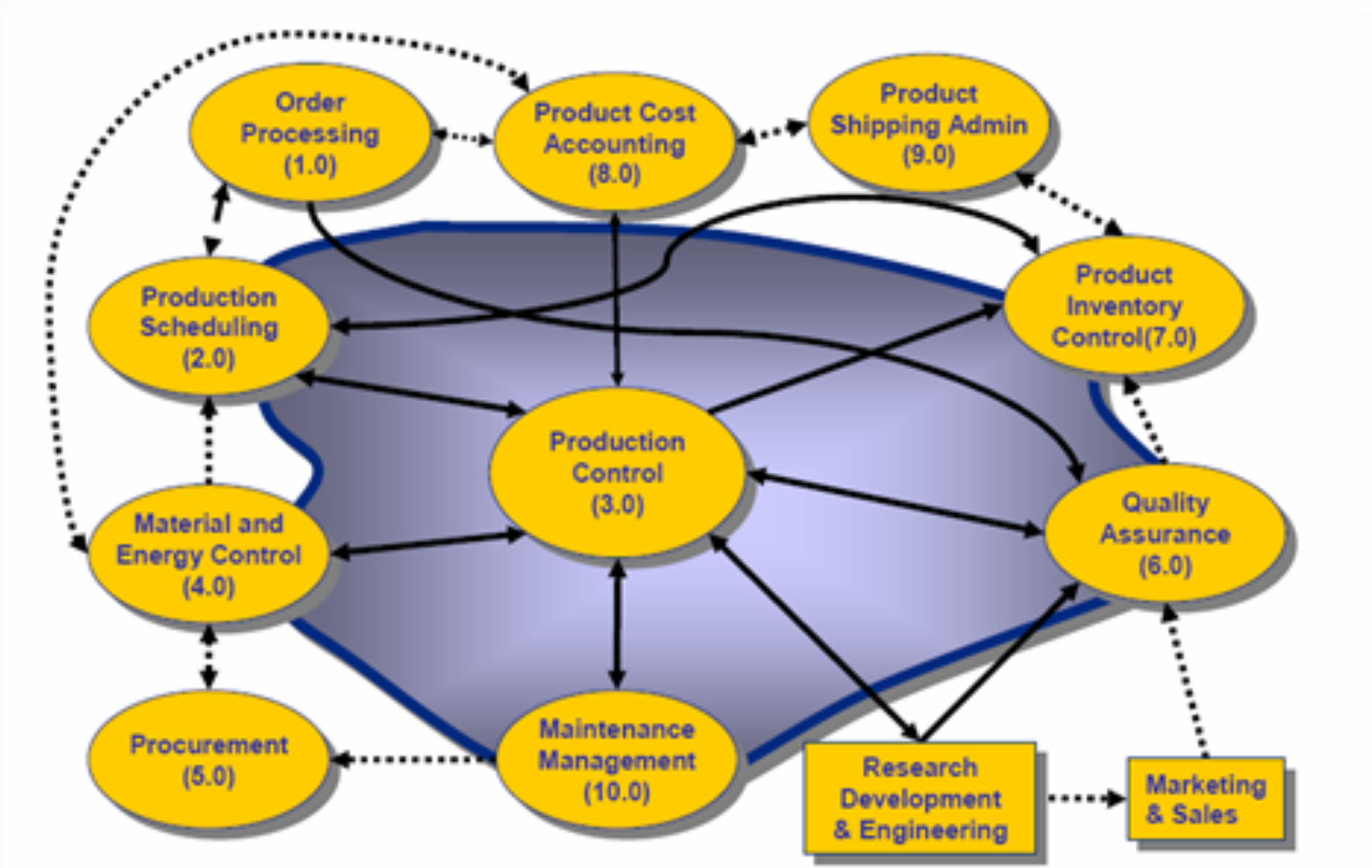
The federally funded award supports the efforts of Manufacturing USA, a network comprising nine public-private research institutes, including DMDII, dedicated to advancing manufacturing innovation, education and collaboration. IMEC and Purdue [illegible] residence" to work within DMDII to engage small and [illegible] needs.

Cybersecurity Module by NIST will be part of the 2017 effort

"We are in the first wa[illegible]gs together complementary expert[illegible], IMEC President. "This collaborative model will addre[illegible] and use of tools and resources that provide manufacturing leaders the roadmap a[illegible] embrace digital technologies."

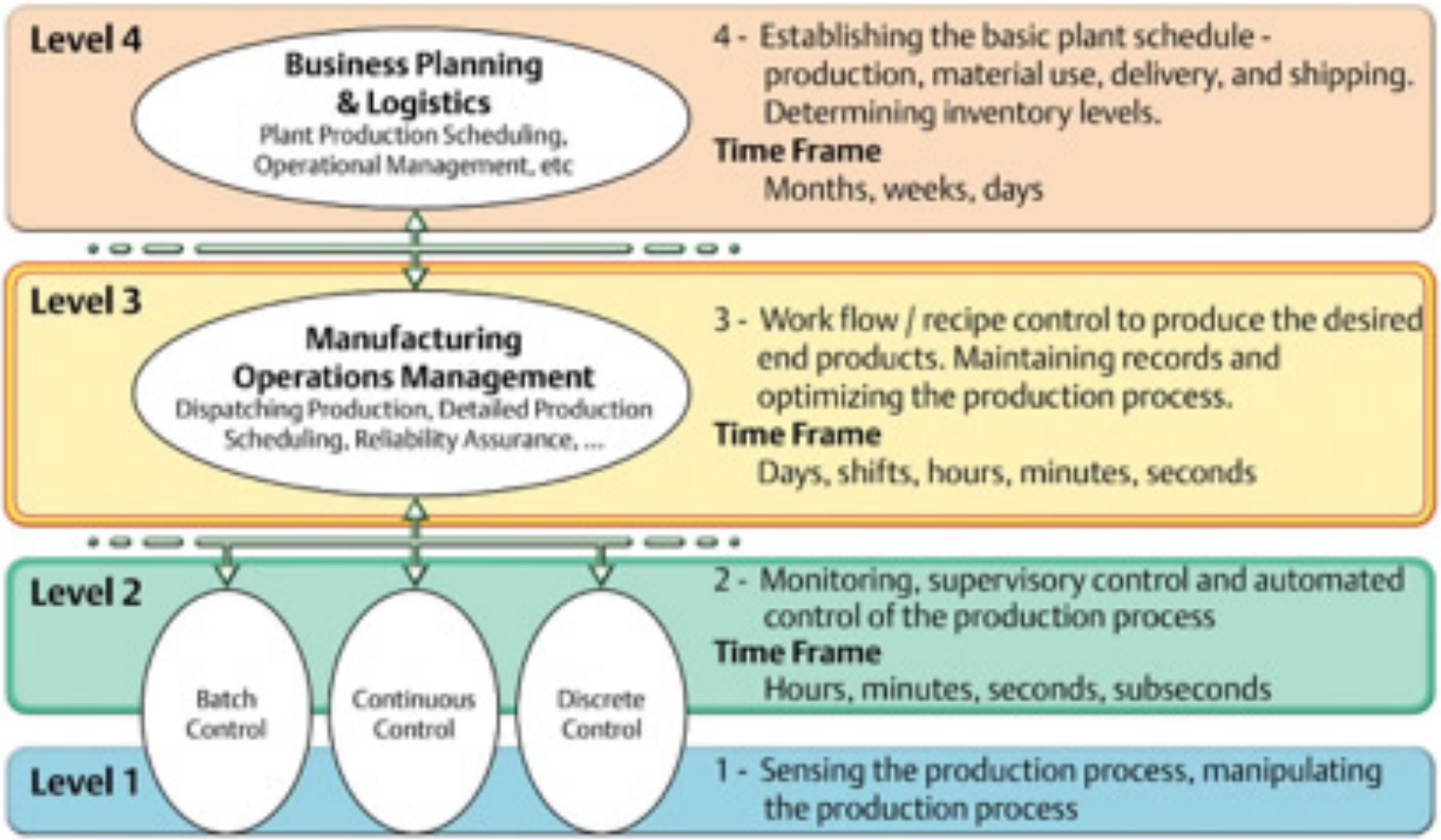
"From this award we can continue to proliferate the rise of the digital factory through our unprecedented partnership with the nation's MEP centers," said Haley Stevens, Director of Workforce Development and Manufacturing Engagement at DMDII. "The interconnectedness of manufacturing through data is changing manufacturing jobs. Through technical assistance, this investment provides the necessary resources to assist small and medium-sized manufacturers in preparing for and adopting digital transformations."

International Society of Automation (ISA)
ANSI/ISA-95.00.01 – Functional Model



Source: ANSI/ISA-95.00.01

ISA-95 - Supporting Activity Model



Standards Based Scope / Definitions: Manufacturing Environment Framework Matrix

NOTE: This matrix is based on the ISA-95 Functional Model.