National Defense Industrial Association

CFAM Manufacturing Environment Team (MET) Update and Manufacturing Boundaries

Dr. Marilyn Gaska

11 April, 2016

Agenda

- MET Membership
- Deliverables
- List of Resources
- SME Interview List
- Education and Training
- Accomplishments / Plan
- TOR Questions for MET Focus
- Manufacturing Boundaries Discussion

Manufacturing Environment Team Members

- Dean Bartles (with DMDII team reachback)
- Michael Dunn
- Aman Gahoonia
- Marilyn Gaska
- Dan Green
- Daryl Haegley
- Greg Larsen
- Tom McCullough
- Adele Ratcliff / Greg Harris
- Keith Stouffer
- Rebecca Taylor
- Irv Varkonyi
- Mary Williams
- Fran Zenzen
- **Integration Team Participants:**
- Larry John
- Kaye Ortiz
- Chris Peters
- Jimmy Poplin

CFAM MET Deliverables (3/28/16)

There are two major components to the MET deliverables. The first is a delineation of the manufacturing environments that are to be included in the CFAM effort. A definition of all environments considered will be included, along with the rationale and supporting materials explaining why each environment was included in or excluded from the CFAM effort. This deliverable will be needed quickly as it informs the actions of the other teams.

The second deliverable is a report outlining the issues in the manufacturing environment, existing initiatives addressing those issues, gaps where an effort is needed and recommendations to address those gaps. The report will answer the following questions posed in the CFAM terms of reference.

- What defines a manufacturing environment for the defense industrial base?
- What are the cybersecurity threats, vulnerabilities, and consequences?
- How can the cybersecurity risks in manufacturing environments be identified and mitigated?
- What use cases are important across the life cycle of the manufacturing environment?
- 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?
- What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership?
- How can cultural and behavior change contribute to increased cybersecurity?

The team will strive to leverage existing research and materials where possible.

List of Resources

- **Include documents already in NDIA shared directories (http://committees.ndia.org/mycommittees/D2760/Pages/default.aspx)**
- **NIST Cybersecurity Framework (www.nist.gov/cyberframework/)**
  - **NIST Cyber Physical Systems Working Group: https://pages.nist.gov/cpspwg/ for latest draft**
  - **NIST Smart Manufacturing: http://www.nist.gov/el/msid/syseng/ and http://www.nist.gov/el/isd/upload/Overview-of-NIST-and-Smart-Mfg-24-Aug-2015.pdf)**
  - **NIST Special Pub on Industrial Control Systems: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf**
- **Industrial Internet Reference Architecture (Dean and Dan as consortium members recommend safety and security overview): http://www.iiconsortium.org/IIRA.htm**
- **DHS Resources:**
  - **Cybersecurity Evaluation Tool (CSET) and On-Site Cybersecurity Consulting : http://ics-cert.us-cert.gov/assessments**

SME Interview List

- Use case coverage
- Manufacturing Network Specialists – certain group
- Adv. Cybersecurity POCs with lessons learned
- Team from DMDII on standardizing mfg. security for suppliers
- Large and small business POCs (e.g. Doug Thomas, LM)
- DHS ICS-CERT - Sean V. Docken (Need question preview) – 11 April Speaker instead
- IP / FBI Critical Infrastructure (InfoGuard)
- National Institute for Cyber Education (NICE) William Newhouse

Education and Training: Independent Supportive Activities

- Better cyber hygiene
- More training
- Cultural changes through awareness campaigns
- NIST Manufacturing Extension Partnership (MEP) centers as resource (http://www.nist.gov/mep/)
- NIST National Initiative for Cyber Education (NICE) (interview list)
- Boundaries will help (Dan has ideas on scope, multiple audiences)
- Resources align with different audiences

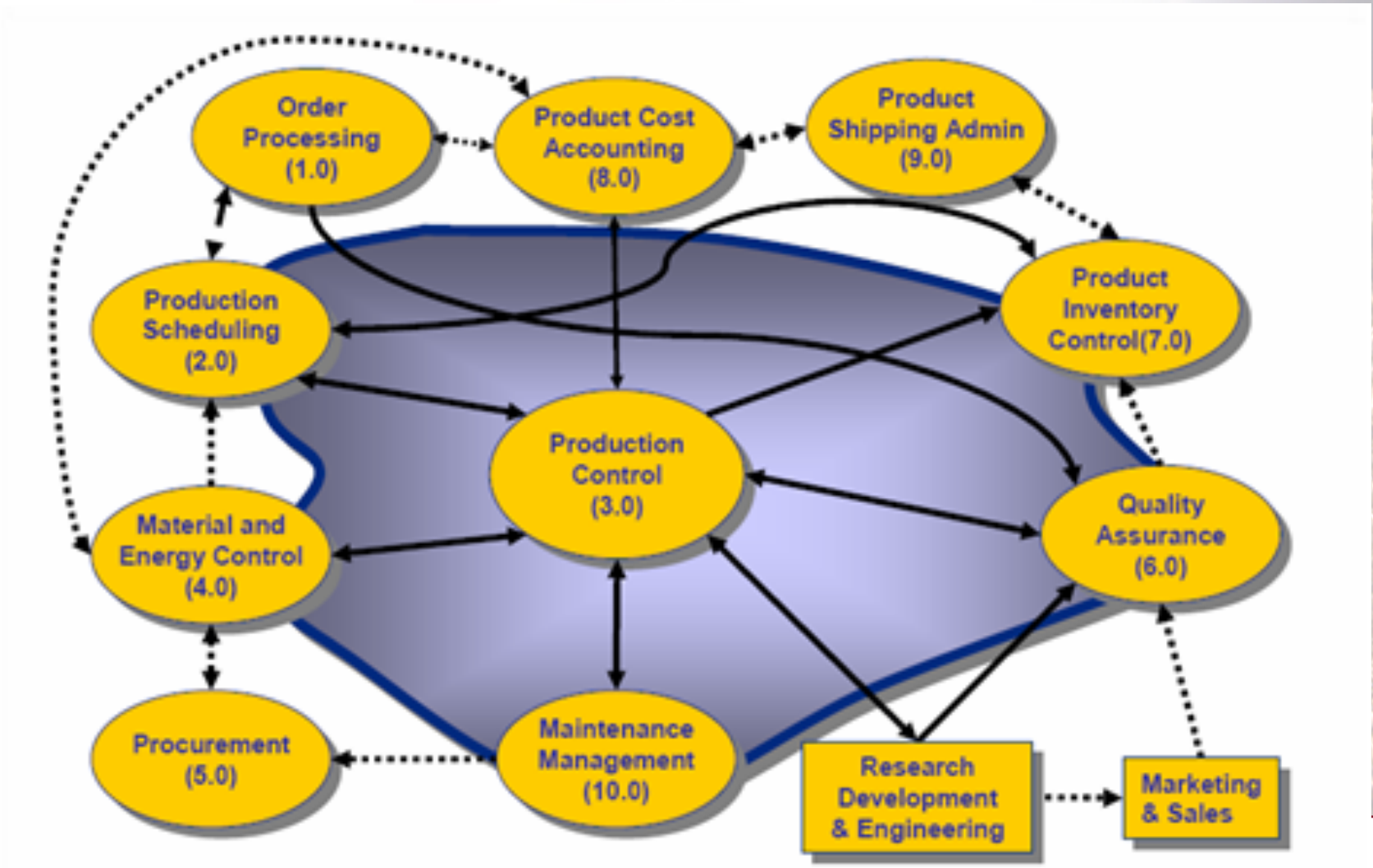
Accomplishments / Plan

- ✓ Definition of MET's deliverable(3): March 30th
- ✓ Confirm Mfg. Env. Scope 11 April
- Next telecon 22 April
  - Collaboration with Haley Stevens, DMDII
  - Integrate NIST effort's (Keith Stouffer)
- Joint telecon with Solutions Team (TBD)
- Training and cultural change approach
- Resource review / Interviews
- Divide and conquer on TOR Questions
- MET deliverable due date: October 14th
- Integration into overall report / review

TOR Questions: MET Focus

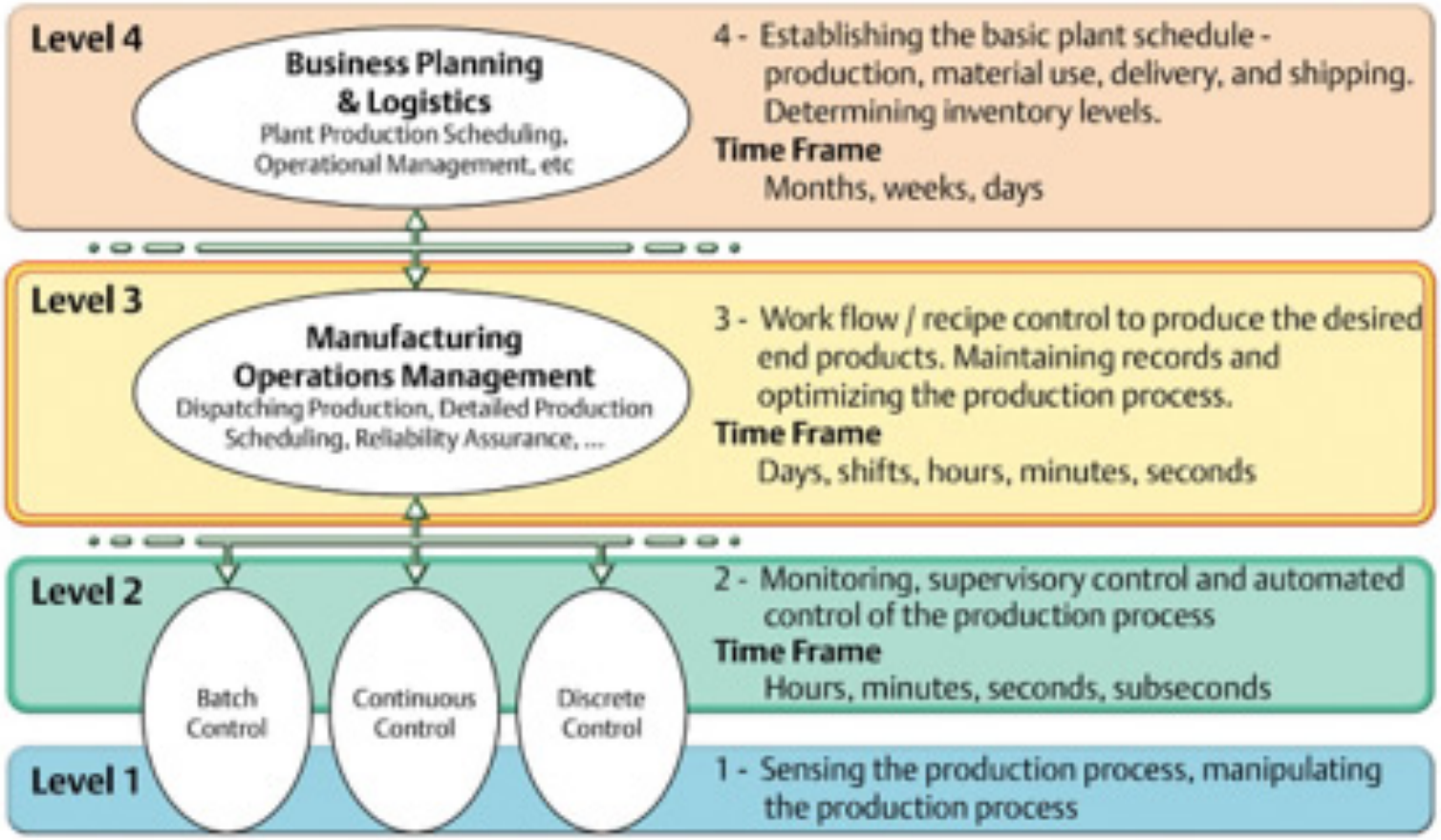
- What defines a manufacturing environment for the defense industrial base (i.e. within and among the members of defense supply chains)? (today) What are the cybersecurity threats, vulnerabilities, and consequences? How can the cybersecurity risks in manufacturing environments be identified and mitigated? (Emily Miller, ICS Cert, 11 April focus)
- What use cases are important across the life cycle of the manufacturing environment? What conditions and practices contribute to cybersecurity or increase cyber risks? Technology Team Collaboration (Coordination Call via Chris/Larry)
- 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? (Bob Metzger, IOT, 11 April focus)
- –What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership? How can cultural and behavior change contribute to increased cybersecurity? (Haley Stevens, DMDII Associate Director Workforce Development, April 22 meeting)

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

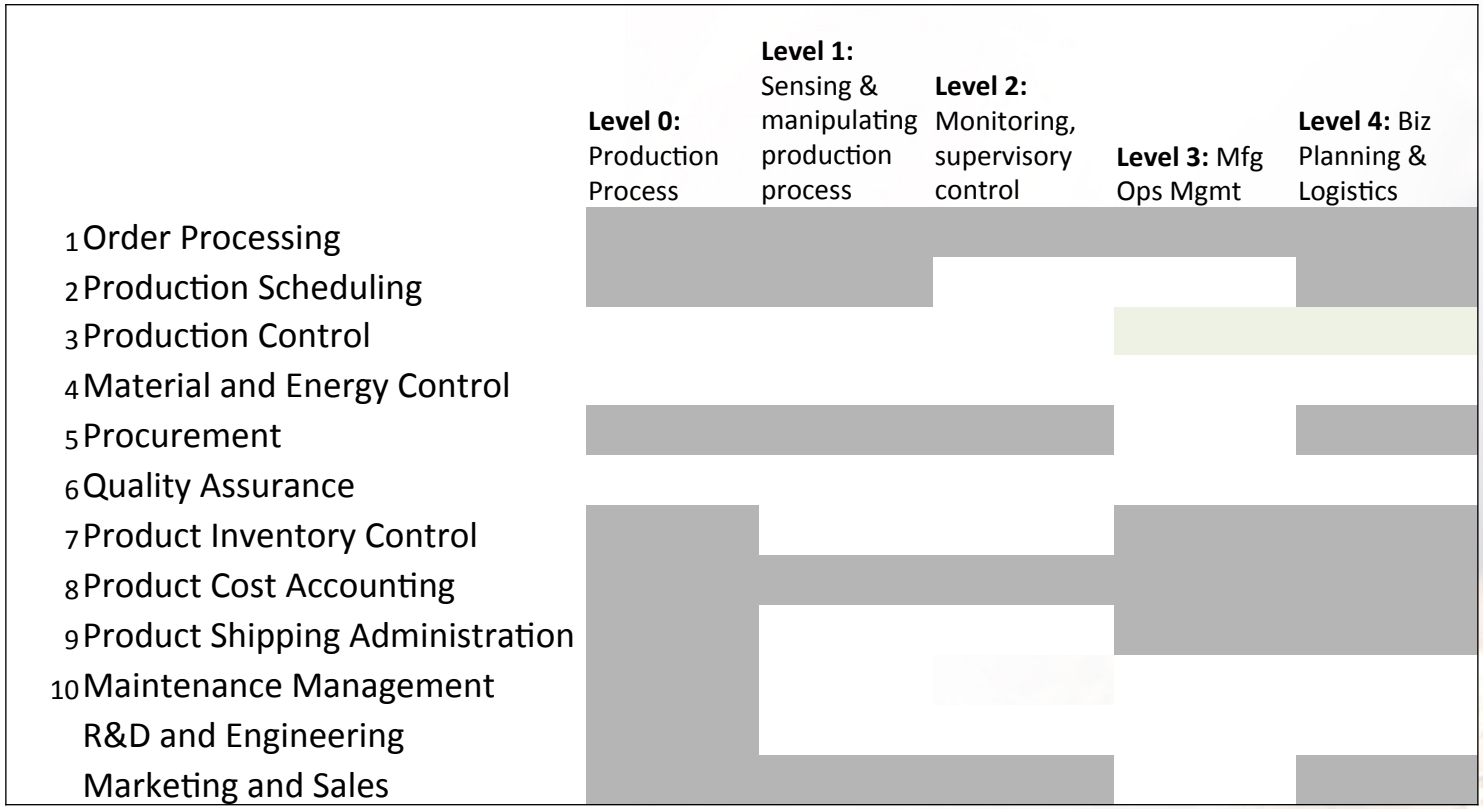


Source: ANSI/ISA-95.00.01

ISA-95 - Supporting Activity Model



Manufacturing Environment Framework Matrix



KEY

CFAM FOCUS
OUT OF SCOPE
Out of scope if covered by enterprise IT, but in scope if specialized systems.