# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attendees</td>
<td>2</td>
</tr>
<tr>
<td>Kennametal Tour</td>
<td>3</td>
</tr>
<tr>
<td>Safety Brief</td>
<td>3</td>
</tr>
<tr>
<td>Introductions</td>
<td>3</td>
</tr>
<tr>
<td>Overview and application of Cyber-Physical security</td>
<td>3</td>
</tr>
<tr>
<td>Antitrust Statement</td>
<td>4</td>
</tr>
<tr>
<td>Cyber-Physical Security</td>
<td>4</td>
</tr>
<tr>
<td>NIST Cyber Framework</td>
<td>4</td>
</tr>
<tr>
<td>Questions from Cyber-Physical Security Working Group</td>
<td>4</td>
</tr>
<tr>
<td>NTMA 6S award</td>
<td>5</td>
</tr>
<tr>
<td>Tech Award</td>
<td>5</td>
</tr>
<tr>
<td>Emerging Leaders</td>
<td>6</td>
</tr>
<tr>
<td>NNMI update</td>
<td>6</td>
</tr>
<tr>
<td>TechTrends Update</td>
<td>7</td>
</tr>
<tr>
<td>MTConnect Student Challenge</td>
<td>7</td>
</tr>
<tr>
<td>IMTS Update</td>
<td>7</td>
</tr>
<tr>
<td>ETC Update</td>
<td>7</td>
</tr>
<tr>
<td>New NNMI update</td>
<td>7</td>
</tr>
<tr>
<td>TIC Breakout</td>
<td>8</td>
</tr>
<tr>
<td>Actions</td>
<td>8</td>
</tr>
<tr>
<td>Meeting Adjourned</td>
<td>8</td>
</tr>
<tr>
<td>Files embedded</td>
<td>9</td>
</tr>
</tbody>
</table>
Attendees
Scott Hibbard (Chairman)
VP of Technology,
Industrial Applications (DC-IA/ENG-AM)
Bosch-Rexroth Corporation
Hoffman Estates, Ill.

Alejandro Aguilar
Mechanical Engineer
Hardinge Inc.
Elmira, N.Y.

AMT STAFF:
Tim Shinbara (Staff Liaison)
VP-Manufacturing Technology
AMT
McLean, Va.

Benjamin Moses
Technical Director
AMT
McLean, Va.

GUEST:
Heather Moyer
Executive Director
CTC
Johnstown, Pa.
hrmoyer@atlanticbb.net

NTMA TECHNOLOGY TEAM:
Jack Burley
BIG Kaiser Precision Tooling Inc.
Hoffman Estates, Ill.

Herb Homeyer
Chairman of the Board
National Tooling & Machining Assn.
Marthasville, Mo.

Robert O'Donnell
O-D Tool & Cutter Inc.
Mansfield, Mass.

David A. Tilstone
President
National Tooling & Machining Assn.
Cleveland, Ohio

Gillen Young
Custom Tool, Inc.
Cookeville, Tenn.

NTMA STAFF LIAISONS:
Tiffany Bryson
National Account Manager
National Tooling & Machining Assn.
Cleveland, Ohio

Pamela Wightman
Board Team Administrative Assistant
National Tooling & Machining Assn.
Cleveland, Ohio
Kennametal Tour
A facilities tour was provided. This location specializes in stage 3 of the product lifecycle development; maturing the concept to a production-ready product.

Safety Brief
A safety brief was provided.

Introductions
Each team member introduced themselves.

Overview and application of Cyber-Physical security
All major industrial countries are focused on manufacturing. Europe Industry 4.0 (http://www.gta.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf), USA NNMI (https://www.manufacturing.gov/nmni/), China Made in China 2025 (https://www.csis.org/analysis/made-china-2025), India Made in India (http://www.makeinindia.com/home). With the increased digital access and government attention, now is the time to increase attention on cyber-physical security.

A joint working of group cyber and manufacturing industry experts are working together to access industrial security needs. NDIA white papers from 2015 characterize a DOD cyber threat. This paper has created awareness that a real threat exists to America’s infrastructure. http://www.ndia.org/Policy/LegislativeandFederalIssuesUpdate/Documents/Cyber_for_Manufacturing_White_Paper_5 may14.pdf Virginia Tech’s Industrial threat experiment reinforces the impact. Virginia Tech ran an experiment where one group was tasked with printing a dog bone for destructive testing. Another group was tasked to infiltrate the machine and induce a flaw. A void was added to the STL (https://en.wikipedia.org/wiki/STL_(file_format)) file. This flaw was not discovered until destructive testing. The test-destructive test results were significantly different from the theoretical. http://namrc-msec-2015.uncc.edu/sites/namrc-msec-2015.uncc.edu/files/media/NAMRC-Papers/paper_81_framed.pdf

Several groups were formed to address threats outlined in the NDIA paper. One group is focused on standards and policy. The second group is defining the problem to manufacturing. The third group is assessing technology solutions – available solutions, emerging technologies and gaps that need investigating.

DFAR (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/) updates will be rolled out in 2017. This will stream down from primes to all subcontractors. The significant challenge will be to ensure that everyone can comply. Penalties of non-compliance will be similar to ITAR infractions (https://www.bis.doc.gov/index.php/forms-documents/doc_view/781-export-licensing). The major concern is that there would be an intrusion to make a bad part, not data being stolen.
Antitrust Statement
The antitrust statement was reviewed.

Cyber-Physical Security

NIST Cyber Framework
The core has five major areas of focus: identify, protect, detect, respond and recover.

NIST is on the fourth iteration of a smart manufacturing test bed that will be used for cybersecurity. Areas of interest are: process control, collaborative robotics, additive manufacturing and assembly. Research outcomes will be used for guidance of industrial best practices for cost effective implementation of cybersecurity standards and guidelines without negatively impacting ICS performance.

Attack vectors are defined as from where the attacks are coming, which aids in problem solving. Common vectors are hacking and thumb drives.

The team brought up concerns of solutions making sure they work together. The focus of the solution should be on discrete machines and flow of information.

A company questioned whether they are liable if they host files for general public usage that have “files” with a virus embedded. Most likely, the originator will be liable. Other questions are still open to debate.

There is not a one-size-fits-all solution. Every company needs to develop a plan based on their business plan and security tolerance.

Questions from Cyber-Physical Security Working Group:

1. How are operational technology (OT) systems fundamentally different from information technology (IT) and affect the types of technologies and solutions that might be applied?
   a. Word brainstorm: operators; different disciplines; different objectives; different priorities; not heavy IT; is expertise up to date; security may need a specialist; who reports to whom; more network protocols; more proprietary networks (lack of openness may limit solutions); are hardware and software separate; human behavior may revert back to previous problems if the interface is too cumbersome; interfaces need to remain simple; definition of risk; IT loss of data; OT loss of physical material and human capital; who is developing Okuma apps.

2. Given the differences between OT and IT, what techniques or technologies that are being used to protect IT systems are unlikely to be suitable for OT systems and/or the operational environment?
   a. Username and password on machines; IT is adaptable while OT has a longer timeframe; what does an update on a machine mean to production; ability to change programs is local – an IT system is centralized; most manufacturing shops want some level of controls at the machine; assessment of machine updates need to be improved; ability to revert to a previous version maybe key; backing up to the cloud is a solution and problem; changes and security may burden CPU to reduce ability to provide a real-time need; HAAS focused on processing speed for new controller to ensure that new graphics don’t effect cycle time.
3. What solutions and best practices can we adopt from IT cyber security to better secure OT?
   a. Force password changes of 30, 60 and 90 days; password protocols are problems – too many passwords; single sign on; define access by sign in – operators can be limited to XX changes on a machine and network; detecting abnormality; networks can be controlled; not a heavy focus on discrete machines;

4. Revised question: How do you protect the entire enterprise? Holistic Enterprise Network. Lights-out factory will greatly gain from remote network control; Industry 4.0 is working on standards to allow MRO similar to an HP being able to order print supplies.

5. Where do you draw the boundary for IT/OT? HVAC? Doors? Facilities?
   a. HVAC are standalone machines, but if they are connected – use cases – system of systems propagating to effect production; hacking an HVAC damper that trickles down to a problem; indirectly affecting production. This is not a real problem because the threshold is so high. Connected HVAC could be a problem. It can still be a problem with a disgruntled employee. If processes are environment dependent, then HVAC is a concern. The facilities department is responsible for HVAC.

6. The group determined that the information flow of data of geographically separate facilities (distributed manufacturing) is not a concern.

7. What risks are known for externally loaded data such as purchase orders, invoices, and engineering data?
   a. Companies that push data for general public use are not sure of security. User of downloaded data is not sure of security.
   b. Among confidentiality, integrity and availability, the greatest risk of breach is IP/confidentiality.
   c. When the question was posed, the group agreed that each of their companies would consider cybersecurity insurance.

8. What is the cost of DFAR’s (Defense Federal Acquisition Regulation) compliance?
   a. It is understood that there is a general cost associated with compliance. Businesses need information on how this impacts cost. There is not enough information currently to understand cost impact. Tier 3 suppliers probably won’t be able to comply due to the perceived cost increase.

**NTMA 6S award**

The NTMA 6S award process was reviewed. NTMA is investigating how to increase 6S adoption through the award process. NTMA is looking for AMT member nominees for the NTMA 6S award. Should there be a chapter competition? A low percentage of NTMA members know about the award. Brand awareness is a common problem for both associations. We need more ideas on how to raise awareness. Chapter competition is one way. AMT members are eligible to nominate themselves and/or NTMA shops. Everyone is eligible to receive the 6S award. The group agreed that the MFG is a good place to name the 6S award winner.

**Tech Award**

The NTMA Tech award process was reviewed.

It was suggested that the joint meeting be moved to the fall. This would allow the TIC/NTMA Tech Team joint meeting to be held on the front end of the NTMA Fall Conference.
Emerging Leaders
The emerging leader program was reviewed. NTMA is interested in expanding this group to include AMT leaders and bring these two groups together for a networking event.

NNMI update
Summary of awarded institutes
https://www.manufacturing.gov/nnmi-institutes/
- America Makes
  - Additive Manufacturing
  - Youngstown, Ohio
  - https://americamakes.us/
- American Institute for Manufacturing Photonics – AIM
  - Integrated photonic circuit manufacturing
  - Rochester, N.Y.
  - http://www.aimphotronics.com/
- Digital Manufacturing and Design Institute - DMDII
  - Digital Manufacturing
  - Chicago, Ill.
  - http://dmdii.uilabs.org/
- Lightweight innovations for Tomorrow – LIFT
  - Advanced lightweight materials
  - Detroit, Mich.
  - http://lift.technology/
- NextFlex
  - Flexible Hybrid Electronics
  - San Jose, Calif.
  - http://www.nextflex.us/
- Institute for Advanced Composites Manufacturing Innovation - IACMI
  - Advanced polymer composites
  - Knoxville, Tenn.
  - http://iacmi.org/
- Power America
  - Wide Bandgap Semiconductors
  - Raleigh, N.C.
  - https://www.poweramericainstitute.org/

The goal is to create 13 to 15 new institutes.

DoD is launching two new institutes with one on Advanced Tissue Biofabrication. DoC is also creating two new institutes. One of them may be machine tool related. Each institute will be independent with different membership and IP agreements.

DoD has clear direction but DoC is more open to industrial input on how technologies will be selected.
An SME business gains from these institutes by project support, trickle down of technologies and work force development and networking.

**TechTrends Update**

The TechTrends initiatives will kick off the first release of tools for the industry. Research and Development Trends will be released through MTInsight. This tool can be used to further understand what research is going on and where to go for more information on a specific paper. The preliminary version will be released at IMTS. The production version will be released Q2 2017.

**MTConnect Student Challenge**

The Student Challenge was reviewed. Ideation winners were announced during the [MC]² Conference. ([http://mc2conference.com/](http://mc2conference.com/)). The application winner will be announced during IMTS.

**IMTS Update**

IMTS was reviewed. The floor has been completely filled with a healthy backlog.

**ETC Update**

The Emerging Technology Center has been renamed Tech Trends.

**New NNMI update**

The Department of Commerce (DoC) is looking to create another National Networking for Manufacturing Innovation (NNMI) focused on machine tool technologies. SME is the target audience.

Manufacturing is a top wealth-generating industry, and its value to our economy and national security cannot be understated. The machine tools and controls market is a roughly $8.39 billion[1] market within the manufacturing technology sector, impacting a $1.99 trillion U.S. manufacturing industry value add.”
The team brought up the following areas of focus:

- Machine tool and control systems – Driving to expand scope of Machine Tools to include accessories
- Affordable automation
- First part correct
- Buying machines and automation is easy compared to the difficulty of finding skilled labor.
- Sensing and prediction
- Lights-out manufacturing
- Big Data
- Improving measurements before they become a problem
- Improve efficiency to reduce the need to increase the workforce

**TIC Breakout**

There weren’t enough TIC members present for a quorum. June meetings have historically low attendance.

To increase the joint meeting attendance it was proposed that the timing of meetings be changed to: January, April and October. The October meeting can be held as the joint meeting to coincide with NTMA’s Fall Conference.

There was discussion as to whether the Technology Issues Committee name still fits and if there should be a name change. The committee has not had many requests for projects, but there is significant value in topics covered.

**Actions**

- The next TIC meeting will be in October.
  - Survey TIC for date/venue
- Proposal to move joint meeting to the fall. This will allow joint work on the Tech award. The proposed overall schedule is January, April and October. For the October joint meeting, a day before the fall conference works with NTMA.
- NTMA and AMT will increase awareness of the 6S survey this year. The survey will be administered next year. Mike Hirsh and Pam Wightman are the points of contact.
- TIC Views article in AMT News on the new NNMI. (Alex)
- Increase engagement with the Emerging Leaders program (Tim and Doug Woods)
- Send out request to NTMA Tech for volunteers as TechTrends preliminary users. (Benjamin)
- Add a slot for AMT Technology in NTMA 2017 Fall Conference program. (Dave)

**Meeting Adjourned**

The meeting was adjourned at 3:15 p.m.
Files embedded
See attachment option in PDF reader to access files.

- Presentation
- NDIA White Paper
- Virginia Tech White Paper
- Tech Time Articles on Cyber Security