Cybersecurity For
Advanced Manufacturing Forum

CFAM Technology Solutions Team

Ms. Heather Moyer, Consultant
Dr. Craig Rieger, Idaho National Laboratory

Lockheed Martin
Global Vision Center
Arlington, VA

November 15, 2016
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Badgett</td>
<td>Consultant</td>
<td></td>
</tr>
<tr>
<td>Anitha Raj</td>
<td>ARAR Technology</td>
<td></td>
</tr>
<tr>
<td>Devu Shila</td>
<td></td>
<td>United Technologies Research Center</td>
</tr>
<tr>
<td>Vicki Barbur</td>
<td></td>
<td>MITRE</td>
</tr>
<tr>
<td>Craig Rieger</td>
<td></td>
<td>Idaho National Laboratory</td>
</tr>
<tr>
<td>Tim Shinbara</td>
<td></td>
<td>The Association for Manufacturing Technology</td>
</tr>
<tr>
<td>Heather Moyer</td>
<td>Consultant</td>
<td></td>
</tr>
<tr>
<td>Frank Serna</td>
<td>DRAPER</td>
<td></td>
</tr>
<tr>
<td>Janet Twomey</td>
<td></td>
<td>Wichita State University</td>
</tr>
</tbody>
</table>
The Challenge

Legacy Manufacturing
• IT and OT air gapped
• IT and OT personnel organizationally stove-piped with separate priorities and risk factors
• OT environment not highly adaptable to change, which is viewed as disruptive
• Average age of industrial equipment >10 years with 20+ year lifespan
• Weak cyber defenses in small to medium-sized companies

Advanced Manufacturing
• IT and OT segregated with boundary interface
• IT and OT personnel cooperate, but little collaboration
• Increasing use of digital manufacturing technologies
• Increasing enterprise need for real-time data
• Low awareness of specific cyber threats
• Cybersecurity bolted on

Smart Manufacturing
• Integrated, seamless IT/OT
• Distributed services enabled by cloud
• Plug and play device connectivity
• Sensors, mobile platforms, and visualization tools drive big data
• Comprehensive security strategies are needed as new technologies will revolutionize attack capabilities as well

Next 10+ years

Future State
Attack Tree Analysis

THREATS
- External hacker
- Insider threat
- Human error
- Supply chain hardware/software
- Third party service personnel
- Open source/downloads

ATTACK VECTORS
- **Remote:** Exploitation of WiFi or other insecure external communications
- **Local:** Exploitation of insecure local area communications within cyber perimeter defense
- **Physical:** Exploitation of insecure physical interfaces such as USB

POTENTIAL IMPACTS
- Maligned human-machine interface
- Changed/deleted control logic, firmware, files, or data
- Data and IP theft
Use Case Reference Architecture
• Basic cyber hygiene and best practices adopted from IT are the “low hanging fruit” but some measures will require a significant culture change on the shop floor

• Enabling operators to be a key partner in cyber defense is critical
  – Training and collaboration are needed to achieve buy-in
  – Viable shop floor concerns and priorities need to be understood and addressed to improve solution adoption

• Operations and network security personnel must develop a good working relationship and increase interaction
Technology Solutions (Near-Term)

• **Security Appliances**
  – Firewalls in use between enterprise and control system networks
  – A demilitarized zone (DMZ) is part of proper configuration and vetting communications
  – Intrusion detection systems that are properly configured for industrial control system (ICS)-specific protocols

• **ICS Configuration**
  – Application of multi-factor logic and sensing to validate application of more advanced logic before applying complex operations

• **Data Protection**
  – Consistent use of hashing or signature verification techniques to ensure the integrity or origin of design files as they are exchanged person to person or person to machine
Technology Solutions (Long-Term)

- **Integration of well recognized cyber defense mechanisms on proprietary networks and digital buses**
  - Secure solutions for legacy systems (bump-in-the-wire) and integration of security protocol advancements
  - Sentinel systems that seek and inhibit illogical control behavior
  - New sensor modalities for advanced attack detection and preventing subversion of security technologies by attacker

- **ICS Configuration**
  - Off-normal physical reporting in fusion with cyber detection mechanisms
  - Need for a combination of physical and cyber technologies for efficient detection
  - Hardware-based mutual authentication

- **Data Protection**
  - Automated, robust comparison of file data/file version against an approved reference file
Selected R&D Recommendations

- Automated vulnerability assessment technologies
- Scalable, high-fidelity autonomic cyber sensors
- Cyber-physical degradation and trust assessment analytics
- Integrated degradation context for human-machine interfaces
- Metrics that correlate investment to benefit
Discussion

• Did anything presented surprise you?

• What does a cyber-resilient manufacturing system look like?