Cybersecurity For
Advanced Manufacturing Forum

CFAM Technology Solutions Team

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

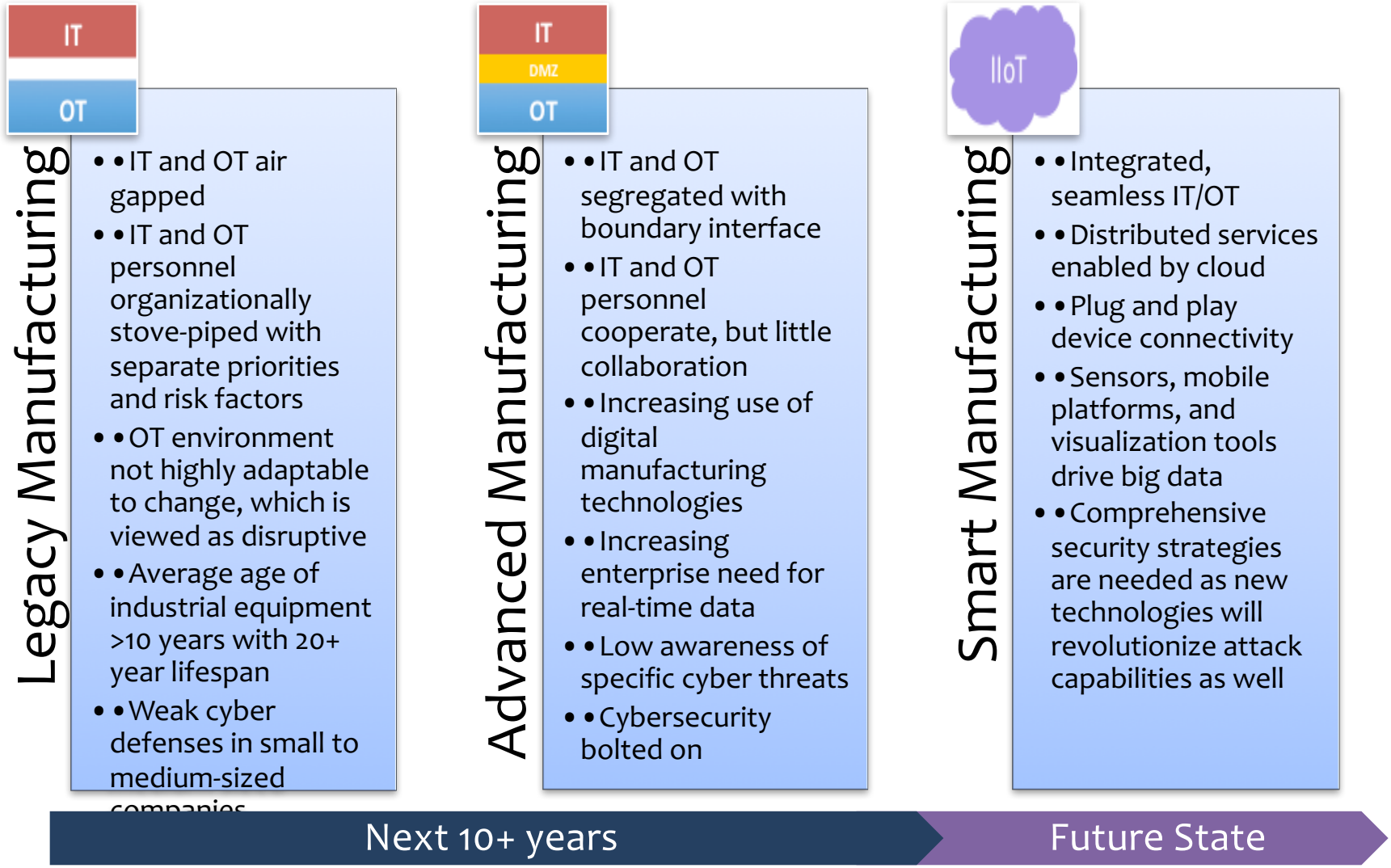
Lockheed Martin
Global Vision Center
Arlington, VA

November 15, 2016

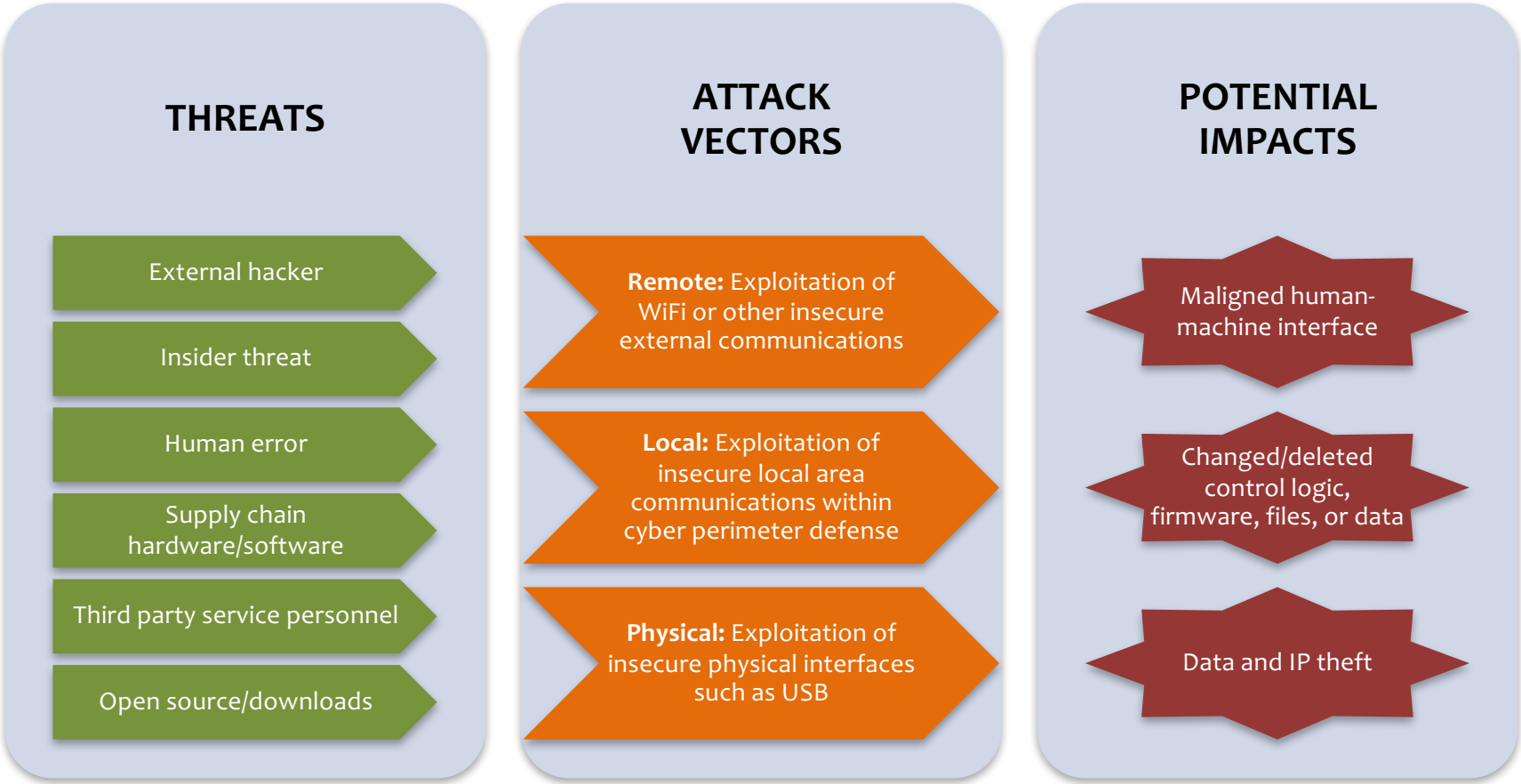
Technology Solutions Team

Robert Badgett Consultant	**Anitha Raj** ARAR Technology	**Devu Shila** United Technologies Research Center
Vicki Barbur MITRE	**Craig Rieger** Idaho National Laboratory	**Tim Shinbara** The Association for Manufacturing Technology
Heather Moyer Consultant	**Frank Serna** DRAPER	**Janet Twomey** Wichita State University

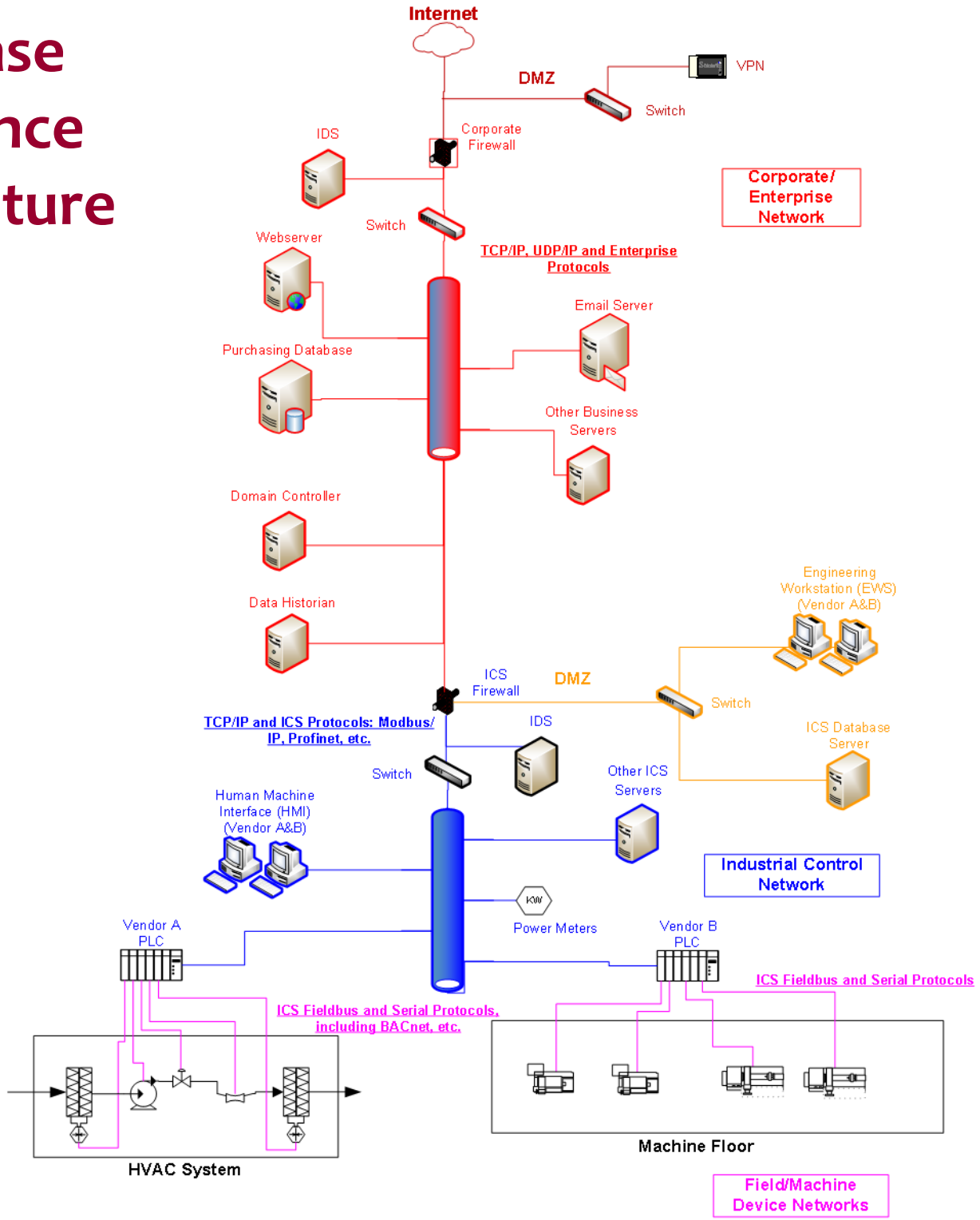
The Challenge



Attack Tree Analysis



Use Case Reference Architecture



Business Process Solutions

- **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**

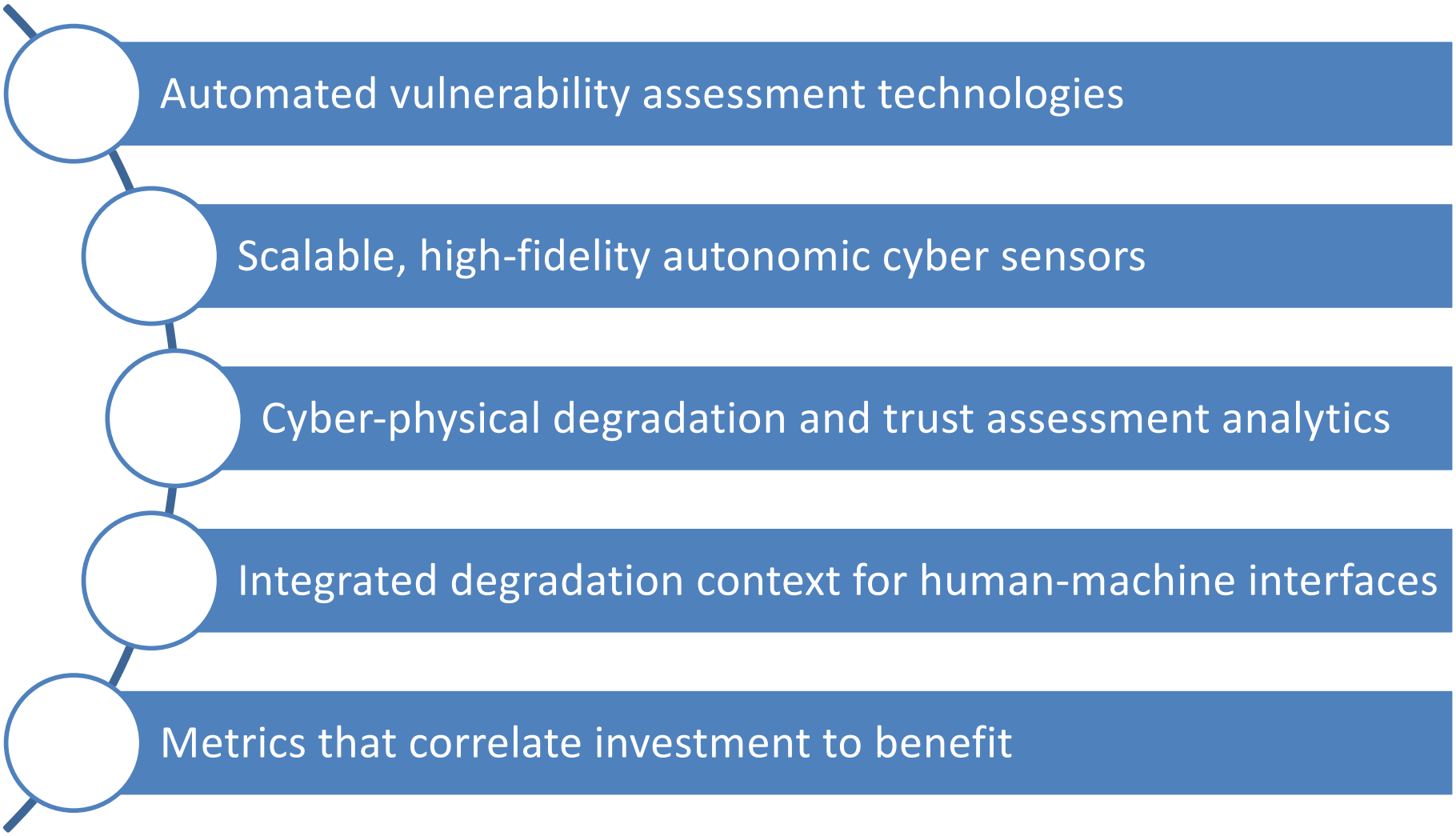
Technology Solutions (Near-Term)

- **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



Discussion

- **Did anything presented surprise you?**

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