Cybersecurity
for
Advanced Manufacturing:
Understanding the Digital Thread

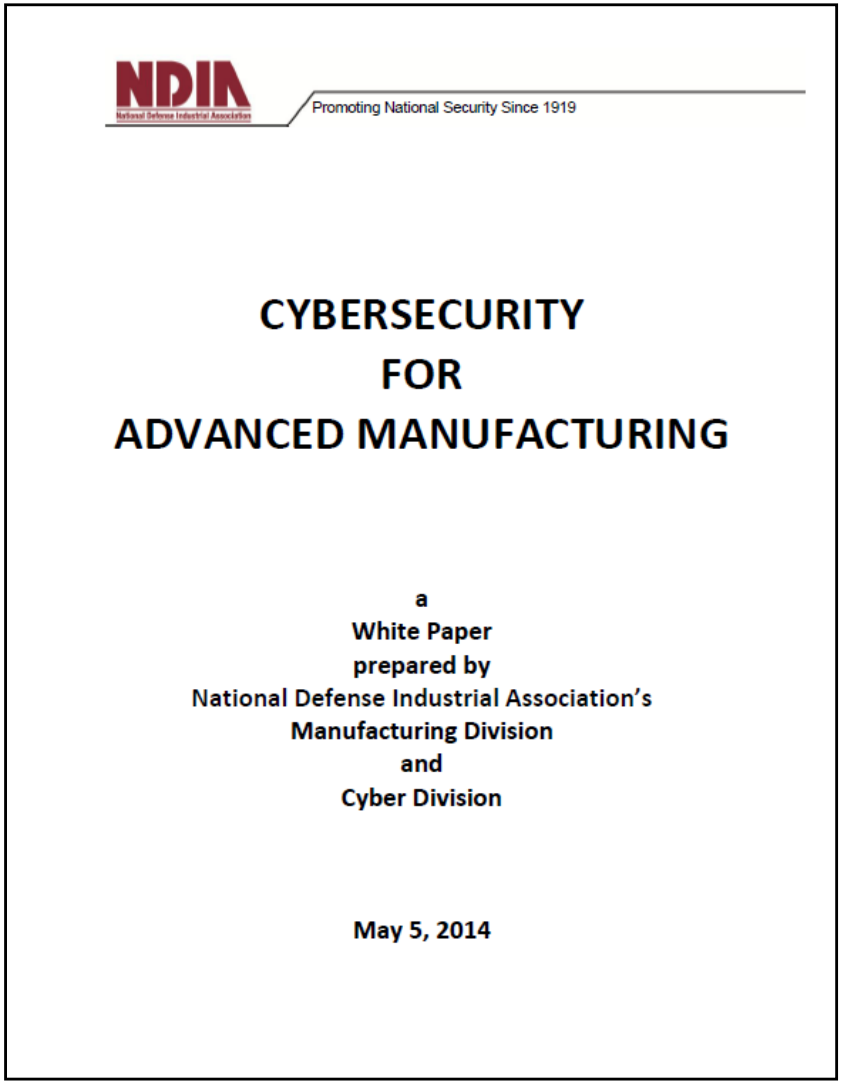
Presented to: NDIA's Cybersecurity for Advanced Manufacturing Forum

Presenter: Larry John, ANSER (Larry.John@anser.org)

Date: 15 November 2016

NDIA White Paper

Protecting the Digital Thread



NDIA National Defense Industrial Association

Promoting National Security Since 1919

CYBERSECURITY
FOR
ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

www.ndia.org/Divisions/Divisions/Manufacturing

Manufacturing Concerns:

- Theft of technical info -- can compromise national defense and economic security
- Alteration of technical data -- can alter the part or the process, with physical consequences to mission and safety
- Disruption or denial of process control -- can shut down production

A risk management problem.
Need resilience!

CFAM JWG Objective

Government and industry members of the CFAM JWG collaborate to build on recommendations in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing*

- **Identify cybersecurity vulnerabilities in the manufacturing environment and mitigations . . . *types and boundaries, highest impact near-term actions, culture changes***
- **Identify ways to incentivize and assist manufacturers to improve cybersecurity in manufacturing systems . . . *policies and contract requirements, security practices, workforce cybersecurity training***
- **Develop implementation plans . . . *coordinated with government and industry groups***

Focus Area

Multiple descriptions of covered information exist, including:

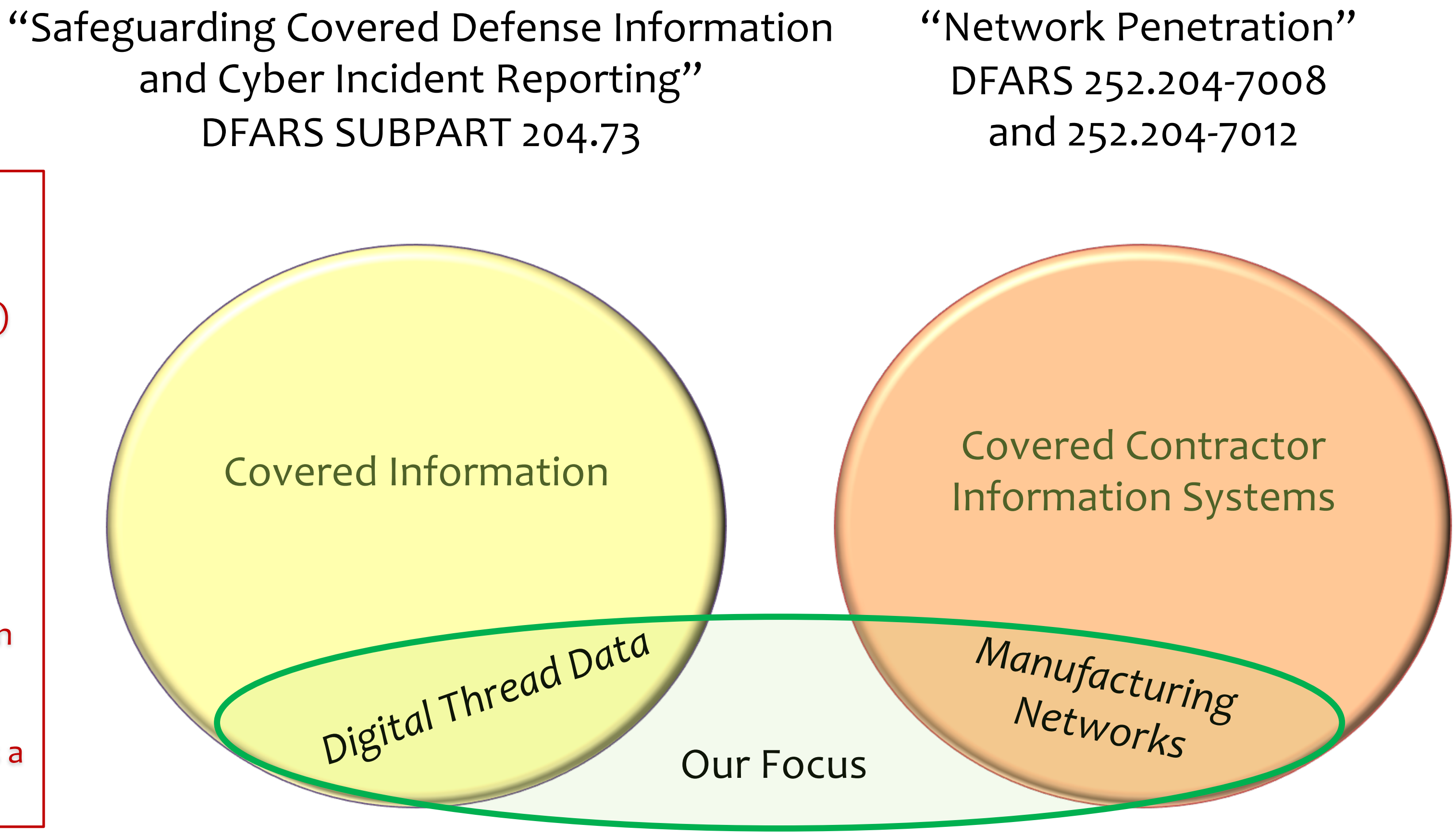
Covered Defense Information (CDI)

Unclassified Controlled Technical Information (UCTI)

Controlled Technical Information (CTI)

Controlled Unclassified Information (CUI)

For our study, we have used CDI as a standard nomenclature.


"Safeguarding Covered Defense Information and Cyber Incident Reporting"
DFARS SUBPART 204.73
"Network Penetration"
DFARS 252.204-7008 and 252.204-7012
Covered Information
Covered Contractor Information Systems
Digital Thread Data
Our Focus
Manufacturing Networks

Focus on:

- Operational technology networks and interfaces, not IT or enterprise networks
- Manufacturing cyber environment, not general cybersecurity

Operational Technology (OT) vs. IT
What's Different?

- **ICS systems are long-lived capital investments (15-20 year life)**
  - Obsolete operating systems and software are common
  - New systems architected for security, but hard to interoperate with old
- **"Production mindset" with little tolerance for OT down time**
  - Operate in real time with critical safety implications – cannot install patches without scheduled downtime and testing
  - Weak privilege management among operators and maintainers. Growing use of wireless devices.
  - Nascent cybersecurity awareness and limited workforce training.
- **Manufacturing differs from other ICS applications (e.g. Power Grid)**
  - Every manufacturing job brings new executable code into system
  - Tech data flowing through the system is a target

Modern Manufacturing

Industry Week Photo

- **Manufacturing is an increasingly digital business**
  - Smart Manufacturing
  - Industrial Internet of Things
  - Industry 4.0
  - …

- Advanced Manufacturing is:
  - <u>Networked</u> at every level to gain efficiency, speed, quality and agility
  - <u>Constantly learning</u> from models and data throughout the life cycle
  - <u>Driven by a "Digital Thread"</u> of product and process information
    - Source of competitive advantage for manufacturers and their customers
    - Source of military advantage for DoD
    - Demands protection throughout the product lifecycle
  - Has a "Digital Twin" (models and simulations) used to mirror and predict activities and performance of processes and products

NDIA Division Representation

Cyber

Dawn Beyer
Lockheed Martin Corporation

James Godwin
BriteWerx, Inc

Jason Gorey
Six O'Clock Ops

Michele Moss
Booz Allen Hamilton

Fran Zenzen
Arizona State Enterprise

Manufacturing

Dean Bartles
ASME

Larry John
ANSER

Michael McGrath
McGrath Analytics LLC

Catherine Ortiz
Defined Business Solutions

Chris Peters
The Lucrum Group

Tim Shinbara
The Association for Manufacturing Technology

Devu Shila
United Technologies Research Center

Joseph Spruill
Lockheed Martin Corp

Rebecca Taylor
Nat'l Center for Mfg. Sciences

Logistics

Marilyn Gaska (Team Leader)
Lockheed Martin Corp

Irv Varkonyi
SCOPE

Systems Engineering

Vicki Barbur
MITRE

David Huggins
Georgia Tech Research Institute

Thomas McCullough
Lockheed Martin Corporation

Thomas McDermott
Georgia Tech Research Institute

Heather Moyer (Team Leader)
Consultant

Frank Serna
Draper

Sarah Stern (Team Leader)
Boeing

CFAM JWG is a Diverse Team

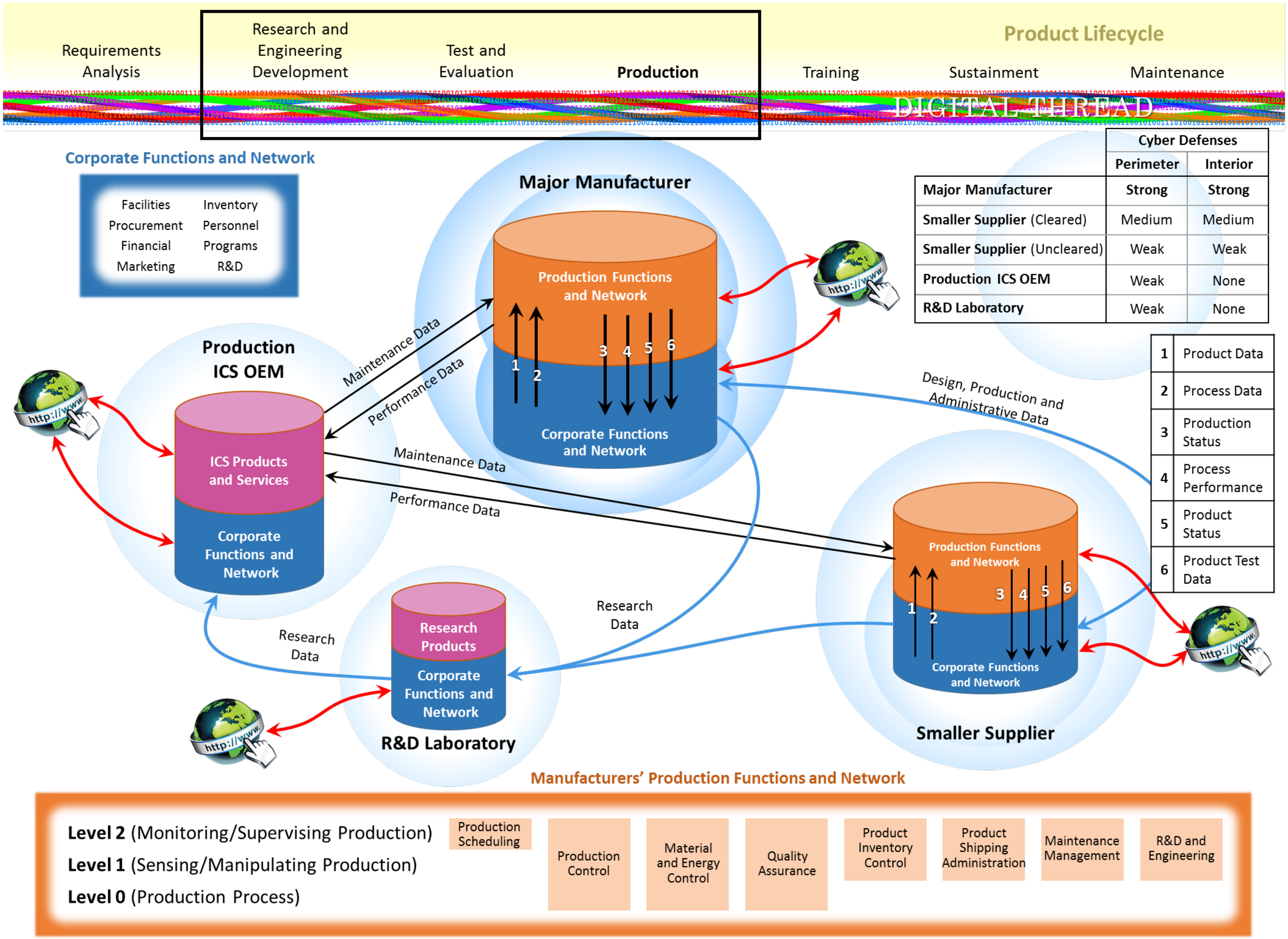
NDIA

48 participants: Government, Academia, Industry, Associations and FFRDCs

- **Government organizations:**
  - DoD Undersecretary for Acquisition, Technology & Logistics
  - DoD Chief Information Officer
  - Department of the Army
  - Space and Naval Warfare Systems Command
  - Air Force Research Laboratory
  - Department of Energy
  - National Institute of Standards and Technology
  - Defense Microelectronics Activity
  - Manufacturing Technology ODASD (MIBP)
  - Defense Intelligence Agency
  - Idaho National Laboratory
- **FFDRCs:**
  - Institute for Defense Analyses
  - MITRE
  - Sandia National Laboratories
- **Industry member organizations:**
  - National Defense Industrial Association (lead)
  - American Society of Mechanical Engineers
  - Association for Enterprise Information
  - Association for Manufacturing Technology
  - National Center for Manufacturing Sciences
- **Industry company representation:**
  - ANSER
  - ARAR Technology
  - Boeing
  - Booz Allen Hamilton
  - Defined Business Solutions LLC
  - DRAPER
  - GLOBALFOUNDRIES
  - IPDE Systems, Inc.
  - Lockheed Martin
  - McGrath Analytics LLC
  - MTEQ
  - PricewaterhouseCoopers
  - Six O'Clock Ops
  - SCOPE
  - The Lucrum Group
  - United Technologies Research Center
- **Academia:**
  - Arizona State University Research Enterprise
  - Georgia Tech Research Institute
  - Wichita State University

The Digital Thread as DoD sees It

NDIA



Product Lifecycle

Requirements Analysis

Research and Engineering Development

Test and Evaluation

Production

Training

Sustainment

Maintenance

DIGITAL THREAD

Corporate Functions and Network

Facilities
Procurement
Financial
Marketing

Inventory
Personnel
Programs
R&D

Major Manufacturer

Production Functions and Network

Corporate Functions and Network

Production ICS OEM

ICS Products and Services

Corporate Functions and Network

R&D Laboratory

Research Products

Corporate Functions and Network

Smaller Supplier

Production Functions and Network

Corporate Functions and Network

Maintenance Data

Performance Data

Research Data

Design, Production and Administrative Data

1 2 3 4 5 6

	Cyber Defenses	
	Perimeter	**Interior**
Major Manufacturer	**Strong**	**Strong**
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

Manufacturers' Production Functions and Network

Level 2 (Monitoring/Supervising Production)

Level 1 (Sensing/Manipulating Production)

Level 0 (Production Process)

Production Scheduling

Production Control

Material and Energy Control

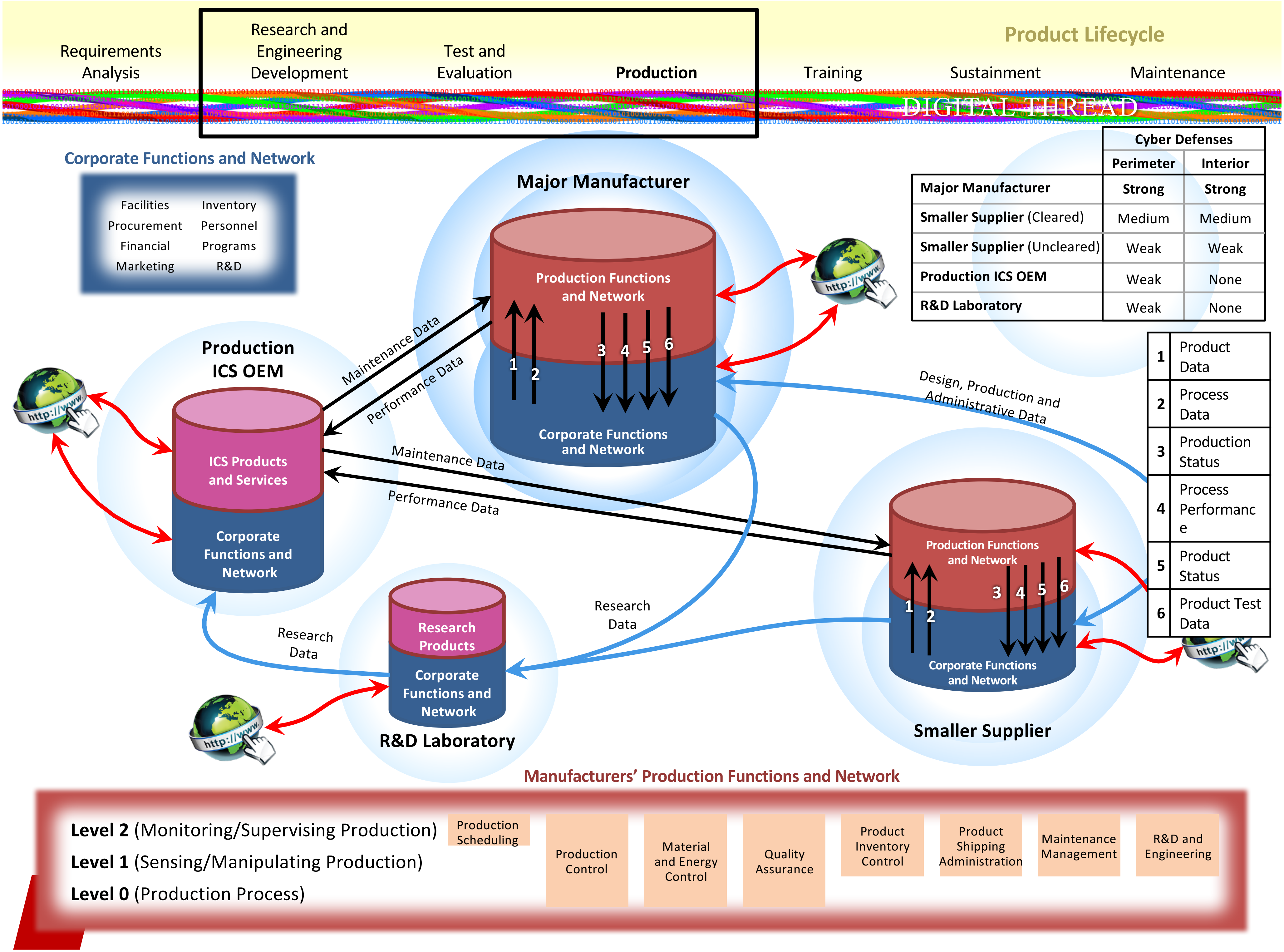
Quality Assurance

Product Inventory Control

Product Shipping Administration

Maintenance Management

R&D and Engineering



Product Lifecycle

Requirements Analysis

Research and Engineering Development

Test and Evaluation

Production

Training

Sustainment

Maintenance

DIGITAL THREAD

Corporate Functions and Network

Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D

Major Manufacturer

Production Functions and Network

Corporate Functions and Network

Production ICS OEM

ICS Products and Services

Corporate Functions and Network

R&D Laboratory

Research Products

Corporate Functions and Network

Smaller Supplier

Production Functions and Network

Corporate Functions and Network

	Cyber Defenses	
	Perimeter	**Interior**
Major Manufacturer	**Strong**	**Strong**
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

Manufacturers' Production Functions and Network

Level 2 (Monitoring/Supervising Production)

Level 1 (Sensing/Manipulating Production)

Level 0 (Production Process)

Production Scheduling

Production Control

Material and Energy Control

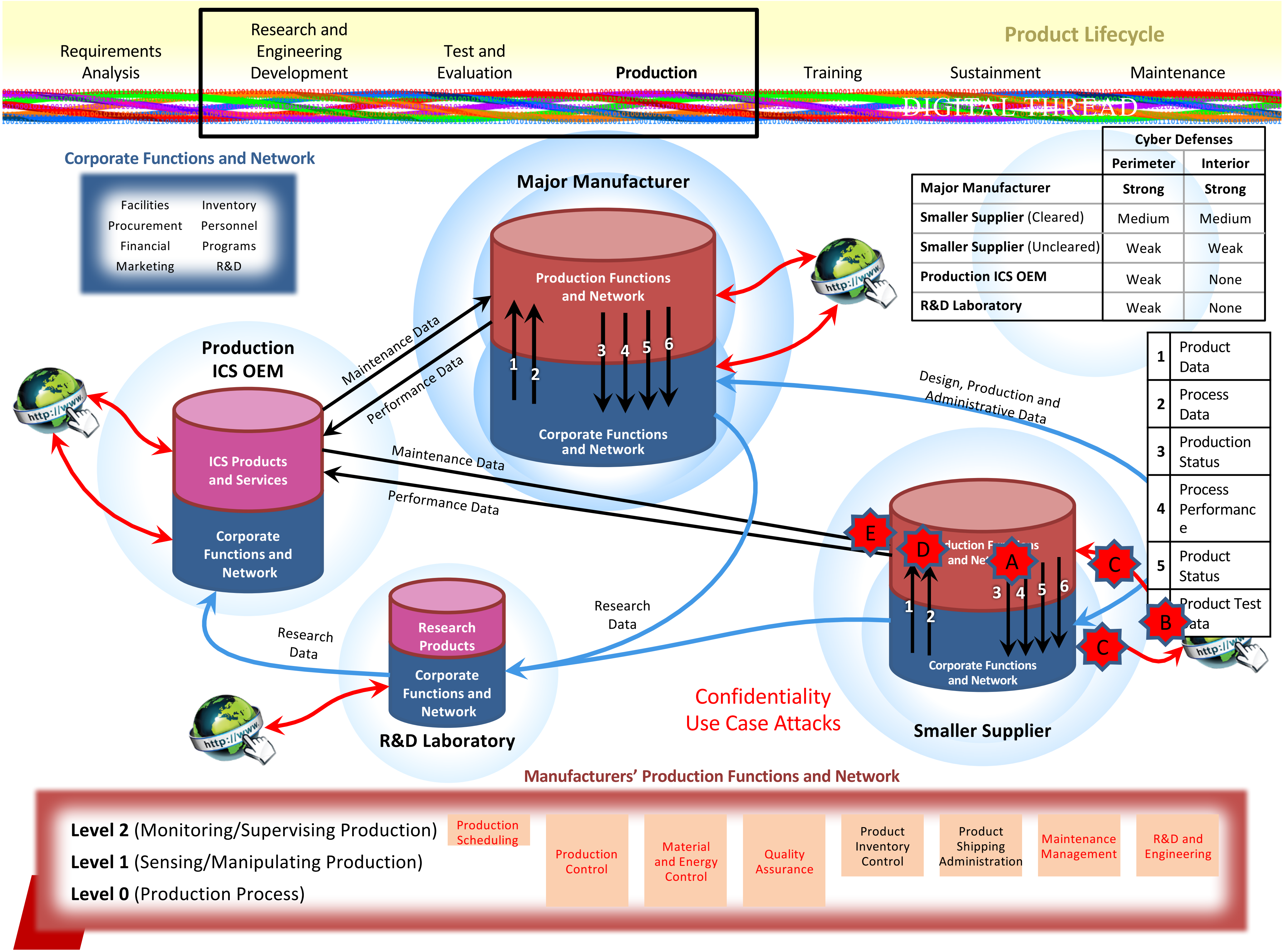
Quality Assurance

Product Inventory Control

Product Shipping Administration

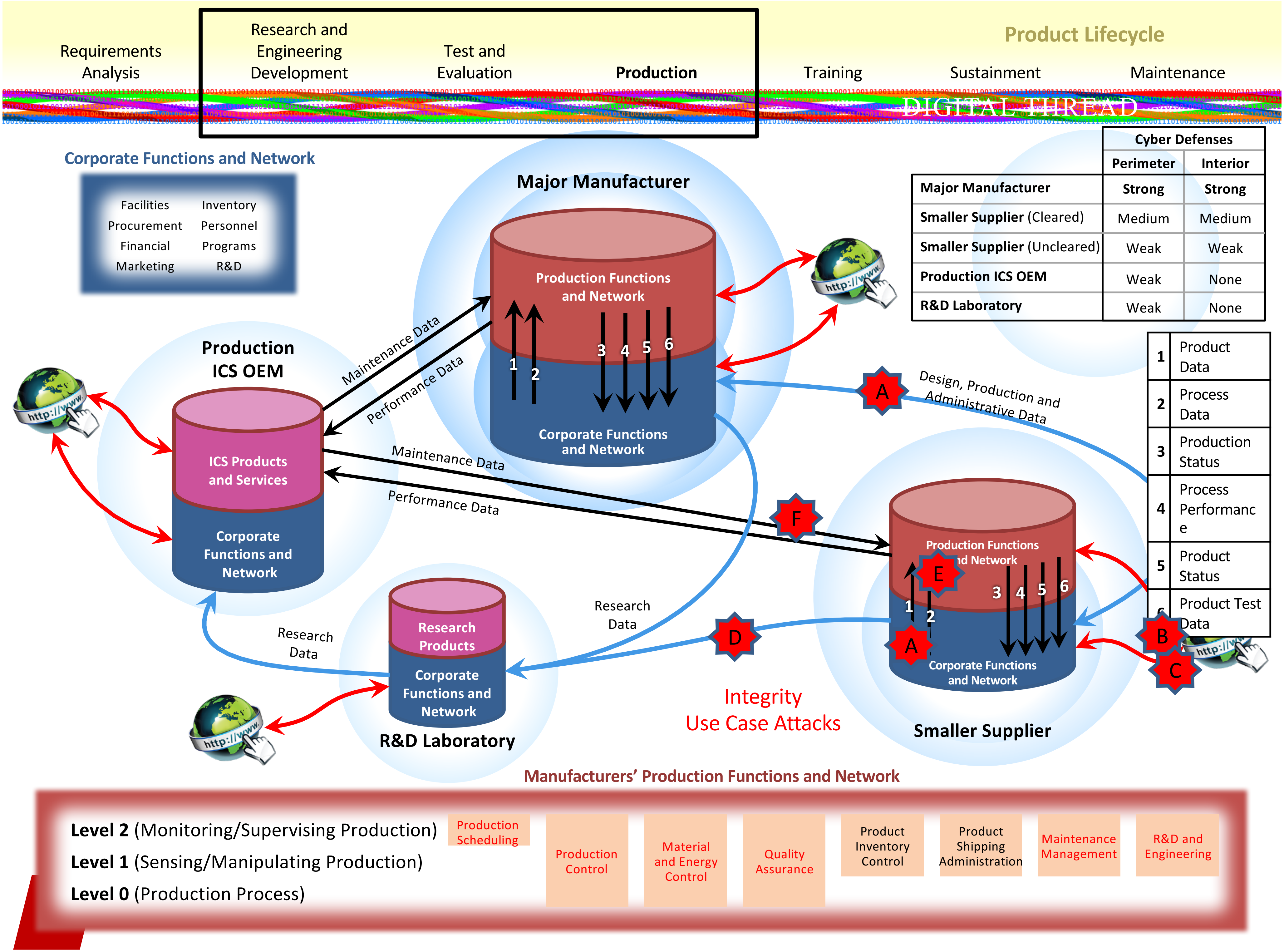
Maintenance Management

R&D and Engineering


Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D
Major Manufacturer
Production Functions and Network
1
2
3
4
5
6
Corporate Functions and Network
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
http://www.
E
D
A
B
C
C
duction F ns
and Ne
1
2
3
4
5
6
Corporate Functions and Network
Smaller Supplier
Confidentiality Use Case Attacks
Manufacturers' Production Functions and Network
Level 2 (Monitoring/Supervising Production)
Level 1 (Sensing/Manipulating Production)
Level 0 (Production Process)
Production Scheduling
Production Control
Material and Energy Control
Quality Assurance
Product Inventory Control
Product Shipping Administration
Maintenance Management
R&D and Engineering

	Cyber Defenses	
	Perimeter	Interior
Major Manufacturer	Strong	Strong
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test ata



Product Lifecycle

Requirements Analysis

Research and Engineering Development

Test and Evaluation

Production

Training

Sustainment

Maintenance

DIGITAL THREAD

Corporate Functions and Network

Facilities, Inventory, Procurement, Personnel, Financial, Programs, Marketing, R&D

	Cyber Defenses	
	Perimeter	**Interior**
Major Manufacturer	**Strong**	**Strong**
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performanc e
5	Product Status
6	Product Test Data

Major Manufacturer
Production Functions and Network
Corporate Functions and Network
1
2
3
4
5
6
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Maintenance Data
Performance Data
Design, Production and Administrative Data
A
F
Smaller Supplier
Production Functions and Network
E
A
B
C
Corporate Functions and Network
Research Data
Research Data
D
Research Products
Corporate Functions and Network
R&D Laboratory
http://www.

Integrity Use Case Attacks

Manufacturers' Production Functions and Network

Level 2 (Monitoring/Supervising Production)

Level 1 (Sensing/Manipulating Production)

Level 0 (Production Process)

Production Scheduling

Production Control

Material and Energy Control

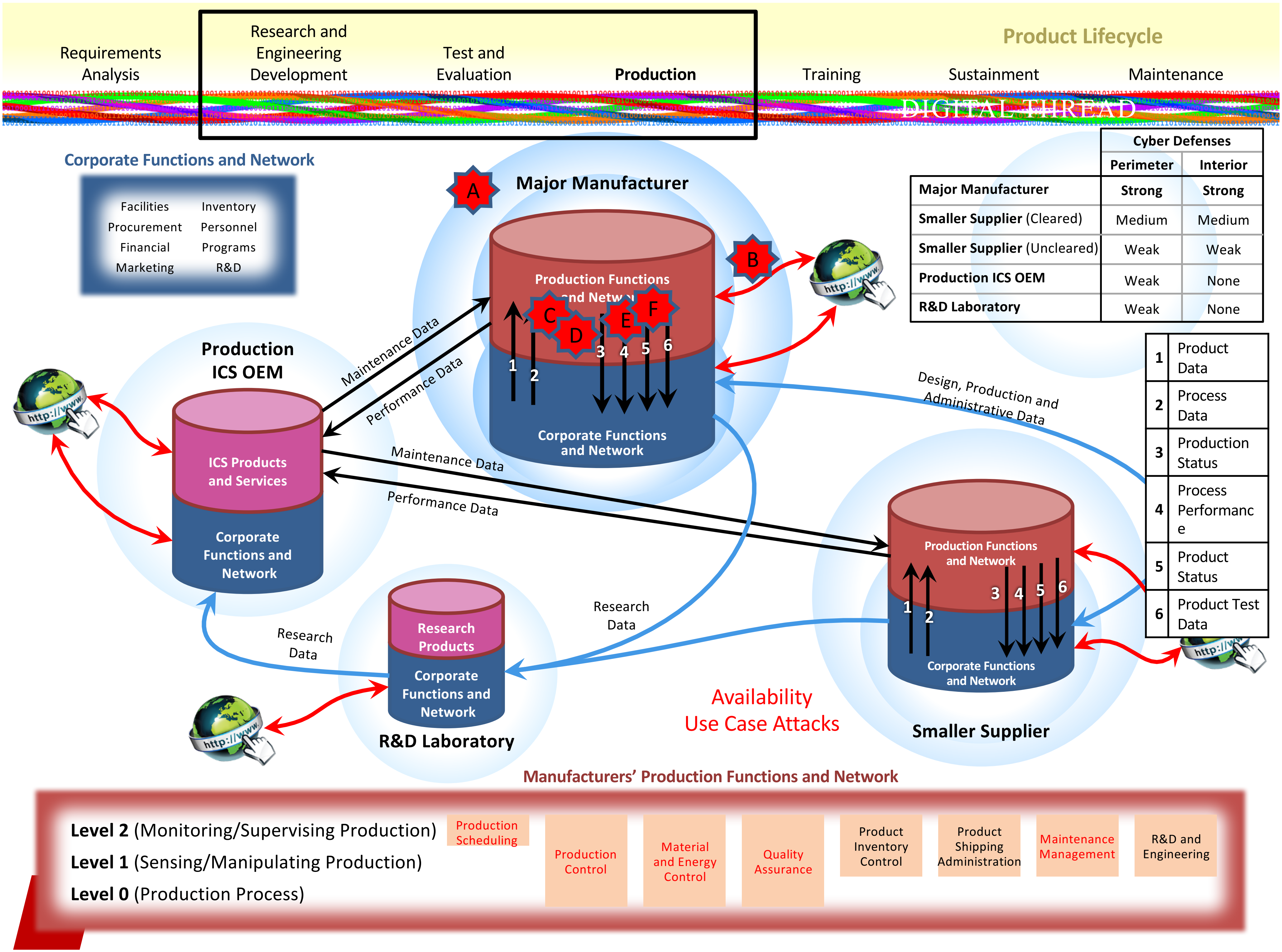
Quality Assurance

Product Inventory Control

Product Shipping Administration

Maintenance Management

R&D and Engineering

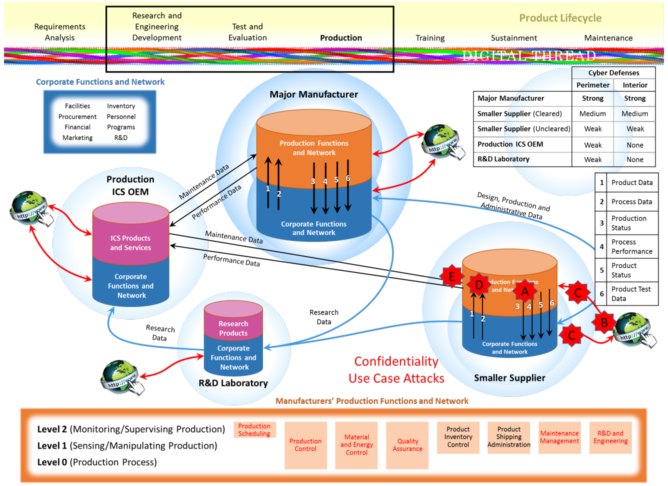

Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D
A
Major Manufacturer
B
Production Functions and Network
C
D
E
F
1
2
3
4
5
6
Corporate Functions and Network
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
Production Functions and Network
1
2
3
4
5
6
Corporate Functions and Network
Smaller Supplier
http://www.
Availability Use Case Attacks
Manufacturers' Production Functions and Network
Level 2 (Monitoring/Supervising Production)
Level 1 (Sensing/Manipulating Production)
Level 0 (Production Process)
Production Scheduling
Production Control
Material and Energy Control
Quality Assurance
Product Inventory Control
Product Shipping Administration
Maintenance Management
R&D and Engineering

	Cyber Defenses	
	Perimeter	Interior
Major Manufacturer	**Strong**	**Strong**
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performanc e
5	Product Status
6	Product Test Data

The Digital Thread is Vulnerable

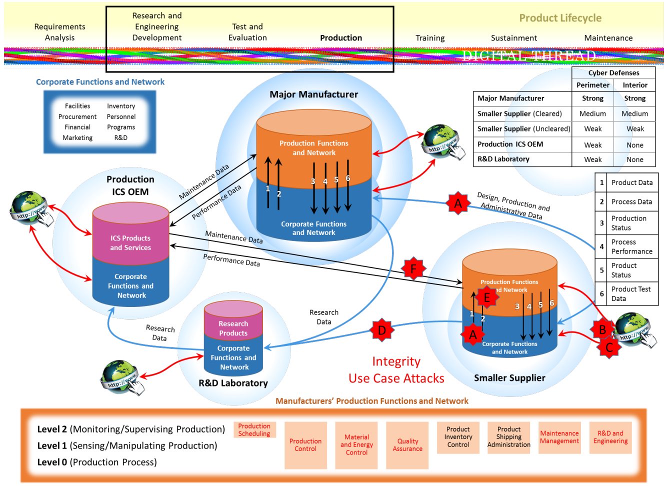
Confidentiality


Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D
Major Manufacturer
Production Functions and Network
Corporate Functions and Network
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
Production Functions and Network
Corporate Functions and Network
Smaller Supplier
A
B
C
C
D
E
1
2
3
4
5
6
http://www.
Confidentiality Use Case Attacks
Manufacturers' Production Functions and Network
Level 2 (Monitoring/Supervising Production)
Level 1 (Sensing/Manipulating Production)
Level 0 (Production Process)
Production Scheduling
Production Control
Material and Energy Control
Quality Assurance
Product Inventory Control
Product Shipping Administration
Maintenance Management
R&D and Engineering

	Cyber Defenses	
	Perimeter	Interior
Major Manufacturer	Strong	Strong
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

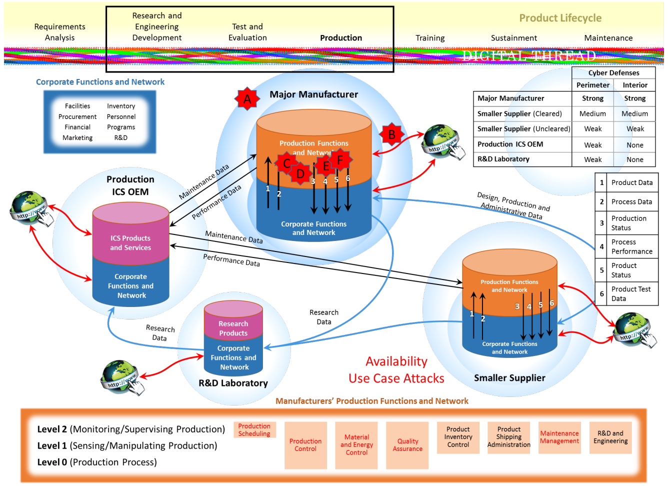
Integrity


Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D
Major Manufacturer
Production Functions and Network
Corporate Functions and Network
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
Production Functions and Network
Corporate Functions and Network
Smaller Supplier
A
A
B
C
D
E
F
1
2
3
4
5
6
http://www.
Integrity Use Case Attacks
Manufacturers' Production Functions and Network
Level 2 (Monitoring/Supervising Production)
Level 1 (Sensing/Manipulating Production)
Level 0 (Production Process)
Production Scheduling
Production Control
Material and Energy Control
Quality Assurance
Product Inventory Control
Product Shipping Administration
Maintenance Management
R&D and Engineering

	Cyber Defenses	
	Perimeter	Interior
Major Manufacturer	Strong	Strong
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

Availability


Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D
Major Manufacturer
Production Functions and Network
Corporate Functions and Network
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
Production Functions and Network
Corporate Functions and Network
Smaller Supplier
A
B
C
D
E
F
1
2
3
4
5
6
http://www.
Availability Use Case Attacks
Manufacturers' Production Functions and Network
Level 2 (Monitoring/Supervising Production)
Level 1 (Sensing/Manipulating Production)
Level 0 (Production Process)
Production Scheduling
Production Control
Material and Energy Control
Quality Assurance
Product Inventory Control
Product Shipping Administration
Maintenance Management
R&D and Engineering

	Cyber Defenses	
	Perimeter	Interior
Major Manufacturer	Strong	Strong
Smaller Supplier (Cleared)	Medium	Medium
Smaller Supplier (Uncleared)	Weak	Weak
Production ICS OEM	Weak	None
R&D Laboratory	Weak	None

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

- Insiders can do recon and data exfiltration or alter design or process control files
- Insecure external/internal communications can be exploited to steal design data
- Sensors embedded in equipment can contain malware
- Visitors and contractors may have extensive or unsupervised access to software, firmware and hardware
- Tainted firmware from supply chain can contain sophisticated malware
- HVAC systems can be used to alter the process environment to damage/destroy products

<u>Threat Types</u>

- Adversarial
- Accidental
- Structural
- Environmental

<u>Vulnerability Types</u>

- Policy and Procedure
- Architecture and Design
- Configuration Management
- Physical
- Software Development
- Communication and Network

NIST 800-82 rev. 2

Large companies may be OK on their own, <u>but</u>

what about the small and mid-size firms that may be connected to the big companies?

Small and Mid-Size Firms

- Often lack cybersecurity knowledge and resources. Most have no full time cybersecurity staff
  - *ISA99 Standards and NIST SP 800-82 are complex. No turnkey solutions.*
  - *Forums available to large companies are often beyond their reach – e.g. DIB CS/IA Program requires facility clearance and COMSEC account*
  - *Cannot afford differing cybersecurity requirements from different customers*

- **Believe they are not targets, so they focus on perimeter defense for IT network**
  - *Lack of compartmentalization despite standards calling for discrete zones and conduits*
  - *Vulnerable to OEM backdoors, default passwords, discoverable IP addresses, connection by portable devices, connection from outside networks*

May simply lack a business case for investing in OT cybersecurity

Status

- **Each working group will present their findings and recommendations** ***. . . comments from today will be incorporated into final white paper***

- **Website will continued to be updated on NDIA portal** ***. . . found under Industrial Working Groups***

- **Outreach plan developed to share progress** ***. . . first public forum was in August, this second forum is to share findings; CFAM session at DMC on November 29th***

- **Goal is to brief senior OSD leadership in December 2016** ***. . . Formal report will be coordinated within DoD, and other government agencies as appropriate, after new leadership team is in place***