NARRATIVE FOR DRAFT DIGITAL THREAD SLIDES

PRODUCTION SLIDE

This slide illustrates what we call the "Digital Thread." The digital thread is the set of digitally created, stored and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle, which is shown across the top of the slide.

1. Assume the existence of a major manufacturer or system integrator. This firm has a set of corporate (blue) and production (tan) functions that are supported by one or more networks. In general, corporate functions and the networks that support them include those listed in the box in the upper left corner of the slide.
2. The major manufacturer is supported by one or more R&D Labs, with whom they exchange research data.
3. The major manufacturer works with one or more smaller suppliers, with whom they share design, production and administrative data, and which may also be connected to some of the R&D labs.
4. The major manufacturer and related suppliers leverage Industrial Control Systems and related ICS maintenance services provided by one or more OEMs. The OEM's clients receive Maintenance Data and Services and provide ICS performance data to the OEM to support current maintenance activities and future product improvements. The OEM may also receive research data from the R&D Lab to support development or refinement of the OEM's products.
5. Each of the organizations is connected to the Internet and has perimeter cyber defense capabilities.
6. The major manufacturer uses a segmented architecture that provides separate internal cyber defense capabilities for its corporate and production networks (darker blue bubbles). The smaller supplier has interior defenses for its corporate network, but its architecture is not segmented and its production network may lack a separate set of defense capabilities.
7. In general, we categorize the efficacy of the cyber defenses at a high level as shown in the box in the upper right side of the slide.
8. Within each firm, data may be exchanged between the corporate and production networks (for simplicity, we show these exchanges in only the major and smaller suppliers). The general types of data are listed in the box on the right side of the slide.
9. Finally, we see a three-level decomposition of the functions that may be executed in the production networks. This list was extracted from the Supporting Activity Model in ISA 95. In terms of cybersecurity, these functions represent portions of the manufacturing process that could be adversely affected by cyber attacks.

Red stars containing letters show potential attack points used in each use case. Also red lettering in the large box at the bottom of the slide indicates production functions that may serve as targets and may be adversely affected by cyber attacks.

Confidentiality Use Case:

A. Adversarial insider with authorized access to production and test equipment.
B. Theft of data from CAD/CAM workstations by malicious 3rd party exploiting insecure external communications and vulnerabilities of perimeter cyber defense.
C. Theft of data on-site from CAD/CAM workstations by malicious 3rd party exploiting insecure local area communications (within cyber perimeter defense).
D. Embedded sensors within manufacturing equipment containing malicious hardware/software capable of transmitting data to an external location.
E. Theft of data by visitors (specifically maintenance personnel) with extensive or unsupervised access to manufacturing equipment.

Integrity Use Case:

A. Rogue designers inserting malicious logic into the CAD model, .STL file or Tool command file.
B. 3rd party models or files embedded with unwanted logic.
C. Malicious 3rd party CAD/CAM software that inserts extraneous or deletes logic into the models/files
D. Tampers models/files/control parameters via Malware infection (by exploiting insecure external communications and software vulnerabilities of CAD/CAM software or operating systems)
E. Modifying files or process control parameters by exploiting insecure local area communications
F. Update controller firmware by exploiting insecure physical interfaces such as USB

Availability Use Case

A. Malicious 3rd party performed reconnaissance to find available WiFi signals emanating from a facility
B. Malicious device inserted through WiFi to BACnet
C. Modification to smart damper identity performed via malicious device
D. M Control signal to exhaust damper modified to drive closed
E. Malicious device replaces smart damper as interface to human machine interface
F. Autonomous system reacts as programmed to loss of damper

SUSTAINNENT SLIDE

This slide illustrates what we call the "Digital Thread." The digital thread is the set of digitally created, stored and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle, including sustainment, which is shown at the top of the slide.

1. Assume the existence of a major manufacturer or system integrator. This firm has a set of corporate (blue) and production (tan) functions that are supported by one or more networks. In general, corporate functions and the networks that support them include those listed in the box in the lower left corner of the slide.
2. The major manufacturer supports the U.S Government Sustainment System, which executes program management, acquisition and logistics functions as well as a set of corporate functions. The government's sustainment system sends product status data, product performance data and maintenance performance data to the Major manufacturer, which responds with proposed updated design data. In response to these, the Major Manufacturer submits proposed design updates and receives approved, updated designs from the Government.
3. Both the major manufacturer and the Government sustainment system work with one or more smaller suppliers. The smaller supplier sends proposed updated designs to the Government and the major manufacturer, as needed, and receives approved updated designs.
4. The major manufacturer and related suppliers leverage Industrial Control Systems and related ICS maintenance services provided by one or more OEMs. The OEM's clients receive Maintenance Data and Services and provide ICS performance data to the OEM to support current maintenance activities and future product improvements. The OEM may also receive research data from the R&D Lab to support development or refinement of the OEM's products.
5. Each of the organizations is connected to the Internet and has perimeter cyber defense capabilities.
6. The major manufacturer uses a segmented architecture that provides separate internal cyber defense capabilities for its corporate and production networks. The smaller supplier has interior defenses for its corporate network, but its architecture is not segmented and its production network may lack a separate set of defense capabilities.
7. In general, we categorize the efficacy of the cyber defenses at a high level as shown in the box in the upper left corner of the slide.
8. Within each firm, data may be exchanged between the corporate and production networks (for simplicity, we show these exchanges in only the major and smaller suppliers). The general types of data are listed in the box in the top tight corner of the slide.
9. Ideally, we would have a decomposition of the functions that would be executed in the sustainment networks, and that model would mirror the Supporting Activity Model in ISA 95. In terms of cybersecurity, such functions would represent portions of the manufacturing process that could be adversely affected by cyber attacks.