# Cybersecurity in Manufacturing, Advanced

## 8496 36 weeks

## Table of Contents

# Acknowledgments

The components of this instructional framework were developed by the following curriculum development panelists:

Matthew Brame, Instructor, Millbrook High School, Frederick County Public Schools
Dr. Gregory Braxton, Senior Computer System Security Analyst, Huntington Ingalls Industries, Newport News Shipbuilding, Newport News
Brittany Carper, Instructor, Sherando High School, Frederick County Public Schools
Kenneth Crowther, Product Security Leader, General Electric, Richmond
Dr. Chuck Gardner, Director of Curriculum, National Integrated Cyber Education Research Center (NICERC), Bossier City, LA

Ivan Gil, Senior Information Security Consultant, SLAIT Consulting, an ePlus Technology Inc., Glen Allen
Bradley Nickens, Staff Product Security Analyst, General Electric, Richmond
Dr. David Raymond, Director, Virginia Cyber Range, Virginia Tech, Blacksburg
Justin Upchurch, Lead Cybersecurity Engineer, Huntington Ingalls Industries, Newport News Shipbuilding, Newport News

Correlations to the Virginia Standards of Learning were reviewed and updated by:

Leslie R. Bowers, English Teacher (ret.), Newport News Public Schools
Vickie L. Inge, Mathematics Committee Member, Virginia Mathematics and Science Coalition
Anne F. Markwith, New Teacher Mentor (Science), Gloucester County Public Schools
Michael L. Nagy, Social Studies Department Chair, Rustburg High School, Campbell County Public Schools

The framework was edited and produced by the CTE Resource Center:

Heather A. Widener, Writer/Editor
Kevin P. Reilly, Administrative Coordinator

Virginia Department of Education Staff

Dr. Lynn Basham, Specialist, Technology Education and Related Clusters
Dr. Tricia S. Jacobs, CTE Coordinator of Curriculum and Instruction
Dr. David S. Eshelman, Director, Workforce Development and Initiatives
George R. Willcox, Director, Operations and Accountability

Office of Career, Technical, and Adult Education
Virginia Department of Education

# Course Description

**Suggested Grade Level:** 10 or 11 or 12
**Prerequisites:** 8499

This course will continue to expose students to the revolutionary and growing field of cybersecurity as it relates to manufacturing. Students will apply the principles of cybersecurity, research emerging technologies, analyze threat intelligence, and design protective measures. Students will participate in enterprise team activities to secure automated production processes, while demonstrating cybersecurity concepts and policies.

# Task Essentials Table

- Tasks/competencies designated by plus icons (⊕) in the left-hand column(s) are essential
- Tasks/competencies designated by empty-circle icons (○) are optional
- Tasks/competencies designated by minus icons (⊖) are omitted
- Tasks marked with an asterisk (*) are sensitive.

| Task Number | 8496 | Tasks/Competencies |
|---|---|---|
| Practicing Safety in Manufacturing | | |
| 39 | ⊕ | Use required personal protective equipment (PPE). |
| 40 | ⊕ | Implement a safety plan. |
| 41 | ⊕ | Maintain safe working practices around production equipment. |
| 42 | ⊕ | Operate lab equipment according to instructor guidelines. |
| Analyzing Automated Production Processes | | |
| 43 | ⊕ | Outline manufacturing processes. |
| 44 | ⊕ | Distinguish among automation systems used by subsectors within manufacturing. |
| 45 | ⊕ | Define *data flow*. |
| 46 | ⊕ | Identify cybersecurity considerations throughout the stages in the engineering design process. |
| 47 | ⊕ | Analyze use of computer-aided design (CAD), three-dimensional (3D) printing, and computer-aided manufacturing (CAM) in manufacturing. |
| 48 | ⊕ | Describe the use of a programmable logic controller (PLC) and microcontroller. |
| 49 | ⊕ | Develop a control system with open and/or closed loops. |
| Exploring Current Issues in Cybersecurity in Manufacturing | | |
| 50 | ⊕ | Describe the current state of cybersecurity in manufacturing. |
| 51 | ⊕ | Research emerging technologies. |

| | | | |
|---|---|---|---|
| 52 | ⊕ | Identify industry challenges. | |
| Applying Cybersecurity Standards and Regulations to Manufacturing Systems | | | |
| 53 | ⊕ | Explain laws and regulations applicable to cybersecurity in manufacturing systems. | |
| 54 | ⊕ | Describe the importance of cybersecurity standards applicable to manufacturing systems. | |
| Evaluating Vulnerabilities, Risks, and Threats in Manufacturing Systems | | | |
| 55 | ⊕ | Describe the relationship among risks, vulnerabilities, and threats. | |
| 56 | ⊕ | Identify resources for vulnerability information specific to manufacturing. | |
| 57 | ⊕ | Describe threats to ICS. | |
| 58 | ⊕ | Explain cybersecurity risks within a supply chain. | |
| 59 | ⊕ | Perform a risk assessment. | |
| Applying System Security Procedures and Risk Management in Automated Production Processes | | | |
| 60 | ⊕ | Develop a system security plan for an automated production process. | |
| 61 | ⊕ | Propose incident response procedures. | |
| 62 | ⊕ | Define *cyber threat intelligence*. | |
| 63 | ○ | Apply digital forensics to an automated production process. | |
| Securing a Manufacturing Enterprise | | | |
| 64 | ⊕ | Apply the engineering design process. | |
| 65 | ⊕ | Plan a product/process. | |
| 66 | ⊕ | Describe trade secrets and proprietary information of a manufacturing enterprise. | |
| 67 | ⊕ | Design the prevention of and protections against cyber threats for a manufacturing enterprise. | |
| 68 | ⊕ | Secure the product using cybersecurity best practices. | |

Legend: ⊕Essential ○Non-essential ⊖Omitted

# Curriculum Framework

# Practicing Safety in Manufacturing

## Task Number 39

## Use required personal protective equipment (PPE).

### Definition

Use should include

- identifying potential hazards
- identifying safety data sheets (SDS)
- describing equipment that protects against each hazard
- wearing PPE when performing hazardous tasks.

### Process/Skill Questions

- What are the names and purposes of five pieces of PPE?
- When would it be necessary to wear PPE?

## Task Number 40

## Implement a safety plan.

### Definition

Implementation should include

- taking a safety proficiency test with a 100 percent pass rate
- adhering to basic safety rules
- pre-job briefing.

### Process/Skill Questions

- Why is it important to pass the safety test with a score of 100 percent?
- What could happen if safety rules are not followed?

## Task Number 41

## Maintain safe working practices around production equipment.

### Definition

Maintenance should include

- identifying potential hazards of each piece of equipment
- demonstrating safe work habits with each type of equipment.

### Process/Skill Questions

- What are the risks of unsafe behavior around production equipment?
- How would safety rules help prevent these risks?
- How does the Occupational Safety and Health Administration (OSHA) affect safety in manufacturing?

## Task Number 42

## Operate lab equipment according to instructor guidelines.

### Definition

Operation should include

- following posted safety rules for each piece of equipment
- using guards as required
- passing a proficiency demonstration with the instructor.

### Process/Skill Questions

- How are the posted safety rules for any two pieces of equipment similar and different?
- Why are guards necessary?
- How would a user know if he or she is using a piece of equipment improperly?

# Analyzing Automated Production Processes

# Task Number 43

## Outline manufacturing processes.

### Definition

Outline should also include the use of automation and the use of additive processes in manufacturing, as well as processes such as:

- Custom (e.g., job shop)
- Intermittent (e.g., job shop, batch, discrete)
- Flexible
- Continuous manufacturing

Outline should include a comparison of manufacturing operations that employ a combination of these types of processes.

### Process/Skill Questions

- What type of manufacturing processes do major automobile makers use?
- What are examples of custom-made products?
- What does continuous manufacturing mean? What might be made using that type of production?
- When would each type of manufacturing be used?

# Task Number 44

## Distinguish among automation systems used by subsectors within manufacturing.

### Definition

Distinction may include subsectors such as

- Food Manufacturing: NAICS 311
- Beverage and Tobacco Product Manufacturing: NAICS 312
- Textile Mills: NAICS 313
- Textile Product Mills: NAICS 314
- Apparel Manufacturing: NAICS 315
- Leather and Allied Product Manufacturing: NAICS 316

- Wood Product Manufacturing: NAICS 321
- Paper Manufacturing: NAICS 322
- Printing and Related Support Activities: NAICS 323
- Petroleum and Coal Products Manufacturing: NAICS 324
- Chemical Manufacturing: NAICS 325
- Plastics and Rubber Products Manufacturing: NAICS 326
- Nonmetallic Mineral Product Manufacturing: NAICS 327
- Primary Metal Manufacturing: NAICS 331
- Fabricated Metal Product Manufacturing: NAICS 332
- Machinery Manufacturing: NAICS 333
- Computer and Electronic Product Manufacturing: NAICS 334
- Electrical Equipment, Appliance, and Component Manufacturing: NAICS 335
- Transportation Equipment Manufacturing: NAICS 336
- Furniture and Related Product Manufacturing: NAICS 337
- Miscellaneous Manufacturing: NAICS 339

Source: https://www.bls.gov/home.htm

Teacher resource: What is industrial automation, Electrical Technology

### Process/Skill Questions

- What manufacturing industries are located in the local geographic area?
- What types of jobs might be available in a manufacturing industry?
- What jobs in a company might be directly related to the production of products?
- Who are the people in the local area that work in manufacturing?
- How might the local geographical area benefit from manufacturing?

## Task Number 45

## Define *data flow*.

### Definition

Definition includes

- understanding communication requirements between automation components
- using a tool (e.g., Wireshark) to confirm and understand actual communications across automated networks
- recognizing industrial protocols (e.g., Modbus, Common Industrial Protocol [CIP]).

Teacher resources:
How to Improve Process Control by Automating Data Flow, Automation  Direct
What is a Data Flow Diagram?, Visual Paradigm

### Process/Skill Questions

- How do industrial protocols differ from traditional network protocols?
- What is the difference between unidirectional and bidirectional data flow?

# Task Number 46

# Identify cybersecurity considerations throughout the stages in the engineering design process.

### Definition

Identification should include a review of the engineering design process, particularly the following stages:

- Identify the requirement and constraints of the design problem, including cybersecurity considerations.
- Evaluate the requirements and constraints of each solution to the design problem, including cybersecurity considerations.
- Justify an optimal solution to the design problem, including cybersecurity considerations.
- Determine the objectives for an engineering test of the solution to the design problem, including cybersecurity considerations.
- Test the solution to the design problem, using mathematical, conceptual, and/or physical modeling, simulating, and optimizing (including cybersecurity considerations).
- Evaluate the test results, including cybersecurity considerations.

Identification includes cybersecurity considerations such as the following:

- Security requirements
- Threat modeling
- Source code review
- Security testing
- Incident response

Teacher resource:
Layered Blueprints: A Method for Engineering OT Security (video), Sarah Fluchs, Security Consultant, Admeritia

### Process/Skill Questions

- What's the earliest stage during which one can perform threat modeling?
- Why is threat modeling important?
- Why is security testing important?

## Task Number 47

## Analyze use of computer-aided design (CAD), three-dimensional (3D) printing, and computer-aided manufacturing (CAM) in manufacturing.

### Definition

Analysis includes

- a 3D CAD model
- the relationship among CAD, computer-aided engineering (CAE), and CAM
- rapid prototyping
- use of computer numerical control (CNC) machine tools.

Teacher resource:
An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity, A SANS Analyst Whitepaper

### Process/Skill Questions

- What is the difference among CAD, CAE, and CAM?
- What is an example of rapid prototyping?
- Why is data security important? What are some considerations for securing design files?

## Task Number 48

## Describe the use of a programmable logic controller (PLC) and microcontroller.

### Definition

Description should include

- ladder logic
- structured text
- function block diagram (FBD)
- sequential function chart (SFC)
- instruction list (IL).

Description also includes

- features of different types of controllers such as a peripheral interface controller (PIC) and a PLC
- examples of microcontrollers used in industry (embedded) applications.

### Process/Skill Questions

- What is the difference between a PLC and a personal computer (PC)?
- What are examples of embedded controllers?
- When is ladder logic used?

## Task Number 49

## Develop a control system with open and/or closed loops.

### Definition

Development should include cybersecurity considerations.

### Process/Skill Questions

- How can security of an existing control system be improved?
- What are the cybersecurity considerations in an open-loop systems? What threats might occur in an open-loop system?
- Which type of system is more susceptible to manipulation?

# Exploring Current Issues in Cybersecurity in Manufacturing

## Task Number 50

## Describe the current state of cybersecurity in manufacturing.

### Definition

Description includes

- consideration of operational technology vs. information technology vs. product security
- issues involved in retrofitting legacy systems
- hardware lifespans and associated security implications.

### Process/Skill Questions

- What security issues are manufacturing facilities in the community facing?
- What are the benefits and challenges in retrofitting legacy systems?

# Task Number 51

# Research emerging technologies.

### Definition

Research could include technologies such as artificial intelligence (AI), augmented reality (AR), additive manufacturing, virtual presence, virtualization, Internet of things (IoT) and industrial Internet of things (IIoT), data analytics, machine learning, cyber insurance and blockchain.

Teacher resource:
Building Security to Achieve Engineering and Business Requirements, General Electric and Dragos

### Process/Skill Questions

- Which emerging technologies may be revolutionary and which may represent more incremental improvement?
- What are the implications of AI?
- What may be the most important technological developments in the next five years?

# Task Number 52

# Identify industry challenges.

### Definition

Identification includes challenges such as

- insider threats
- the involvement of manufacturing systems in global conflicts
- labor force issues (e.g., retention)
- cyberespionage

- the need for collaboration among professionals of various specializations due to complexity of the industry
- the supply chain.

### Process/Skill Questions

- What is the difference between an insider threat and cyberespionage? Are they always different?
- What are the challenges inherent in a supply chain?
- Why does cybersecurity in manufacturing depend on many specialties?
- Why are labor force issues a challenge in manufacturing?

# Applying Cybersecurity Standards and Regulations to Manufacturing Systems

## Task Number 53

## Explain laws and regulations applicable to cybersecurity in manufacturing systems.

### Definition

Explanation may include, but not be limited to,

- federal laws, regulations, policies
  - Defense Federal Acquisition Regulation Supplement (DFARS)
  - Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience
  - Privacy Act of 1974
  - Electronic Communications Privacy Act of 1986 (ECPA)
  - Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
  - Cyber Security Information Sharing Act of 2015 (CISA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Telecommunications Act of 1996
  - Chemical Facility Anti-Terrorism Standards (CFATS)
- international laws and standards
  - General Data Protection Regulation (GDPR)
  - European Union (EU) directive on security of network and information systems (NIS Directive)

    - North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP).

### Process/Skill Questions

- Why is EO 13636 important to the manufacturing industry?
- What effect has HIPAA had on the product security in the manufacturing of medical devices?
- How do older regulations affect the current state of cybersecurity?

# Task Number 54

# Describe the importance of cybersecurity standards applicable to manufacturing systems.

### Definition

Description should include

- U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (NIST Special Publication [SP] 800-37)
- Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53)
- Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82)
- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171)
- International Society of Automation (ISA)/IEC 62443 Cybersecurity Certificate Programs
- Enterprise-control System Integration, International Standards Organization (ISO)/IEC 62264 (Purdue Enterprise Reference Architecture).

Teacher resource:
Building Security to Achieve Engineering and Business Requirements, General Electric and Dragos

### Process/Skill Questions

- What is the significance of the Purdue model?
- Why did NIST have to publish rules specific to control systems (e.g., SP 800-82)?
- Why are standards important?
- What is the difference between a standard and a law?

# Evaluating Vulnerabilities, Risks, and Threats in Manufacturing Systems

## Task Number 55

## Describe the relationship among risks, vulnerabilities, and threats.

### Definition

Description should include

- the definition of *risk, threat,* and *vulnerability*
- an explanation of the relationship among the three
- the consequences for the manufacturing industry
  - loss of intellectual property
  - machine-to-machine communication disruption or manipulation
  - disruption or manipulation of production processes
  - disruption or manipulation of IIoT
  - disruption or manipulation resulting in threats to human health and safety
  - loss of trust in automated systems and processes.

Teacher resources:
Risk, Utility, and the Public Good (video), Eireann Leverett, Founder and Cyber-Risk Specialist, Concinnity Risks
U.S. Department of Homeland Security (DHS) Risk Lexicon

### Process/Skill Questions

- Why do disagreements exist within the manufacturing industry regarding risks, vulnerabilities, and threats?
- What might cause machine-to-machine disruption or manipulation?

## Task Number 56

## Identify resources for vulnerability information specific to manufacturing.

### Definition

Identification should include resources such as

- NIST National Vulnerability Database (NVD)
- Industrial Control Systems-Computer Emergency Response Team (ICS-CERT) Advisories
- vendor websites.

### Process/Skill Questions

- Why are vendor websites valuable resources when identifying vulnerability information?
- How is the NIST NVD helpful?

## Task Number 57

## Describe threats to ICS.

### Definition

Description may include threats such as

- ICS-specific malware (e.g., Stuxnet, Havex, BlackEnergy 3, CrashOverride, and Triton)
- physical security access
- supply chain
- social engineering.

Teacher resources:
Open Web Application Security Project
Richard Clarke Keynote (Video)
Understanding Threats will Promote the "Right Amount" of Security, General Electric and Dragos

### Process/Skill Questions

- What was new about Stuxnet?
- What is social engineering?
- Why is physical security part of cybersecurity?

## Task Number 58

## Explain cybersecurity risks within a supply chain.

### Definition

Explanation includes

- counterfeit parts
- malicious code injection
- use of open-source hardware and/or software
- data leakage (either by error or through industrial espionage)
- chain of custody tampering
- modifications to design components.

Teacher resources:
Best Practices in Cyber Supply Chain Risk Management, NIST
Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800-161)

### Process/Skill Questions

- What is risk?
- What is chain of custody, and why is it important?

# Task Number 59

## Perform a risk assessment.

### Definition

Performance includes identifying risks within an ICS. Performance should consider the effects of unmitigated risks (e.g., system downtime and financial effects).

Teacher resources:
Guide for Conducting Risk Assessments (NIST SP 800-30)
Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39)
The factor analysis information risk (FAIR) Institute

### Process/Skill Questions

- Why is system downtime detrimental?
- Why are risk assessments important? What resources may assist with a risk assessment?
- Who should be involved in a risk assessment?

# Applying System Security Procedures and Risk Management in Automated Production Processes

## Task Number 60

## Develop a system security plan for an automated production process.

### Definition

Development is based on a risk assessment.

Development includes consideration of

- policies and governance
- personnel safety
- equipment safety
- digital infrastructure
- physical security
- access control
- monitoring
- configuration management
- compensating controls specific to manufacturing systems (e.g., pressure release valves, manual overrides, emergency stops)
- incident response procedures.

### Process/Skill Questions

- How can both security and costs be addressed?
- What role does physical security play in a system security plan?
- Why is safety more important in manufacturing than in some other industries?

## Task Number 61

## Propose incident response procedures.

### Definition

Proposal should include the following:

- Incident symptoms
- Classification of incidents
- Incident response plan:
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements, both internal and external (e.g., Occupational Safety and Health Administration [OSHA], Environmental Protection Agency [EPA], Food and Drug Administration [FDA], product recall requirements)
  - Cyber-incident response teams
  - Exercise/drill/simulation
- Incident response process:
  - Preparation
  - Detection and analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

### Process/Skill Questions

- What is the difference between an incident response plan and an incident response process?
- Why is it important to have incident response exercises?

## Task Number 62

## Define *cyber threat intelligence*.

### Definition

Definition includes the concept that there are organizations (e.g., Dragos, Nozomi Networks) that capture and analyze malware and report on the targets, capabilities, infrastructure, and attribution of the malware.

### Process/Skill Questions

- What is the intelligence cycle?
- How does cyber threat intelligence relate to manufacturing operations?

## Task Number 63

## Apply digital forensics to an automated production process.

### Definition

Application includes

- network traffic analysis
- hypotheses related to incident
- supporting data
- analysis of data to support or refute hypothesis.

Teacher resources:
Making Digital Forensics a Critical Part of Your Cyber Security Defenses, Control Engineering

### Process/Skill Questions

- What is digital forensics?
- How does analyzing the past help prepare for the future?
- How is data analyzed and qualified?

# Securing a Manufacturing Enterprise

## Task Number 64

## Apply the engineering design process.

### Definition

Application should include the concept that the engineering design process is a systematic, creative process for solving problems concerning real objects, products, systems, and environments. The engineering design process includes the following steps:

1. Identify the need or opportunity for an engineering solution.
2. Define an engineering design problem.
3. Identify the requirement and constraints of the design problem, including cybersecurity considerations.
4. Research potential solutions to the design problem.

5. Generate (brainstorm) multiple solutions to the design problem.
6. Sketch the multiple solutions to the design problem.
7. Evaluate the requirements and constraints of each solution to the design problem, including cybersecurity considerations.
8. Justify an optimal solution to the design problem, including cybersecurity considerations.
9. Create a model or prototype for the chosen solution to the design problem, using appropriate materials and processes.
10. Determine the objectives for an engineering test of the solution to the design problem, including cybersecurity considerations.
11. Test the solution to the design problem, using mathematical, conceptual, and/or physical modeling, simulating, and optimizing (including cybersecurity considerations).
12. Evaluate the test results, including cybersecurity considerations.
13. Formulate an alternate solution to the design problem, if needed.
14. Test the alternate solution, if needed.
15. Present the final project report.
16. Document the final project report.

### Process/Skill Questions

- How can design problems be identified?
- What are the types of problems that concern product developers?
- Why is it important to identify criteria and constraints?
- What techniques are used to refine a design?
- How can a design be evaluated?
- What is quality control?
- Why should final solutions be re-evaluated? How is this done?
- What are the basic requirements of design?
- What is ergonomics?
- What are functional requirements?
- How important is it to document every phase of the design process?
- How can a sketch created in the beginning of the engineering design process be important in an eventual product redesign?

# Task Number 65

# Plan a product/process.

### Definition

Plan includes

- incorporation of the design process
- characteristics and purpose of the product
- resources necessary for production
- automated production process design.

### Process/Skill Questions

- How does a company plan for its supply chain?
- How does cybersecurity fit into product planning?

## Task Number 66

## Describe trade secrets and proprietary information of a manufacturing enterprise.

### Definition

Description should include

- product design
- production process
- competitive advantage.

### Process/Skill Questions

What is meant by *trade secrets*?
What is competitive advantage?

## Task Number 67

## Design the prevention of and protections against cyber threats for a manufacturing enterprise.

### Definition

Design should include

- securing documents
- securing access to manufacturing processes
- securing the network connected to the manufacturing equipment
- developing a risk management plan for the manufacturing enterprise
- considering the effect of cybersecurity decisions on business.

### Process/Skill Questions

- What are the basic steps an organization should take to safeguard against cyber threats for a manufacturing enterprise?
- How can a manufacturing organization prevent cyber threats?

## Task Number 68

## Secure the product using cybersecurity best practices.

### Definition

Securing should include

- identifying vulnerabilities and risks
- testing access points to the product
- using input/output validations
- applying the confidentiality, integrity, and availability (CIA) triad model as appropriate (e.g., authentication/encryption)
- identifying methods of remediation.

### Process/Skill Questions

- How are the cybersecurity principles applicable to ICS, control systems, and IIoT?

# SOL Correlation by Task

| | | |
|---|---|---|
| 39 | Use required personal protective equipment (PPE). | English: 11.5, 12.5<br>History and Social Science: VUS.8, WHII.8<br>Science: CH.1 |
| 40 | Implement a safety plan. | English: 11.1, 12.1<br>History and Social Science: VUS.8, WHII.8 |
| 41 | Maintain safe working practices around production equipment. | English: 11.5, 12.5<br>History and Social Science: VUS.8, WHII.8 |
| 42 | Operate lab equipment according to instructor guidelines. | English: 11.5, 12.5<br>History and Social Science: VUS.8, WHII.8 |
| 43 | Outline manufacturing processes. | English: 11.6, 11.7, 12.6, 12.7 |
| 44 | Distinguish among automation systems used by subsectors within manufacturing. | English: 11.5, 12.5 |
| 45 | Define *data flow*. | English: 11.3, 12.3 |

| | | |
|---|---|---|
| 46 | Identify cybersecurity considerations throughout the stages in the engineering design process. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14<br>Mathematics: COM.1, COM.17<br>Science: PH.1 |
| 47 | Analyze use of computer-aided design (CAD), three-dimensional (3D) printing, and computer-aided manufacturing (CAM) in manufacturing. | English: 11.5, 12.5 |
| 48 | Describe the use of a programmable logic controller (PLC) and microcontroller. | English: 11.5, 12.5 |
| 49 | Develop a control system with open and/or closed loops. | |
| 50 | Describe the current state of cybersecurity in manufacturing. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 51 | Research emerging technologies. | English: 11.8, 12.8 |
| 52 | Identify industry challenges. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 53 | Explain laws and regulations applicable to cybersecurity in manufacturing systems. | English: 11.5, 11.8, 12.5, 12.8<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 54 | Describe the importance of cybersecurity standards applicable to manufacturing systems. | English: 11.5, 11.8, 12.5, 12.8 |
| 55 | Describe the relationship among risks, vulnerabilities, and threats. | English: 11.3, 11.5, 11.8, 12.3, 12.5, 12.8<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 56 | Identify resources for vulnerability information specific to manufacturing. | History and Social Science: VUS.14, WG.17, WHII.14 |
| 57 | Describe threats to ICS. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 58 | Explain cybersecurity risks within a supply chain. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 59 | Perform a risk assessment. | English: 11.5, 12.5 |

| | | |
|---|---|---|
| 60 | Develop a system security plan for an automated production process. | English: 11.1, 12.1<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 61 | Propose incident response procedures. | English: 11.1, 11.3, 11.6, 11.7, 12.1, 12.3, 12.6, 12.7<br>History and Social Science: VUS.13, VUS.14, WG.17, WHII.14 |
| 62 | Define *cyber threat intelligence*. | English: 11.3, 12.3<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 63 | Apply digital forensics to an automated production process. | English: 11.5, 12.5<br>Mathematics: PS.1*, PS.2*, PS.3*, PS.4*, PS.7* |
| 64 | Apply the engineering design process. | English: 11.1, 11.3, 11.5, 11.6, 11.7, 11.8, 12.1, 12.3, 12.5, 12.6, 12.7, 12.8<br>Science: PH.1, PH.4 |
| 65 | Plan a product/process. | English: 11.1, 12.1 |
| 66 | Describe trade secrets and proprietary information of a manufacturing enterprise. | English: 11.5, 12.5 |
| 67 | Design the prevention of and protections against cyber threats for a manufacturing enterprise. | English: 11.1, 12.1<br>History and Social Science: VUS.14, WG.17, WHII.14 |
| 68 | Secure the product using cybersecurity best practices. | English: 11.5, 12.5<br>History and Social Science: VUS.14, WG.17, WHII.14 |

# Teacher Resource

AFA CyberPatriot the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.

# Appendix: Credentials, Course Sequences, and Career Cluster Information

**Industry Credentials: Only apply to 36-week courses**

- Automated Manufacturing Technology Examination
- Certified Production Technician (CPT) Program Examinations
- College and Work Readiness Assessment (CWRA+)
- Manufacturing Specialist Certification Examination
- Manufacturing Technician Level I Certification Examination
- Manufacturing Technology Assessment
- National Career Readiness Certificate Assessment
- Workplace Readiness Skills for the Commonwealth Examination

**Concentration sequences:** *A combination of this course and those below, equivalent to two 36-week courses, is a concentration sequence. Students wishing to complete a specialization may take additional courses based on their career pathways. A program completer is a student who has met the requirements for a CTE concentration sequence and all other requirements for high school graduation or an approved alternative education program.*

- Cybersecurity Fundamentals (6302/36 weeks)
- Cybersecurity in Manufacturing (8499/36 weeks)

| Career Cluster: Information Technology | |
|---|---|
| **Pathway** | **Occupations** |
| **Information Support and Services** | **Computer Numerical Control Programmer (CNC Programmer)**<br>**Systems Analyst** |
| **Network Systems** | **Computer Security Specialist**<br>**Computer Software Engineer** |
| **Programming and Software Development** | **Computer Software Engineer**<br>**Programmer**<br>**Systems Analyst** |

| Career Cluster: Manufacturing | |
|---|---|
| **Pathway** | **Occupations** |
| **Manufacturing Production Process Development** | **Industrial Engineer**<br>**Industrial Engineering Technician**<br>**Manufacturing Systems Engineer** |

| Career Cluster: Manufacturing | |
|---|---|
| **Pathway** | **Occupations** |
| | Network Designer<br>Programmer |
| Production | Automated Manufacturing Technician |
| Quality Assurance | Quality Control Technician |

| Career Cluster: Science, Technology, Engineering and Mathematics | |
|---|---|
| **Pathway** | **Occupations** |
| Engineering and Technology | Computer Hardware Engineer<br>Computer Programmer<br>Computer Software Engineer<br>Engineering Technician<br>Industrial Engineer<br>Industrial Engineering Technician<br>Manufacturing Systems Engineer<br>Network and Computer Systems Administrator<br>Network Systems and Data Communication Analyst<br>Systems Analyst |