UNIT 24: Cyber Physical Systems

Estimated Time in Hours: 9

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 4 Data Security 2 Establishing Trust 8 Implications		- Research the types of CPS in various sectors. - Later, identify vulnerabilities which may affect those CPS. - Replicate a developed IoT system and enhance it with a plan for cybersecurity additions.

Guiding Questions:

- What is a Cyber-Physical System and how is it different from a computer?
- What industries or workforce sectors use CPS?
- How are CPS vulnerable to cyber attack?
- What kind of harm can a CPS cyber attack cause?
- What is the benefit of CPS compared to the risk?
- Why is fail-safe design important to CPS?
- How are CPS and Internet of Things intertwined?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.4.2a EK: A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users.	• Examples of Cyber-Physical Systems (first minute of the video): "Cyber-Physical Systems | UC BerkeleyX on edX | About Video." *YouTube*, uploaded by edX, 8 May 2014, https://youtu.be/7zSCnnJE1cs	• Define and introduce CPS. This will need to be introduced as a system before adding cyber elements to it. Cover the basics such as actuators, sensors, and human-machine interfaces, and network connections.
5.4.2b EK: Industries that employ CPS include energy management,	• Example of CPS in industry:	• Explain how CPS fits in to various sectors.

health care, manufacturing, transportation, telecommunications, infrastructure, and military.	"Cyber-physical Production Systems." *YouTube*, uploaded by Siemens, 20 June 2018, https://youtu.be/wro3uoHR-ZY • CPS overview with a focus on ethics (prescreen – for a mature class): "The Ethics of Cyber-Physical Systems." *YouTube*, uploaded by MySTOA, 22 May 2016, https://youtu.be/c5gu8xmmum4	• Discuss the implications of integrating CPS into so many industrial. Show the linked CPS overview YouTube video to promote discussion. Are these CPS additions good or bad? What are the repercussions of these changes? Who should be held responsible when CPS fail? • Challenge students with researching the types of CPS in different sectors (energy, health, transit, etc.) to include equipment, efficiencies derived from CPS, and how it improves the goal of the industry.
5.4.2c EK: A smart grid is an electrical grid which includes a variety of operation and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources.	• Smart grid overview: "What is the smart grid? – by Scientific American." *YouTube*, uploaded by Scientific American, 30 Mar 2011, https://youtu.be/-8cM4WfZ_Wg • Power grid cyber attack: Sussman, Bruce. "Revealed: Details of 'First of Its Kind' Disruptive Power Grid Attack." SecureWorld,	• Ask students to explain the advantages and disadvantages of the smart grid. Do you think the smart grid is vulnerable to a cyber attack? • Cyber-physical implies that a cyber attack can have tangible, physical consequences. What kind of harm could a CPS attack cause?

	SecureWorldExpo.com, 8 Oct 2019, https://www.secureworldexpo.com/industry-news/first-u.s.-power-grid-attack-details	
5.4.2 LO: Students will predict how physical systems that rely on software may be vulnerable to future attacks. 5.4.2d EK: Increased industry connectivity will cause increased attacks from adversaries such as cyber criminals, disgruntled employees, terrorists, organized crime, and nation states.		• The benefit of CPS is convenience, efficiency, and safety. The risk is an exploitable system. • Discuss with students why CPS systems may be of particular interest to an adversary. Why might it attract the attention of the most powerful adversaries: nation states?
5.4.2e EK: Vulnerabilities may allow adversaries to interfere with connected devices.		• Delve into specific vulnerabilities of CPS. This can be dependent on the industry, but there is commonality. Most CPS use commercial grade programmable logic controllers and have feedback control with a human machine interface. • Task students with researching CPS vulnerabilities which relate to the CPS in the sector(s) they identified earlier. Are these vulnerabilities dire? Do they have mitigations?

5.4.2f EK: The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment.	• Aurora power grid generator attack demo: "Aurora Test Footage." *YouTube*, uploaded by MuckRock, 9 Nov 2016, https://youtu.be/LM8kLaJ2NDU	• Show the linked Aurora demo YouTube video to demonstrate how a cyber attack can destroy a power grid generator. • Ask students to explain the impact of CPS attacks and back it up with reasonable examples. How can they impact hospitals that depend on power?
5.4.2g EK: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users.		• A common CPS attack vector is to gain access to the human machine interface. The CPS can often be controlled from this interface. It also receives sensor feedback data from the devices and is vulnerable to man-in-the-middle attacks. • Ask students what measures they would take to secure trusted resources such as the HMI. Do they need continuous monitoring?
2.3.8 LO: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. 2.3.8a EK: When something does not work or the system fails, the system must return to a secure state. 2.3.8b EK: A secure state is a condition when no subject can access any object in an unauthorized manner		• Review fail-safe defaults and secure states. Why are these important in the context of CPS? • Ask students to explain how to secure CPS from different industrials with fail-safe design. Does the risk of human life play a factor in the design? • Note the trade-offs between availability, confidentiality, and safety. Students should navigate through complex ethical scenarios involving system fail-safe defaults and permissions.

2.3.8c EK: Turning off permission causes a security problem.		
8.1.2d EK: The Internet has evolved to include new types of devices and the "Internet of Things." 8.1.2e EK: The "Internet of Things," benefits our daily lives by providing easier access to information, the ability to offload menial tasks, and coordinate necessary information. 8.1.2f EK: The Internet and IoT devices create new vulnerabilities an adversary can exploit. 8.1.2g EK: The increasing dependence on the Internet and IoT devices introduces problems when these systems become unavailable.	• IoT in manufacturing: "How it Works: The Internet of Things and Manufacturing." *YouTube*, uploaded by IBM Think Academy, 10 Nov 2016, https://youtu.be/R5RfSQ3Nxzg • IoT student design projects: Hasan, Mehedi. "Top 20 Best Internet of Things Projects (IoT Projects) That You can Make Right Now." UbuntuPIT, *UbuntuPIT.com*, https://www.ubuntupit.com/best-internet-of-things-projects-iot-projects-that-you-can-make-right-now/	• Review the Internet of Things. Students should be able to identify IoT devices present in the classroom or at home. • Introduce the future of an expanded CPS network, sometimes called the Industrial Internet of Things or Industrie 4.0. These concepts combine CPS and IoT with machine learning for enhanced efficiency. • Show the linked YouTube video for IoT in manufacturing. What enhancements does IoT bring to the world of CPS? Use a video viewing guide to assess student comprehension. How does this contribute to the complexity of cyberspace? • If resources allow, students can undertake a simple IoT design project. The project can be a recreation of an existing design with an added plan for cybersecurity enhancements. Some ideas are linked to the left.
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order		• Explore a relevant career, such as cyber intel planner.

to prepare people for these new types of jobs.		