Embedded Systems and Specialized Devices

- Computing capabilities can be integrated into appliances and other devices
- An embedded system is computer hardware and software contained within a larger system designed for a specific function
- These devices can pose security risks

Types of Devices (1 of 7)

- Categories of embedded and specialized devices include the hardware and software that can be used to create these devices, specialized systems, industrial systems, other devices, and IoT devices
- Hardware and Software
  - One of the most common hardware components is the **Raspberry Pi**, which is a low-cost, credit-card-sized computer motherboard
    - It can perform almost any task that a standard computer can and can be used to control a specialized device
  - A **field-programmable gate array (FPGA)** is a hardware “chip” that can be programmed by the user to carry out one or more logical operations
  - A **system on a chip (SoC)** combines all the required electronic circuits of the various computer components on a single chip
    - SoCs often use a **real-time operating system (RTOS)**

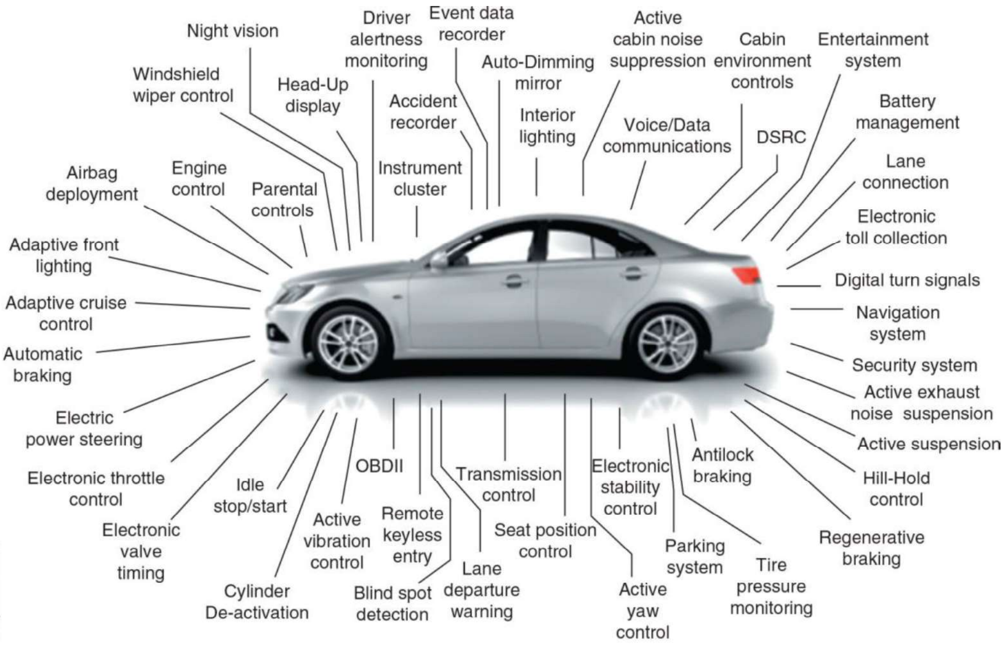
Types of Devices (2 of 7)

- Specialized Systems
  - Digital smart meters are used to measure the amount of utilities consumed
    - Smart meters have several advantages over analog meters (see Table 5-8 on the following slide)
  - Other specialized systems include medical systems, aircraft, and vehicles
    - Embedded systems in cars use sonar, radar, and laser emitters to control brakes, steering, and the throttle
- Industrial Systems
  - **Industrial control systems (ICSs)** in local or at remote locations collect, monitor, and process real-time data so that machines can directly control devices such as valves, pumps, and motors without human intervention
  - ICSs are managed by **supervisory control and data acquisition (SCADA)** systems

Types of Devices (3 of 7)

Action	Analog meter	Smart meter
Meter readings	Employee must visit the dwelling each month to read the meter.	Meter readings are transmitted daily, hourly, or even by the minute to the utility company.
Servicing	Annual servicing is required in order to maintain accuracy.	Battery replacement every 20 years.
Tamper protection	Data must be analyzed over long periods to identify anomalies.	Can alert utility in the event of tampering or theft.
Emergency communication	None available	Transmits “last gasp” notification of a problem to utility company.

Types of Devices (4 of 7)



ChipsEtc.com

Figure 5-9 Embedded systems in cars

Figure 5-9 Embedded systems in cars

Types of Devices (5 of 7)

- Other Specialized Systems
  - Other examples of specialized systems include **heating, ventilation, and air conditioning (HVAC)** environmental systems
  - A **multifunctional printer (MFP)** combines the functions of a printer, copier, scanner, and fax machine
  - An **unmanned aerial vehicle (UAV)** commonly known as a drone, is an aircraft without a human pilot on board to control its flight
    - They are commonly used for policing and surveillance, product deliveries, aerial photography, infrastructure inspections, and drone racing

Types of Devices (6 of 7)

Source: Den Rozhnovsky/Shutterstock.com

Figure 5-10 Drone

Figure 5-10 Drone

Types of Devices (7 of 7)

- Internet of Things
  - **Internet of Things** (**IoT**) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon
  - IoT devices include wearable technology as well as every home automation items such as thermostats, coffee makers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs
  - *Body area networks* (*BAN*) is a network system of IoT devices in close proximity to a person's body that cooperate for the benefit of the user
  - *Autonomous body sensor network* (*ABSN*) introduces actuators in addition to the sensors so that immediate effects can be made on the human body

Security Issues Table (1 of 2)

Constraint	Explanation
Power	To prolong battery life, devices and systems are optimized to draw very low levels of power and thus lack the ability to perform strong security measures.
Compute	Due to their size, small devices typically possess low processing capabilities, which restricts complex and comprehensive security measures.
Network	To simplify connecting a device to a network, many device designers support network protocols that lack advanced security features.
Cryptography	Encryption and decryption are resource-intensive tasks that require significant processing and storage capacities that these devices lack.
Inability to patch	Few, if any, devices have been designed with the capacity for being updated to address exposed security vulnerabilities.
Authentication	To keep costs at a minimum, most devices lack authentication features.
Range	Not all devices have long-range capabilities to access remote security updates.
Cost	Most developers are concerned primarily with making products as inexpensive as possible, which means leaving out all security protections.
Implied trust	Many devices are designed without any security features but operate on an “implied trust” basis that assumes all other devices or users can be trusted.
Weak defaults	User names (such as “root,” “admin,” and “support”) and passwords (“admin,” “888888,” “default,” “123456,” “54321,” and even “password”) for accessing devices are often simple and well known.

CENGAGE

Security Issues (2 of 2)

- Over several years, many industry-led initiatives have attempted to address security vulnerabilities in IoT and embedded devices
  - The initiatives were scattered and did not represent a comprehensive solution to the problem
- Governments have begun to propose or enact legislation to require stronger security on embedded systems and specialized devices
- *The Internet of Things* (*IoT*) *Cybersecurity Improvement Act of 2019* was legislation introduced in the U.S. Senate in May 2019
- California and Oregon passed state laws addressing IoT security that went into effect in January 2020
  - Requires that connected devices be equipped with “reasonable security features” appropriate for the nature and function of the device and the information the device collects, contains, or transmits

Knowledge Check Activity 3

Which of the following is used to manage industrial control systems (ICSs)?

a. SoC
b. SCADA
c. Real-time OS
d. Embedded system

Knowledge Check Activity 3: Answer

Which of the following is used to manage industrial control systems (ICSs)?

Answer: b. SCADA

Supervisory control and data acquisition (SCADA) systems are used to manage ICSs and are crucial in maintaining efficiency and reducing downtime.

CENGAGE

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective. If you self-score less than 4 you should consider reviewing the module and related exercises:

1. List and compare the different types of mobile devices and how they are deployed

2. Explain the ways to secure a mobile device

3. Describe the vulnerabilities and protections of embedded and specialized devices

4. Explain the issues surrounding securing specialized devices

Summary (1 of 2)

- There are several types of mobile devices: tablet computers, smartphones, and wearable technology devices are a few
- Portable computers are devices that closely resemble standard desktop computers
- Connectivity methods used to connect mobile devices to networks include cellular telephony, which divides the coverage area into cells
- It is not always feasible to require an employee to carry a company-owned smartphone along with a personal cell phone
    - Bring your own device (BYOD) allows users to use their own personal mobile devices for business purposes
    - Choose your own device (CYOD) gives employees a limited selection of approved devices, though the employee pays the upfront cost of the device while the business owns the contract

Summary (2 of 2)

- Several risks are associated with using mobile devices
- Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have
- Users should consider security when initially setting up a mobile device
- Several support tools can facilitate the management of mobile devices in the enterprise
  - Mobile device management (MDM) tools allow a device to be managed remotely by an organization
  - Mobile application management (MAM) covers application management
  - A mobile content management (MCM) system provides content management to mobile devices used by employees in an enterprise
- Embedded and specialized devices can be classified into several categories
- Security in embedded systems is lacking and can result in a wide range of attacks

CENGAGE