9.9.5 Embedded and Specialized Systems Facts

More and more devices are becoming connected to the internet through embedded technology that allows the device to send and receive information.

This lesson covers the following topics:

- Types of embedded devices
- Security risks

Types of Embedded Devices
The following table describes some of the most common embedded devices:

Device Type	Description
Appliances	Many appliances contain integrated technology that allows internet communication. For example, smart laundry appliances can send notifications when a load is complete or when laundry detergent needs to be refilled. Other common smart home appliances include: - Refrigerators - Dishwashers - Microwaves
Environment controls	Many homes and businesses use environmental control devices that can send real-time information and can be controlled via the internet. These devices can be as basic as controlling a home's HVAC system (such as a Nest thermostat) or as complex as controlling the humidity, temperature, and other environmental factors in a data center.
Building/facility automation	Some facilities use a network of integrated devices that control various aspects, creating what is known as facility automation. Some of the devices that are integrated with facility automation include: - Lighting controls - Security systems - Door locks - Sprinkler systems - Garage doors - Smart meters
Wearable devices	In recent years, companies have started producing wearable devices that can connect to the internet for a variety of purposes. These devices include: - Watches - Headphones - Fitness trackers
Automobiles	Modern cars use integrated technologies and in-vehicle systems that can perform various tasks, such as: - Starting the car remotely using a smart phone - Warning a driver about nearby cars

- ▪ Applying the brakes automatically to avoid collision
- ▪ Performing parallel parking autonomously

Industrial equipment	Some industrial equipment also fits into the category of a smart device. Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment. For example, a SCADA system could be used to monitor factory pipes and automatically open valves if pressure in the pipe system reaches a specific threshold. SCADA is a subset of Industrial Control Systems (ICS), which refers to all types of industrial automation.
Mainframe computer	A lesser known category of embedded devices are mainframe computers. A mainframe computer is a large, powerful computer that is capable of processing extremely large amounts of data. Mainframe computers typically run proprietary operating systems. Because these operating systems are rarely updated, they are considered a static environment. In addition, mainframe computers often contain large amounts of sensitive data, making them an attractive target for hackers.
Real-time operating system (RTOS)	A RTOS is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint. Because RTOS are often used as critical components of an application, a successful attack on the RTOS can harm an entire system, including physical machinery.
System on a chip (SoC)	A SoC is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions. The Raspberry Pi is a common device that uses a SoC. Because of their relatively low cost, SoCs are often used by hobbyists.
Multi-function display (MFD)	An MFD is a screen surrounded by configurable buttons that can be used to display information in a variety of ways. MFDs are often used on airplanes, helicopters, and ships.
Medical devices	Much of today's medical technology for daily monitoring and maintenance uses embedded systems. Instead of having to visit a physician every day, wearable devices can be used to collect information on heart rate, glucose levels, weight, blood pressure, and other parameters. This information can then be sent to a doctor automatically or used for self-monitoring.
Unmanned aerial vehicles (UAV)	UAVs are used for military campaigns, search and rescue, weather monitoring, and recreation. UAVs use embedded computers for collecting and transmitting data and for receiving commands.
Digital cameras	Most modern digital cameras use embedded systems for processing captured images, storing images, and uploading images to a PC or other storage device.
Media gateways	A media gateway is a translation device that converts media streams for use by different telecommunication technologies.
Wireless keyboards and mice	Wireless keyboards and mice use Bluetooth or other proprietary radio frequency connections.
Displays	In the past, display devices had a single use as a monitor for a computer. Today's monitors and other display devices are increasingly embedded with smart features and

	have wireless connections.
Wi-Fi-enabled microSD cards	Wi-Fi-enabled MicroSD cards can wirelessly transfer data to and from other devices. Many of them connect directly to the internet.
Multifunction printers (MFPs)	Multifunction printers can connect to wireless networks and to the internet for additional functionality.
External storage devices	External storage devices such as USB flash drives, HDDs, and SSDs can connect to traditional computing equipment, as well as to many smart devices.
Arduino	Arduino is an open-source hardware and software company. They design and manufacture single-board microcontrollers as well as kits to build digital devices.
Field Programmable Gate Array (FPGA)	A Field Programmable Gate Array is an integrated circuit manufactured and then later configured by the customer. The configuration happens through a hardware description language (HDL), similar to application-specific integrated circuit (ASIC).
Voice over IP (VoIP)	Voice over IP is a protocol optimized for the transmission of voice data (telephone calls) through a packet-switched IP network. VoIP routes phone calls through an IP network, including the internet. VoIP solutions can integrate with the public switched telephone network (PSTN) to allow VoIP customers to make and receive external calls.

Security Risks

As with any networked system, there are security risks associated with smart devices. Not only do you have little or no control over the smart technology within static environments, smart device vendors can be slow to take steps to protect their products against security threats. They tend to respond only after an exploit has occurred instead of proactively updating systems. This is why smart devices are attractive to hackers. However, there are some steps you can take to secure a network from these devices and reduce the damage that a compromised device can cause.

- Some static devices (such as home routers, game consoles, and SCADA devices) require manual firmware updates. With these devices, it is important to keep the firmware updated.
- For devices that cannot be manually updated, the best approach is to minimize the amount of damage a compromised device can cause. This is done by segmenting the network using VLANs or encrypting all network communications.