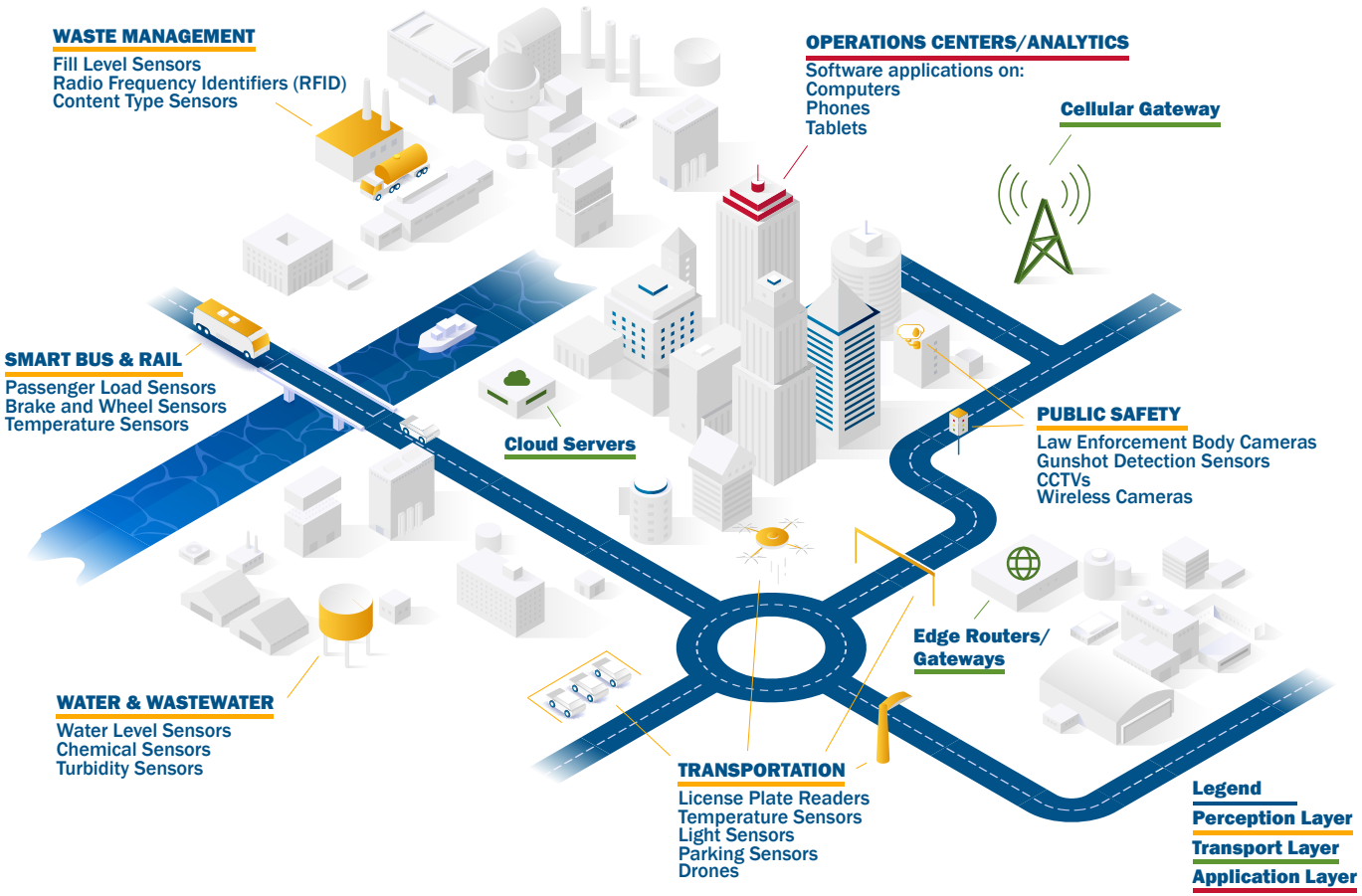
IoT IN CONNECTED COMMUNITIES
Risk and Mitigation Measures

A connected community, also known as a smart city, is a municipality of any size that converges smart, emerging, or connected technology on the same network to provide optimized municipal services to citizens.

IoT Risk Landscape

Increasing use of Internet of Things (IoT) and the collection of data make connected communities an attractive target for malicious actors. Vulnerabilities within IoT devices and systems could provide malicious actors with unauthorized access into connected communities' ecosystems and permit the lateral movement across interconnected critical infrastructure networks. Compromise of IoT devices and systems provides malicious actors with the ability to steal sensitive data and disrupt services or critical processes, resulting in significant impacts throughout connected community critical infrastructure systems.



Common IoT Threats may include:

Denial of Service (DoS): An attack that consumes IoT network resources by flooding the networks with unnecessary data traffic.

Eavesdropping: A passive attack that includes infiltrating networks, digitally observing, and possibly collecting network data.

Machine-in-the-Middle (MITM): An active attack where a malicious actor impersonates one of two legitimate parties involved in ongoing communication or information sharing.

Compromised Node: An attack that captures a network node or nodes to obtain sensitive information such as encrypted data.

Resonance Attack: An attack that forges an IoT sensor using different frequencies to disrupt communication among legitimate components.

Common IoT Vulnerabilities may include:

Non-Compliant Credentialing: Devices and user accounts can be compromised by the use of default passwords or weak or guessable credentials provided by IoT vendors or organizations not enforcing their authorization protocols.

Limited Segmentation: Unsegmented networks increase the overall risk to IoT systems by allowing Operational Technology (OT) networks to be exposed to vulnerabilities in connected IT networks, enabling malicious actors to move laterally across networks and limiting the detection of malicious actors due to increased network traffic.

Vulnerable User Interfaces: Insecure user interfaces intended only for internal networks may not support the use of logical access privileges to restrict network communications to and from a device. This may allow malicious actors to have greater network access than intended.

Risk Mitigation Measures

Critical mitigation practices for improving IoT device, system, and data security include:

- **Inventory IoT Devices, Systems, and IoT-Related Data**
- **Include IoT in Risk Management Planning**
- **Plan for and Deploy Resilient IoT Systems**
- **Build IoT Security into Acquisition and Vendor Contracts**
- **Ensure Appropriate Password Practices**
- **Make Data Security a Key Component for IoT**
- **Segment IoT Networks from Critical Networks**
- **Regularly Monitor IoT Networks and Sub-Nets**
- **Conduct Vulnerability Assessments**
- **Provide Training According to Role Practices**

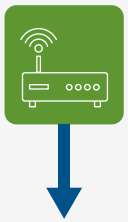
IoT IN CONNECTED COMMUNITIES

IoT Device Data Flow Example

IoT data flows from the perception layer where it is collected and then transmitted to the transport layer, before it is analyzed within the application layer.

Traffic Sensors

Signal management sensors send data to an edge device



Edge gateway collects device data and sends to cloud

Cloud server collects data and stores it

Cloud-based applications allow for real-time monitoring of signal sensor data

Perception Layer

The perception layer captures data from the physical environment and the hardware and software that run them. Devices include sensors, actuators, and a broad range of hardware and software sometimes deployed in publicly accessible areas. Perception layer devices are characterized by limited processing power and memory. Devices are often located in open and adverse environments.

Common IoT Perception Layer Devices

- License Plate Readers
- Ultrasound Sensors
- Radar Sensors
- Closed Circuit Televisions
- Gunshot Detection Sensors
- Radio Frequency Identifiers (RFID) and GPS Sensors
- Law Enforcement Body Cameras
- Water Level Sensors
- Parking Sensors
- Light Sensors
- Rail Passenger Load Sensors
- Near Field Communicators (NFC)
- Actuators
- Wireless Cameras

Transport Layer

The transport layer includes wired and wireless communication systems and protocols that connect IoT devices to data analysis and storage platforms that make up the application layer. The transport layer transmits and routes data and functions like a bridge between the perception layer and application layer. It connects and translates IoT devices across a network. This layer could face radio interference, data leakage, and interruption problems.

Common IoT Transport Layer Devices

- Edge Devices/Gateways
- Cloud Servers
- Cellular Transmitters

Application Layer

Data gathered from sensors and moved through the IoT device's network is stored, managed, and interpreted in the application layer. The application layer faces threats related to user data, privacy, and unauthorized access to resources.

Common IoT Application Layer Devices

- Computers
- Phones
- Firewalls
- Tablets
- Load Balancers
- Servers