Threat Modelling: IoT & ICS Use Cases

Clarisa Grijalva

Fall 2023

Outline

- Threat modeling review
- Internet of Things
  - Overview
  - IoT security vs. IT security
  - IoT threat modeling
- Industrial Control Systems
  - Overview
  - ICS security vs. IT security
  - ICS threat modeling

Threat Modeling Framework

1. Model the system/assets (i.e., identify the assets and analyze them)
2. Find threats using that model
3. Address threats using existing approaches
4. Validate your work for completeness and effectiveness
5. Rate/Prioritize threats based on their impacts

Model the system

- What are you building?

- Define the system/assets
  - Things attackers want
  - Things you want to protect
  - Stepping stones for either of those

Find threats

- What can go wrong?
- Identify threats that can be exploited to target the assets
- STRIDE: Categorized list of threat types
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privilege

Address threats

- Mitigate
- Eliminate
- Transfer
- Accept the risk

Validate

- Simulation based approaches
- Actual testing

Rate

- Risk analysis
- Identify threat potential and prioritize each threat
- DREAD
  - Damage potential
  - Reproducibility
  - Exploitability
  - Affected users
  - Discoverability

Threat	D	R	E	A	D	Total
Auth cookie theft (eavesdropping)	3	2	3	2	3	13
Auth cookie theft (XSS)	3	2	2	2	3	12

Prioritized Risk

Potential for damage is high (spoofed identifies, etc.)

Cookie can be stolen any time, but is only useful until expired

Anybody can run a packet sniffer; XSS attacks require moderate skill

All users could be affected, but in reality most won't click malicious links

Easy to discover; just type a <script> block into a field

Threat Modeling: Internet of Things

Internet of Things

- IoT refers to the network of physical objects, devices, vehicles, appliances, and other items embedded with sensors, software, and connectivity capabilities
- IoT devices gather and share data with each other, often without human intervention, using wired or wireless communication protocols
- Allows remote monitoring and control of devices and systems, enabling real-time tracking, management, and automation from a distance

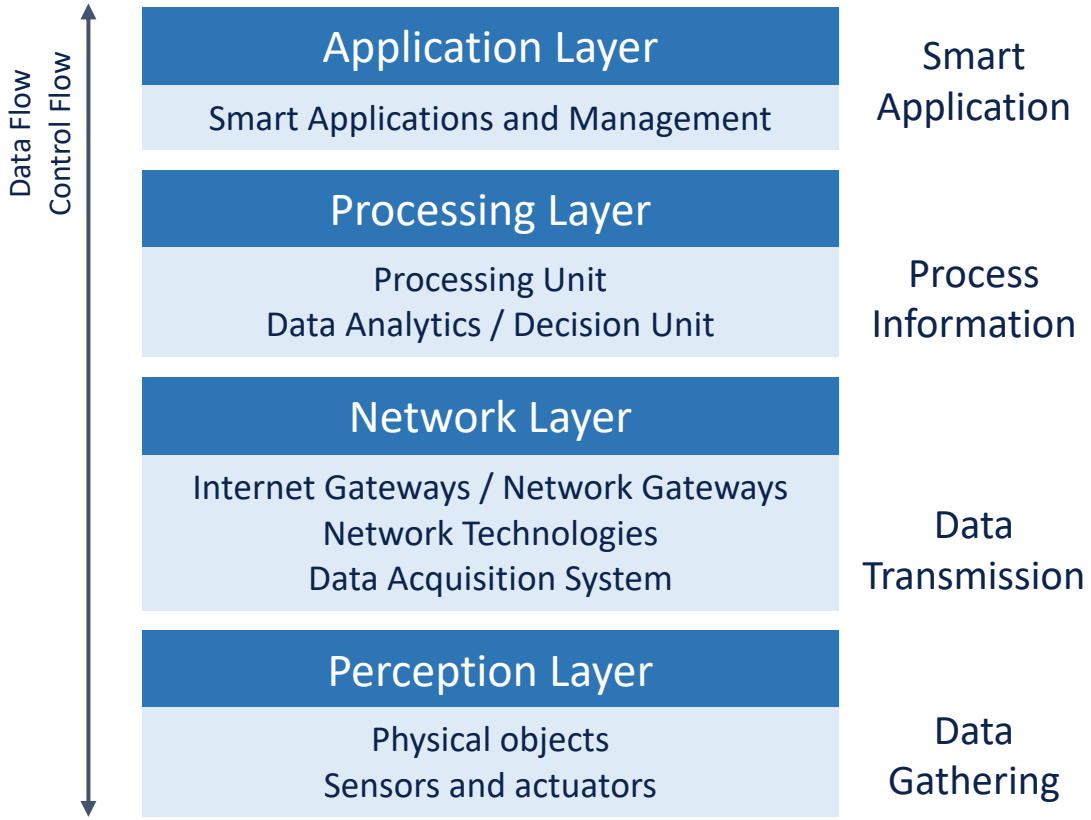
Internet of Things

- IoT devices use sensors to collect information from their environment (e.g., temperature, humidity, motion), and actuators to perform actions based on that data (e.g., turning on lights, adjusting thermostats)

- Used in various industries
  - Healthcare - remote patient monitoring
  - Transportation - smart cars
  - Agriculture - precision farming
  - Manufacturing - smart factories

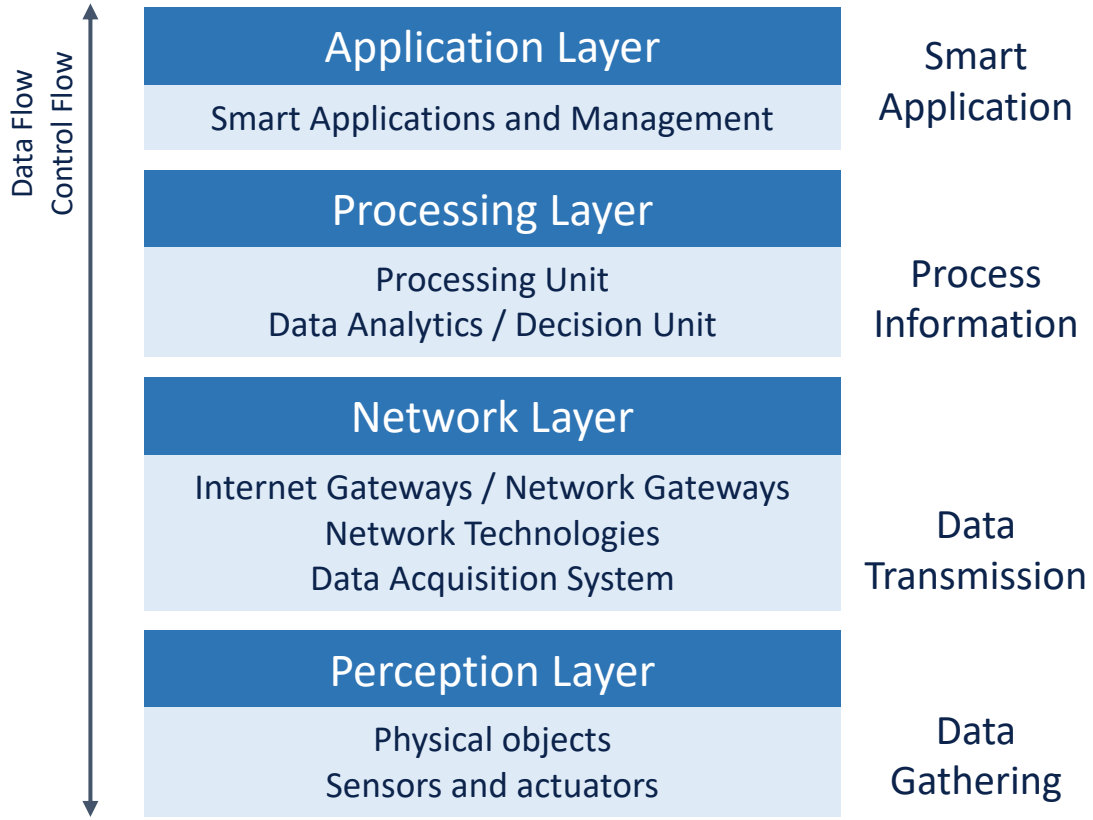
IoT Architecture

- Perception Layer
  - Physical devices that collect data from the environment
- Network Layer
  - Transport of data from the perception layer to the others



IoT Architecture

- Processing Layer
  - Processing of data collected from the perception layer
  - Located on the edge of the network and/or the cloud
- Application Layer
  - Provide services to users
  - Smart home applications
  - Healthcare applications



IoT vs IT Security

Internet of Things

- Security of devices, sensors, and systems
- Challenged by their interconnected nature, limited processing power, memory, energy, and security features
- May face attacks that exploit their specific vulnerabilities, such as weak default passwords, lack of security updates, and the potential for unauthorized physical access

Information Technology

- Security of information systems, networks, computers, and data within traditional computing environments
- Allow the implementation of more complex security control and measures
- Susceptible to a broad range of attacks, including malware, phishing, social engineering, and other methods that target software vulnerabilities, network weaknesses, and user behavior

IoT vs IT Security

Internet of Things

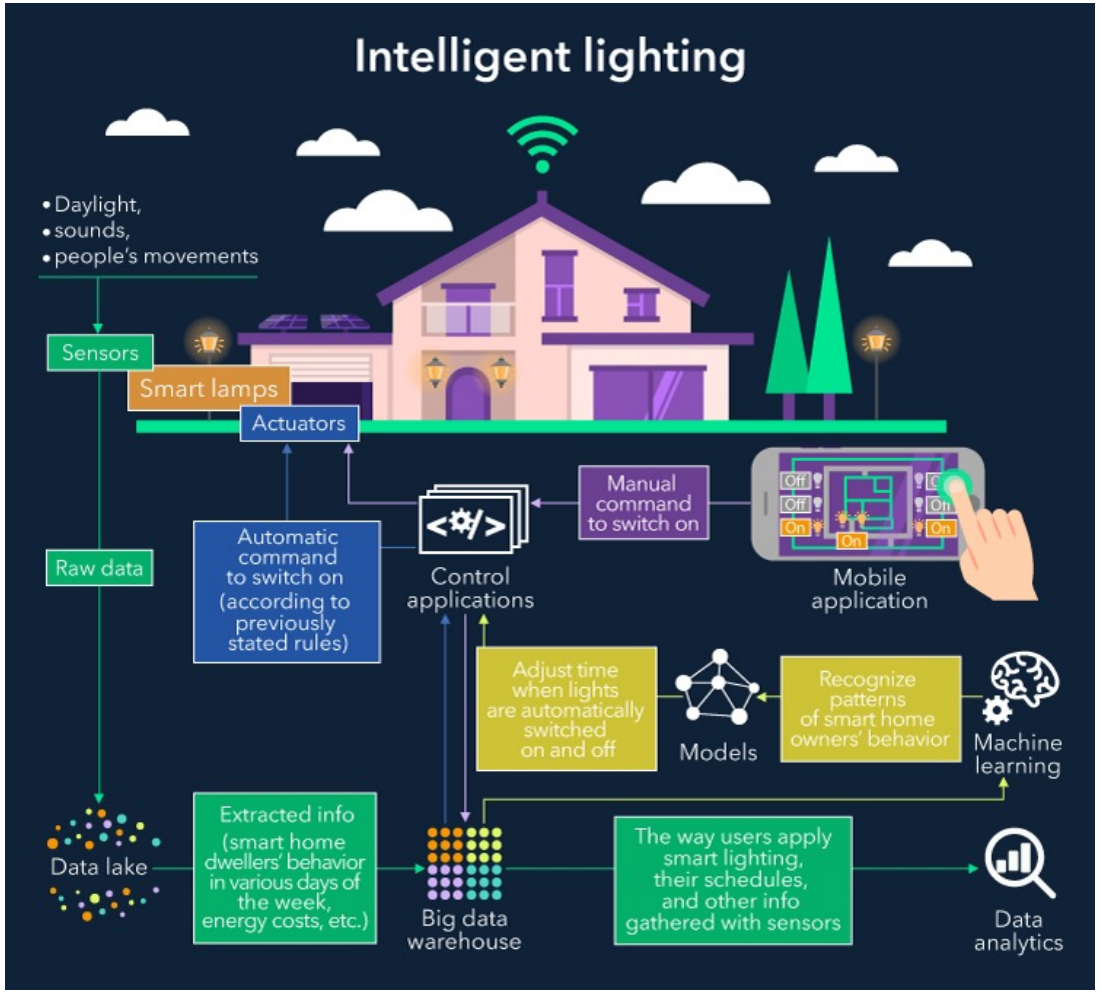
- Communicate through various network protocols and may connect through different types of networks
- Ensuring the privacy of this data while in transit and at rest is a significant concern
- Lacks consistent security standards and regulations across all devices and industries

Information Technology

- Typically operate within more controlled and established network environments
- Data privacy concerns, especially in industries like finance, healthcare, and e-commerce
- Has established security frameworks, best practices, and regulatory requirements that help guide organizations in protecting their systems and data

Threat modeling: IoT

1. Model system
   - Sensors
     - Light
     - Motion
     - Sound
   - Actuators
     - Smart lamps
   - Mobile application



Source: https://www.scnsoft.com/blog-pictures/internet-of-things/intelligent-lighting.png

Threat modeling: IoT

2. Find Threats

Threat Description	Threat Category (STRIDE)					
	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privileges
Denial of service on network gateway					X	
Manipulation of light sensors data		X				
Main-in-the-middle attack modifying sensor data	X	X				X
Spoofing of authentication credentials of mobile application	X					X

Threat modeling: IoT

3. Address Threats

Threat Description	**Mitigation strategies**
Denial of service on network gateway	Introduction of challenges
Manipulation of light sensors data	Intrusion Detection System that monitors the data between devices
Main-in-the-middle attack modifying sensor data	Encryption of data between sensor and network gateway
Spoofing of authentication credentials of mobile application	Dual authentication

Threat modeling: IoT

5. Rate Threats

Threat Description	Threat Risk Assessment (DREAD)					
	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	DREAD Score
Denial of service on network gateway	5	4	4	5	5	23
Manipulation of light sensors data	3	2	3	3	4	15
Main-in-the-middle attack modifying sensor data	4	2	3	4	3	16
Spoofing of authentication credentials of mobile application	4	3	4	4	5	20

Threat Modeling: Industrial Control Systems

Clarisa Grijalva | University of Arizona

Industrial Control Systems

- Industrial Control Systems (ICS) are computer-based systems designed to control, monitor, and automate various industrial processes and critical infrastructure

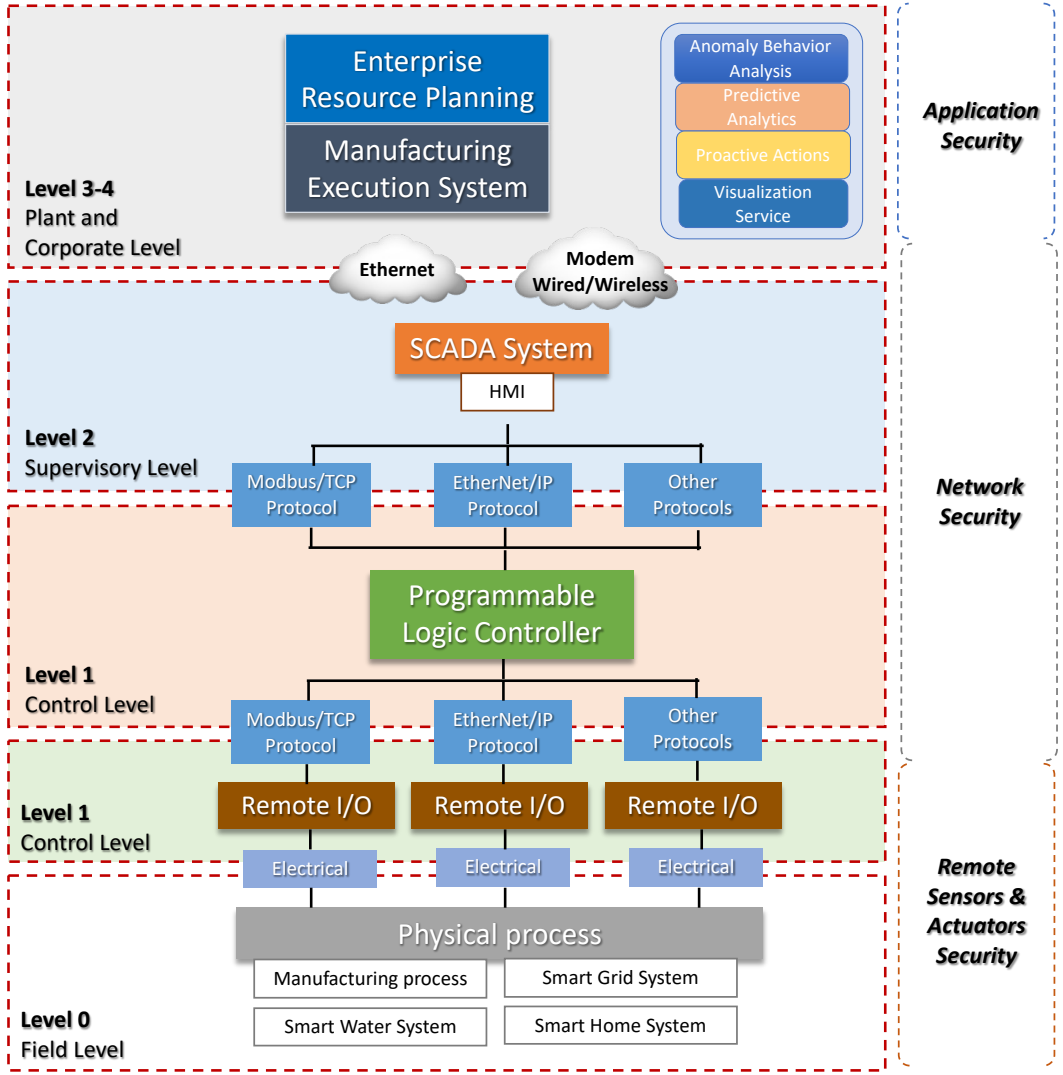
- Used in sectors such as
  - Energy - power generation and distribution
  - Manufacturing - factory automation
  - Water treatment
  - Transportation - traffic control systems

Industrial Control Systems

- Automate tasks that were traditionally performed manually, improving efficiency, accuracy, and consistency in industrial processes
- ICS control physical processes such as adjusting temperatures, pressures, flows, and levels in manufacturing and infrastructure systems
- ICS components communicate through specialized networks like industrial Ethernet, fieldbus protocols, and proprietary communication protocols

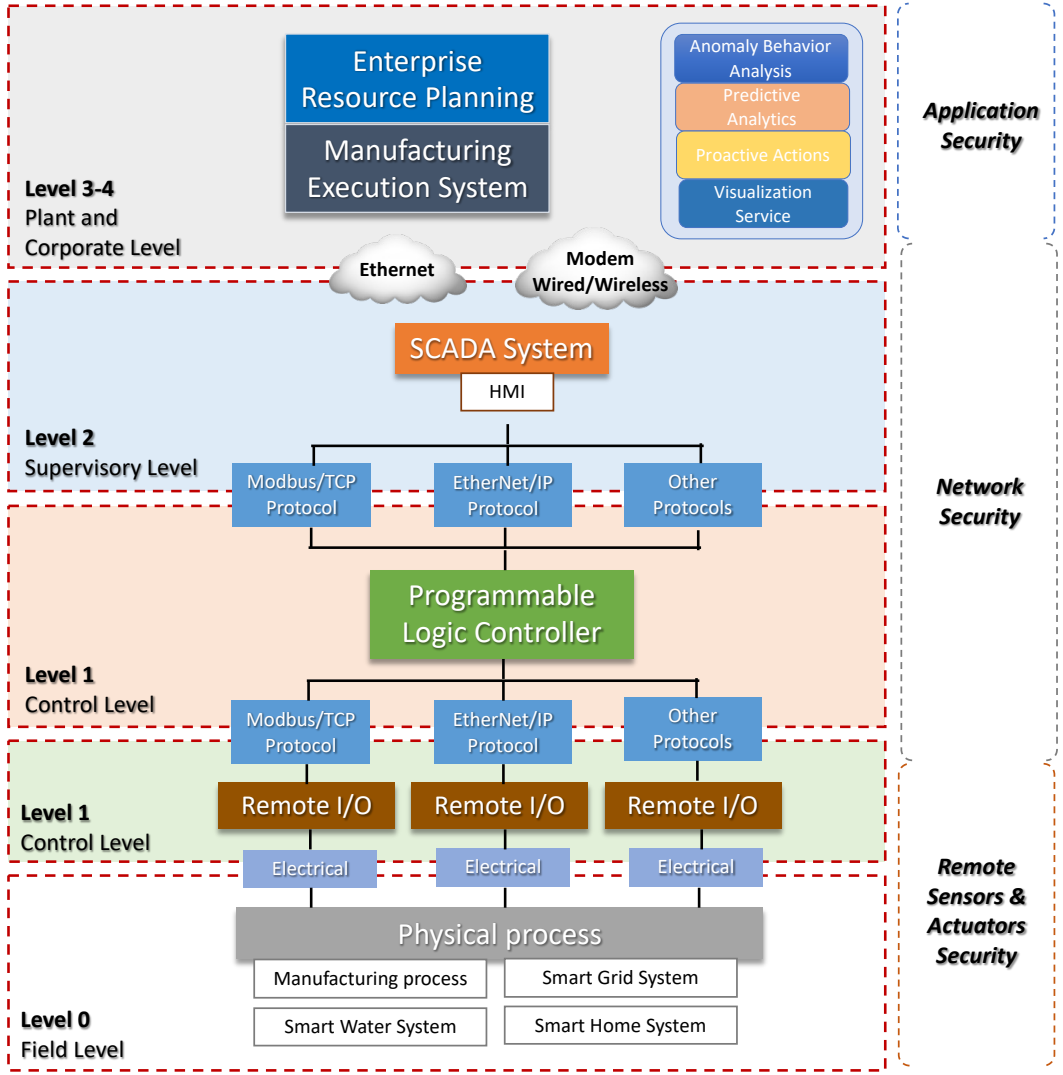
ICS Architecture

- Level 0 – Field
  - Physical process devices
  - Sensors, actuators, switches, valves that interact directly with the industrial process
- Level 1 – Control
  - Control functions to manage specific processes
  - PLCs, RTUs



ICS Architecture

- Level 2 – Supervisory
  - Coordination of Level 1 controllers
  - HMIs and SCADA software
- Level 3 & 4 – Manufacturing, Enterprise and Business Planning
  - Production scheduling
  - Supply chain management



ICS vs IT Security

Industrial Control Systems

- Focus on operational technology
- Deal with processes that have physical consequences
  - Industrial processes
  - Critical infrastructure
  - Energy sector
  - Manufacturing
  - Transportation
- Ensure the availability, integrity, and safety of industrial processes

Information Technology

- Primarily handle data and business processes
- Focuses on preserving the confidentiality, integrity, and availability of digital information and computer systems
- Usually do not pose direct physical threats

ICS vs IT Security

Industrial Control Systems

- Comprise physical devices
  - Programmable logic controllers (PLCs)
  - Sensors
  - Actuators
  - Supervisory control and data acquisition (SCADA) systems
- ICS networks often have unique architectures, including isolated networks and industrial protocols
- Prioritize operational stability and safety

Information Technology

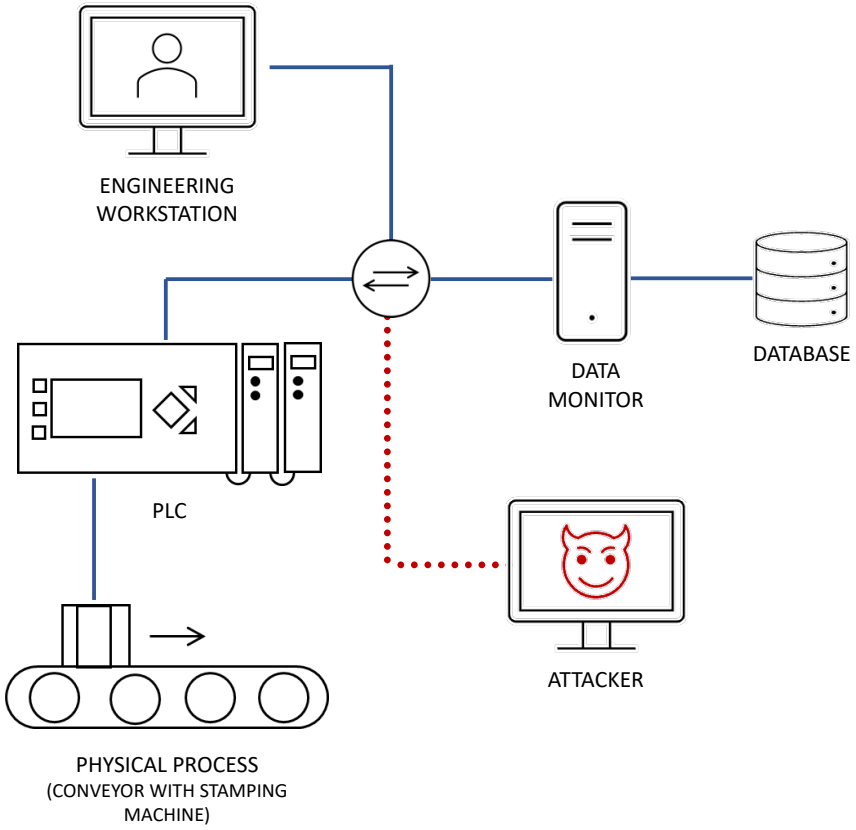
- Comprised of
  - Servers
  - Workstations
  - Databases
  - Network devices
- IT networks are more interconnected and operate within standard network architectures
- More flexibility when addressing certain types of risks

ICS vs IT Security

Industrial Control Systems	Information Technology
• Successful attacks on ICS environments can lead to disruptions in critical infrastructure, physical harm, and environmental damage	• Attacks on IT systems often result in data breaches, identity theft, financial loss, and reputational damage
• Malfunctions in industrial processes could have severe societal and economic impacts	• The impact is primarily on digital assets and information
• ICS security is subject to industry-specific regulations and standards	• IT security is guided by a broader range of frameworks, such as NIST Cybersecurity Framework,

Threat modeling: ICS

1. Model system
   - Motor
   - Stamping system
   - Object detector sensor
   - Programmable logic controller (PLC)
   - Engineering workstation (Windows machine)



Threat modeling: ICS

2. Find Threats

Threat Description	Threat Category (STRIDE)					
	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privileges
An attacker might tamper with sensor data transmitted to the PLC	X	X				X
Manipulation of PLCs control settings						X
Spoof and modification of the data reported to the engineering workstation	X	X		X		
Manipulation of PLC commands and data	X	X				

Threat modeling: ICS

3. Address Threats

Threat Description	**Mitigation strategies**
An attacker might tamper with sensor data transmitted to the PLC	Introduce an Intrusion Detection System for the industrial protocol in use
Manipulation of PLCs control settings	Add authentication to the PLCs control settings
Spoof and modification of the data reported to the engineering workstation	Encryption and authentication between PLC and engineering workstations
Manipulation of PLC commands and data	Filtering of unauthorized commands

Threat modeling: ICS

5. Rate Threats

Threat Description	Threat Risk Assessment (DREAD)					
	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	DREAD Score
An attacker might tamper with sensor data transmitted to the PLC	5	2	2	4	2	15
Manipulation of PLCs control settings	3	2	2	3	3	13
Spoof and modification of the data reported to the engineering workstation	2	3	3	2	3	13
Manipulation of PLC commands and data	4	2	3	4	3	16