IoT in Safety-Critical Contexts

Dr Ayman El Hajjar

CyBOK Mapping

The lecture maps to the following CyBOK Knowledge Areas:

Full Coverage:

- **Infrastructure Security → Cyber-Physical Systems Security**
- **Human, Organisational and Regulatory Aspects → Risk Management & Governance**

Partly Covered:

- **Infrastructure Security → Network Security**
- **Infrastructure Security → Physical Layer and Telecommunications Security**

Outline

Characteristics of Safety-Critical IoT Systems

Why Safety-Critical IoT?

IoT technologies are increasingly used to monitor and control **safety-critical systems**, where failures may have direct consequences for **people**, **physical assets**, or the **environment**.

Safety-critical IoT systems are widely deployed in domains where safe and reliable operation is essential.

- **Healthcare:** Connected medical devices and patient monitoring.
- **Industry:** Automated manufacturing and process control.
- **Transportation:** Connected and autonomous vehicles.
- **Critical Infrastructure:** Energy, water, and public services.

Failures in these environments may result in physical rather than purely digital consequences.

What Makes an IoT System Safety-Critical?

A **safety-critical IoT system** is a connected system where failures can lead to **unsafe physical consequences**.

Safety-critical IoT systems differ from conventional IoT in several important ways:

- **Physical Interaction:** Directly monitors or controls physical processes.
- **Safety Consequences:** Failures may affect people, equipment, or the environment.
- **Connectivity:** Wireless and networked communication increases system complexity and exposure.

Unlike conventional IoT systems, failures may directly affect the physical world.

Characteristics of Safety-Critical IoT Systems

Safety-critical IoT systems share several engineering characteristics that support safe and dependable operation.

- **Real-Time Operation:** Data and control actions must be delivered within defined time constraints.
- **Dependability:** Systems are expected to operate reliably and predictably throughout their operational lifetime.
- **Continuous Availability:** Critical services must remain operational with minimal interruption.
- **Trustworthy Communication:** Sensor readings and control messages must remain accurate and timely.
- **Functional Safety:** Systems must continue to operate safely when faults or failures occur.

The loss of any of these characteristics can increase the likelihood of unsafe system behaviour.

Failure Propagation in Safety-Critical IoT

Why Failure Propagation Matters

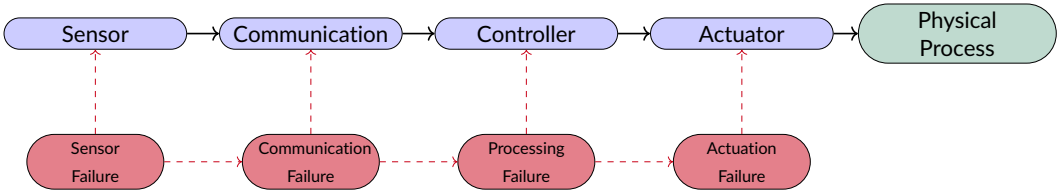
Failure propagation describes how a fault or security incident can spread through an interconnected system, ultimately affecting the **physical process**.

Safety-critical IoT systems rely on multiple components working together, allowing failures to propagate beyond their point of origin.

- **Interconnected Components:** Sensors, networks, controllers, and actuators operate as a single system.
- **Cascading Effects:** A failure in one component may trigger failures elsewhere.
- **Physical Consequences:** Propagated failures can ultimately affect the physical environment.

In safety-critical IoT systems, the impact of a failure often depends on how it propagates through the system rather than where it originated.

Failure Propagation in Safety-Critical IoT



Failures may propagate through interconnected components, resulting in unsafe system behaviour.

Sources of Failure Propagation

Failures may originate from different parts of a safety-critical IoT system. Regardless of their origin, they can propagate through interconnected components and influence the physical process.

- **Sensor Failures:** Faulty, manipulated, or unavailable sensor data.
- **Communication Failures:** Delayed, disrupted, or corrupted data exchange.
- **Processing Failures:** Software errors, incorrect decisions, or compromised controllers.
- **Actuation Failures:** Incorrect or delayed execution of control actions.

Understanding where failures originate is the first step towards preventing them from becoming safety hazards.

Operational Challenges in Safety-Critical IoT

Operational Challenges in Safety-Critical IoT

Safety-critical IoT systems must maintain safe and reliable operation despite changing conditions and operational demands.

Operating these systems introduces several practical challenges.

- **Real-Time Constraints:** Decisions must be made within strict time limits.
- **Continuous Operation:** Critical services cannot tolerate prolonged interruptions.
- **System Complexity:** Interconnected components increase operational dependencies.
- **Dynamic Environments:** Operating conditions may change over time.

Operational challenges can increase the likelihood of unsafe system behaviour.

Human Factors and Situational Awareness

Human operators remain essential for supervising, monitoring, and responding to abnormal conditions in many safety-critical IoT systems.

Safe operation depends on maintaining accurate situational awareness.

- **Monitoring:** Decisions rely on accurate and timely information.
- **Human Intervention:** Operators may need to override or stop system operation.
- **Trust:** Incorrect information can reduce confidence and lead to poor decisions.

Poor situational awareness can increase the likelihood of unsafe system behaviour.

Balancing Safety, Security and Performance

Safety-critical IoT systems must balance multiple operational requirements while maintaining safe and dependable operation.

Engineering decisions often involve trade-offs between competing objectives.

- **Safety:** Protect people, equipment, and the environment.
- **Security:** Prevent unauthorised access and system misuse.
- **Performance:** Meet real-time and operational requirements.

Changes that improve one objective should not introduce unacceptable risks to another.

Safety-Critical Domain Examples

Safety-Critical IoT in Practice

Safety-critical IoT systems are deployed across many sectors where failures may affect people, infrastructure, or the environment.

The engineering principles discussed so far are applied across a wide range of real-world domains.

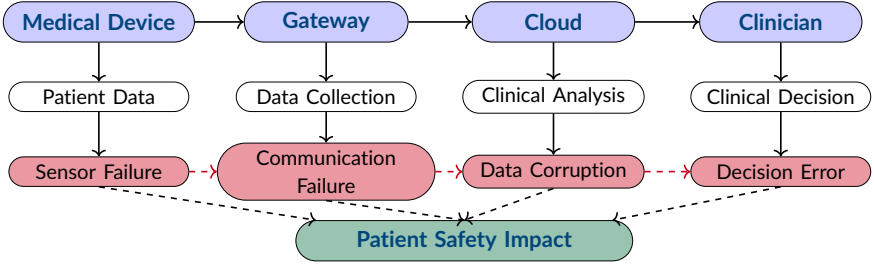
- Medical IoT
- Industrial IoT
- Connected Transportation
- Critical Infrastructure

Although these domains differ, they share the same challenge of maintaining safe operation despite failures and cyber attacks.

Medical IoT Systems

Medical IoT systems connect medical devices, sensors, and healthcare services to support patient monitoring, diagnosis, and treatment.

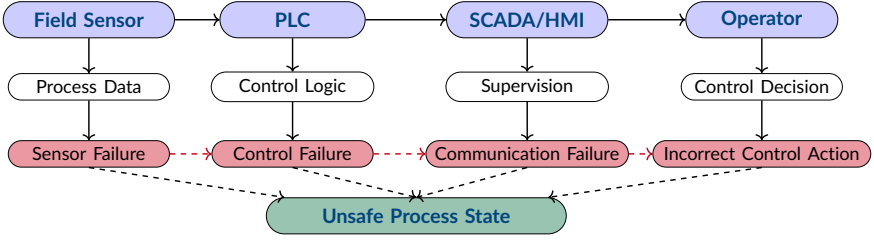
Medical IoT systems rely on the accurate flow of information from sensing to clinical decision making.



Failures can propagate through the system and affect **patient safety**.

Industrial IoT systems connect sensors, controllers, and supervisory systems to monitor and control industrial processes.

Industrial IoT systems rely on continuous monitoring and control of physical processes.

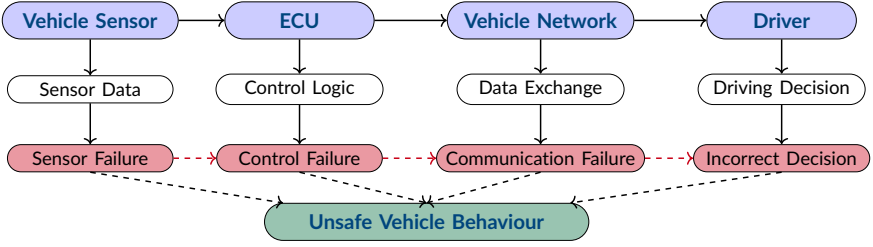


Failures can propagate through the system and affect **industrial safety**.

Connected Transportation Systems

Connected transportation systems integrate sensors, communication networks, and vehicle control systems to support safe transportation.

Connected transportation systems rely on accurate information and timely control decisions.

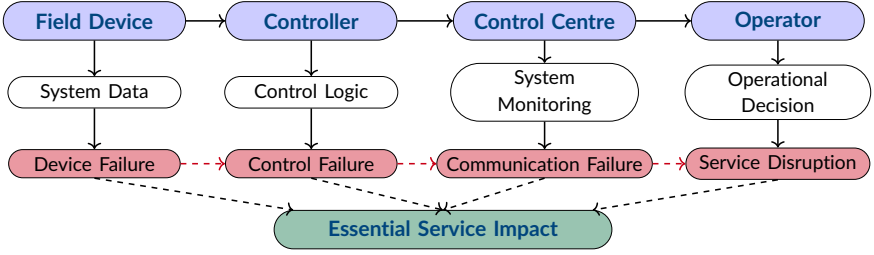


Failures can propagate through the system and affect **transportation safety**.

Critical Infrastructure

Critical infrastructure systems use sensors, controllers, and communication networks to deliver essential services such as energy and water.

Critical infrastructure systems rely on continuous operation to support essential services.



Failures can propagate through the system and affect **essential services**.

Real-World Security Incidents

From Theory to Practice

The challenges faced by safety-critical IoT systems are not theoretical. Numerous cyber incidents have demonstrated how attacks can disrupt physical systems and essential services.

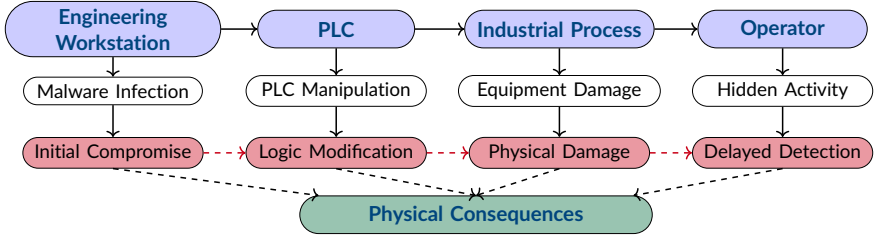
The examples in this section illustrate how cyber attacks have affected different safety-critical domains.

Real-world incidents reinforce the importance of designing secure and dependable safety-critical systems.

Stuxnet (2010)

Stuxnet was a sophisticated malware campaign that targeted industrial control systems by modifying PLC logic while concealing its actions from operators.

Stuxnet demonstrated that cyber attacks can manipulate industrial control systems and produce physical consequences.

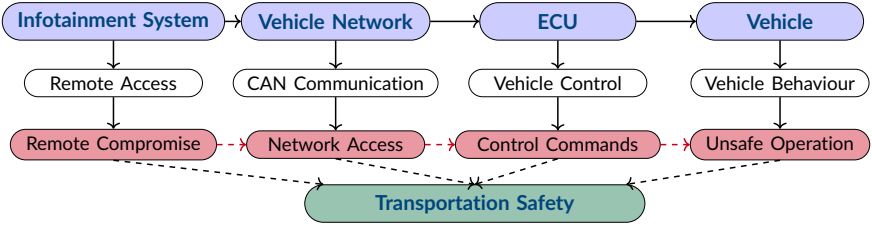


Stuxnet demonstrated that cyber attacks can manipulate industrial processes and lead to **physical damage**. .

Jeep Cherokee Remote Hack (2015)

In 2015, security researchers remotely compromised a Jeep Cherokee through its infotainment system, demonstrating the safety risks of connected vehicles.

The attack showed that compromised in-vehicle systems can influence vehicle behaviour.

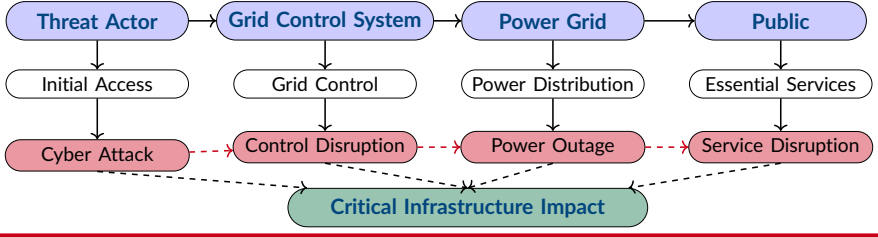


Compromised vehicle systems can influence control functions and affect **transportation safety**.

Cyber Attacks on the Ukrainian Power Grid (2022)

During the Russia-Ukraine conflict, cyber attacks targeted Ukraine's power grid, demonstrating the vulnerability of critical infrastructure.

The attacks highlighted the dependence of critical infrastructure on secure industrial control systems.

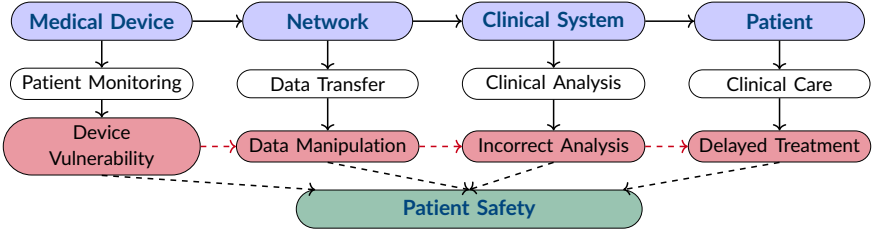


Cyber attacks on critical infrastructure can disrupt **essential services** and affect lives.

Medical Device Security Advisories

Regulatory agencies have issued security advisories for connected medical devices, highlighting that cyber vulnerabilities may affect patient safety if left unaddressed.

Medical device security requires protecting both clinical functions and patient data.



Cyber vulnerabilities in medical devices may affect **patient safety**.

Summary

- **Safety-Critical IoT:** Connected systems interact with physical processes where failures may affect people, infrastructure, or the environment.
- **Failure Propagation:** Faults and cyber attacks may propagate across interconnected components and produce physical consequences.
- **Operational Challenges:** Safety depends on dependable communication, timely operation, and resilient system behaviour.
- **Application Domains:** Medical, industrial, transportation, and critical infrastructure systems share common security and safety challenges.
- **Real-World Incidents:** Practical examples demonstrate that cyber attacks can directly affect safety-critical operations.

In safety-critical IoT systems, cyber attacks may extend beyond the digital domain and produce **physical** and **societal consequences**.

Key References

- NIST. (2023). *Cybersecurity Framework (CSF) 2.0*. **[Link]**
- NCSC. *Cyber Assessment Framework (CAF)*. **[Link]**
- NCSC. *Cyber Security Design Principles for Operational Technology*. **[Link]**
- ENISA. (2024). *Good Practices for the Security of IoT*. **[Link]**
- NIST. (2023). *Cybersecurity of Genomic Data*. NIST IR 8432. **[Link]**
- IEC 62443. *Security for Industrial Automation and Control Systems*. **[Link]**
- FDA. *Cybersecurity in Medical Devices*. **[Link]**
- NCSC. *Operational Technology Guidance*. **[Link]**
- MITRE. *ATT&CK for ICS*. **[Link]**