

Security-Informed Safety Educational Resource

Author: Dr Hossein Abroshan

Episode Title: Cloud-Connected Infusion Pump Ecosystem Failure (Architecture and Supply-Chain Safety)

Associated Video: Episode 5 – Cloud-Connected Infusion Pump Ecosystem Failure

Prerequisites:

- Basic cyber security concepts
- Basic safety concepts
- Familiarity with cyber-physical systems (recommended)

1. Episode Overview

Purpose

Contemporary healthcare systems are becoming dependent on interconnected medical devices, electronic health records, wireless communications, and cloud-supported services. Smart infusion pumps are one of the most representative manifestations of this revolution. These devices aid in accurate drug delivery and work with drug libraries, electronic medication administration records (eMAR), barcode medication administration (BCMA) systems, and centralised device management platforms.

These technologies support medication safety, operational efficiencies, and clinical visibility. But they also create dependencies on digital infrastructure that can be disrupted by cyber security incidents or service failures.

Cyber events often do not induce equipment failure to the level of conventional safety incidents. Instead, they can erode confidence in operational information, create uncertainty concerning system status, and compel healthcare workers to use degraded operating procedures.

This episode is about a cloud-connected infusion pump ecosystem affected by a service disruption caused by a cyber attack. The infusion pumps continue to deliver therapy normally, but supporting digital services are no longer available. The resulting loss of visibility and confidence creates operational challenges and, if recovery decisions are not managed carefully, patient risk could increase.

This episode illustrates an essential precept of Security-Informed Safety:

Patient safety depends not only on device functionality but also on the trustworthiness of the digital systems that support clinical decision-making.

2. Learning Outcomes

After completing this episode, students should be able to:

1. Describe the architecture of a modern smart infusion pump ecosystem.
2. Explain the purpose of drug libraries and Dose Error Reduction Systems (DERS).
3. Distinguish between device failure and loss of operational assurance.
4. Explain how cyber incidents can indirectly affect patient safety.
5. Identify risks associated with degraded clinical workflows.
6. Explain the importance of resilience during healthcare service disruption.
7. Describe the role of clinical staff, biomedical engineers, and cyber security teams during recovery.
8. Analyse cyber-to-physical escalation pathways in healthcare environments.
9. Apply Security-Informed Safety principles to connected medical technologies.
10. Evaluate safe recovery strategies for healthcare cyber incidents.

3. Security-Informed Safety Focus

Core Principle

Patient safety depends not only on device functionality but also on the trustworthiness of the digital systems that support clinical decision-making.

Cyber-to-Physical Relationship

The progression from cyber disruption to patient risk occurs through a sequence of linked events.

Cloud Service Disruption → Loss of Connected Clinical Services → Reduced Operational Visibility → Increased Reliance on Manual Procedures → Greater Potential for Human Error → Patient Safety Risk

The incident demonstrates that cyber security events and safety hazards are not necessarily the same event.

The disruption creates conditions under which unsafe decisions become more likely.

The hazard emerges from uncertainty rather than direct device manipulation.

4. Suggested Teaching Plan

Introduction

Introduce:

- Smart infusion pumps
- Drug libraries
- Dose Error Reduction Systems (DERS)
- eMAR systems
- BCMA systems
- Connected healthcare technologies
- Healthcare resilience

Questions to ask:

- What makes medication administration safe?
- What information do healthcare professionals rely upon?
- Can a system remain operational yet still become less safe?

Video Activity

Students watch the episode.

Encourage students to identify:

- Assets
- Threats
- Hazards
- Safety consequences
- Digital dependencies
- Resilience mechanisms

Worksheet Activity

Students complete:

- Hazard–Threat Mapping
- Cyber-to-Physical Escalation Analysis
- Incident Response Exercise
- Mitigation Analysis

Discussion

Facilitate discussion around:

- Operational assurance

- Degraded-mode operation
- Human factors
- Healthcare resilience
- Security-Informed Safety implications

Debrief

Summarise key lessons.

Reinforce Security-Informed Safety concepts.

5. Discussion Questions

Technical Discussion

1. What role do drug libraries and DERS play within smart infusion pump ecosystems?
2. Why can infusion pumps continue operating when supporting services become unavailable?
3. What information is lost during the service disruption?
4. Why is operational visibility important in connected healthcare environments?

Security-Informed Safety Discussion

1. Why can a cyber incident create patient safety risks even when infusion pumps remain operational?
2. Why is loss of operational assurance different from device failure?
3. How can manual workarounds introduce new risks?
4. Why should cyber security and safety teams collaborate during incident response

Reflection Questions

1. What stakeholders should participate in recovery decisions?
2. How does resilience support patient safety?
3. Why is trustworthiness of information important during clinical decision-making?
4. How does this scenario demonstrate a cyber-to-physical escalation pathway?
5. How does Security-Informed Safety improve healthcare resilience?

6. Instructor Facilitation Notes

The worksheet activities are intended to support discussion and critical analysis rather than produce a single correct answer.

Students should be encouraged to:

- distinguish cyber events from hazards and harm
- identify cyber-to-physical escalation pathways
- consider both cyber security and safety perspectives
- evaluate trade-offs between operational, security, and safety objectives
- justify their decisions using evidence from the scenario

Instructors may adapt discussions and expected outcomes according to the background, experience, and level of the student cohort.

Many activities are intentionally open-ended and designed to encourage multidisciplinary reasoning rather than recall of specific facts.

7. Key Technical Concepts

- Smart infusion pumps
- Drug libraries
- Dose Error Reduction Systems (DERS)
- eMAR systems
- BCMA systems
- Clinical engineering
- Healthcare resilience
- Operational assurance
- Degraded-mode operation
- Human factors
- Cyber-to-physical escalation
- Recovery assurance

8. CyBOK Knowledge Area Mapping

Learning Activity	CyBOK Knowledge Area(s)
Hazard–Threat Mapping	Risk Management & Governance; Cyber-Physical Systems Security
Cyber-to-Physical Escalation Analysis	Cyber-Physical Systems Security
Incident Response Exercise	Security Operations & Incident Management; Cyber-Physical Systems Security
Connected and Cloud-Service Dependency Analysis	Distributed Systems Security; Cyber-Physical Systems Security
Mitigation Analysis	Risk Management & Governance; Security Operations & Incident Management; Cyber-Physical Systems Security

Healthcare Resilience Discussion	Cyber-Physical Systems Security; Human Factors
Degraded-Mode Operation Discussion	Human Factors; Cyber-Physical Systems Security
Recovery Assurance and Multidisciplinary Coordination Discussion	Security Operations & Incident Management; Risk Management & Governance; Human Factors
Security-Informed Safety Discussion	Cyber-Physical Systems Security; Human Factors

9. Alignment with Security-Informed Safety

Key Message

This scenario is not primarily about hacking an infusion pump.

It is about maintaining safe clinical operation during loss of trusted digital services.

The pumps continue operating.

The hazard emerges from uncertainty.

Clinical teams seek continuity of care.

Cyber security teams seek secure restoration.

Engineering teams seek technical validation.

Patient safety teams seek assurance that risks remain controlled.

All objectives are reasonable.

The challenge is ensuring that operational, cyber security, and patient-safety objectives remain aligned.

Security-Informed Safety recognises that effective risk reduction requires coordinated consideration of cyber threats, human factors, operational resilience, and patient safety.

10. Additional Resources

Relevant Standards and Frameworks:

- FDA Cyber Security Guidance for Medical Devices
- AAMI TIR57
- AAMI TIR97
- IEC 80001-1
- IEC 62304
- ISO 14971

- NIST Cyber Security Framework (CSF)
- NIST SP 800-82
- Security-Informed Safety

Instructor Notes

The primary objective is not to teach medical device hacking.

The primary objective is to help students understand how loss of trusted digital services can influence clinical operations and create patient safety risks.

Students should leave the session understanding the distinction between:

- Cyber incident
- Service disruption
- Operational uncertainty
- Patient safety risk

and the importance of resilience, degraded-mode operation, recovery assurance, multidisciplinary coordination, and trustworthy information.

The key Security-Informed Safety lesson is that connected healthcare technologies can continue functioning correctly while uncertainty about supporting digital services creates conditions that increase patient risk.