

Security-Informed Safety Educational Resource

Author: Dr Hossein Abroshan

Episode Title: Smart Manufacturing Robot Cell Ransomware (Organisational Culture, Co-Design and Safe Recovery)

Associated Video: Episode 4 – Smart Manufacturing Robot Cell Ransomware

Prerequisites:

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

1. Episode Overview

Purpose

Current manufacturing environments rely more and more on integrated OT, industrial control systems, engineering workstations, HMIs, and industrial communication networks. These technologies enhance productivity, flexibility, and operational visibility. But at the same time, they also form dependencies on digital systems that could be interrupted in the event of cyber security incidents.

Ransomware is often viewed primarily as an availability problem. In manufacturing environments, however, the most significant safety risks frequently emerge during recovery rather than during the initial cyber incident itself. When operators lose trusted visibility of machine status, controller configurations, production recipes, or operational conditions, pressure to restore production can create circumstances in which unsafe assumptions are made.

This episode looks at a realistic smart-manufacturing robot cell affected by a ransomware incident. The attack does not alter robot motion or safety systems in a direct way. Rather, it impacts operational visibility and creates uncertainty regarding the trustworthiness of engineering and control systems. When production pressure increases, workers must decide if and how to restart the robot cell.

This episode illustrates a fundamental Security-Informed Safety principle:

It is not always safe to restart a system that has recovered from a cyber incident.

Safe recovery depends on effective coordination between cyber security, operations, maintenance, controls engineering, and safety personnel.

2. Learning Outcomes

After completing this episode, students should be able to:

1. Describe the safety architecture of a modern industrial robot cell.
2. Explain the functions of interlocked guards, light curtains, emergency stops, and safety PLCs.
3. Distinguish between operational disruption and safety hazards.
4. Explain how ransomware can indirectly create safety risks.
5. Identify unsafe restart conditions following a cyber incident.
6. Explain the importance of validating safety functions before recommissioning.
7. Describe the role of organisational culture during incident recovery.
8. Explain how co-design supports Security-Informed Safety.
9. Analyse cross-functional decision-making during OT incident response.
10. Apply Security-Informed Safety principles to manufacturing environments.

3. Security-Informed Safety Focus

Core Principle

It is not always safe to restart a system that has recovered from a cyber incident.

Safe recovery depends on effective coordination between cyber security, operations, maintenance, controls engineering, and safety personnel.

Cyber-to-Physical Relationship

The progression from cyber incidents to safety risk occurs through a sequence of linked events.

Ransomware Incident → Loss of Trusted Operational Information → Robot Cell Safe Stop
→ Production Pressure → Unsafe Restart Temptation → Incomplete Validation →
Unexpected Robot Motion Hazard → Potential Injury or Equipment Damage

The incident demonstrates that cyber security events and safety hazards are not always identical.

The ransomware incident creates conditions under which unsafe decisions become more likely.

The hazard emerges from uncertainty rather than from direct cyber manipulation.

4. Suggested Teaching Plan

Introduction

Introduce:

- Industrial robot cells
- Functional safety
- Safety PLCs
- Interlocked guards
- Light curtains
- Emergency stops
- OT environments
- Safe recovery

Questions to ask:

- What makes a robot cell safe during normal operation?
- What information is required before restarting industrial equipment?
- Why might recovery create new safety risks?

Video Activity

Students watch the episode.

Encourage students to identify:

- Assets
- Threats
- Hazards
- Safety consequences
- Recovery challenges
- Safety barriers

Worksheet Activity

Students complete:

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

Discussion

Facilitate discussion around:

- Security-Informed Safety implications
- Recovery governance
- Organisational culture
- Co-design
- Cross-functional decision making

Debrief

Summarise key lessons.

Reinforce Security-Informed Safety concepts.

5. Discussion Questions

Technical Discussion

1. What role does the Safety PLC play within the robot cell?
2. Why are interlocked gates, light curtains, and emergency stops considered independent safety functions?
3. What information is lost during the ransomware incident?
4. Why does the robot cell stop safely?

Security-Informed Safety Discussion

1. Why can ransomware create safety risks even when safety systems remain operational?
2. Why is guard closure not equivalent to safe restart?
3. How can production pressure contribute to unsafe decisions?
4. Why should safety functions be validated following recovery activities?

Reflection Questions

1. Which stakeholders should participate in restart decisions?
2. How does co-design support Security-Informed Safety?
3. What role does organisational culture play during incident response?
4. What evidence should be required before returning to automatic production?
5. How does this scenario illustrate Security-Informed Safety?

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

- Industrial robot cells
- Functional safety
- Safety PLCs
- Interlocked access gates
- Safety light curtains
- Emergency stop systems
- OT architecture
- Engineering workstations
- HMI systems
- Ransomware
- Recovery assurance
- Restart governance
- Co-design
- Organisational culture

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
Ransomware Incident Analysis	Malware and Attack Technologies; Cyber-Physical Systems Security
Mitigation Analysis	Risk Management & Governance; Cyber-Physical Systems Security

Recovery and Restart Governance Discussion	Security Operations & Incident Management; Risk Management & Governance
Organisational Culture and Co-Design Discussion	Human Factors; Risk Management & Governance
Security-Informed Safety Discussion	Cyber-Physical Systems Security; Human Factors

9. Alignment with Security-Informed Safety

Key Message

This scenario is not primarily about ransomware.

It is about decision-making under uncertainty.

The robot cell stops safely.

The hazard appears during recovery.

Cyber security teams seek rapid restoration.

Operations teams seek rapid production recovery.

Safety personnel seek verification and validation.

All objectives are reasonable.

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

Security-Informed Safety recognises that effective risk reduction requires coordinated consideration of both cyber threats and safety hazards.

10. Additional Resources

Relevant Standards and Frameworks:

- ISO 12100
- ISO 10218-1
- ISO 10218-2
- ISO 13849
- IEC 62061
- ISO 14118
- ISO 13850
- IEC 62443
- NIST SP 800-82

- Security-Informed Safety (CyBOK)

Instructor Notes

The primary objective is not to teach ransomware.

The primary objective is to help students understand how loss of trusted operational information can influence recovery decisions and create safety hazards.

Students should leave the session understanding the distinction between:

- Cyber incident
- Operational disruption
- Hazard
- Potential harm

and the importance of recovery assurance, functional safety validation, organisational culture, co-design, and cross-functional decision making.

The key Security-Informed Safety lesson is that a system can stop safely during a cyber incident, yet still become unsafe if recovery and restart activities are not managed correctly.