

Security-Informed Safety Educational Resource

Author: Dr Hossein Abroshan

Episode Title: Chemical Overdose in Water Treatment (Hazard-Threat Convergence)

Associated Video: Episode 1 - Chemical Overdose in Water Treatment

Prerequisites:

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

1. Episode Overview

Purpose

This episode covers an example of an operational municipal water treatment plant where sodium hydroxide is used to keep the pH of the water consistent with standards of operation. Using this realistic cyber-physical scenario, students examine how a compromise of the maintenance pathway can impact process control, introduce unsafe operational conditions, and, ultimately, workers, consumers, infrastructure, and the environment.

This episode illustrates a key insight of Security-Informed Safety:

When cyber security works, hazards are prevented; when cyber security does not, safety systems reduce the consequences.

Instead of distinguishing cyber security and safety as separate, independent subjects, Security-Informed Safety recognises that cyber events make safety hazards possible and safety engineering needs to take into account any cyber compromise.

2. Learning Outcomes

After completing this episode, students should be able to:

1. Describe the significance of pH control in municipal water treatment.
2. Explain how sensors, PLCs, SCADA systems and actuators interact in an OT environment.
3. Explain how cyber compromise can be propagated through industrial control systems and affect physical processes.
4. Determine unsafe control actions that create hazardous situations.

5. Explain what independent safety functions and Safety Instrumented Systems (SIS) are.
6. Differentiate cyber events, hazards, and safety implications.
7. Assess how safety barriers and security controls correlate with each other to mitigate risk.
8. Relate concepts from Security-Informed Safety to industrial standards and frameworks.

3. Security-Informed Safety Focus

Core Principle

When cyber security works, hazards are prevented; when cyber security does not, safety systems reduce the consequences.

Cyber events make safety hazards possible and safety engineering needs to take into account any cyber compromise.

Cyber-to-Physical Relationship

The maintenance pathway is compromised.

The attacker is able to access systems inside the OT environment.

PLC-201 is modified.

The sodium hydroxide dosing rate increases.

Water chemistry starts to deviate from normal operating conditions.

The likelihood of hazardous conditions increases.

This sequence illustrates a distinction between cyber incident and safety issue.

The compromise itself does not directly affect workers or consumers. The danger here is the compromise alters a physical process's behaviour.

4. Suggested Teaching Plan

Introduction

Introduce:

- Municipal water treatment
- pH control
- Sodium hydroxide dosing
- Cyber-physical systems
- Operational objectives

- Safety objectives

Questions to ask:

- Why is pH control important?
- What could happen if dosing is incorrect?
- What systems are responsible for maintaining safe operation?

Video Activity

Students watch the episode.

Encourage students to identify:

- Assets
- Threats
- Hazards
- Safety consequences
- Security controls
- Safety controls

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
- Trusted maintenance pathways
- Unsafe control actions
- Independence of safety functions
- Operational decision-making

Debrief

Summarise key lessons.

Reinforce Security-Informed Safety concepts.

5. Discussion Questions

Technical Discussion

1. Why is pH control important in municipal water treatment?
2. What role does PLC-201 play in the control loop?
3. Why is the Engineering Workstation considered a critical asset?
4. What unsafe control action occurred in the scenario?

Security-Informed Safety Discussion

1. Why is PLC manipulation a safety concern rather than just a cyber security issue?
2. What was the engineering workstation's role in the attack?
3. How crucial is the distinction between a cyber event and a physical hazard?
4. What did SIF-201 do that mitigated the effects of the incident?

Reflection Questions

1. What kind of cyber security controls could have minimized the risk of this compromise actually happening?
2. What safety controls reduced the consequences after the compromise occurred?
3. Why should safety functions remain independent from normal control systems?
4. How would the scenario be different without the Safety Instrumented Function?
5. How does this episode show the relationship between cyber security and functional 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

- Municipal water treatment
- pH control
- Industrial control systems
- Sensors and actuators
- PLCs
- SCADA and HMI systems
- Engineering workstations
- Remote maintenance
- Unsafe control actions
- Cyber-to-physical escalation
- Safety Instrumented Functions (SIF)
- Security-Informed Safety.

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
Mitigation Analysis	Risk Management & Governance; Cyber-Physical Systems Security
Remote Access and Engineering Workstation Discussion	Authentication, Authorisation & Accountability; Network Security; Cyber-Physical Systems Security
Security-Informed Safety Discussion	Cyber-Physical Systems Security; Risk Management & Governance

9. Alignment with Security-Informed Safety

Key Message

The cyber compromise creates the conditions for risk, while the safety function lowers the chances that risk will develop into injury.

Cyber security controls reduce the likelihood of unauthorised access. If those controls break, safety functions help reduce the effect.

Neither discipline is enough in and of itself.

An understanding of how cyber security and safety interrelate is at the heart of Security-Informed Safety and one of the key takeaways from this episode.

10. Additional Resources

Relevant Standards and Frameworks:

- IEC 62443
- IEC 61508
- NIST SP 800-82
- Security-Informed Safety

Instructor Notes

The primary objective is not to teach a cyberattack.

The primary objective is to help students understand how cyber security events can influence safety outcomes and why cyber security, safety, engineering, and operational perspectives must be considered together.

Students should leave the session understanding the distinction between:

- Cyber event
- Hazard
- Potential harm

and the role of both cyber security controls and independent safety functions in reducing overall risk.