SISEN: Teaching and Integration Guide

Security-Informed Safety

Dr Ayman El Hajjar
University of Westminster

Purpose of this Guide

This guide explains how SISEN can be used and integrated into teaching. It is intended for lecturers, module leaders, laboratory tutors, and curriculum designers who are deciding how the lecture materials, practical scenarios, activity guidance, demonstration videos, and hazard-analysis resources should be used together.

SISEN introduces a security-informed safety perspective for wireless, IoT, and cyber-physical systems. Students observe normal operation, examine communication and telemetry, perform a bounded attack or disruption within the SISEN environment, collect evidence, and connect the resulting technical effect to a possible safety hazard and mitigation strategy. The three main scenarios are accessed through a common launcher and a unified read-only dashboard, while scenario control, attack execution, and packet capture remain terminal-controlled.

1 What the SISEN Resource Pack Contains

The resource pack contains:

- **eight lecture sets**, covering security and safety fundamentals, security-informed safety, hazard analysis and assurance, IoT and cyber-physical systems, wireless threats, safety-critical IoT, resilience and mitigation, and applied case studies;
- **three practical scenario guides**, covering Smart Building IoT, Medical IoT, and 6LoWPAN Industrial IoT;
- the **SISEN Attack and Disruption Guide**, which explains the controlled attack categories, helper-based activities, observable effects, safety relevance, and the distinction between automated and manual activities;
- the **SISEN Student Guide**, which provides common installation, environment setup, launcher, dashboard, evidence, and working-practice guidance;
- the **Security-Informed Safety Hazard Analysis and Evidence Sheet**, which supports baseline recording, evidence collection, security-event classification, system-effect analysis, hazard development, mitigation, assurance evidence, and residual-risk reasoning;
- the **Instructor Guide**, which provides detailed delivery, preparation, troubleshooting, and assessment guidance; and
- a **multi-part demonstration series**, covering installation, normal use, traffic observation, controlled attacks, Wireshark investigation, wireless infrastructure activities, and hazard-analysis reporting.

The materials are available through the SISEN repository and the SISEN project site. Current commands, launcher options, scenario documentation, capture guidance, and troubleshooting information are maintained in the repository documentation.

2 CyBOK Alignment

SISEN supports teaching across several CyBOK knowledge areas, including introductory concepts, risk management and governance, adversarial behaviours, authentication and authorisation, network security, cyber-physical systems security, and physical-layer and telecommunications security.

The detailed lecture-level and section-level mapping is provided separately within the SISEN teaching materials. Instructors may therefore use the complete sequence or select only the material relevant to a particular module or learning outcome.

3 Ways to Integrate SISEN

SISEN can be used in several formats.

- **Single practical session:** Use one scenario to introduce the relationship between a security event, an operational effect, a safety hazard, and a mitigation.
- **Short teaching block:** Combine selected lectures with one or more practical scenarios over two or three sessions.
- **Module topic:** Use the lectures and labs as a focused block within cyber security, networking, IoT, cyber-physical systems, wireless security, or safety and risk modules.
- **Assessment activity:** Ask students to submit selected evidence, a security-to-safety chain, a completed hazard analysis, and justified mitigation recommendations.
- **Advanced extension:** Ask students to compare scenarios, inspect packet captures, evaluate trust boundaries, distinguish observation from inference and assumption, or propose resilience improvements.

For introductory use, instructors may provide the exact activity commands and focus student effort on observation and explanation. For advanced use, students may be expected to interpret captures, distinguish failures across communication layers, compare normal and attack traffic, and justify controls using both security and safety principles.

4 Selecting a Practical Scenario

- **Smart Building IoT** is suitable for teaching MQTT telemetry, environmental and occupancy monitoring, authenticity, integrity, replay, availability, and the effect of misleading or missing building-state information.
- **Medical IoT** is suitable for teaching trustworthy and timely patient telemetry, wearable and gateway trust, message authenticity, freshness, and the consequences of false or missing clinical data.
- **6LoWPAN Industrial IoT** is suitable for teaching constrained wireless networking, layered trust, border-router behaviour, IPv6 adaptation, UDP telemetry, MQTT relay behaviour, and end-to-end security reasoning.

Each scenario can be delivered independently. The selected scenario should match the module topic, available time, technical level of the students, and the evidence or analysis expected from the activity.

Manual wireless infrastructure activities that require a physical wireless adaptor, monitor mode, packet injection, or a hardware access point are maintained separately under `ap/hw-ap/docs/`. General manual-activity guidance is provided in `docs/manual-attacks.md`. These activities should not be treated as launcher-managed SISEN scenarios.

5 Recommended Teaching Sequence

A typical SISEN activity follows this sequence:

1. introduce the relevant security and safety concepts;
2. ask students to start the selected scenario and establish normal behaviour using the dashboard, telemetry, traffic, or logs;
3. identify the relevant namespaces, interfaces, topics, or communication paths before collecting evidence;
4. capture or observe the relevant traffic, telemetry, dashboard state, or logs;
5. perform one bounded observation, attack, or disruption activity;
6. compare the system behaviour before, during, and after the activity, including evidence of recovery where normal telemetry resumes;
7. identify the initiating security event, affected component or trust boundary, weakened security property, observed system effect, possible hazard, and potential harm;
8. distinguish direct observation from inference and any assumptions required for the safety consequence;
9. propose preventive, detective, fail-safe, resilience, and recovery controls, together with evidence that would demonstrate their effectiveness; and
10. record residual risk and limitations.

6 Getting Started

Before delivery, the instructor should:

1. review the relevant lecture and practical materials;
2. select the scenario and bounded activity;
3. decide whether the activity is formative, summative, or demonstration-based;
4. test the current repository installation, launcher command, selected scenario, attack command, capture point, and cleanup procedure using the Instructor Guide;
5. provide students with the Student Guide, relevant scenario guide, SISEN Attack and Disruption Guide, capture or manual-activity documentation where required, and the hazard-analysis worksheet; and
6. provide any local assessment instructions, evidence requirements, submission conventions, or marking criteria.

Detailed setup, delivery, troubleshooting, expected observations, and assessment guidance are provided in the SISEN Instructor Guide.