SISEN: Smart Building

Security-Informed Safety in Wireless Networks

Pre-Lab Checks

Before starting this scenario, refer to the SISEN Student Guide and confirm that SISEN has been installed and configured correctly.

The student guide is available **online** and in the SISEN repository under `teaching-materials/labs/`.

Activity Worksheet

Complete the practical activity using the SISEN Hazard Analysis and Evidence Sheet.
The worksheet is available **online** and in the SISEN repository under `teaching-materials/labs/`.

Scenario Purpose

This scenario introduces a simulated smart building environment in which environmental monitoring and building operation depend on trustworthy and timely sensor data.

Simulated wireless sensors generate temperature, humidity, air-quality, and occupancy data. The sensors connect through the SISEN wireless infrastructure, publish readings to an MQTT broker, and provide information to a building monitoring dashboard.

The scenario demonstrates how a security failure affecting the wireless infrastructure, communication path, or building telemetry can develop into a safety-relevant condition for building occupants.

Learning Outcomes

By completing this activity, you should be able to:

- explain how smart building operation depends on trustworthy and timely environmental telemetry;
- describe the data flow between wireless sensors, the access point, MQTT broker, and monitoring dashboard;
- observe normal building telemetry using the dashboard and MQTT tools;
- identify how spoofed, missing, delayed, or disrupted telemetry affects system behaviour;
- collect evidence of normal and abnormal system operation;
- distinguish between a security event, an operational effect, and a safety-relevant hazard;
- complete a structured hazard analysis for the scenario; and
- evaluate appropriate mitigation and resilience controls.

Scenario Overview

The scenario represents a simplified smart building monitoring system.

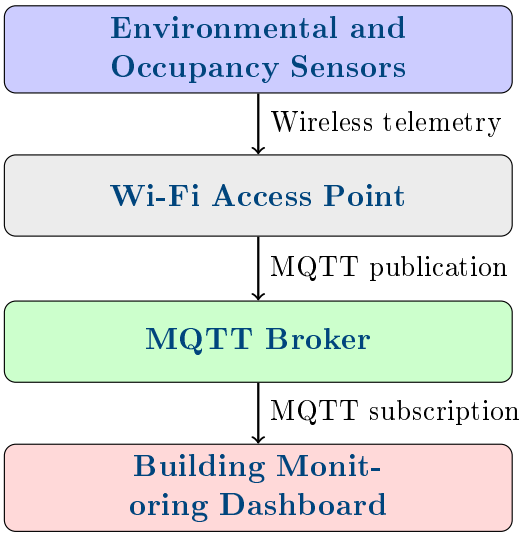
Simulated wireless sensors produce environmental and occupancy readings. The sensors connect through a selected Wi-Fi access point and publish their readings through MQTT. The dashboard presents the latest information that building operators may use to assess environmental conditions and support ventilation, heating, cooling, evacuation, or occupancy decisions.

The system assumes that received telemetry is trustworthy. It does not independently verify that readings are authentic, current, complete, or physically plausible.

- System focus: simulated smart building monitoring
- Communication path: wireless sensors to Wi-Fi access point to MQTT broker to dashboard
- Core services: sensor simulators, wireless infrastructure, MQTT broker, and building monitoring dashboard
- MQTT namespace: `building/#`
- Safety relevance: incorrect or unavailable environmental data may lead to delayed or inappropriate building-management decisions

Scenario Architecture

Shown here is the simplified system architecture. The simulated sensors generate environmental and occupancy readings. The wireless access point provides network connectivity. The MQTT broker distributes the telemetry to subscribed services. The dashboard displays the latest building conditions and associated status information.



Main Components

Environmental and Occupancy Sensors

The simulated sensors generate building data, including:

- temperature;
- humidity;
- air quality, including CO_2 where supported; and
- room occupancy.

The readings vary over time to represent normal changes in building conditions.

Wi-Fi Access Point

The access point provides wireless connectivity between the simulated sensors and the wider monitoring environment.

Its configuration determines how devices associate with the network and which wireless security properties are available. A failure or attack affecting this infrastructure may interrupt several sensor streams simultaneously.

MQTT Broker

The MQTT broker receives telemetry from the sensor publishers and distributes it to subscribed services.

The building telemetry is published under:

```
building/#
```

The broker provides the central communication mechanism for the scenario.

Building Monitoring Dashboard

The dashboard displays the latest building readings.

During normal operation, it should show continuously updating values for:

- temperature;
- humidity;
- air quality; and
- occupancy.

The dashboard trusts the telemetry received through MQTT and does not independently confirm whether the readings are authentic, current, or physically plausible.

Safety Context

Smart building systems support environmental control, occupancy awareness, emergency response, and safe operation.

If environmental conditions become unsafe, accurate telemetry may allow building operators or automated systems to recognise the change and respond. If the data is false, delayed, replayed, or unavailable, the displayed building state may no longer reflect actual conditions.

Examples of possible consequences include:

- elevated CO_2 or poor air quality being reported as normal;
- safe environmental conditions being reported as hazardous;
- occupied rooms being shown as empty;
- temperature or humidity problems remaining undetected;
- several sensor streams disappearing following an infrastructure disruption; and
- building operators losing confidence in the monitoring system.

The security properties of the wireless and telemetry paths are therefore directly connected to occupant safety.

1 Start the Smart Building Scenario

Activity Worksheet

Complete the practical activity using the SISEN Hazard Analysis and Evidence Sheet.
The worksheet is available **online** and in the SISEN repository under `teaching-materials/labs/`.

Before starting the scenario, decide how the wireless environment will be configured.

1.1 Wireless Access Point

The scenario runs through the SISEN wireless environment. When prompted, select the required Wi-Fi access point mode.

The selected access point determines how the simulated devices connect to the network and which wireless security properties are available for observation or testing.

Use the access point mode specified by the instructor.

1.2 Number of Simulated Nodes

The direct launch example creates four simulated building rooms or zones. The `-nodes` option accepts a value from 1 to 10.

Each node publishes telemetry appropriate to its room or zone. Increasing the number of nodes increases the amount of traffic generated and the number of dashboard cards and MQTT streams visible in the scenario.

Use the number of nodes specified by the instructor.

1.3 Start the Scenario

From the project root directory, run:

```
python3 launch_sisen.py --scenario smart-building --ap-mode open --nodes 4 --
    capture-hints
```

2 Observe Normal Operation

Open the building monitoring dashboard using the address shown by the scenario runner.

```
http://localhost:5000
```

Observe the dashboard for at least two minutes. During normal operation, you should see:

- continuously updating temperature readings;
- continuously updating humidity readings;
- air-quality or CO_2 readings where supported;
- occupancy readings for the simulated rooms or zones;
- values changing gradually rather than remaining completely static; and
- no persistent missing-data or critical warning.

Do not perform any attack or disruption during this observation period. Record in your activity document:

- the normal range of environmental values displayed;
- the occupancy state of the monitored rooms or zones; and
- how frequently the dashboard appears to update.

3 Optional: Inspect MQTT Telemetry

This step is not required for the scenario to operate. The dashboard already subscribes to the relevant MQTT topics automatically.

Use this additional step to inspect the raw telemetry directly and compare it with the values displayed on the dashboard.

Open a second terminal and subscribe to the building telemetry namespace:

```
mosquitto_sub -h localhost -t 'building/#' -v
```

Observe the messages for at least one minute. Identify:

- the MQTT topics used;
- the sensor or zone represented by each topic;
- the values contained in each message;
- the frequency of publication;
- whether timestamps are included; and
- whether the messages are readable in plaintext.

Compare the MQTT messages with the values shown on the dashboard. Record in your activity document:

- the MQTT topics observed;
- one set of readings shown in both the MQTT messages and the dashboard; and
- whether the MQTT data appears to be encrypted or protected from unauthorised subscribers.

4 Examine the Communication Flow

Use the relevant packet capture activity from the SISEN Attack and Disruption Guide.

Capture the traffic on the interface specified for the selected scenario and examine the communication between the sensor nodes, access point, MQTT broker, and dashboard.

Use Wireshark and apply the following MQTT display filter:

```
mqtt
```

Observe the traffic generated during normal operation. Identify:

- the source and destination addresses;
- the MQTT broker port;
- MQTT publish messages;
- MQTT topic names;
- the sensor or zone associated with each message; and
- whether the payload is visible.

Record in your activity document:

- one example MQTT publish message;
- the associated topic and payload; and
- what information an unauthorised observer could learn from the captured traffic.

5 Perform a Bounded Attack or Disruption

This activity demonstrates how attacks or disruptions at different layers of the system can influence building monitoring and create a safety-relevant effect for occupants. Attacks may fall into one or more of the following categories:

- **Infrastructure Attack:** An infrastructure attack affects the supporting wireless or network environment, such as the Wi-Fi access point, wireless sensor connectivity, network infrastructure, or MQTT services.
- **Communication or Protocol Attack:** A communication or protocol attack affects the exchange, forwarding, or delivery of data, such as Wi-Fi communication, MQTT publication or subscription, replay, message injection, topic misuse, or traffic disruption.
- **Telemetry or Application-Layer Attack:** A telemetry or application-layer attack affects the environmental or occupancy readings, timing, freshness, authenticity, plausibility, or availability of the data presented to the building monitoring dashboard.

5.1 Select the Disruption Activity

Use the relevant activity from the SISEN Attack and Disruption Guide. Available helper-based activities can be listed from the repository root using `python3 attacks/run_attack.py -list -scenario building`. The guide provides the available bounded attacks and disruptions, including:

- the disruption type;
- the target component or communication path;
- the affected security property;
- the expected technical effect;
- the required command or helper script; and
- the stopping and recovery procedure.

Use the disruption activity specified by the instructor.

5.2 Before Running the Disruption

Confirm that:

- the Smart Building scenario is running;
- the selected access point is active;
- the dashboard is displaying normal telemetry;
- the simulated sensor processes are active;
- normal telemetry has been observed on the dashboard; and
- any required packet capture is already running.

Record the most recent normal building readings before continuing.

5.3 Run the Disruption

Run the selected bounded activity using the current attack runner command in the SISEN Attack and Disruption Guide. Smart Building activities are organised under categories including authenticity, integrity, replay, availability, and safety-case. Some interface-level availability activities require `sudo` and may use a namespace target such as `room-101`.

While it is active, do not restart the scenario or manually publish additional MQTT messages unless instructed.

6 Observe the System Effect

Compare the system behaviour during the disruption with the normal baseline recorded earlier. Examine:

- the building monitoring dashboard;
- the MQTT telemetry;
- the wireless access point and connection state;
- the sensor process output; and
- the packet capture, where available.

Determine:

- which component first showed evidence of the disruption;
- whether the dashboard displayed false, stale, missing, or inconsistent data;
- whether one sensor, one zone, or several sensor streams were affected;
- whether the wireless infrastructure or broker detected the abnormal condition;
- whether the displayed building state could lead to an unsafe operational decision; and
- whether the system recovered automatically after the disruption stopped.

Record the findings in the separate activity document.

7 Stopping the Disruption

Helper-based telemetry attacks are bounded demonstrations. Where an attack needs to remain visible, the helper refreshes the injected value for approximately ten seconds and then exits. Normal scenario telemetry continues during the activity and should restore the dashboard afterwards. For interface-level or manual activities, use the stopping or recovery procedure provided in the SISEN Attack and Disruption Guide.

Confirm that the abnormal activity has stopped. Observe whether normal telemetry and wireless connectivity resume automatically. Record in your activity document:

- whether the system recovered automatically;
- how long recovery took;
- whether all affected sensor nodes reconnected; and
- whether any stale or abnormal data remained visible.

8 Distinguish the Security Event from the Hazard

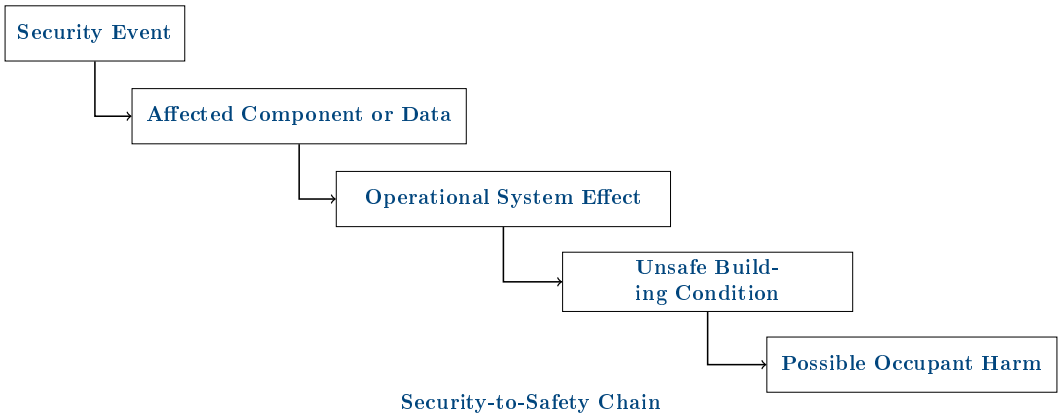
A security event and a safety hazard are not the same.

The security event is the compromise or disruption that affects the system. The operational effect is the resulting change in system behaviour.

The hazard is the condition that may contribute to occupant harm.

Using the observed disruption, complete the **security-to-safety chain** in your activity document. Address the following points:

- What security event occurred?
- Which component, connection, or data item was affected?
- What immediate operational effect followed?
- What unsafe building condition could result?
- What occupant harm could occur if the problem were not detected?



Security-to-Safety Chain

9 Hazard Analysis

Complete a structured hazard analysis for the observed event in your activity document.

Your analysis should identify:

- the initiating security event;
- the affected asset or function;
- the loss of confidentiality, integrity, availability, authenticity, or accountability;
- the immediate system effect;
- the safety-relevant hazard;
- the possible consequence for occupants;
- existing controls;
- proposed mitigations; and
- remaining residual risk.

Use the following questions to guide your analysis:

- What evidence confirms that the wireless infrastructure or telemetry was disrupted or falsified?
- Was integrity, availability, authenticity, or more than one property affected?
- Did the dashboard fail visibly or continue to present misleading information?
- Did the event affect one sensor, one zone, or the wider building-monitoring system?
- Who or what would rely on the affected information?
- What incorrect operational decision might be made?
- What condition could expose occupants to harm?

- What control could prevent the event?
- What control could detect the event?
- What control could reduce the safety impact after detection?

10 Mitigation and Resilience

Consider how the system could be improved. Possible controls include:

- secure Wi-Fi configuration;
- protected management frames where supported;
- access-point and client monitoring;
- MQTT authentication;
- encrypted MQTT communication;
- topic-level access control;
- message authentication or digital signatures;
- sensor identity validation;
- physical and environmental plausibility checking;
- replay protection;
- timestamps and freshness checks;
- rate limiting;
- missing-data detection;
- redundant sensors or communication paths;
- local fail-safe building controls;
- independent alarms;
- audit logging; and
- manual verification of critical conditions.

For each selected control, explain whether it:

- prevents the security event;
- detects the event;
- limits the operational effect;
- reduces the safety consequence; or
- supports recovery and investigation.

Select three controls and explain in your activity document:

- where each control would be implemented;
- what failure or attack it addresses;
- how it improves safety or resilience; and
- what limitation or residual risk remains.

11 Evidence to Collect

Collect the following evidence during the activity:

- scenario startup output;
- selected access-point mode;
- dashboard during normal operation;
- normal MQTT telemetry;
- one normal network capture observation;
- the attack or disruption command or helper used;
- dashboard behaviour during the disruption;
- abnormal, stale, or missing MQTT telemetry;
- relevant wireless, sensor, or scenario logs;
- evidence showing whether normal operation resumed or manual recovery was required;
- the completed security-to-safety chain; and
- the completed hazard analysis.

Evidence references should identify the relevant application, command, timestamp, packet number or time range, topic, interface, filename, or reading clearly.

Do not submit screenshots without explaining what each screenshot demonstrates.

12 Reflection Questions

Answer the following questions in your activity document:

1. Why can falsified environmental data be more dangerous than visibly unavailable data?
2. How can an attack on the wireless access point affect several safety-relevant sensor streams simultaneously?
3. Which component acts as the main trust boundary in this scenario?
4. Why is MQTT broker authentication alone insufficient to guarantee trustworthy building data?
5. How could replayed occupancy or air-quality data create a safety hazard?
6. What should the dashboard do when one or more sensor streams become unavailable?
7. What should the system do when it receives physically implausible or inconsistent readings?
8. Which controls primarily improve security, and which primarily reduce the safety impact?
9. What evidence would be required to demonstrate that the proposed controls are effective?

13 Stopping the Scenario

Stop the Smart Building scenario using the provided cleanup command:

```
python3 launch_sisen.py --stop
```

Confirm that:

- the simulated sensor processes have stopped;
- the wireless access-point processes have stopped;
- the dashboard has stopped;
- temporary namespaces and interfaces have been removed;
- no stale MQTT publishers remain; and
- the environment is ready for another scenario run.

14 Summary

This activity demonstrated how a smart building monitoring system depends on the integrity, authenticity, and availability of its wireless infrastructure and environmental telemetry.

The technical security event was examined alongside its operational effect and possible consequence for occupant safety. The activity also demonstrated that protecting the MQTT channel alone is not sufficient. A safety-relevant building system must detect implausible, stale, missing, or unauthorised telemetry, recognise loss of wireless connectivity, and respond in a fail-safe manner.