SISEN: 6LoWPAN

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 6LoWPAN environment in which constrained wireless devices exchange telemetry through a low-power IPv6 network.

Simulated 6LoWPAN IoT devices generate telemetry and send it across an IEEE 802.15.4 low-power wireless network. 6LoWPAN provides IPv6 adaptation for this constrained link. A 6LoWPAN border router connects the constrained network to the wider IPv6 environment, while an application gateway or MQTT relay receives the UDP telemetry, translates or republishes it where required, and forwards it to the MQTT broker and monitoring dashboard.

The scenario demonstrates how a security failure affecting constrained wireless communication, routing, the border router, or telemetry can develop into a safety-relevant system condition.

Learning Outcomes

By completing this activity, you should be able to:

- explain how constrained IoT systems depend on trustworthy and timely wireless communication;
- describe the data flow between 6LoWPAN IoT devices, the IEEE 802.15.4 network, 6LoWPAN adaptation layer, border router, application gateway or MQTT relay, MQTT broker, and dashboard;
- observe normal IPv6, UDP, and MQTT telemetry;
- identify how spoofed, replayed, extreme, missing, or disrupted telemetry affects system behaviour;
- explain the role of the 6LoWPAN border router as a trust and availability boundary;
- 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 constrained wireless sensing system.

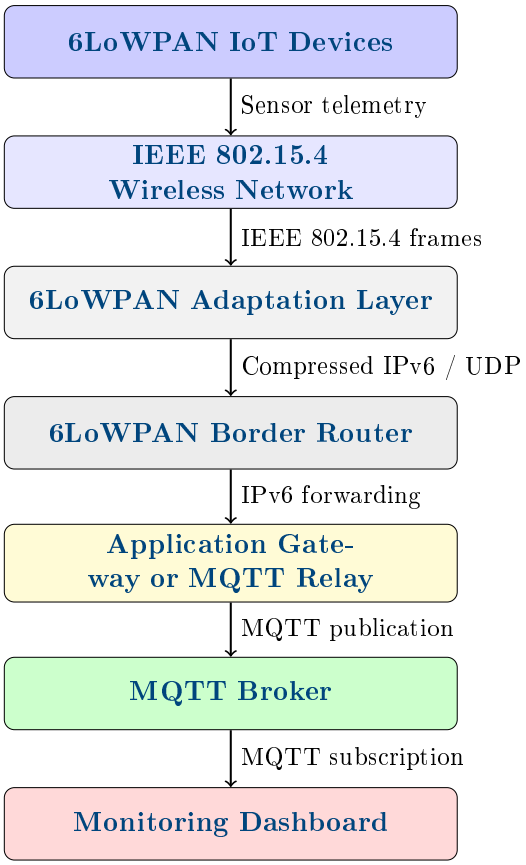
Simulated 6LoWPAN IoT devices produce telemetry and transmit it using UDP over IPv6. IEEE 802.15.4 provides the low-power wireless link, while 6LoWPAN adapts IPv6 packets for constrained communication. A 6LoWPAN border router connects this network to the wider IPv6 environment. An application gateway or MQTT relay receives the forwarded UDP telemetry, interprets or translates it where required, and republishes it through MQTT to the SISEN dashboard.

The system assumes that received telemetry is trustworthy and sufficiently current. It does not independently guarantee that messages are authentic, fresh, complete, or within expected operational limits.

- System focus: simulated constrained wireless monitoring
- Communication path: 6LoWPAN IoT devices to IEEE 802.15.4 network to 6LoWPAN adaptation layer to border router to application gateway or MQTT relay to MQTT broker to dashboard
- Core services: simulated IoT devices, 6LoWPAN network, border router, application gateway or MQTT relay, MQTT broker, and dashboard
- Primary protocols: IEEE 802.15.4, 6LoWPAN, IPv6, UDP, and MQTT
- Safety relevance: incorrect, delayed, or unavailable telemetry may result in an unsafe operational decision or delayed response

Scenario Architecture

Shown here is the simplified system architecture. The IoT devices generate telemetry. IEEE 802.15.4 provides the low-power wireless link, while 6LoWPAN adapts IPv6 packets for constrained communication. The border router connects the constrained network to the wider IPv6 environment. The application gateway or MQTT relay receives the UDP telemetry and republishes it through MQTT. The broker then distributes the data to the dashboard.



Main Components

6LoWPAN IoT Devices

The simulated IoT devices represent constrained sensors or actuators. They generate telemetry for the scenario and transmit it using UDP over IPv6.

Depending on the final scenario configuration, the telemetry may represent:

- environmental conditions;
- equipment state;
- process measurements;
- alarm status; or
- another safety-relevant sensor value.

The readings vary over time to represent normal operation.

6LoWPAN Border Router

The border router connects the constrained IEEE 802.15.4 and 6LoWPAN network to the wider IPv6 environment.

It forwards traffic between the low-power network and the receiving service. Because multiple devices may depend on it, the border router is both a trust boundary and a potential single point of failure.

Application Gateway or MQTT Relay

The application gateway receives the UDP telemetry forwarded through the border router.

It interprets, transforms, or republishes the received data through MQTT so that conventional applications and the dashboard can consume it. This is distinct from the border router: the border router connects and forwards between networks, while the application gateway operates on the application data.

The gateway may not independently verify message authenticity, freshness, source identity, or operational plausibility.

MQTT Broker

The MQTT broker receives relayed telemetry and distributes it to subscribed services.

The 6LoWPAN telemetry is published under the following MQTT namespace:

```
industrial/6lowpan/#
```

Monitoring Dashboard

The dashboard displays the latest telemetry and system state.

During normal operation, it should show:

- continuously updating sensor values;
- the identity of the source node where supported;
- current status or alarm information; and
- no persistent missing-data or communication warning.

The dashboard trusts the data received through the relay and MQTT path unless additional validation is implemented.

Safety Context

Constrained wireless networks are often used where low-power devices monitor physical conditions, equipment, or processes.

If an unsafe condition develops, accurate and timely telemetry may allow an operator or automated system to recognise the change and respond. If data is false, delayed, replayed, extreme, or unavailable, the displayed state may no longer reflect the physical condition being monitored.

Examples of possible consequences include:

- an unsafe condition being reported as normal;
- a safe condition being reported as hazardous;
- old telemetry being presented as current;
- extreme values causing an inappropriate response;
- several sensor streams becoming unavailable because the border router fails; and
- operators losing confidence in the monitoring system.

The security and resilience of the constrained network, border router, relay, and telemetry path are therefore directly connected to system safety.

1 Start the 6LoWPAN Scenario

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

1.1 Number of Simulated Nodes

The direct launch example creates four simulated industrial assets. The `-nodes` option accepts a value from 1 to 10.

With four active nodes, the scenario represents the Boiler Room, Process Line, Cold Storage, and Loading Bay. Each asset publishes node-specific telemetry, and fields are not forced onto assets that do not support them.

Use the number of nodes specified by the instructor.

1.2 Start the Scenario

From the project root directory, run:

```
python3 launch_sisen.py --scenario 6lowpan --ap-mode open --nodes 4 --capture-
    hints
```

2 Observe Normal Operation

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

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

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

- the 6LoWPAN sensor nodes running;
- the border router forwarding traffic;
- continuously updating telemetry;
- values changing within an expected range;

- the application gateway or MQTT relay processing UDP messages;
- MQTT updates where the relay is enabled; and
- no persistent missing-data or communication warning.

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

- the normal range of values displayed;
- the number of active sensor nodes;
- the apparent update frequency; and
- the normal status of the border router and application gateway or MQTT relay.

3 Inspect 6LoWPAN and UDP Communication

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

Capture the traffic on the interface specified for the 6LoWPAN scenario:

```
sudo ip netns exec node1 sudo ip netns exec node1 tcpdump -i lowpan0 -n -vv -s
    0 -Z "$USER" -w captures/6lowpan-node1-lowpan.pcap
```

Use Wireshark to inspect the IPv6 and UDP traffic. Apply the relevant display filters:

```
ipv6
udp
```

Observe the traffic generated during normal operation. Identify:

- the source and destination IPv6 addresses;
- the UDP source and destination ports;
- the sensor node associated with each message;
- the message payload;
- the frequency of transmission;
- whether sequence numbers or timestamps are included; and
- whether the payload is visible in plaintext.

Record in your activity document:

- one example UDP telemetry message;
- the source and destination addresses and ports;
- the associated payload; and
- what information an unauthorised observer could learn from the captured traffic.

4 Optional: Inspect MQTT Telemetry

This step applies where the application gateway or MQTT relay republishes received 6LoWPAN telemetry through MQTT.

Open a second terminal and subscribe to the final 6LoWPAN MQTT namespace:

```
mosquitto_sub -h localhost -p 1883 -t 'industrial/6lowpan/#' -v
```

Observe the messages for at least one minute. Identify:

- the MQTT topics used;
- the node represented by each topic;
- the values contained in each message;
- whether the MQTT output matches the UDP telemetry;
- the frequency of publication; and
- whether timestamps are included.

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

- the MQTT topics observed;
- one reading shown in the UDP message, MQTT output, and dashboard; and
- whether any transformation or delay is visible between the communication stages.

5 Perform a Bounded Attack or Disruption

This activity demonstrates how attacks or disruptions at different layers of the system can influence the monitoring process and create a safety-relevant effect. 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, IEEE 802.15.4 link, 6LoWPAN network, border router, or gateway.
- **Communication or Protocol Attack** A communication or protocol attack affects the exchange, forwarding, or delivery of data, such as IPv6, UDP, MQTT, routing, replay, or message injection.
- **Telemetry or Application-Layer Attack**: A telemetry or application-layer attack affects the values, timing, freshness, authenticity, or availability of the data presented to the monitoring system.

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 6lowpan`. 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 6LoWPAN scenario is running;
- the sensor nodes are transmitting;
- the border router is active;
- the application gateway or MQTT relay is processing telemetry;

- the dashboard is displaying normal telemetry;
- normal communication has been observed; and
- any required packet capture is already running.

Record the most recent normal telemetry and communication state 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. General 6LoWPAN helper attacks use the `protocol` category and inject through the active lab namespace path without rebuilding the topology.

General attacks select one eligible industrial asset at the start of the run and keep that target fixed for the full bounded window. Repeated runs use a shuffled per-attack rotation so that eligible nodes are used before reshuffling. The selected payload remains node-specific.

The selected activity may demonstrate spoofed telemetry, replayed telemetry, extreme values, missing fields, or a scenario-focused safety case such as masked boiler pressure, hidden emergency-stop state, or hidden machine-overheat state.

While it is active, do not restart the scenario or generate additional traffic unless instructed.

6 Observe the System Effect

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

- the monitoring dashboard;
- the UDP and IPv6 traffic;
- the MQTT telemetry where enabled;
- the border-router output;
- the sensor-node output;
- the application gateway or MQTT relay; and
- the packet capture.

Determine:

- which component first showed evidence of the disruption;
- whether the dashboard displayed false, stale, extreme, missing, or inconsistent data;
- whether the border router forwarded, dropped, or altered the affected traffic;
- whether the application gateway or MQTT relay detected or rejected the abnormal telemetry;
- whether one node or several nodes were affected;
- whether the displayed 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 forwarding resume automatically. Record in your activity document:

- whether the system recovered automatically;
- how long recovery took;
- whether all affected nodes resumed communication;
- whether the border router required manual recovery; and
- whether any stale or abnormal data remained visible.

8 Distinguish the Security Event from the Hazard

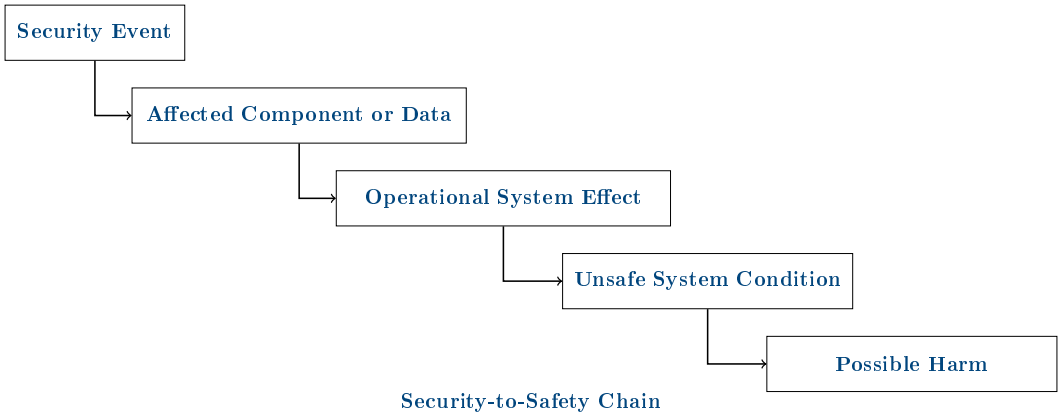
A security event and a safety hazard are not the same.

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 physical, operational, environmental, or human harm.

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

- What security event occurred?
- Which node, route, component, connection, or data item was affected?
- What immediate operational effect followed?
- What unsafe system condition could result?
- What 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, route, or function;
- the loss of confidentiality, integrity, availability, authenticity, or accountability;
- the immediate system effect;
- the safety-relevant hazard;
- the possible physical, operational, environmental, or human consequence;
- existing controls;
- proposed mitigations; and
- remaining residual risk.

Use the following questions to guide your analysis:

- What evidence confirms that the constrained network or telemetry was disrupted or falsified?
- Was integrity, availability, authenticity, freshness, or more than one property affected?
- Did the dashboard fail visibly or continue to present misleading information?
- Did the event affect one node, one route, or the wider constrained network?
- Did the border router increase the scope of the failure?
- Who or what would rely on the affected information?
- What incorrect operational decision might be made?
- What unsafe condition could result?
- 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:

- IEEE 802.15.4 link-layer security;
- device authentication;
- secure key management;
- source-address validation;
- authenticated application messages;
- replay protection;
- sequence numbers and freshness checks;
- payload validation;
- operational plausibility checking;
- rate limiting;
- missing-data detection;
- route and neighbour monitoring;
- border-router health monitoring;
- redundant border routers or communication paths;
- local fail-safe behaviour;
- MQTT authentication and access control;
- encrypted communication where appropriate;
- 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;
- active 6LoWPAN nodes and interfaces;
- border-router status;
- dashboard during normal operation;
- one normal UDP or IPv6 capture observation;
- normal MQTT telemetry where enabled;
- the attack or disruption command or helper used;
- dashboard behaviour during the disruption;
- abnormal, replayed, extreme, stale, or missing telemetry;
- relevant device, IEEE 802.15.4, adaptation-layer, border-router, gateway, 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, address, port, interface, topic, 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 telemetry be more dangerous than visibly unavailable telemetry?
2. Why is the border router a significant trust and availability boundary?
3. How could a failure affecting the border router influence several sensor nodes at once?
4. Why are source addresses alone insufficient to prove the authenticity of a UDP message?
5. How could replayed telemetry create a safety-relevant hazard?
6. What should the receiving service do when telemetry becomes unavailable or stale?
7. What should the system do when it receives extreme or operationally impossible values?
8. Which controls are best implemented on the IoT device, 6LoWPAN layer, border router, application gateway, and dashboard?
9. Which controls primarily improve security, and which primarily reduce the safety impact?
10. What evidence would be required to demonstrate that the proposed controls are effective?

13 Stopping the Scenario

Stop the 6LoWPAN scenario using the provided cleanup command:

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

Confirm that:

- the simulated sensor nodes have stopped;
- the border-router process has stopped;
- the application gateway or MQTT relay has stopped;
- the dashboard has stopped;
- temporary interfaces and namespaces have been removed;
- no stale MQTT publishers remain; and
- the environment is ready for another scenario run.

14 Summary

This activity demonstrated how a constrained wireless monitoring system depends on the integrity, authenticity, freshness, and availability of its 6LoWPAN communication path and telemetry.

The technical security event was examined alongside its operational effect and possible safety consequence. The activity also demonstrated that protecting only the final MQTT stage is not sufficient. A safety-relevant constrained IoT system must detect abnormal, replayed, stale, missing, or unauthorised telemetry, monitor the health of the border router and communication path, and respond in a fail-safe manner.