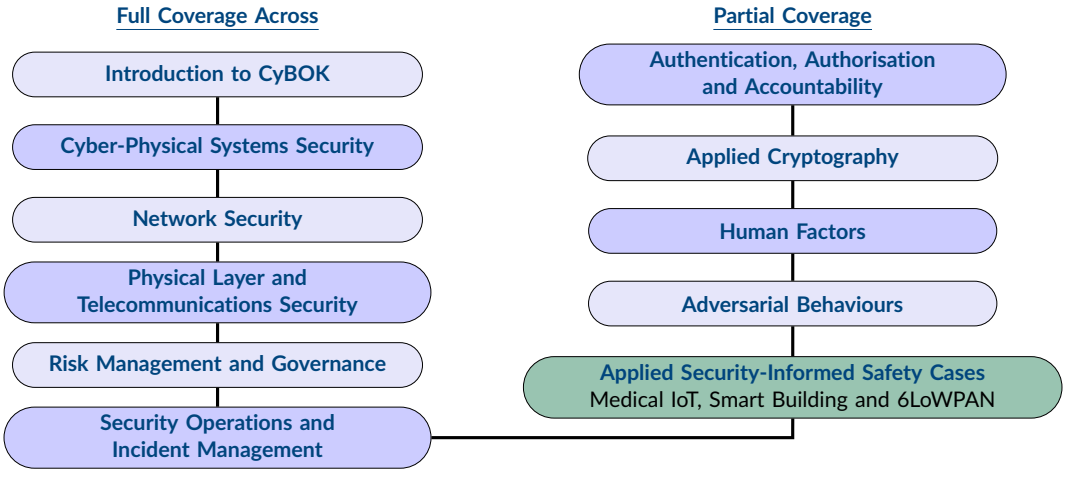
Applied Security-Informed Safety Case Studies

Dr Ayman El Hajjar

Security-Informed Safety Course summary



Outline

Applying Security-Informed Safety

From Concepts to Applied Cases

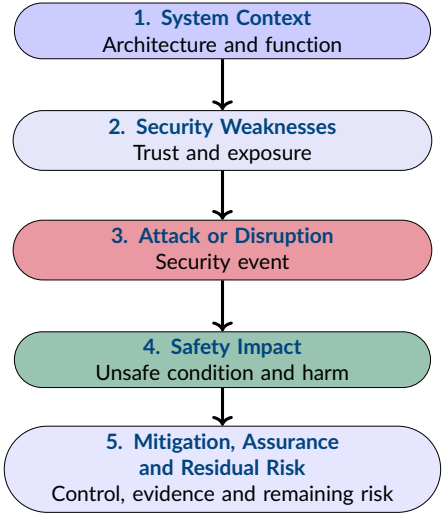
Applied Security-Informed Safety

Uses **security analysis**, **hazard reasoning**, and **safety consequences** together to examine how attacks and disruptions affect real system behaviour.

- Previous lectures introduced security failures, hazards, assurance, wireless threats, safety-critical IoT, and resilience.
- Applied cases bring these concepts together within a **complete system context**.
- The focus is not only on whether an attack succeeds.
- The analysis traces how a security event changes **data**, **communication**, **system behaviour**, and possible **safety outcomes**.

The same security event can have very different safety consequences depending on the system in which it occurs.

A Common Case Study Analysis Method



- Each case uses the **same analysis sequence**.
- This supports comparison across technologies and operational environments.
- The objective is to identify how security weaknesses create or amplify **safety-relevant behaviour**, while distinguishing direct observation, inference and assumptions.

A case study should connect technical evidence to operational effects, unsafe conditions and appropriate controls.

Three Categories of Attack and Disruption

Infrastructure Attacks and Disruptions
Affect supporting components, services, gateways, access points, brokers, or network availability.

Communication and Protocol Attacks
Exploit wireless links, protocol behaviour, message exchange, association, pairing, or transport mechanisms.

Telemetry and Application-Layer Attacks
Manipulate sensor values, application messages, commands, state, or the interpretation of system data.

- An attack may fall into **more than one category**.
- The category identifies where the security event occurs, not the final safety consequence.
- Safety analysis must trace how the event affects **system behaviour**.

The same safety hazard may be reached through attacks at different layers of the system.

Medical IoT Case Study

Medical IoT

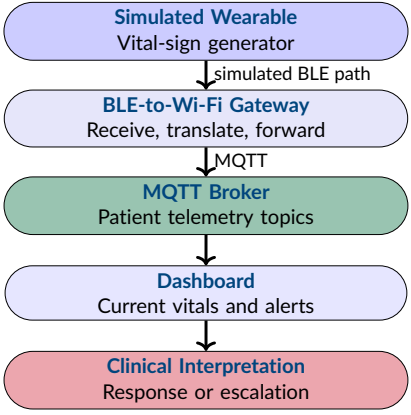
SISEN Scenario Context

The **Medical IoT scenario** simulates a wearable patient monitoring system in which generated vital-sign data is forwarded through a **BLE-to-Wi-Fi gateway**, published over MQTT and displayed on a monitoring dashboard.

- The scenario represents **heart rate**, **SpO_2** and **blood pressure** telemetry.
- The current SISEN implementation simulates the BLE communication path rather than capturing over-the-air Bluetooth traffic.
- The gateway log, MQTT packets and dashboard state provide the main sources of evidence.
- Safety relevance comes from whether the displayed patient state remains **authentic**, **current**, **complete** and **clinically plausible**.

A patient may be physically deteriorating while the monitoring system continues to present a stable or incomplete clinical picture.

Medical IoT System Architecture



- The gateway is the key **translation point** between wearable telemetry and IP-based monitoring.
- MQTT topics such as patient vital-sign streams expose structure, identifiers and values.
- The dashboard represents the patient through received telemetry rather than direct observation.
- Evidence comes from **gateway logs**, **MQTT captures**, subscriptions and dashboard changes.

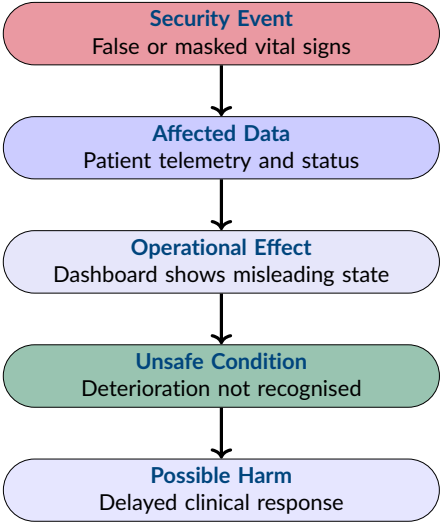
The dashboard may be technically consistent with the received data while still being clinically misleading.

Medical IoT Activities Implemented in SISEN

- **Gateway log observation** shows whether wearable telemetry reaches the BLE-to-Wi-Fi gateway and is forwarded.
- **MQTT topic observation** exposes the topic hierarchy, payload structure and reporting frequency.
- **Telemetry spoofing** and **extreme telemetry** test whether correctly formatted but false or implausible vitals are accepted.
- **Malformed telemetry** tests how the receiving path handles incomplete or invalid payloads.
- **Replay** tests whether previously valid patient telemetry can be presented as though it were current.
- **Scenario-focused safety cases** include critical vitals, suppressed fall or panic alerts, and falsely normal battery state.

The implemented activities focus on how patient telemetry can become false, stale, malformed, inconsistent or difficult to trust.

Medical IoT Security-to-Safety Escalation



- The activity does not directly harm the patient.
- Harm becomes possible because untrusted telemetry changes the **clinical representation**.
- The evidence chain links packet contents, gateway logs, dashboard state and hazard analysis notes.

The escalation point is reached when untrusted data is allowed to influence a safety-relevant clinical interpretation.

Smart Building Case Study

Smart Building Automation

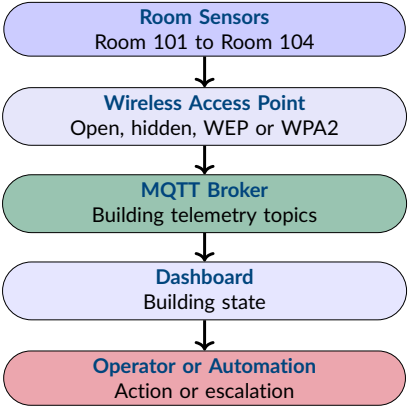
SISEN Scenario Context

The **Smart Building scenario** uses wireless zone sensors, an access point, MQTT telemetry and a dashboard to monitor environmental and occupancy state.

- The launcher supports open, hidden, WEP and WPA2 modes, together with a Smart Building MAC-filtering example activity.
- Sensor telemetry may include environmental state such as temperature, humidity, CO_2 or occupancy indicators.
- Students observe normal telemetry, capture traffic, trigger bounded activities and analyse safety relevance.
- The key safety question is whether building state remains **accurate**, **timely** and **available** for monitoring or automation.

Automation may respond correctly to the displayed data while still being unsafe if the displayed building state is false or incomplete.

Smart Building System Architecture



- The access point is both a communication dependency and a security boundary.
- MQTT exposes the application-level representation of each room or zone.
- A loss affecting one room is different from a sensor-layer blackout affecting all rooms.
- Wireless evidence and MQTT evidence help locate the affected layer.

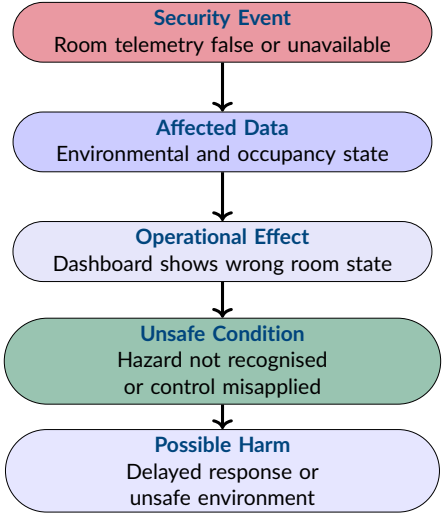
A building may appear operational while one room, one wireless mode, or the complete sensor layer is no longer trustworthy.

Smart Building Activities Implemented in SISEN

- **Wireless and MQTT observation** establish the normal traffic pattern and exposed metadata.
- **Telemetry spoofing**, **extreme values**, **replay** and **telemetry noise** test source trust, integrity, freshness and availability.
- **Single-client disconnection** interrupts one room while other rooms continue reporting.
- **Sensor blackout** interrupts all active room sensors while scenario infrastructure remains running.
- Separate **AP activities** include hidden SSID observation, MAC spoofing, WEP IV collection, WPA2 handshake capture and bounded deauthentication.

The same dashboard symptom may result from application-layer injection, wireless disruption or infrastructure-level failure.

Smart Building Security-to-Safety Escalation



- A single-client loss creates a local blind spot.
- A sensor blackout creates a wider loss of environmental visibility.
- Spoofed or extreme telemetry may create false reassurance or inappropriate response.

The safety question is whether the building system knows when its view of the environment can no longer be trusted.

6LoWPAN Case Study

6LoWPAN Monitoring

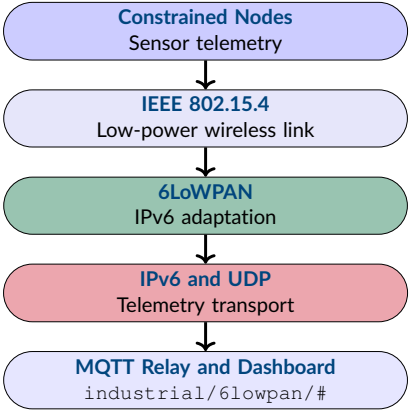
SISEN Scenario Context

The **6LoWPAN scenario** uses constrained wireless nodes, IEEE 802.15.4, 6LoWPAN adaptation, IPv6 and UDP telemetry, with relay into MQTT.

- Constrained nodes represent low-power sensing devices with limited communication and processing resources.
- IEEE 802.15.4 and 6LoWPAN provide the low-power network path.
- Students can capture both **wpan** and **lowpan** views of the same communication path.
- Safety depends on telemetry being current, complete and correctly interpreted despite constrained networking.

A constrained sensor network can fail silently from the perspective of a conventional dashboard unless missing or stale telemetry is detected.

6LoWPAN System Architecture



- The same telemetry can be inspected at the 802.15.4, 6LoWPAN, IPv6/UDP and MQTT-facing stages.
- UDP telemetry provides low overhead but requires separate thinking about identity, integrity and freshness.
- The MQTT relay makes constrained telemetry visible to conventional monitoring tools.
- Layered capture helps identify where loss, delay or manipulation begins.

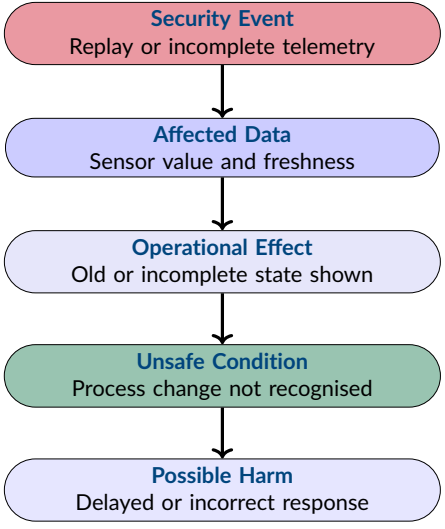
Trust in the dashboard depends on every adaptation and forwarding stage between the constrained node and the monitoring view.

6LoWPAN Activities Implemented in SISEN

- **Wireless and protocol capture** records IEEE 802.15.4 and 6LoWPAN traffic using `wpan1` and `lowpan0` views.
- **MQTT topic observation** shows the relayed constrained telemetry under `industrial/6lowpan/#`.
- General **protocol-path attacks** include spoofed, extreme, replayed, malformed and incomplete telemetry injected through the active namespace path.
- **Replay and freshness** demonstrate how an old but plausible value may be treated as current.
- **Missing-field activity** shows that a packet may be delivered successfully while the application payload remains incomplete.
- **Scenario-focused safety cases** include masked boiler pressure, hidden emergency-stop state and hidden machine-overheat state.

In constrained systems, replay, incomplete payloads and delayed recognition may be as important as obvious packet-level failure.

6LoWPAN Security-to-Safety Escalation



- The repeated message may be syntactically valid and even plausible.
- The safety problem is that it no longer represents the current physical or operational condition.
- Incomplete telemetry may omit a field required to establish the current safety-relevant state.

Freshness is a security property and a safety dependency in time-sensitive constrained monitoring.

Comparing the Applied Cases

Comparing the Three SISEN Scenarios

Scenario	Main Evidence	Security Failure	Safety-Relevant Effect
Medical IoT	Gateway log, MQTT capture, dashboard	False, malformed, noisy or masked vitals	Incorrect clinical representation
Smart Building	Wireless capture, MQTT capture, dashboard	Spoofing, client loss, blackout or wireless infrastructure weakness	Incorrect or incomplete building state
6LoWPAN	wpan, lowpan, UDP and MQTT evidence	Replay, missing telemetry, spoofing or extreme values	Loss of timely operational awareness

The scenarios differ technically, but all require evidence-based reasoning from security event to system behaviour and safety consequence.

Common Mitigation and Resilience Priorities

- Establish the **identity and authority** of devices, gateways, publishers, and relays before accepting telemetry.
- Protect **integrity and freshness** using authenticated communication, sequence information, timestamps, expiry checks, and replay detection.
- Validate telemetry using **physical ranges**, **rates of change**, and consistency between related measurements.
- Detect **missing**, **stale**, **duplicated**, **malformed**, and conflicting data rather than continuing to display it as current.
- Use evidence from multiple layers to distinguish failures affecting the wireless link, protocol path, gateway, broker, or dashboard.
- Enter a visible **degraded or fail-safe state** when the current physical or operational condition cannot be established confidently.

A resilient system must recognise when its evidence is no longer trustworthy enough to support safe decisions.

SISEN Resources for the Applied Cases

The three cases are supported by the practical guidance and reporting resources provided with SISEN.

- **SISEN Repository**: scenario implementation, attack and disruption activities, technical documentation, and teaching materials.
- **SISEN Student Guide**: installation, scenario operation, evidence collection, stopping, and recovery guidance.
- **SISEN Hazard Analysis and Evidence Sheet**: structured recording of the security event, system effect, unsafe condition, mitigation, assurance evidence, and residual risk.

The slides introduce the applied reasoning; the repository guidance provides the complete practical workflow and evidence requirements.