Section 1: Executive Summary

This threat assessment model covers the Hydroficient HYDROLOGIC water flow management system as deployed at The Grand Marina, a 500-room luxury hotel. The deployment consists of three field devices (Main Building, Pool/Spa, and Kitchen/Laundry), a cloud-based monitoring and control backend, a web dashboard used by hotel staff, and emergency shutoff capability that can actuate valves in each of the three areas.

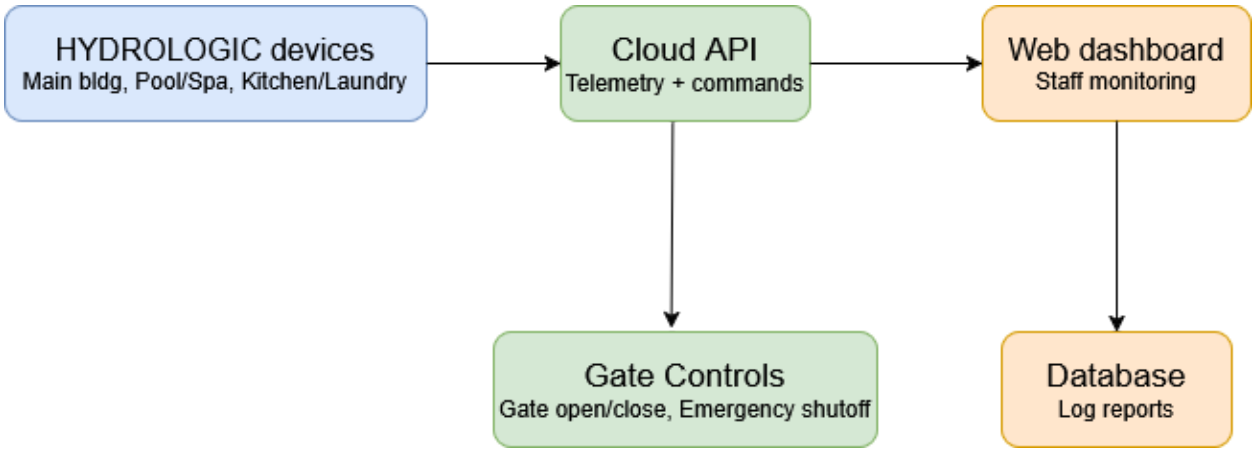
This assessment was commissioned following a $4.2M water damage incident in which a leak alert was generated but not followed up on. The reported root cause of that incident was operational because an alert was received and was taken care of in time, rather than a confirmed cyberattack. However, the incident is directly relevant to this threat model for two reasons: it demonstrates that the physical and financial consequences of a failure anywhere in the sensor-to-action chain are severe, and every stage of that chain; sensing, transmission, cloud processing, alert generation, alert delivery, and human response, is also a stage that a malicious actor could target, deliberately or opportunistically, to produce the same outcome or worse.

The highest-priority findings in this assessment are:

- Alert-path integrity and delivery assurance is the single most consequential control gap. If an attacker (or a system fault) can suppress, delay, or desensitize staff to alerts, the result mirrors the $4.2M incident — this time potentially triggerable on demand.
- Remote shutoff is a high-value target. Unauthorized triggering of the emergency shutoff across a 500-room property is a significant business-disruption and a pathway to extortion; unauthorized prevention of a legitimate shutoff risks a flood.
- Dashboard account security (credential strength, MFA, per-user accounts, session handling) is the most likely initial access path into both of the above.

Section 2: System Overview

The Grand Marina is a 500-room luxury hotel and a Hydroficient customer. The property uses three HYDROLOGIC flow management devices, one on each major water service line: Main Building, Pool/Spa, and Kitchen/Laundry. Each device measures water flow in its area and can remotely close a shutoff valve for that area. The devices report continuously to Hydroficient's cloud backend, which runs the leak-detection logic, stores historical usage data, and generates alerts. Hotel operators and management access the system through a web dashboard, which displays live and historical flow data and allows staff to issue remote shutoff or gate-control commands and to acknowledge or reset alerts.



Each device sends flow telemetry up to the Cloud API, which evaluates it against leak-detection rules, stores it, and pushes alerts and dashboard updates. The dashboard is the primary interface operators use both to view that data and to issue commands — gate adjustments or emergency shutoff — back down through the Cloud API to the physical devices.

Section 3: Asset Inventory

List the key assets and their CIA priorities (use your work from Step 2):

Asset	Description	C Priority	I Priority	A Priority
HYDROLOGIC Devices	3 flow management units (Main building, Pool/Spa, Kitchen/Laundry)	Low	High	High
Web Dashboard	Operator monitoring interface	Medium	High	High
Cloud API	Device-to-cloud communication; carries commands between devices and the dashboard	Medium	Critical	High
Remote Controls	Gate adjustments, emergency shutoff actuation	Medium	Critical	Critical
Consumption Data	Savings reports, billing records	Low	Medium	Low

Section 4: STRIDE Analysis

This is the core of your threat model. For **each major component**, analyze all six STRIDE categories:

Component 1: HYDROLOGIC Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker connects a fake device to the network and impersonates one of the devices and submits fake readings to the cloud leaving a real leak in that area that can not be noticed	Low	High	Medium
Tampering	An intruder manually overrides a valve or disconnects a sensor leaving no alert generated and water running unmonitored	Medium	High	High
Repudiation	A valve reset or override performed through a local maintenance port on the device itself leaves no timestamped, individually-attributable record, so if a valve is later found in the wrong state during an investigation, no one can be held accountable.	Medium	Medium	Medium
Info Disclosure	The device exposes a local configuration or debug interface, common on unmanaged IoT hardware, that if reachable on the hotel network reveals the Wi-Fi credentials or the API key the device uses to authenticate to Hydroficient's cloud.	Low	Medium	Low
Denial of Service	An attacker on the same network segment floods the device or its access point with traffic, knocking it offline. Because the device fails silently, staff cannot distinguish “no leak detected” from “device is blind.”	Medium	High	High
Elevation of Privilege	A device running outdated firmware with a known vulnerability is compromised and used as a foothold to pivot onto the hotel's broader IoT or guest network if segmentation between them is weak.	Low	High	Medium

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker sends a staff member a phishing email disguised as a “Hydroficient account verification” notice, harvests their login credentials, and signs into the dashboard as that user.	Medium	High	High
Tampering	An attacker who has obtained dashboard access mutes alert notifications for a specific area or raises the leak-detection threshold, so a real leak never generates a visible alert.	Medium	Critical	Critical
Repudiation	Multiple staff share a single generic login detail and when an alert is dismissed or a detection setting is changed, there is no way to determine which individual took the action.	High	Medium	High
Info Disclosure	Dashboard session tokens are transmitted without adequate protection over an unsecured hotel Wi-Fi connection, letting an attacker on the same network capture a valid session and access the dashboard without a password.	Low	Medium	Low
Denial of Service	An attacker repeatedly submits failed logins against a known staff username, triggering an account-lockout policy and denying that staff member dashboard access during an active incident.	Low	High	Medium
Elevation of Privilege	A staff account intended to be view-only is still able to reach admin-level functions, such as issuing a shutoff command, because permissions are enforced only by hiding buttons in the interface rather than on the server.	Medium	High	High

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker who has extracted a device API key (for example, via the debug-port exposure noted for the field devices) uses it to authenticate directly to Hydroficient's cloud API as if they were a legitimate HYDROLOGIC unit, submitting falsified telemetry.	Low	High	Medium
Tampering	An Insecure Direct Object Reference in the API allows a request built for one device ID to be edited to reference a different area's, or a different customer's, device ID — letting the requester alter settings outside their intended scope.	Low	Critical	High
Repudiation	API requests that change device configuration or issue commands are processed without a persistent, centralized audit log, so after an incident there is no reliable way to reconstruct exactly what command was issued, by what credential, and when.	Medium	Medium	Medium
Info Disclosure	A misconfigured or overly-permissive API endpoint returns more data than intended in its response — for example, another property's usage data — exploitable simply by enumerating device or account IDs.	Low	High	Medium
Denial of Service	An attacker sends a high volume of requests against an unthrottled API endpoint, degrading processing of real alerts and dashboard responsiveness precisely when they are most needed.	Medium	High	High
Elevation of Privilege	A Hydroficient support or admin API credential is compromised (e.g., a phished support engineer), granting cross-customer	Low	Critical	High

	administrative access to the API well beyond a single hotel's device set.			

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker captures a previously-issued, legitimate shutoff command and replays it later. Because the command channel lacks message-level authentication or timestamps, the cloud accepts it as a new, valid instruction.	Low	Critical	High
Tampering	An attacker with dashboard or API access deliberately issues a full-building emergency shutoff during peak occupancy, either to cause disruption or to extort the business	Medium	Critical	Critical
Repudiation	A shutoff command executed directly through the API, rather than the dashboard UI, bypasses the dashboard's action log, making it unclear afterward whether the command was operator-initiated or automated.	Medium	Medium	Medium
Info Disclosure	Real-time gate/valve status is exposed through an API response without adequate access control, letting an attacker time an action for a window when an area is open and unmonitored.	Low	Medium	Low
Denial of Service	An attacker with access issues a shutoff and then immediately re-triggers it each time staff attempt to restore service, effectively locking staff out of restoring water to an area.	Low	High	Medium
Elevation of Privilege	A command intended to be scoped to a single area is instead executed against all three area because the shutoff endpoint does not strictly validate the area parameter, turning a targeted action into a property-wide outage.	Low	Critical	High

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

- Dashboard-enabled alert suppression (Web Dashboard – Tampering). An attacker with dashboard access can mute notifications or raise detection thresholds for an area, directly replaying the failure behind the $4.2M incident, except now it can be triggered on demand by the attacker.
- Unauthorized full-building emergency shutoff (Remote Controls – Tampering). An attacker with dashboard or API access can shut off water across the property during peak occupancy, causing severe guest disruption and creating a viable extortion threat.

High Risks:

- Physical tampering causing silent monitoring loss at a device (HYDROLOGIC Devices – Tampering).
- Device knocked offline with no distinct “offline” alert, indistinguishable from “no leak” (HYDROLOGIC Devices – Denial of Service).
- Dashboard account takeover via phishing (Web Dashboard – Spoofing).
- Shared/generic dashboard login preventing individual accountability (Web Dashboard – Repudiation).
- Missing server-side enforcement of role permissions on the dashboard (Web Dashboard – Elevation of Privilege).
- API object-reference flaw (IDOR) allowing cross-area or cross-customer tampering (Cloud API – Tampering).
- Unthrottled API endpoints allowing request flooding during an active incident (Cloud API – Denial of Service).
- Compromised Hydroficient support credential granting cross-customer access (Cloud API – Elevation of Privilege).
- Replayed or forged shutoff commands due to lack of message authentication (Remote Controls – Spoofing).
- Insufficient parameter validation letting a single-area command affect all areas (Remote Controls – Elevation of Privilege).

Medium Risks:

- Unattributed local valve resets/overrides at the device level (HYDROLOGIC Devices – Repudiation).
- Firmware vulnerability enabling network pivot from a compromised device (HYDROLOGIC Devices – Elevation of Privilege).
- Account-lockout abuse denying legitimate staff access mid-incident (Web Dashboard – Denial of Service).
- Missing centralized audit log for API-issued commands (Cloud API – Repudiation).
- API commands bypassing the dashboard's action log, obscuring attribution (Remote Controls – Repudiation).

- Repeated re-triggering of shutoff blocking service restoration (Remote Controls – Denial of Service).

Section 6: Recommended Mitigations

For each Critical and high-risk, propose a defense:

Risk	Proposed Mitigation	Implementation Complexity
Dashboard-enabled alert suppression	Require a second approval or automatic manager notification for any alert-rule change or mute action; log and alert on all rule changes in real time.	Medium
Unauthorized full-building shutoff	Require step-up confirmation for property-wide (multi-zone) shutoff commands, with a short delay and an override notice sent to a second contact before execution.	Medium
Physical device tampering	Add locked enclosures, tamper-evident seals, and tamper-alert wiring so physical interference itself generates an alert.	Low
Device offline indistinguishable from no-leak	Add heartbeat / dead-man monitoring that raises a distinct “device offline” alert, separate from a “no leak detected” state.	Low
Dashboard account takeover (phishing)	Enforce multi-factor authentication on all dashboard accounts.	Low
Shared/generic dashboard login	Migrate to unique per-user accounts with role-based permissions; deprovision immediately on staff turnover.	Low–Medium
Missing server-side role enforcement	Enforce authorization checks on the server for every dashboard action, not just by hiding controls in the interface.	Medium (vendor-dependent)

API IDOR / cross-zone tampering	Add server-side authorization checks on every API object reference, scoped strictly to the requesting property and zone.	Medium–High (vendor-dependent)
Unthrottled API endpoints	Implement rate limiting and anomaly detection on all API endpoints, particularly those handling commands.	Medium
Compromised vendor support credential	Require MFA and least-privilege scoping for all Hydroficient support/admin accounts; audit cross-customer access regularly.	Medium (vendor-dependent)
Replayed/forged shutoff commands	Add message signing, timestamps, and replay protection to the command channel between dashboard/API and devices.	High (protocol change, vendor-dependent)
Single-zone command affecting all zones	Add strict server-side parameter validation so commands can only execute against their intended, explicitly-scoped zone(s).	Low–Medium (vendor-dependent)