Section 1: Executive Summary

The Grand Marina relies on HYDROLOGIC devices to monitor and manage water flow across its 500-room luxury hotel. These three devices continuously measure flow and pressure, sending data to the cloud where it's processed and displayed on the operator dashboard. Gate controls and emergency shutoffs can respond automatically or manually based on system readings.

This threat model identifies security risks that could affect hotel operations, guest safety, and water infrastructure. IoT systems like HYDROLOGIC are increasingly targeted by attackers, and a disruption could cause water service outages, flooding, or operational delays. Understanding these risks helps prioritize protections before incidents occur.

Our analysis identified three critical concerns requiring immediate attention:

- Tampering with sensor data: Attackers could manipulate readings from the Hydrologic devices, causing false normal flow reports while real issues go unnoticed.
- Denial of service on the cloud or dashboard: If overwhelmed with false data or requests, operators could lose visibility and control of the water system.
- Unauthorized remote control access: Weak security could allow someone to operate gates or trigger emergency shutoffs without authorization, potentially disrupting water service.

We recommend prioritizing device authentication, secure network communications, and access controls for remote operations to keep the system reliable and protect hotel infrastructure and guests.

Section 2: System Overview

The Grand Marina's HYDROLOGIC system:

- 500-room luxury hotel (Hydroficient customer)
- 3 HYDROLOGIC flow management devices (one per water service line)
- Cloud-based monitoring and control
- Web dashboard for operators and management
- Remote shutoff and gate control capability

Data flow diagram:

```
None
[HYDROLOGIC Devices] → [Cloud API] → [Dashboard]
        ↓                    ↓
  [Gate Controls]      [Database]
  [Emergency Shutoff]  [Reports]
```

How It Works:

- HYDROLOGIC devices measure water flow and pressure in real time.
- Device data transmits via local network to the Cloud API.
- The Cloud API aggregates and processes sensor readings.
- Processed data is forwarded to the Web Dashboard for operator monitoring.
- Gate Controls receive commands from the Cloud API to adjust flow levels.
- Emergency Shutoff can be triggered by the Dashboard or automated thresholds in the Cloud API.
- Database stores historical data, while Reports summarize consumption, usage trends, and alerts.
- Operators use the Dashboard to monitor system health and take action when necessary.

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	Low	High	High
Web Dashboard	Operator monitoring interface	Medium	High	High
Cloud API	Device-to-cloud communication	Medium	High	High
Remote Controls	Gate adjustments, emergency shutoff	Medium	Critical	Critical
Consumption Data	Savings reports, billing records	Medium	Medium	Medium

Priority Rationale:

- **Integrity is High** for devices and cloud API— wrong readings could lead to incorrect treatment decisions
- **Availability is High** for dashboard and alerts — downtime during emergency could cost lives
- **Confidentiality is Medium** for consumption data— savings reports, billing records

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	Attacker introduces fake Hydrologic device to the broker for non-existent "~/device-01/flow /rate".	Medium	High	High
Tampering	Attacker changes hydrologic sensor data on the way to the broker device reporting a falsified normal reading report while the real device is reporting abnormal flow.	High	Critical	Critical
Repudiation	Hydrologic device an alert but provides no log of what device or when it happened.	Medium	Medium	Medium
Info Disclosure	Attacker eavesdropping on the data moving from sensor	High	High	Critical

	device to the broker device.			
Denial of Service	Attacker sends thousands of alerts to the broker device to where the broker device can't process the real messages.	Medium	Critical	Critical
Elevation of Privilege	Attacker gains access to the Hydrologic device network to hotel systems.	Low	Medium	Medium

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker uses stolen credentials or a weak password to log in as another user and view or modify device data	Medium	High	High
Tampering	Attacker injects JavaScript via a vulnerable dashboard input to modify displayed sensor readings for all users	Medium	High	High
Repudiation	Dashboard does not log user actions, so a user	Medium	Medium	Medium

	can deny sending a critical gate or shutoff command			
Info Disclosure	Dashboard traffic is unencrypted or uses weak TLS; attacker eavesdrops on sensor data and user credentials	High	High	Critical
Denial of Service	Attacker floods the dashboard with automated requests, preventing legitimate users from accessing device controls	Medium	Critical	Critical
Elevation of Privilege	Attacker modifies a client-side role parameter in requests to gain admin access due to missing server-side authorization checks	Low	Critical	High

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker captures a valid API token from a compromised client and uses it to send authenticated API requests	Medium	High	High

Tampering	Attacker intercepts API traffic and changes sensor thresholds before forwarding to the cloud	Medium	High	High
Repudiation	API does not log requests with user identity, allowing denial of malicious commands	Medium	Medium	Medium
Info Disclosure	API exposes sensitive endpoints without authentication, allowing attacker to enumerate devices and read sensor data	High	High	Critical
Denial of Service	Attacker sends many resource-intensive requests, causing the API to fail for legitimate users	Medium	Critical	Critical
Elevation of Privilege	Attacker exploits an insecure direct object reference by modifying device IDs to access unauthorized devices	Low	High	High

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker replays previously captured MQTT control messages to trigger gates or shutoffs without authorization	Medium	Critical	Critical
Tampering	Attacker intercepts and modifies remote control commands in transit to trigger unintended operations	Medium	Critical	Critical
Repudiation	Remote control actions are not logged; operators can deny issuing shutdown commands	Medium	High	High
Info Disclosure	Attacker eavesdrops on control traffic and learns operational schedules or emergency status	High	High	Critical
Denial of Service	Attacker floods the control channel with invalid commands, preventing legitimate commands from executing	Medium	Critical	Critical
Elevation of Privilege	Attacker exploits weak	Low	Critical	High

	authentication to gain persistent access and control of remote devices			

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. **Sensor data tampering (Tampering):** Attackers could alter Hydrologic device readings, making the system report normal flow while real issues occur. This could cause flooding, water waste, or delayed emergency response.
2. **Dashboard or Cloud DoS (Denial of Service):** Flooding the dashboard or cloud API with fake data or requests could prevent operators from seeing real-time system status, risking delayed responses to emergencies.
3. **Unauthorized remote control access (Elevation of Privilege / Spoofing):** Weak access controls could allow attackers to operate gates or trigger emergency shutoffs without authorization, potentially disrupting hotel water supply.

High Risks:

1. .**Device network pivot (Elevation of Privilege):** A compromised Hydrologic device could provide an entry point to other hotel systems.
2. **Database or report exposure (Info Disclosure):** Sensitive consumption data or historical reports could be accessed by unauthorized users if cloud storage is not secured.
3. **Dashboard tampering (Tampering):** Users with dashboard access could modify water control thresholds or settings, intentionally or accidentally affecting operations.
4. **Emergency shutoff spoofing (Spoofing):** Attackers could send fake commands to trigger unnecessary emergency shutoffs.

Medium Risks:

1. **Device spoofing on the network:** Fake devices could attempt to connect to the cloud API.
2. **Dashboard audit gaps (Repudiation):** Actions taken on the dashboard may not be fully logged, making it hard to track user activity.
3. **False data injection:** Fake sensor readings could be sent, causing minor system confusion or false alerts.

4. **Delayed report generation (DoS/Repudiation):** System may take longer to generate reports under load, affecting operational planning.

Section 6: Recommended Mitigations

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

Risk	Proposed Mitigation	Implementation Complexity
Sensor data tampering	Implement encrypted and signed communications between devices and cloud; add integrity checks	Medium — firmware and cloud configuration update
Dashboard or Cloud DoS	Add rate limiting, traffic monitoring, and anomaly detection on dashboard and cloud endpoints	Medium — cloud/network configuration
Unauthorized remote control access	Enforce strong authentication, multi-factor for remote control operations; restrict access by role	Low — configuration and policy update

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

Risk	Proposed Mitigation	Implementation Complexity
Device network pivot	Segment Hydrologic devices on a separate VLAN, isolated from other hotel systems	Low — configuration change
Database or report exposure	Apply access controls, encryption at rest, and re-authentication for report access	Medium — cloud configuration

Dashboard tampering	Require admin approval for threshold changes; add confirmation dialogs	Low — application update
Emergency shutoff spoofing	Implement command signing and authentication verification on all remote commands	Medium — device and cloud update