Section 1: Executive Summary

The Grand Marina hotel relies on Hydroficient's water system to manage, monitor and control the flow of water in the whole hotel. This water system consists 3 hydrologic devices each managing a specific part of the hotel: the main building, laundry/kitchen and spa/pool. These devices send water pressure readings of to the manager's dashboard. They also raise alerts when leaks are detected.

This threat model identifies security risks that could affect customers' access to water, data privacy, and the hotel operations. This threat model also aims at preventing leaks from going undetected as well as avoiding floods as has been the case in the hotel 8 months ago, thereby preserving the hotel's reputation.

Our analysis identified three critical concerns requiring immediate attention:

- Weak authentication on the manager's dashboard could allow unauthorized access to sensor readings and logs, thereby divulgating the functioning of the system to unauthorized people. This would also give access to alert settings and important commands such as the emergency shutoff command.

- Unencrypted device communications could be intercepted and modified or dropped down, resulting in missed alerts and could cause floods because leaks went undetected.

- Improper configuration of cloud settings may allow huge amounts of trash request to render the cloud processing unusable, thereby affecting the display of data on the manager's dashboard.

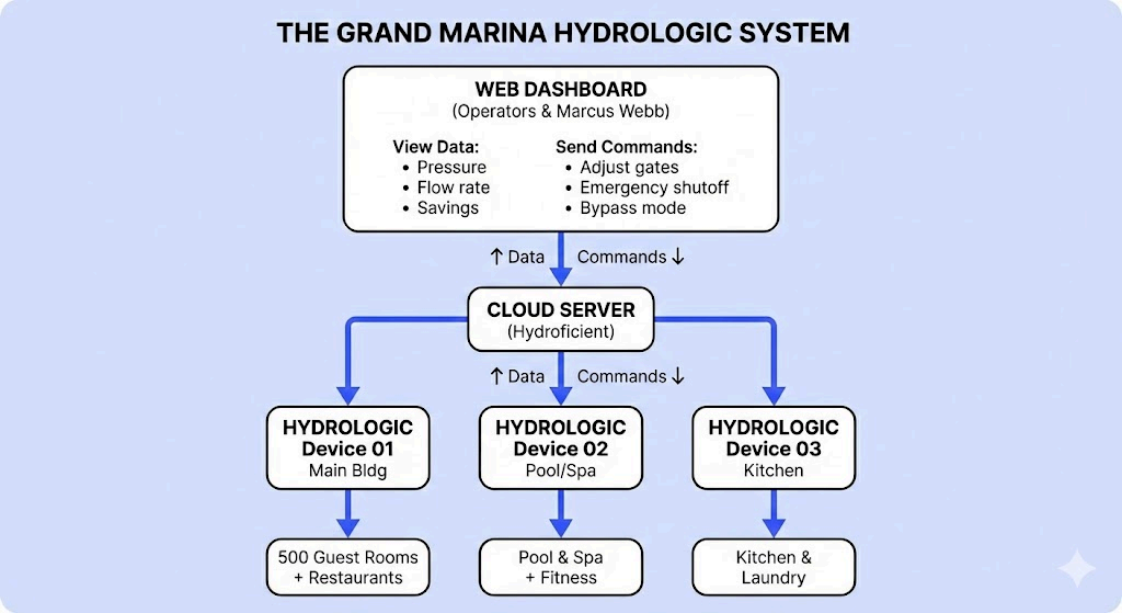
We recommend prioritizing multi-factor authentication, encrypted communication, and proper cloud configuration.

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



How it Works:

1. Hydroficient devices measur and send ~5-10 readings per second¬¬¬¬¬¬ (water pressure, flow, gate positions)
2. Data transits via hotels WiFi to the broker.
3. The broker forwards the data to Hydroficient's cloud server
4. The cloud server processes the data, checks thresholds, triggers alerts
5. The dashboard displays real time data about each hydrologic device readings to the manager.
6. The manager can decide to take action depending on what his dashboard displays. For example push a command to rotate a valve to a certain degree or use the emergency shutoff command in case the situation is critical.
7. These commands trace a backward path from the dashboard back to the devices (actuator)

Section 3: Asset Inventory

Asset	Description	C Priority	I Priority	A Priority

HYDROLOGIC Devices	3 flow management units	low	high	high
Web Dashboard	Operator monitoring interface	high	medium	critical
Cloud API	Device-to-cloud communication	medium	high	critical
Remote Controls	Gate adjustments, emergency shutoff	low	high	high
Consumption Data	Savings reports, billing records	high	high	medium

Section 4: STRIDE Analysis

Component 1: HYDROLOGIC Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker introduces fake device on the network pretending to be device 1 and sending false readings	low	high	medium
Tampering	Attacker with physical access modifies device firmware to report normal readings regardless of actual pressure readings	low	high	medium
Repudiation	Device sends alert but logs do not show which device sent the alert	Medium	Medium	Medium
Info Disclosure	Unencrypted readings in transit get intercepted and the attacker learns water usage patterns in hotels	high	high	critical
Denial of Service	Attacker jams WiFi network with wireless signals rendering devices incapable of transmitting through WiFi	medium	Critical	critical
Elevation of	Attacker exploits device vulnerability to	low	critical	critical

Privilege	gain access to hotel's WiFi and gain administrative rights to control the network.			

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker uses stolen credentials (from phishing email) to access manager dashboard	high	critical	critical
Tampering	Attacker with dashboard access modifies savings data and logs	medium	high	high
Repudiation	Technical staff claims didn't receive alerts	Medium	Medium	Medium
Info Disclosure	Attacker gains dashboard access, collects data from the whole hotel	low	high	medium
Denial of Service	Attacker floods dashboard with requests during leakages, manager can't detect there is a leakage	Medium	medium	medium
Elevation of Privilege	Attacker gets access to simple technical staff account and exploits bug to gain admin rights	low	critical	high

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker impersonates Hydroficient's cloud endpoint. Hotel sends all data to attacker's website	Medium	high	high
Tampering	Attacker with cloud server access	medium	high	high

	modifies database records			
Repudiation	Cloud server applies a configuration change or processes a command with no per-request logging of the source account, so if a valve setting is altered there is no way to prove which admin or automated process issued it.	Low	Medium	Medium
Info Disclosure	Cloud database breach exposes hydroficient devices' data and savings	medium	medium	medium
Denial of Service	DDoS attack on hydroficient's cloud server takes down monitoring and processing of data for all hydrologic devices	medium	critical	critical
Elevation of Privilege	Attacker exploits an insecure or leaked cloud API key to escalate from read-only device access to full administrative control	medium	high	critical

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker sends fake shutoff command. Cutting hotel residents from access to water	medium	high	high
Tampering	Attacker intercepts and modifies a gate amount to rotate to a certain degree	medium	medium	medium
Repudiation	Shutoff command is pushed unto the devices but there is no proof it comes from the manager's dashboard	low	medium	medium
Info Disclosure	Attacker intercepts unencrypted gate/valve control traffic and learns the hotel's water distribution schedule and valve configuration,	Low	Medium	Low

	information that can be used to plan a more damaging spoofing or replay attack.			
Denial of Service	Attacker floods the gateway that relays commands to the gate and shutoff actuators with junk traffic, so a legitimate emergency shutoff command sent by the manager cannot reach the device during a leak.	Medium	Critical	Critical
Elevation of Privilege	Attacker with a lower-privilege operator account (e.g. a technician who can only view gate status) exploits a permissions bug to gain the ability to issue shutoff and gate-rotation commands hotel-wide.	Low	Critical	High

For each scenario, be specific. "Attacker does bad thing" is not acceptable. Describe HOW they would execute the attack.

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. **Unencrypted device communication (Info Disclosure):** Sensor and control data travels in plaintext between devices, broker, and cloud. This is critical because an attacker on the hotel WiFi can intercept or alter readings so a leak alert never reaches the dashboard - directly risking the kind of undetected flood the hotel suffered 8 months ago.
2. **WiFi network flooding (DoS):** An attacker jams or floods the hotel WiFi so HYDROLOGIC devices can't transmit readings or receive commands. This is critical because it blocks both leak visibility and the emergency shutoff exactly when they're needed most.

3. **Misconfigured role-based WiFi access (Elevation of Privilege):** A low-privilege network account can be exploited to gain administrative control of the hotel WiFi. This is critical because it lets an attacker pivot from one small foothold to every connected device, the dashboard, and the cloud link at once.

4. **Weak dashboard authentication (Spoofing):** Dashboard accounts rely only on a password, so a phished credential grants full access. This is critical because the dashboard controls gate positions and the emergency shutoff, letting an attacker trigger unwanted shutoffs or hide an active leak.

5. **Cloud service single point of failure (DDoS):** All 3 HYDROLOGIC devices depend on one cloud service with no redundancy. This is critical because a DDoS against that single endpoint blinds the entire hotel at once, not just one device, leaving staff unable to detect leaks or send commands anywhere.

High Risks:

1. **Integrity of dashboard data (Tampering):** An attacker with dashboard access can alter savings/consumption records or event logs after the fact. This is high risk (not critical) because it doesn't stop water flow directly, but it undermines billing accuracy and can hide evidence of an intrusion, delaying detection.

2. **Elevation of privilege - technical staff account (Web Dashboard):** A basic technical-staff account exploits a bug to gain administrator rights. This is high risk because it needs an attacker to first obtain a valid low-level account, making it somewhat less likely than the critical risks, but the eventual impact - full admin control - is just as severe.

3. **Cloud endpoint spoofing (Cloud API):** An attacker impersonates Hydroficient's cloud endpoint so hotel devices send readings to and accept commands from a malicious server. This is high risk because it needs more setup than the critical risks, but it can expose all device data and inject false commands.

Medium Risks:

1. Device spoofing on the network
2. Data interception
3. Alert repudiation
4. Command interception
5. Dashboard action audit gaps

Section 6: Recommended Mitigations

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

Risk	Proposed Mitigation	Implementation Complexity
Weak dashboard authentication	Enable multi-factor authentication	Low – configuration change
Unencrypted device communicaton	Encrypt all device-to-broker and broker-to-cloud traffic	Medium - requires certificate provisioning and firmware updates on all devices
WiFi Network Flooding	Segment IoT devices onto a dedicated network separate from guest WiFi, and set up a wired or cellular backup link for critical alerts.	Medium-High - network redesign and possibly new hardware
Misconfigured role based access	Apply least-privilege role-based access control on the WiFi/network layer, disable default credentials	Low-Medium - configuration and process change
Cloud service single point failure	Deploy redundant cloud instances across multiple regions and place a rate-limiting DDoS protection service in front of the API.	High - infrastructure redesign, likely vendor-dependent
Dashboard integrity	Add write-audit logging with user attribution for every change to savings/consumption data, and use checksums or digital signatures to detect tampering.	Medium - application-level changes and log storage
Elevation of privilege - technical staff account (Web Dashboard)	Enforce strict role separation between staff and admin accounts, patch the privilege-escalation bug.	Low-Medium - access control and patching

Cloud endpoint spoofing (Cloud API)	Implement TLS so devices only trust a certificate-pinned Hydroficient endpoint, preventing traffic redirection to a fake server.	Medium-High - certificate infrastructure and device updates