Section 1: Executive Summary

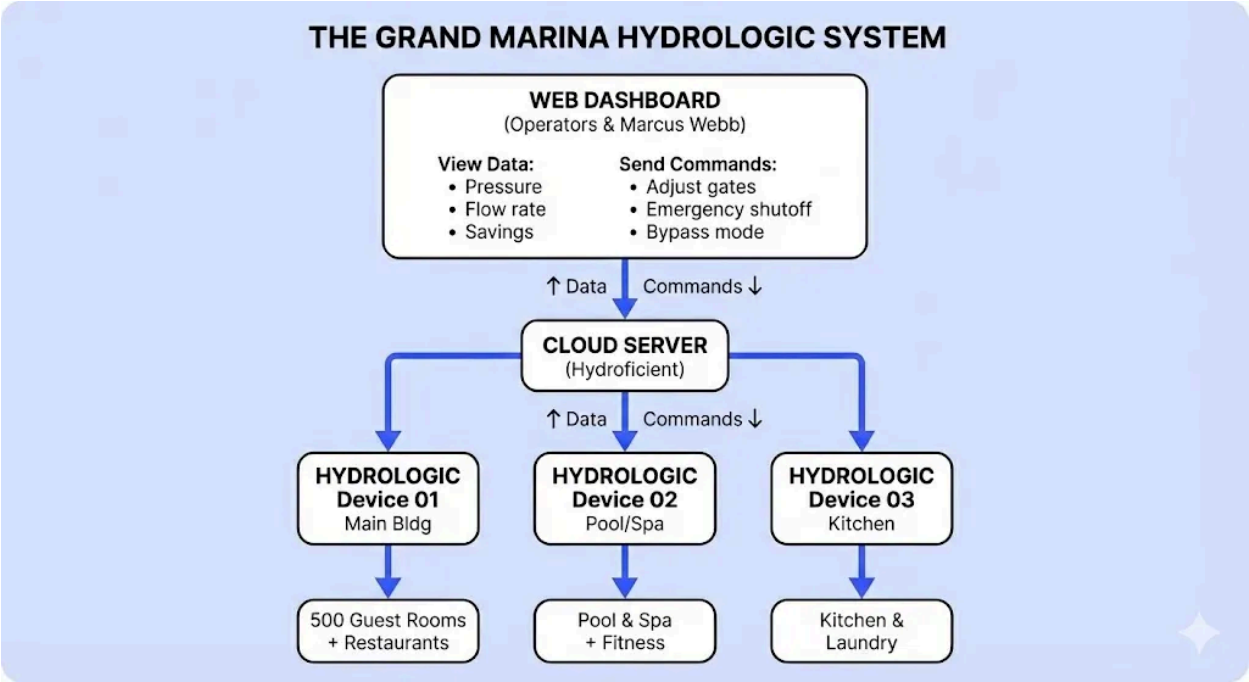
The Grand Marina uses a HYDROLOGIC water flow management system to monitor and control water flow throughout the hotel's 500 guest rooms and facilities. Three HYDROLOGIC devices are used to track water usage and pressure across the hotel's main service lines in order to prevent leaks, reduce water waste, and ensure uninterrupted water service for the hotel.

Threat modeling matters for this system because a failure or misuse of the system could lead to losing water availability, damage to property from leaks, data lost.

The analysis identified three highest priority threats:

- Unauthorized access to the system control dashboard.
- Intercepted, altered communication between HYDROLOGIC devices and server.
- The cloud-based server represents a single point of failure.

Section 2: System Overview



How It Works:

1. Hydrologic devices send data via hotel WiFi to the cloud server continuously.
2. Cloud server store, process and transfer data to the web dashboard.
3. Web dashboard displays received data, alerts.

4. Send commands if needed to modify water pressure, shutoff, etc.

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

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	Attackers use fake devices on the hotel network to send fake water flow data.	Medium	Critical	Critical

Tampering	Attackers using MITM attack to alter data sent from hydro devices to send false positive data.	Medium	Critical	Critical
Repudiation	Devices send alerts but no log to prove which device sent it or when.	Low	Medium	Low
Info Disclosure	Attacker using the hotel WiFi and being able to see unencrypted data transmissions from hydro devices.	High	High	Critical
Denial of Service	Attackers flood the hotel WiFi with trash connections, leaving the devices with no bandwidth left to transmit data.	High	Medium	High
Elevation of Privilege	Attackers exploit the device vulnerability and allow that device to control water gates itself.	Low	Critical	High

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers create a fake web dashboard to steal operator login credentials.	High	Critical	Critical
Tampering	Attackers access the dashboard and send false alerts or hide true alerts.	Medium	Critical	Critical
Repudiation	Operators claim they did not change the water gates' angles.	Medium	Medium	Medium
Info Disclosure	Attackers with dashboard access could send out all water flow data for competitor companies or the public.	Low	Medium	Medium
Denial of Service	Attackers flood the dashboard website with garbage connection so no one else can access it.	Medium	Critical	Critical
Elevation of Privilege	Attackers exploit the web dashboard	Low	Critical	High

	vulnerability to gain control access from view-only accounts.			

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers gained an employee account and were able to access the cloud database.	Medium	High	High
Tampering	Attackers with access can delete or modify water data logs. alerts.	Medium	Critical	Critical
Repudiation	The hydrologic devices claim to have sent alerts and the web dashboard claims to have never received it.	Medium	High	High
Info Disclosure	All water data logs can be sent to competitor companies or the public.	Low	Medium	Medium

Denial of Service	Attackers flooding the cloud server with garbage connections can stop the whole system.	Medium	Critical	Critical
Elevation of Privilege	Cloud servers allow accounts with read-only access to delete, modify data.	Low	High	Medium

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers claim to be the web dashboard and send control commands.	Medium	Critical	Critical
Tampering	Attackers intercept and block control commands so that they never reach the devices.	Medium	High	High
Repudiation	No one claims responsibility for the recent water shutoff.	Medium	High	High
Info Disclosure	Data about gate settings can be sent to	Low	Medium	Low

	competitors or the public			
Denial of Service	Attackers flooding the web dashboard with garbage connections so operators can not access the remote control.	Medium	High	High
Elevation of Privilege	Accounts with dashboard read-only privilege gaining remote control privilege.	Medium	Critical	Critical

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. Weak dashboard authentication (Spoofing) - If successfully logged in, attackers gain full control over the water management system.
2. Data and command tampering (Tampering) - Intercepting and modifying data or control commands could cause false alerts, hide real leaks or trigger unsafe system actions.
3. Cloud API Denial of Service (DoS) - Flooding the cloud service with traffic could disrupt communication between all devices and the dashboard simultaneously, leaving staff without visibility or control over the water system.

High Risks:

1. Loss of Hydrologic device connectivity (DoS) - Attacks targeting the hotel network could prevent devices from sending flow data or alerts. This reduces the hotel's ability to detect leaks or abnormal conditions in a timely manner.

2. Elevation of privilege on devices or dashboard (EoP) - Exploiting vulnerabilities that allow read-only users or sensor-only devices to gain control capabilities could enable unauthorized water gate or shutoff operations.
3. Dashboard availability disruptions - Temporary denial-of-service attacks against the dashboard could prevent operators from monitoring or responding to issues, even if the underlying devices continue operating.

Medium Risks:

1. Information disclosure of Water Usage Data (Info Disclosure) - While water consumption data is not highly sensitive, unauthorized disclosure could reveal operational patterns or cost information and provide competitors with insights into hotel usage trends.
2. Repudiation of critical actions (Repudiation) - Insufficient logging makes it difficult to determine who initiated changes or shutoffs, slowing down incident response and accountability during emergencies.
3. Cloud Data Integrity Issues - Unauthorized modification or deletion of historical water data and alerts could impact reporting, audits, and long-term optimization efforts.

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
Data and command tampering	Encrypt all device-to-cloud and dashboard communications using TLS and enforce message integrity checks.	Medium - requires certificate management and configuration
Cloud API Denial of Service	Implement rate limiting, traffic filtering, and basic DDoS protection on cloud endpoints.	Medium - cloud-native security controls
Loss of HYDROLOGIC device connectivity	Segment IoT devices onto a dedicated network and	Medium - network configuration changes

	prioritize their traffic using network.	
Elevation of privilege on devices or dashboard	Enforce role-based access control (RBAC) and regularly audit permissions for devices and users.	Low to Medium - access control review and enforcement
Dashboard availability disruptions	Deploy dashboard redundancy and uptime monitoring with alerting for outages.	Medium - infrastructure and monitoring setup