Section 1: Executive Summary

The Grand Marina hydrologic system uses 3 devices to send water monitoring data. Operators use this data to make decisions that prevent excessive water bills, leaks and property damages.

This threat model identified security risks that could affect hotel operations.

We found 4 critical risks that require immediate attention:

- *If data from sensors stop flowing, operators become useless and can't react during emergencies.*
- *Weak authentication can lead to attackers taking over the operation and issuing commands as they please.*
- *If attackers tamper with data from sensors, we may be influenced to make bad decisions and unknowingly cause damage.*
- *If attackers take over our powerful remote controls features such as the emergency shut off button, they can cause reputation damage to the hotel,*

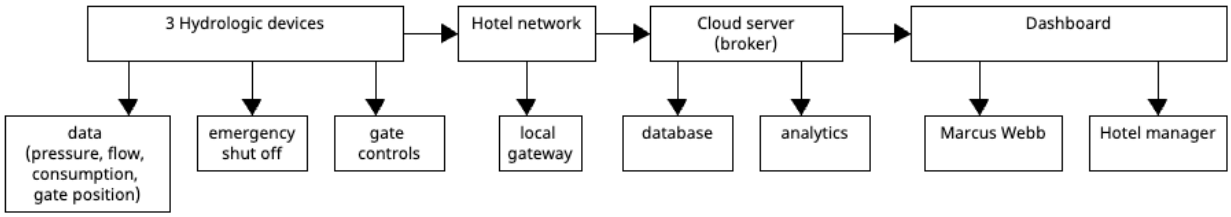
We recommend prioritizing redundancy, multi-factor authentication, encrypted communications and integrity checking.

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:

- *Hydrologic devices measure readings (pressure, flow, consumption, gate position)*

- *Readings are sent to cloud server via a private hotel WIFI.*
- *Cloud server processes the data.*
- *Dashboard displays real time readings to operators and hotel manager. Commands can also be sent to emergency shut off and gate control features from here.*

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	Critical
Web Dashboard	Operator monitoring interface	Medium	Critical	Critical
Cloud Server	Broker between devices and dashboard.	Medium	Critical	Critical
Remote Controls	Gate adjustments, emergency shutoff	Medium	Critical	Critical
Consumption Data	Savings reports, billing records	Low	Medium	Low

Priority rationale:

- **Integrity is critical** for devices, dashboard, cloud api and remote controls, because wrong readings and commands can lead to incorrect decisions and damages.
- **Availability is critical** for devices, dashboard, cloud api and remote controls because lack of data and commands mean not being able to react during emergencies.
- **Confidentiality is medium** because the data the system is working with isn't conventionally valuable.

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 creates a fake device that sends made up readings.	Medium	High	High
Tampering	Attacker modifies high flow rate reading to normal.	Medium	High	High
Repudiation	Device sends readings but logs don't show which device.	Medium	Medium	Medium
Info Disclosure	Attacker gets into the wifi network and captures unencrypted readings	Medium	Low	Low
Denial of Service	Attacker sends too many connection attempts to the device, exhausting its resources	Medium	Critical	Critical
Elevation of Privilege	Attacker uses the device to get into the hotel wifi and pivot to other systems.	Low	Critical	High

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker uses a stolen operator's credentials to login to the dashboard	High	Critical	Critical
Tampering	Attacker modifies password of an operator, causing them to be locked out.	Medium	Low	Low
Repudiation	Logs don't show who clicked the emergency shut off button.	Medium	Medium	Medium

Info Disclosure	Attacks gets into dashboard and leaks data and command history.	Medium	Low	Low
Denial of Service	Attacker uses a botnet to take down the dashboard, operators can't view data or send commands.	High	Critical	Critical
Elevation of Privilege	Attacker gets access of an account with view data access, exploits vulnerability to get command operator access.	Low	Critical	High

Component 3: Cloud Server

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker creates a fake cloud server and captures readings from hydrology devices.	Low	High	Medium
Tampering	Attacker modifies readings from cloud server, corrupting data.	Medium	Critical	Critical
Repudiation	Device says an emergency shutdown command was received but cloud server doesn't show any record of it.	Medium	Critical	Critical
Info Disclosure	Attacker breaks into the cloud database and exports readings and command history.	Low	Low	Low
Denial of Service	Attacker uses a botnet to take down the cloud server. Monitoring and command issuing is stopped.	High	Critical	Critical
Elevation of Privilege	Cloud reader role exploits a database vulnerability to get admin rights.	Low	Critical	High

Component 4: Remote Controls (Gate/Emergency Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker sends a fake emergency shut down command.	Medium	Critical	Critical
Tampering	Attacker changes set gate position 45° to 0°, causing water damage.	Medium	Critical	Critical
Repudiation	Attacker used a replay attack, log says the emergency shut off command was issued by operator 1, but he denies it.	Low	Medium	Low
Info Disclosure	Remote command history is leaked.	Medium	Low	Low
Denial of Service	Attacker performs a DoS attack causing remote commands features to not work.	High	Critical	Critical
Elevation of Privilege	Attacker uses a stolen command history reader account to perform reconnaissance and move up to a command operator account.	Low	Critical	High

Component 5: Consumption data

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker sends a consumption data report which skews our understanding of how much water is being used.	Low	Medium	Low
Tampering	Attacker changes water consumption at night from 1% to 150%, causing a guard on duty to inspect the situation.	Low	Medium	Low

Repudiation	We aren't sure which device's consumption data we received.	Low	Low	Low
Info Disclosure	Consumption data of customer is leaked and robbers use it to attack low usage areas.	Low	High	Medium
Denial of Service	Attacker deletes this year's annual consumption report, now we don't know how effective the hydrologic system is.	Medium	Medium	Medium
Elevation of Privilege	Attacker uses an account with view consumption data privileges to move up to an admin account	Low	High	Medium

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. **Denial of service of devices, dashboard, cloud server and remote controls:** Data from sensors doesn't reach dashboard, real time monitoring stops. Command issuing stops. We are unaware and unable to do anything during emergencies.
2. **Stolen dashboard credentials:** One compromised set of credentials (username/email and password) can give an attacker access to all our data and the ability to issue commands.
3. **Tampering of data in cloud server:** Attacker modifies data in cloud server, leading to us getting false readings. Operators won't be able to make the right decisions.
4. **Spoofing and tampering remote controls:** Fake remote controls can lead to unwanted commands being issued.

High Risks:

1. **Spoofing of hydrologic devices:** can send fake data and hamper our ability to make the right decision.
2. **Tampering of data coming from hydrologic devices:** messes up our ability to make the right decisions.
3. **Elevation of privileges to private hotel wifi** can lead to hotel customer information, billing information being leaked.

4. **Elevated privileges on dashboard, server and remote controls** can lead to a person performing tasks that they were not authorized to do.

Medium Risks:

1. Repudiation can lead to confusion and bad decision making.
2. Spoofed cloud server can lead to our real cloud server not receiving data.
3. Robbers use consumption data to attack low usage areas.

Section 6: Recommended Mitigations

For critical risks:

Risk	Proposed Mitigation	Implementation Complexity
Denial of service	Use Cloudflare DDoS protection services.	Medium - connect all system to Cloudflare, configure DNS.
Stolen dashboard credentials	Implement strong password protection policies and multi factor authentication.	Low - configuration change
Tampering of data in cloud server	Secure database credentials and limit admin/editor roles.	Medium - database configuration change.
Spoofing and tampering of remote controls	Implement encryption and digital certificates to only allow trusted remote control messages.	Medium - implement strong encryption and digital certificates.

For high risks:

Risk	Proposed Mitigation	Implementation Complexity

Spoofing hydrologic devices	Use digital certificates to prove identity of hydrologic devices.	Low - get digital certificates from a CA (certificate authority).
Tampering of data coming from hydrologic devices	Encrypt MQTT communication, use mutual TLS and verify data before accepting.	Medium - build secure MQTT pipeline.
Elevation of privileges to hotel wifi	Use separate networks for hotel and IoT system. Harden both networks.	Medium - network security.
Elevation of privileges on IoT systems	Implement high level security on admin accounts and use principle of least privileges to reduce damage.	Medium - not hard but would require auditing and fixing.