## Section 1: Executive Summary

Dear Marcus,

This executive summary presents the security threat model evaluation for The Grand Marina's water infrastructure, specifically focusing on the HYDROLOGIC flow management system supplied by Hydroficient. Our 500-room luxury property relies on three physical HYDROLOGIC devices to continuously monitor water pressure and manage flow control gates across main service lines. These devices communicate wirelessly with Hydroficient's cloud platform, enabling automated alerts and remote valve controls via an online management dashboard used by our engineering staff.

Threat modeling is a proactive process used to identify operational vulnerabilities before malicious actors or technical failures can exploit them. For a premier hotel, water system integrity is directly linked to guest satisfaction, health and safety, and business continuity. A cyber or operational compromise could lead to unaddressed water leaks, physical flooding damage, or sudden disruptions to guest services. Evaluating these risks allows us to implement targeted safeguards that protect our infrastructure, reputational standing, and financial performance.

Our analysis identified three primary high-priority risks that require immediate mitigation:

- **Communication Interception (Man-in-the-Middle):** Unencrypted wireless signals between devices and the cloud could allow an attacker to alter pressure readings or suppress leak alerts, masking active physical damage.
- **System Service Disruption (Denial of Service):** Overwhelming the web dashboard or cloud server with artificial traffic could prevent staff from monitoring live conditions or triggering emergency water shutoffs during a major breach.
- **Unauthorized Control Access:** Weak credential management or hijacked operator sessions could allow unauthorized individuals to remotely manipulate water gates or trigger property-wide water shutoffs.

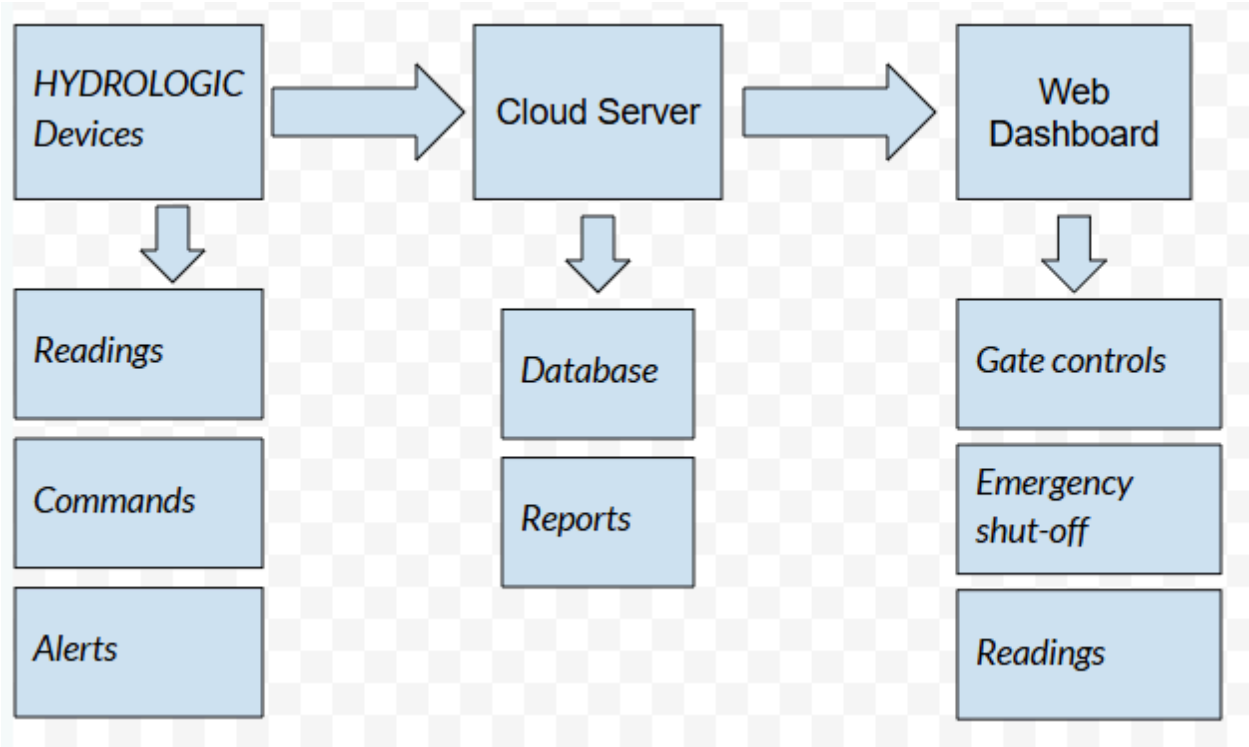
## Section 2: System Overview

*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:**

1. Hydrologic devices measure water pressure continuously
2. Data transmitted via hotel WiFi to service broker
3. Gateway forwards to Hydroficient cloud server
4. Cloud processes data, checks thresholds, triggers alerts
5. Dashboard displays real-time readings and controls to hotel staff
6. Alerts are displayed on the dashboard

## 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 | High | High | Critical |
| Cloud API | Device-to-cloud communication | High | Critical | Critical |
| Remote Controls | Gate adjustments, emergency shutoff | Medium | Critical | Critical |
| Consumption Data | Savings reports, billing records | High | 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 | Attacker introduces a fake device in the hotel network that sends false readings to the dashboard | Medium | High | High |
| Tampering | Attacker that is positioned in the middle of | Medium | Critical | Critical |

| | | | | |
|---|---|---|---|---|
| | communication changes pressure readings. (MITM) | | | |
| Repudiation | A Leak was noticed by a staff member but devices did not send an alert to the dashboard, no history of alerts is kept | Medium | Medium | Medium |
| Info Disclosure | Attacker on hotel WiFi captures unencrypted vital transmissions, learns communication structure and how the system is built | High | High | Critical |
| Denial of Service | Attacker sends thousands of commands to devices | Medium | Critical | Critical |
| Elevation of Privilege | Attacker pivots from HYDROLOGIC network to hotel systems | Low | Critical | High |

## Component 2: Web Dashboard

| Threat | Scenario | Likelihood | Impact | Risk |
|---|---|---|---|---|
| Spoofing | Attacker creates phishing site mimicking Hydroficient dashboard | High | Critical | Critical |

| | | | | |
|---|---|---|---|---|
| Tampering | Attacker Modifies readings and alerts on dashboard | Medium | Critical | Critical |
| Repudiation | Hotel claims alerts was not shown on dashboard | Medium | Medium | Medium |
| Info Disclosure | Attacker gets access to the dashboard and sees all data and customer information | Medium | High | High |
| Denial of Service | Attacker triggers account lockouts, and no one can login to the dashboard | Medium | Critical | Critical |
| Elevation of Privilege | Guest account exploits bug to gain access to admin, and now can modify system configurations | Low | High | High |

## Component 3: Cloud API

| Threat | Scenario | Likelihood | Impact | Risk |
|---|---|---|---|---|
| Spoofing | Attacker impersonates an authorized device or operator to issue unauthorized commands. | Medium | High | High |

| | | | | |
|---|---|---|---|---|
| Tampering | Attacker intercepts and alters water pressure readings or consumption records in transit via Man-in-the-Middle. | Medium | Critical | Critical |
| Repudiation | Lack of audit logging on API endpoints prevents tracing unauthorized requests or parameter modifications. | Medium | Medium | Medium |
| Info Disclosure | Attacker eavesdrops on unencrypted API traffic or accesses database backups left on a public server. | High | High | High |
| Denial of Service | Attacker overwhelms the cloud API with excessive traffic, blocking legitimate device communication. | Medium | Critical | Critical |
| Elevation of Privilege | Attacker exploits an unauthenticated endpoint or weak API auth token to gain administrator access. | Low | Critical | High |

## Component 4: Remote Controls (Gate/Shutoff)

| Threat | Scenario | Likelihood | Impact | Risk |
|---|---|---|---|---|
| Spoofing | Attacker logs in with stolen credentials to issue unauthorized gate opening/closing commands. | High | Critical | Critical |
| Tampering | Attacker records emergency shutoff commands during maintenance and replays them during operational hours. | Medium | High | High |
| Repudiation | Control actions are executed without user or timestamp logging, allowing attackers or operators to deny actions taken. | Medium | Medium | Medium |
| Info Disclosure | Attacker intercepts unencrypted control commands over Wi-Fi, revealing control structure and valid payload formats. | High | Medium | Medium |
| Denial of Service | Attacker floods the command broker, preventing operators from sending emergency shutoff signals during a leak. | Medium | Critical | Critical |
| Elevation of Privilege | Low-privileged user account exploits control interface flaws to execute | Low | Critical | High |

| | | | | |
|---|---|---|---|---|
| | emergency shutoffs or gate adjustments. | | | |

.

## Section 5: Risk Summary

List your findings by risk level:

**Critical Risks:**

1. Man-in-the-Middle Attack on Device/API Communications: Interception and modification of pressure readings or gate commands go unnoticed, leading to undetected leaks or physical water damage.
2. Denial of Service on Cloud API & Dashboard: Traffic flooding prevents operators from viewing alerts or triggering emergency shutoffs during critical failure events.
3. Unauthorized Access & Remote Control Spoofing: Attackers gaining credential access can manipulate water flow gates, shut off water supplies, or delete historical usage records.

**High Risks:**

1. Replay Attack on Emergency Controls: Capture and retransmission of maintenance shutoff signals disrupt hotel operations during normal hours.
2. Unencrypted Network Eavesdropping: Sniffing guest/hotel Wi-Fi traffic exposes device parameters, credentials, and network communication structures.

**Medium Risks:**

1. Lack of Audit Logging: Inability to track historical commands or alert deliveries hinders post-incident investigation.

## Section 6: Recommended Mitigations

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

| Risk | Proposed Mitigation | Implementation Complexity |
|---|---|---|
| Man-in-the-Middle & Eavesdropping | Implement TLS/mTLS encryption for all device-to-cloud communications. | Medium — certificate deployment & configuration |
| Unauthorized Access & Remote Control Spoofing | Enforce Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) on the Web Dashboard. | Low — configuration change |
| Denial of Service (DoS) | Implement API rate limiting, network segmentation, and DDoS protection. | Medium — network policy & infrastructure updates |
| Replay Attacks | Use cryptographic nonces and short-lived timestamps on control payloads. | Medium — software code update |