Threat Model: The Grand Marina HYDROLOGIC Water Management System

Section 1: Executive Summary

The system analyzed in this assessment is The Grand Marina's HYDROLOGIC water management platform. The marina operates a 500-room luxury hotel and uses three HYDROLOGIC flow management devices to monitor and control water usage. These devices connect to a cloud platform that provides monitoring, reporting, remote management, and emergency shutoff capabilities through a web-based dashboard.

Threat modeling is important because this system directly supports hotel operations and guest services. If the system becomes unavailable, is manipulated, or is accessed by unauthorized individuals, the marina could experience service disruptions, financial losses, operational delays, and damage to its reputation. Understanding potential threats allows management to prioritize security investments before incidents occur.

The three highest-priority findings are: (1) unauthorized access to the web dashboard through compromised credentials, which could allow attackers to issue commands or view sensitive information; (2) manipulation of cloud communications between devices and the management platform, potentially resulting in inaccurate data or unauthorized control actions; and (3) misuse of remote shutoff and gate control capabilities, which could disrupt water service throughout the property and affect hotel operations.

Section 2: System Overview

The Grand Marina is a 500-room luxury hotel that uses Hydroficient's HYDROLOGIC system to monitor and manage water consumption.

System Components

- 3 HYDROLOGIC flow management devices
- Cloud-based monitoring platform
- Web dashboard for operators and management
- Remote gate control functionality
- Emergency shutoff capability
- Reporting and consumption analytics database

Data Flow Diagram

[HYDROLOGIC Devices]
|
v
[Cloud API]
/
v v
[Database] [Dashboard]
| |
v v
[Reports] [Operators]
|
v
[Gate Controls]
[Emergency Shutoff]

Data Flow Description

1. HYDROLOGIC devices collect flow and consumption information.
2. Information is transmitted to the cloud API.
3. The cloud platform stores information in a database.
4. Operators access data through the web dashboard.
5. Authorized personnel can issue gate control or emergency shutoff commands remotely.

Section 3: Asset Inventory

Asset	Description	C Priority	I Priority	A Priority
HYDROLOGIC Devices	Three flow management units	Medium	High	High
Web Dashboard	Operator monitoring interface	High	High	High
Cloud API	Device-to-cloud communication service	High	High	High
Remote Controls	Gate adjustments and emergency shutoff	Medium	High	Critical
Consumption Data	Usage reports and billing information	High	High	Medium

Key:

- C = Confidentiality
- I = Integrity
- A = Availability

Section 4: STRIDE Analysis

Component 1: HYDROLOGIC Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Unauthorized device attempts to identify itself as a legitimate sensor	Medium	High	High
Tampering	Device configuration altered without authorization	Medium	High	High

Repudiation	Activity occurs on device but cannot be traced to responsible user	Low	Medium	Low
Information Disclosure	Device telemetry intercepted during transmission	Medium	Medium	Medium
Denial of Service	Device overwhelmed with traffic and stops reporting	Medium	High	High
Elevation of Privilege	Software vulnerability allows higher-level permissions	Low	High	Medium

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Stolen employee credentials used to access dashboard	High	High	Critical
Tampering	Unauthorized user changes system settings	Medium	High	High
Repudiation	User denies changing configurations due to weak audit logs	Medium	Medium	Medium
Information Disclosure	Sensitive reports exposed to unauthorized users	Medium	High	High
Denial of Service	Dashboard becomes unavailable during operations	Medium	High	High
Elevation of Privilege	User account gains administrative permissions improperly	Medium	High	High

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk

Spoofing	Unauthorized system attempts to communicate with API	Medium	High	High
Tampering	Data modified during processing or transmission	Medium	High	High
Repudiation	Incomplete logs prevent investigation	Low	Medium	Low
Information Disclosure	Exposure of operational and consumption data	Medium	High	High
Denial of Service	API becomes unavailable due to excessive requests	Medium	High	High
Elevation of Privilege	Application flaw grants elevated permissions	Low	High	Medium

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Unauthorized user issues control commands	Medium	Critical	Critical
Tampering	Gate or shutoff settings modified without authorization	Medium	Critical	Critical
Repudiation	No record of who initiated a control action	Low	High	Medium
Information Disclosure	Operational control information exposed	Low	Medium	Low
Denial of Service	Control functionality becomes unavailable during emergency	Medium	Critical	Critical
Elevation of Privilege	Standard user gains control permissions	Medium	Critical	Critical

---

Section 5: Risk Summary

Critical Risks

1. Unauthorized access to the web dashboard through compromised credentials.
    - Could provide direct access to monitoring and control functions.
2. Unauthorized execution of remote shutoff or gate control commands.
    - Could interrupt hotel water services and business operations.
3. Loss of availability of remote control functions.
    - Could prevent operators from responding to emergencies.

High Risks

1. Modification of device configurations.
2. Exposure of operational or consumption data.
3. Denial of service against cloud API services.
4. Privilege escalation within dashboard applications.

Medium Risks

1. Interception of telemetry data.
2. Incomplete logging and audit records.
3. Limited information disclosure from individual devices.

Section 6: Recommended Mitigations

Risk	Proposed Mitigation	Implementation Complexity
Compromised dashboard credentials	Enable multi-factor authentication	Low

Unauthorized remote commands	Require MFA and role-based access control	Medium
Device configuration changes	Implement configuration management and approval workflows	Medium
API abuse or disruption	Deploy rate limiting and monitoring	Medium
Data exposure	Encrypt data in transit and at rest	Medium
Privilege escalation	Apply least-privilege access controls and periodic reviews	Medium
Insufficient logging	Centralized logging and audit retention	Low
Service outages	Implement redundancy and disaster recovery procedures	High

Conclusion

The Grand Marina's greatest security concerns involve unauthorized access to management functions, misuse of remote control capabilities, and disruption of critical water management services. By prioritizing strong authentication, access controls, encryption, logging, and system resilience, management can significantly reduce both cybersecurity risk and operational impact.