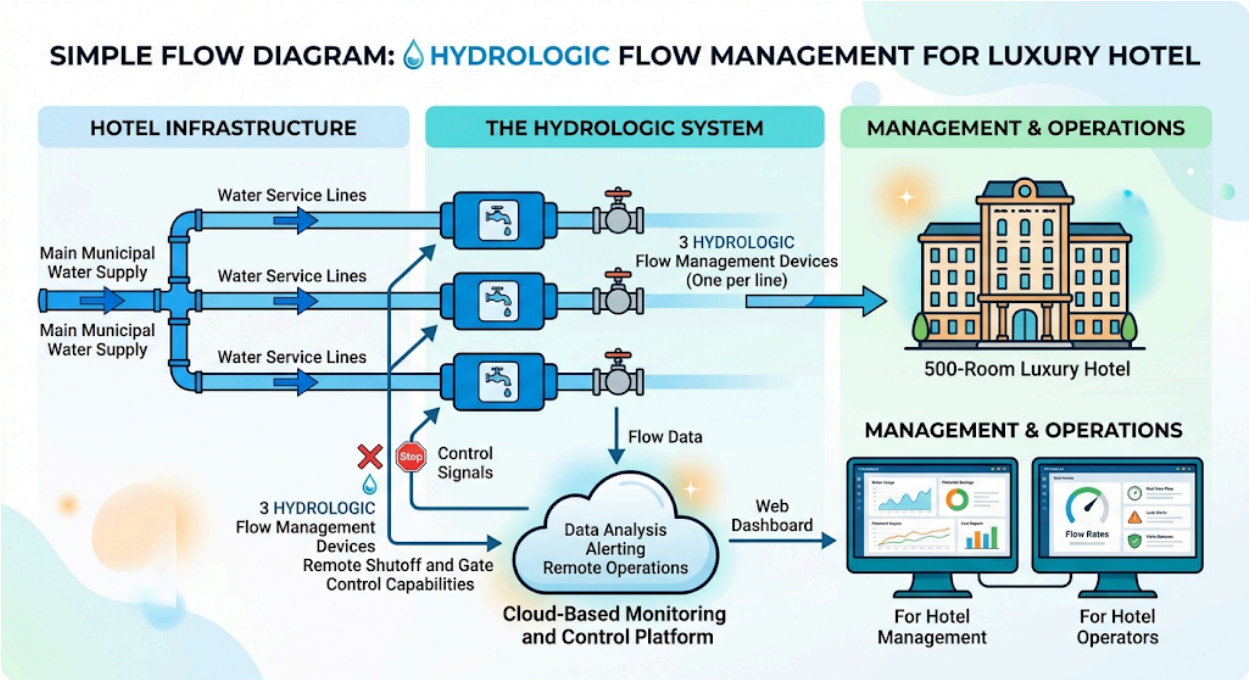
Section 1: Executive Summary

This threat model looks at how The Grand Marina connects its business computers and public Wi-Fi directly to its physical machinery. The review focused on three main areas: sensors measuring water pressure and flow, mechanical controls that open gates or trigger emergency shutoffs, and management tools like administrative dashboards and leak alerts.

Analyzing these threats is critical because business computers (IT) and heavy machinery (OT) operate with completely different goals. IT systems focus on keeping private data safe, while OT systems focus on human safety and keeping the physical facility running smoothly. Without a structured method like STRIDE to map out potential entry points, a hacker could use a weak entry point—like guest Wi-Fi or a stolen staff password—to hop into the control network. Threat modeling helps security teams stop a simple digital break-in from causing physical destruction, toxic spills, or severe flooding.

Section 2: System Overview

- 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 capabilities



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	1	5	5
Web Dashboard	Operator monitoring interface	3	5	5
Cloud API	Device-to-cloud communication	3	5	5
Remote Controls	Gate adjustments, emergency shutoff	1	5	5
Consumption Data	Savings reports, billing records	5	5	1

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	an attacker impersonates a legitimate HYDROLOGIC device to send fake sensor data (e.g., false flow rates) to the Cloud API.	medium	high	high

Tampering	An attacker physically accesses the device or intercepts firmware updates to alter the flow control logic or sensor calibrations.	low	high	medium
Repudiation	A device logs a critical gate state change without cryptographic signing, allowing an operator or compromised system to deny altering the setting.	medium	medium	medium
Info Disclosure	Unencrypted device storage or local serial interface allows an attacker to extract Wi-Fi credentials or hard-coded API keys.	medium	medium	medium
Denial of Service	An attacker floods the device's network interface or manipulates physical power states, causing the flow	medium	high	high

	management unit to go offline or freeze up.			
Elevation of Privilege	An attacker exploits a vulnerability in the device firmware execution stack to gain root access, bypassing flow control boundaries.	low	high	medium

Component 2: Web Dashboard (Same table structure)

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker steals an operator's session token via session hijacking or phishing and logs in as a legitimate operator.	High	High	High
Tampering	An attacker executes Cross-Site Scripting (XSS) to inject malicious scripts into the dashboard interface, altering operational displays seen by operators.	Medium	High	High

Repudiation	An operator performs a manual override, but audit logging on the web application is disabled or easily overwritten, preventing non-repudiation.	Medium	Medium	Medium
Information Disclosure	Sensitive operational topologies or customer telemetry are exposed due to missing authorization checks on dashboard API endpoints (IDOR).	Medium	Medium	Medium
Denial of Service	An attacker launches an HTTP flood against the web application, rendering the monitoring interface unavailable to operators during a system alert.	High	High	High
Elevation of Privilege	A standard user exploits broken access controls to gain access to administrative functionalities on the dashboard.	Medium	High	High

Component 3: Cloud API (Same table structure)

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker uses rogue credentials or spoofed headers to interact with the API endpoints directly without passing through proper gateway authentication.	Medium	High	**High**
Tampering	Man-in-the-middle (MitM) interception alters API payloads containing control configurations in transit between the API and the backend database.	Low	High	**Medium**
Repudiation	API requests are processed without retaining client request IDs, source IPs, or digital signatures in immutable transaction logs.	Medium	Medium	**Medium**
Information Disclosure	API response payloads return excessive data objects (e.g., system keys, debugging traces, full customer profiles) beyond what was requested.	High	Medium	**High**

Denial of Service	An attacker overwhelms API endpoints with high-frequency telemetry requests lacking rate limiting, exhausting cloud database connection pools.	High	High	**High**
Elevation of Privilege	An attacker exploits an unpatched web framework vulnerability on the API server to execute arbitrary code and gain host-level privilege.	Low	Critical	**High**

Component 4: Remote Controls (Gate/Shutoff) (Same table structure)

Component 4: Remote Controls

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An unauthorized entity sends emergency shutoff or gate adjustment commands using compromised API tokens or weak authentication headers.	Medium	Critical	**High**
Tampering	An attacker intercepts and alters remote control payload parameters in transit to force an	Low	Critical	**High**

	unexpected valve opening state.			
Repudiation	Remote shutoff trigger events lack cryptographic timestamps and non-repudiable operator signatures, masking who initiated an emergency action.	Medium	Medium	**Medium**
Information Disclosure	Command status and acknowledge messages broadcast over unencrypted channels reveal current operational states and physical valve positions.	Medium	Low	**Low**
Denial of Service	An attacker intentionally floods the remote control messaging queue (e.g., MQTT broker/WebSockets), delaying critical emergency shutoff execution.	Medium	Critical	**High**
Elevation of Privilege	An operator with basic gate adjustment privileges exploits parameter tampering to execute high-impact emergency shutoff routines without approval.	Medium	High	**High**

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. **Unauthorized Remote Control Execution (Remote Controls - Spoofing / Tampering / Elevation of Privilege)**
    a. **Why it's Critical:** Emergency shutoffs and gate adjustments directly interface with physical infrastructure. An attacker successfully spoofing or tampering with remote control commands can manipulate physical water flow, leading to localized flooding, physical equipment destruction, or sudden water supply denial.
2. **Host/Platform Compromise via Cloud API (Cloud API - Elevation of Privilege)**
    a. **Why it's Critical:** Exploiting underlying host or execution stack vulnerabilities on the Cloud API grants full system access to the central server environment. A compromised API backend compromises all downstream devices, sensitive databases, and control pathways simultaneously.

High Risks:

1. **Device Impersonation & Telemetry Spoofing (HYDROLOGIC Devices - Spoofing)**
    a. Fraudulent telemetry sent to the cloud misleads operators, triggering improper automated or manual flow adjustments.
2. **Local Physical & Operational Interruption (HYDROLOGIC Devices - Denial of Service)**
    a. Network flooding or localized disruption of flow units prevents physical devices from receiving operational adjustments or reporting status updates.
3. **Session Hijacking & Account Takeover (Web Dashboard - Spoofing)**
    a. Stolen operator credentials give attackers direct access to administrative monitoring and manual system controls.
4. **Dashboard Script Injection (Web Dashboard - Tampering)**
    a. XSS attacks allow attackers to manipulate the operator interface, concealing real-world operational hazards or falsifying system alerts.
5. **Monitoring Interface Downtime (Web Dashboard - Denial of Service)**
    a. HTTP floods make the dashboard unavailable, blinding operators during critical alarms or operational anomalies.
6. **Dashboard Access Escalation (Web Dashboard - Elevation of Privilege)**
    a. Broken access controls allow low-privileged web accounts to execute high-impact system changes.
7. **Unauthenticated API Access (Cloud API - Spoofing)**
    a. Bypassing authentication protocols lets unauthorized entities inject data directly into backend infrastructure.

8. **Data Over-exposure via API (Cloud API - Information Disclosure)**
    a. Excessive payload disclosures expose internal system configurations, operational keys, and customer data via public endpoints.
9. **Telemetry Flooding & Resource Exhaustion (Cloud API - Denial of Service)**
    a. Unthrottled request surges deplete database connections, taking down real-time tracking across all units.
10. **Command Queue Denial of Service (Remote Controls - Denial of Service)**
    a. Messaging queue saturation delays or blocks time-sensitive emergency shutoff execution.
11. **Remote Control Privilege Abuse (Remote Controls - Elevation of Privilege)**
    a. Lower-level operators or compromised limited tokens triggering high-impact shutoffs without required approvals.
12. **Historical Data Tampering (Consumption Data - Tampering)**
    a. Falsifying billing or consumption metrics corrupts financial transactions, causes revenue loss, and breaches legal compliance.
13. **Unencrypted PII & Billing Exposure (Consumption Data - Information Disclosure)**
    a. Unauthorized access to consumption histories and personal customer records leads to regulatory non-compliance (e.g., GDPR/CCPA) and reputational damage.

Medium Risks:

1. **Physical Device Firmware Tampering (HYDROLOGIC Devices - Tampering)**
    a. Requires local physical access to rewrite logic or sensor calibration, limiting immediate widespread threat scale.
2. **Unsigned Device Action Logs (HYDROLOGIC Devices - Repudiation)**
    a. Lack of signed local logs complicates forensic analysis following a device-level failure or manipulation.
3. **Local Credential Extraction (HYDROLOGIC Devices - Info Disclosure)**
    a. Local extraction of hardcoded credentials requires close-proximity physical/serial access.
4. **Device Stack Exploitation (HYDROLOGIC Devices - Elevation of Privilege)**
    a. Exploiting local hardware execution layers to gain root access requires specialized physical or local network exploits.
5. **Unauthenticated Dashboard Overrides (Web Dashboard - Repudiation)**
    a. Missing or editable operator action logs prevent establishing accountability for bad operational decisions.
6. **API Endpoint Data Harvesting (Web Dashboard - Information Disclosure)**
    a. Exploiting direct object references exposes topology details but does not grant direct control over hardware.
7. **In-Transit Parameter Tampering (Cloud API - Tampering)**
    a. Intercepting backend API payloads is difficult if basic TLS transport security is active.
8. **Unlinked API Transaction Logs (Cloud API - Repudiation)**

    a. Incomplete API client tracing impairs forensic investigations into malicious requests.
9. **Command Sequence Repudiation (Remote Controls - Repudiation)**
    a. Unsigned emergency actions complicate accountability during post-incident investigations.
10. **Financial Ledger Impersonation (Consumption Data - Spoofing)**
    a. Inserting fake billing data requires backend database or API credentials.
11. **Missing Financial Audit Trails (Consumption Data - Repudiation)**
    a. Absence of immutable change logs prevents tracking unauthorized modifications to financial records.
12. **Database Analytical Flooding (Consumption Data - Denial of Service)**
    a. Resource-heavy analytical queries slow down reporting availability without threatening physical operations.
13. **Reporting Account Privilege Escalation (Consumption Data - Elevation of Privilege)**
    a. Read-only reporting roles gaining modify/delete permissions on reporting tables.

Section 6: Recommended Mitigations

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

Risk	Proposed Mitigation	Implementation Complexity
Unauthorized Remote Control Execution	Implement cryptographic digital signatures on control payloads; restrict emergency triggers via role-based access control (RBAC).	High — requires public key infrastructure (PKI) integration on hardware and backend.
Host/Platform Compromise via Cloud API	Deploy runtime application self-protection (RASP), enforce strict container isolation, and conduct routine automated dependency vulnerability scans.	Medium — infrastructure setup and pipeline integration.

Device Impersonation & Telemetry Spoofing	Require Mutual TLS (mTLS) with hardware-backed client certificates (TPM/Secure Element) for device-to-cloud authentication.	High — hardware provisioning and certificate lifecycle management.
Local Physical & Operational Interruption	Implement local hardware watchdogs, rate-limiting on physical interfaces, and fallback safe-state logic when network link drops.	Medium — firmware updates and fail-safe testing.
Session Hijacking & Account Takeover	Enforce multi-factor authentication (MFA) for dashboard access and use short-lived, cryptographically signed OAuth 2.0 session tokens.	Low — IAM configuration change.
Dashboard Script Injection (XSS)	Enforce a strict Content Security Policy (CSP) header and sanitize all dynamic inputs using context-aware encoding frameworks.	Low — code refactoring and header configuration.
Monitoring Interface Downtime (DoS)	Place the web dashboard behind a Cloud Web Application Firewall (WAF) with automated anti-DDoS and rate-limiting rules.	Low — DNS/cloud proxy configuration.
Dashboard Access Escalation	Perform server-side validation for all administrative API requests and enforce strict object-level access controls (AOAC).	Medium — backend endpoint access control checks.
Unauthenticated API Access	Enforce API Gateway authentication policies using mandatory bearer tokens (JWT) and API key validation for all endpoints.	Low — gateway routing policy configuration.

Data Over-exposure via API	Implement field-level response filtering and Data Transfer Objects (DTOs) to limit API outputs to requested scopes only.	Medium — API controller refactoring.
Telemetry Flooding & Resource Exhaustion	Apply per-device IP and client ID rate limiting at the API Gateway level; decouple ingest processing using scalable message queues.	Medium — architecture adjustments and gateway policy configuration.
Command Queue Denial of Service	Isolate remote control commands into dedicated high-priority messaging topics with dedicated worker pools and connection limits.	Medium — message broker topic and worker node re-configuration.
Remote Control Privilege Abuse	Enforce multi-party authorization (four-eyes principle) for high-impact emergency actions and cryptographically bind user scopes to API tokens.	Medium — workflow and authorization logic updates.
Historical Data Tampering	Enforce database write-once-read-many (WORM) controls, cryptographically hash historical logs, and restrict database WRITE permissions.	Medium — database schema and permission restructuring.
Unencrypted PII & Billing Exposure	Apply transparent database encryption (TDE / AES-256) at rest, strictly limit database export privileges, and mask sensitive customer data.	Low — database configuration and policy update.