

Section 1: Executive Summary

This report looks at the security of HYDROLOGIC, the water management system Hydroficient has installed at The Grand Marina. Because the hotel sits close to the municipal water source, water arrives at around 85 PSI. That is more pressure than the building's plumbing should take long-term, and it wastes water. HYDROLOGIC's three devices, one on each water supply line, measure the pressure and adjust gates to bring it down. This protects the pipes and lowers water bills. Staff monitor and control the system through a web dashboard, which includes the ability to shut off the water remotely in an emergency.

That remote control is why security matters. Anyone who gains control of the system, not just authorised staff, could shut off water to all 500 rooms, the pool and spa, and the kitchens and the laundry. This could also open the gates fully, letting full pressure through and risking burst pipes and flooding. Internet of Things devices like these are common targets for attackers. They often come with default passwords, are rarely updated, and stay in service for years after their software becomes outdated.

We identified three priority concerns:

- Weak dashboard login. One stolen or guessed password could give an outsider control of alerts, gate settings and the emergency shutoff.
- Unprotected device communications. Messages between the devices and the cloud may not be properly encrypted or verified.
- Total reliance on the cloud service. If the cloud service goes down or is compromised, the hotel loses sight and control of all three devices at once, with no local backup.

We recommend three steps first: require multi-factor authentication for every dashboard account, encrypt and verify all device communications, and make sure the devices fall back to a safe setting that staff can operate manually if the cloud connection is lost.

Section 2: System Overview

Describe The Grand Marina's HYDROLOGIC system:

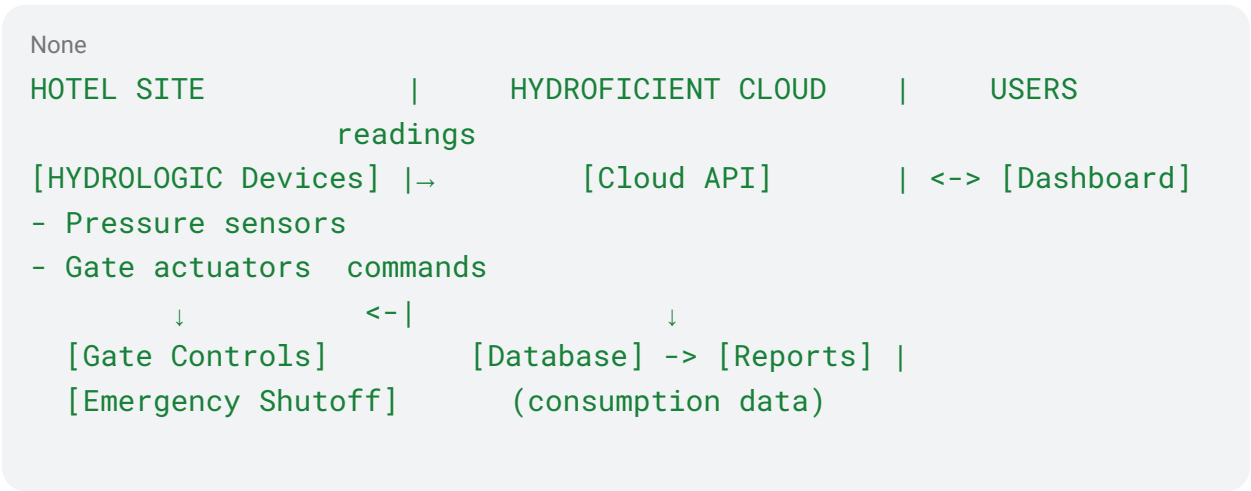
- 500-room luxury hotel (Hydroficient customer)
- 3 HYDROLOGIC flow management devices (one per water service line)
- Cloud-based monitoring and control
- Web dashboard for operators and management
- Remote shutoff and gate control capability

Include a simple data flow diagram (can be ASCII art or describe the flow):

The Grand Marina is a 500 room luxury hotel and a Hydroficient customer. Because of its location, mains water arrives at roughly 85 PSI. Three HYDROLOGIC flow management devices are installed, one on each water service line. Each device contains pressure sensors and motorised gates.

The system works like this:

- 1. The sensors measure pressure and flow continuously and send readings to Hydroficient’s cloud API over the internet.
- 2. The cloud API stores the readings in a database and makes them available to a web dashboard. Engineering staff and management use the dashboard to monitor the system.
- 3. When pressure moves outside the set limits, the system raises an alert. Gate adjustment commands are then sent back to the devices, either automatically or by an operator.
- 4. Authorised users can trigger an emergency shutoff remotely, for example during a burst pipe.
- 5. Consumption data feeds savings reports and billing records.



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	Low	High	High

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

Integrity matters most across the system as a false reading or an altered command causes physical damage.

Availability matters most for the devices and the API. Losing them means losing control of the water supply.

Consumption data is mainly a confidentiality concern, as water usage patterns reveal occupancy, and billing data is commercially sensitive.

Section 4: STRIDE Analysis

Component 1: HYDROLOGIC Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker reads a device ID from its label or from captured network traffic, then sends fake readings to the cloud while pretending to be Device 2. The fake readings say “normal pressure” while real pressure spikes, so no alert fires.	Medium	High	High
Tampering	A contractor or insider with plant room access opens a unit, connects to an exposed debug port, and installs modified firmware. The firmware could report false readings, ignore shutoff commands, or apply a calibration offset.	Medium	High	High
Repudiation	Someone uses the manual override button on a device. Logs are only kept on the device and are overwritten, so no-one can show who did it or when.	Medium	Medium	Medium
Info Disclosure	If traffic isn’t encrypted and the guest WiFi isn’t separated from the device’s network, an attacker on the guest Wifi can capture device	High	Medium	High

	traffic. The traffic could contain device credentials, API keys and flow data.			
Denial of Service	An attacker near the plant room jams the wireless signal or floods the device with network requests. The device goes offline and can't report a real leak or receive a shutoff command.	Medium	High	High
Elevation of Privilege	An attacker scans the network or uses an Internet search engine for connected devices and finds a device's admin interface. They log in with the default manufacturer password, gain full control, and use the device to move into the rest of the hotel network.	Medium	High	High

Component 2: Web Dashboard (Same table structure)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An operator reuses a password that was exposed in a breach of another website. An attacker tries the leaked username and password pairs on the dashboard. With no MFA, one match gives full operator access. Phishing emails to engineering staff work the same way.	High	High	Critical
Tampering	A logged in attacker changes the high pressure alert threshold, for example from 85PSI to 100PSI. Real overpressure events then raise no alarms while the dashboard still looks normal.	Medium	High	High
Repudiation	Staff share a single generic login. When a gate is changed or water is shut off, there is no way to tell which person did it, so mistakes can't be traced	High	Medium	High
Info Disclosure	The URL contains a property ID. Changing that number shows another customer's data, or a different report shows billing records.	Medium	Medium	Medium
Denial of Service	An attacker makes repeated failed logins against every known operator username, which triggers account lockouts. Staff are then locked out during a real incident	Medium	Medium	Medium

Elevation of Privilege	A finance user has “view only” access, but the server doesn’t check permissions and only the screen hides the control buttons. The user can then send gate controls directly and it works.	Medium	High	High
------------------------	--	--------	------	------

Component 3: Cloud API (Same table structure)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	The same API key is built into every device’s firmware. An attack extracts it from a firmware download or a stolen unit, then calls the API as a legitimate device or as the dashboard.	Medium	High	High
Tampering	A device doesn’t properly check the server’s TLS certificate. An attacker on the network intercepts the connection and alters commands in transit.	Medium	High	High
Repudiation	The API doesn’t record who sent each command and when, or its logs can be edited. After an incident, the hotel then can’t reconstruct events for insurers or investigators.	Medium	Medium	Medium
Info Disclosure	A cloud storage location holding reports or database backups is accidentally made public. Consumption and billing data leak. Usage patterns could reveal which floors are occupied and when.	Medium	Medium	Medium
Denial of Service	There is no rate limiting, so a botnet floods the API and it stops responding. A cloud outage has the same effect. Either way, all three devices lose their control channel at once, because the cloud is a single point of failure.	Medium	High	High
Elevation of Privilege	The API trusts a customer ID sent in each request. A user from another Hydroficient customer changes that ID and gains control of the hotel’s gates. A compromised Hydroficient admin account would also control every customer’s devices	Low	High	High

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

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Using a stolen dashboard session or a forged command, an attacker triggers an emergency shutoff at peak time.	Medium	High	Critical
Tampering	An attacker records a legitimate “open gate fully” command and replays it later. Full water pressure flows through the building, putting pressure on old pipework and risking a burst and flooding.	Medium	High	Critical
Repudiation	Remote shutoffs need no confirmation and leave no attributable audit record. After an outage, nobody can tell whether it was an attack, mistake or fault	Medium	Medium	Medium
Info Disclosure	Gate schedules and shutoff history reveal maintenance windows and low occupancy periods. Someone planning a physical intrusion or a well-timed attack could use that information	Low	Medium	Low
Denial of Service	An attacker spams open and close commands. The sudden changes cause pressure surges that damage pipes and valves, and staff can’t hold the gates in a safe position.	Medium	High	High
Elevation of Privilege	Every logged-in user can trigger the emergency shutoff. There is no separate permission or second approval, so a low-level or compromised account can cut water to the whole premise.	Medium	High	High

Section 5: Risk Summary

List your findings by risk level:

Critical Risks:

1. Dashboard account takeover (due to no MFA). One reused or phished password gives full control of alerts, gates and shutoff. Credential stuffing is cheap, automated and very common, so likelihood is high.
2. Forged, altered or replayed control commands. If commands aren't encrypted and signed, attacks can trigger a shutoff or force the gates fully open. Both outcomes cause direct physical and financial harm.
3. Cloud as a single point of failure. If the cloud API is unavailable or compromised, all three devices lose monitoring and control. Without a local safe mode, the hotel wouldn't be able to respond to a real emergency.

High Risks:

1. Default passwords on device admin interfaces, allowing device takeover and a route into the hotel network.
2. Physical tampering with devices in poorly secured plant rooms.
3. Fake sensor readings hiding real overpressure.
4. Alert thresholds changed silently.
5. Broken access control: view-only users can still send control commands.
6. Shared logins, so actions can't be traced to a person.
7. API keys extractable from firmware.
8. Weak separation between Hydroficient customers on the API.
9. Unencrypted traffic visible from the guest WiFi.
10. Devices knocked offline by jamming or flooding.

Medium Risks:

1. Missing or editable audit logs on devices and the API.
2. Consumption and billing data exposed through misconfiguration or URL manipulation.
3. Deliberate account lockouts during an incident.

Low Risks:

1. Gate schedules revealing maintenance windows.

Section 6: Recommended Mitigations

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

Risk	Proposed Mitigation	Implementation Complexity
Weak dashboard authentication	Required MFA for all accounts. Connect the dashboard to the hotel's staff login system so leavers lose access automatically.	Low — configuration change
Forged, altered or replayed commands	Encrypt all traffic with TLS and require devices to check the server's certificate. Sign each command and include a timestamp and a one-time number so old commands can't be replayed.	Medium - needs firmware and API changes from Hydroficient
Cloud single point of failure	Devices fall back to a safe gate position if they lose the cloud connection. Provide an on-site manual override. Fit a mechanical pressure reducing valve as a backstop that works with no software at all.	Medium - hardware plus firmware changes.
Default device passwords	Give every device a unique strong password, or disable local admin interfaces entirely.	Low
Physical tampering	Lock plant rooms, fit tamper evident seals, disable debug ports, and use secure boot with signed firmware updates.	Low (locks) and High (secure boot)
Fake sensor readings	Give each device its own certificate so the cloud can verify which device is talking. Flag readings that don't match the water meter or other devices.	Medium
Silent threshold changes	Alert managers when thresholds change. Require a second person to approve changes to safety limits.	Low
Broken access control	Use role-based access and check permissions on the server for every request, not just in the interface.	Medium
Shared logins/no audit trail	Give every user a named account. Send logs to a central system that staff can't edit.	Low to medium
API keys in firmware	Use per-device certificates or credentials that can be revoked one at a time, not one shared key.	Medium
Weak customer separation	Have Hydroficient enforce customer separation on the server based on who is logged in, not on an ID that requests supplies.	Medium
Traffic visible from guest WiFi	Put the HYDROLOGIC devices on their own network segment, firewalled from guest and	Medium

	corporate WiFi, so they can only take to the cloud API.	
Devices knocked offline	Use wired connections where possible. Alert on device heartbeat loss and rely on the local safe mode.	Medium