

SECURITY ASSESSMENT

Grand Marina Hotel Water Monitoring System

Prepared for: Marcus Webb, General Manager

Prepared by: Sok Leng Chan

Date: July 27, 2026

Decision: Approve protected communications, with certificate verification enforced

EXECUTIVE SUMMARY

I recommend enabling TLS - the security setting that encrypts network traffic - for the Grand Marina Hotel water monitoring system, but only with certificate verification turned on. Before protection, sensor readings traveled in readable form. A person with access to the hotel or IoT network could observe device and pressure information, creating risk to guest safety, daily operations, and the hotel's reputation.

The four tests show that TLS protects the readings with almost no performance cost. Average delivery time increased from 50.88 milliseconds to 50.98 milliseconds - a difference of 0.10 milliseconds, or 0.197%. The protected system also passed every tested load, from 10 messages per second in normal operation to 100 messages per second, which was beyond the stated requirement.

SECURITY RISKS BEFORE AND AFTER TLS

Before protection

The system was sending water-pressure information like a postcard: anyone able to observe the network traffic could read it. Exposed device IDs and pressure patterns could reveal where equipment is active, when abnormal conditions occur, or when monitoring is weakest. The test did not attempt to change commands, so it does not prove that an attacker could alter valves or shutoffs; however, readable traffic makes it easier to learn about the system and weakens confidence in a safety-related service.

- Guest safety: hidden or delayed leak and pressure problems could affect rooms, public areas, the pool/spa wing, kitchen, or laundry.
- Operations: a monitoring outage or false information could slow engineering response and increase water damage or service disruption.
- Reputation: guests expect connected hotel systems to be protected, especially when a failure could affect access to rooms or essential services.

After protection

With TLS on, the eavesdropping attempt was rejected and the five transmitted readings were not exposed to the listening terminal. A connection using the correct trusted certificate succeeded, while a connection using the wrong certificate authority failed with a certificate-verification error.

One important gap remains: the system also connected successfully when certificate verification was disabled. Encryption alone seals the envelope, but verification checks the recipient's ID. If that check can be bypassed, the hotel cannot be sure it is talking to a trusted device. Production settings must therefore prevent 'no verification' connections.

PERFORMANCE IMPACT

The key question for hotel operations: does protection delay an alert when a pipe leaks or pressure changes?

Measure	TLS off	TLS on	Plain-language result
Average delay	50.88 ms	50.98 ms	+0.10 ms (0.197%): not noticeable
Fastest reading	0.62 ms	0.74 ms	+0.12 ms
Slowest reading	101.17 ms	101.21 ms	+0.04 ms

The bottom line: TLS added one tenth of one millisecond to the average reading. That is about three thousand times shorter than a typical 300-millisecond blink. Staff and guests would not notice it, and the slowest protected reading was 101.21 milliseconds - just over one tenth of a second.

TESTING EVIDENCE

We ran four tests, each framed around a question hotel management would reasonably ask.

1. Can someone on the network see the sensor readings?

Before TLS, the water-monitoring traffic was readable. With TLS on, the same listening attempt was refused and exposed no sensor readings. During that attempt, the system sent five readings - 82.5, 83.5, 84.5, 85.5, and 86.5 PSI - but the listening terminal could not read them. This shows that TLS blocked this eavesdropping attempt.

2. Does the system reject an untrusted connection?

Three connection checks were performed. The correct certificate connected successfully. A certificate signed by the wrong authority failed with the message 'certificate verify failed.' However, a connection with verification disabled succeeded. The first two results show the security control works when used correctly; the third shows why the hotel must lock the setting so verification cannot be turned off.

3. Does protection slow down readings?

Average delivery time was 50.88 milliseconds without TLS and 50.98 milliseconds with TLS. The measured increase was 0.10 milliseconds, equal to 0.197%. Minimum latency changed from 0.62 to 0.74 milliseconds, and maximum latency changed from 101.17 to 101.21 milliseconds. This is a measurable difference, but not one people would notice in hotel operations.

4. Can the protected system handle a crisis?

The system was tested at four message rates. Every rate succeeded both before and after TLS:

Operating level	Message rate	TLS off	TLS on
Normal	10/sec	SUCCESS	SUCCESS
Moderate	25/sec	SUCCESS	SUCCESS
Emergency	50/sec	SUCCESS	SUCCESS
Beyond requirement	100/sec	SUCCESS	SUCCESS

The protected system therefore met the full 50-message-per-second emergency test and still succeeded at 100 messages per second. The test found no failure or degradation at any tested rate.

WHAT THE TESTS DO - AND DO NOT - PROVE

These results are strong evidence for this test setup. They do not yet prove performance across every hotel floor, during poor Wi-Fi, after repeated reconnects, or during a real equipment failure. Published research on the same type of sensor messaging likewise finds that the performance cost depends on the network, hardware, settings, and reconnect behavior. A controlled hotel pilot is therefore the right final check before full deployment.

RECOMMENDATION

Approve TLS deployment now, with one condition: certificate verification must be mandatory on every sensor, service, and monitoring dashboard.

This decision closes the demonstrated readable-data exposure while adding only 0.10 milliseconds of average delay. Capacity remained successful at twice the tested emergency rate. The operational cost of this protection is therefore very small compared with the possible cost of exposed or disrupted hotel systems.

The risk is real in hospitality. A 2024 cyberattack at Omni Hotels disrupted reservations and other hotel functions, illustrating how a technical incident can quickly become a guest-service problem. IBM's 2024 study placed the global average cost of a data breach at \$4.88 million and reported that 70% of studied organizations experienced significant or moderate operational disruption. These are industry benchmarks, not a forecast of Grand Marina's loss, but they show why preventive controls matter.

NEXT STEPS

- 1. Close the verification gap before launch:** Remove or disable every option that allows a connection without certificate verification. Confirm that correct credentials succeed, the wrong authority fails, and no-verification attempts fail.
- 2. Give each device its own trusted identity:** Issue separate credentials to each monitoring device and service. Keep an inventory, set renewal dates, and create a way to cancel one device's access without affecting the rest of the hotel.
- 3. Separate guest Wi-Fi from water-monitoring traffic:** Place sensors, the central monitoring server, and the dashboard on a restricted network. Guest devices should have no direct path to the water system.
- 4. Pilot under real hotel conditions:** Repeat the four tests across the Main Building, Pool/Spa Wing, and Kitchen/Laundry. Include weak Wi-Fi, device restarts, repeated reconnects, and the 50-message-per-second emergency rate. Record message loss as well as delay.
- 5. Prepare operations for a failure:** Alert engineering staff when a device disconnects, a certificate expires, or readings stop. Document a manual response for leaks, pressure anomalies, and emergency shutoff if the monitoring system is unavailable.
- 6. Keep evidence and review it regularly:** Store the test results, approved settings, device inventory, and incident contacts. Re-test after major network, software, or device changes.

SOURCES AND EVIDENCE

- Grand Marina Hotel TLS Security Experiment Worksheet, July 26, 2026
- [IBM, Cost of a Data Breach Report 2024](#)
- [Cybersecurity Dive, Omni Hotels & Resorts hit by cyberattack, April 2024](#)
- [Gentile et al., A Network Performance Analysis of MQTT Security, Applied Sciences, 2024](#)