SECURITY ASSESSMENT

Grand Marina Hotel Water Monitoring System

Prepared for: Marcus Webb, General Manager

Prepared by: Mubarak Adam

Date: November 2, 2026

EXECUTIVE SUMMARY

I recommend moving Grand Marina's water-monitoring system to encrypted connections, with device-access controls added before full rollout. In four tests, encryption blocked the unprotected monitoring attempt, added only 0.04 milliseconds to average message time, and maintained successful publishing at normal and emergency loads. This protects operational information without a meaningful slowdown in our tested setup.

SECURITY RISKS ADDRESSED

Before Security:

Before encryption, someone able to connect to the hotel's unsecured message service could read water sensor updates as they arrived. In our test, a basic subscriber immediately saw all five readings, including a sensor identifier, water pressure, flow rate and time. Exposed readings could reveal building operations and help someone monitor sensitive equipment activity. A disruption or misuse of this information could interfere with leak detection, create costly maintenance delays and undermine confidence in the hotel's ability to protect its property and guests.

After Security:

With encryption turned on, our unencrypted listener was rejected and saw no readings. A device using the correct trusted certificate information connected, while one using a false certificate authority was rejected. However, an application that disabled certificate checking still connected, and our broker did not require each device to prove its own identity. Encryption protects readings as they travel, but stronger device sign in rules are still needed before claiming unauthorized access is fully prevented.

PERFORMANCE IMPACT

What We Measured	Before Security	After Security	Verdict
How fast readings arrive	0.05232 seconds	0.05236 seconds	No meaningful change in test
Message publishing rate (tested load)	Up to 96.8/sec	Up to 96.8/sec	Emergency requirement covered

The average message took 0.05232 seconds without encryption and 0.05236 seconds with it, an increase of just 0.00004 seconds (0.08%), far shorter than an eye blink. Across our 30 second load tests, secured publishing kept pace with unsecured publishing; longer deployments and poor network conditions still need separate checks.

TESTING EVIDENCE

We ran four security tests on the water monitoring system:

1. Can outsiders see sensor data?

Before security, an unprotected listener read all five test messages in full. After security, repeating that unencrypted connection returned “Error: Protocol error,” and no messages were visible to that listener. This demonstrates protection against the specific unencrypted connection we tested; it is not proof that all network threats are eliminated.

2. Does the system block unauthorized connections?

A connection using the correct trusted certificate succeeded, while a connection using an incorrect certificate authority failed with a certificate verification error. When the client deliberately skipped checking the broker’s certificate, it connected anyway. That last result shows why identity checks must stay enabled, and why unique device credentials and access restrictions should be added.

3. Does security slow things down?

The average time increased from 52.32 to 52.36 milliseconds: only 0.04 milliseconds more per reading, or about 0.08%. That difference is imperceptible to a person and was negligible in this test. Published research also cautions that reconnecting devices and weak networks can show higher encryption costs, so these lab results are not a universal guarantee.

4. Can the system handle a crisis?

We ran eight 30 second tests, with security on and off at targets of 10, 25, 50 and 100 messages per second. Every run reported SUCCESS, 100% publishing success and zero errors. With security on, observed rates were 9.7, 24.2, 48.4 and 96.8 messages per second, matching the unsecured runs at the reported precision. That covers the hotel’s estimated normal demand of 10 readings per second and emergency demand of 50. These results measure successful publishing, not independently verified receipt by every dashboard.

RECOMMENDATION

Approve encryption for the hotel’s water monitoring system but make the production launch conditional on strong device authentication, restricted access and operational testing. All five readings were exposed before security, whereas the unencrypted listener was blocked after it. Our measured additional delay was only 0.00004 seconds, and every simulated load test reported success. The importance of security is not hypothetical: Marriott confirmed a 18.4 million UK privacy regulator fine following its earlier guest data incident. That was a different type of breach, not an estimated loss for Grand Marina, but it illustrates how weaknesses can lead to substantial consequences. Our findings support deploying protection without sacrificing the monitoring performance observed in these tests. Source: Marriott International, October 30, 2020 (marriott.gcs-web.com/node/30631).

NEXT STEPS

1. Enable encrypted monitoring for the hotel’s sensor network after a controlled deployment check. Disable the unsecured connection, install and validate trusted server certificates, and confirm that every intended sensor and dashboard reconnects successfully.

2. Require each sensor and dashboard to authenticate and limit which readings or commands it may access. Keep certificate verification enabled, assign device-specific credentials, and test that an unapproved device is denied access.

3. Monitor the rollout and rehearse failures. Alert staff about disconnected sensors and expiring certificates; test emergency traffic, message delivery and reconnection on actual hotel networks. Record the results for ongoing maintenance and management review.