

# SECURITY ASSESSMENT

## Grand Marina Hotel Water Monitoring System

**Prepared for:** Marcus Webb, General Manager

**Prepared by:** Aly Kane

**Date:** July 29,

---

### EXECUTIVE SUMMARY

Grand marina should deploy TLS encryption with certificate validation enabled across its water -monitoring system Testing showed that encryption prevented sensor readings from being viewed through an unsecured connection and rejected connections using an incorrect cert while adding up to no measurable delay in the local performance test

### SECURITY RISKS ADDRESSED

#### Before Security:

Without encryption, anyone with access to the hotel network could subscribe to the sensor-data feed and view water-pressure, flowrate, device, and location information in plain text. This info could help ana tracker monitor hotel operations, identify abnormal conditions, or interfere with the system affecting the company overall.

#### After Security:

With encryption enabled unencrypted subscribers couldn't connect or view the sensor messages a client using the wrong cert fails verification protecting sensor readings while they travel across the network and helps devices confirm they are communicating with legitimate Grand Marina staff/server. Cert validation must stay, testing showed disabling allowed a client connect making the server vulnerable for a fake server or man-in-the-middle-attack

## PERFORMANCE IMPACT

| What We Measured         | Before Security   | After Security     | Verdict                |
|--------------------------|-------------------|--------------------|------------------------|
| How fast readings arrive | [_.00013] seconds | [_.00013_] seconds | No slowdown measurable |
| How many sensors at once | [_100] per sec    | [_100] per sec     | Yes                    |

The readings arrived in about 13 ten thousandths of a second far faster than a person could even notice. Based on the displayed averages encryption added 0% measurable latency, meaning hotel staff would not experience any visible delay when monitoring water conditions.

## TESTING EVIDENCE

We ran four security tests on the water monitoring system:

### 1. Can outsiders see sensor data?

Prior to security being enabled a subscriber on the network could connect and view the sensor readings. With the encryption however the unencrypted connection will fail with a protocol error.

### 2. Does the system block unauthorized connections?

A client using the correct certificate authority connected successfully. A client using the wrong certificate authroitty failed cert verification and couldnot publish data. Separate test showed that a client could connect when cert verification was deliberately disabled. Although the connection succeeded, this configuration is dangerous because the client could accept a fraudulent server. Cert verfication should therefore always remain enabled.

### 3. Does security slow things down?

.13-.13/.13 x 100 = 0% it slows down by 0% so no, not to a human it doesn't slow down.

### 4. Can the system handle a crisis?

The system was tested at:

- 10 messages per second for normal operation
- 25 messages per second for moderate load
- 50 messages per second for emergency operation
- 100 messages per second beyond normal requirements

The system remained **[SUCCESS]** at 10 messages per second, **[SUCCESS]** at 25 messages per second, **[SUCCESS]** at 50 messages per second, and **[SUCCESS]** at 100 messages per second with encryption enabled. The highest successful encrypted rate was 3000 **messages per second**, meaning the system **[did/did not]** meet Grand Marina's emergency-load requirements.

## RECOMMENDATION

1. Grand Marina should deploy TLS encryption with certificate validation enabled. The testing demonstrated that encryption prevents sensor information from being read through an unsecured connection and that certificate validation rejects connections that cannot verify the legitimate server. The security benefits significantly outweigh the performance cost. The test showed no measurable latency increase, and readings still arrived almost instantly. Grand Marina should never disable certificate verification, should protect its certificate and private-key files, and should periodically renew certificates before they expire.