# DEFENSE COMPARISON REPORT

## Grand Marina Hotel - HYDROLOGIC Water Monitoring System

**Prepared for:** Marcus Webb, General Manager, and Sandra, Insurance Auditor
**Prepared by:** Sok Leng Chan, Junior Cybersecurity Analyst
**Date:** August 3, 2026
**Decision:** Deploy all three replay protections on every hotel water-monitoring device

## 1. EXECUTIVE SUMMARY

Grand Marina's water-monitoring system could not tell a new instruction or sensor reading from a legitimate message recorded and reused later. We tested four defense configurations against immediate, delayed, and altered replays; the single-defense setups left gaps, while all three protections together rejected 100% of the tested attacks. The hotel should deploy all three protections across every HYDROLOGIC device and monitor rejected messages for signs of suspicious activity.

## 2. THE PROBLEM: A REAL MESSAGE USED AT THE WRONG TIME

A replay attack is like someone recording a garage-door opener signal and playing it back later. The signal is genuine, so the door responds - but the command is no longer authorized for that moment. The same problem can affect water commands, sensor readings, and usage events even when the network connection itself is encrypted.

- **Phantom shutoff.** An attacker replays a legitimate maintenance shutoff after service has been restored, stopping water again in guest rooms, the kitchen, laundry, or pool/spa area and creating an avoidable operations emergency.
- **Stale reading.** A previously normal pressure or flow reading is played back while a real leak or pressure problem develops, causing the dashboard to look safe and delaying the engineering team's response.
- **Repeated billing event.** A legitimate high-use or overage message is replayed several times, creating false charges and a dispute that could affect the hotel's finances and insurer confidence.

## 3. DEFENSES TESTED

- **Message freshness check (timestamp validation).** Each message is accepted only during its approved time window, like a parking ticket that expires after its valid period.
- **Message numbering (sequence counter).** Each message receives a number that can be accepted only once, like a concert ticket that cannot be scanned a second time.
- **Message signing (HMAC).** Each message carries a tamper-evident seal, like a wax seal on a letter, so any change to the message breaks the seal and triggers rejection.

## 4. TESTING RESULTS

We tested four defense configurations against three replay types, with five attack attempts in each combination. That produced 12 test combinations and 60 total replay attempts. A 100% rejection rate means all five attempts in that combination were blocked.

| Protection setup | Immediate replay (within 5 sec) | Delayed replay (after 60 sec) | Altered replay (tampered data) |
|---|---|---|---|
| No protection | 0% | 0% | 0% |
| Freshness check only | 0% | 100% | 0% |
| Message numbering only | 100% | 100% | 0% |
| **All three protections** | 100% | 100% | 100% |

The chart shows the same pattern at a glance: partial defenses stop only selected replay types, while the combined setup reaches 100% across all three tested categories.

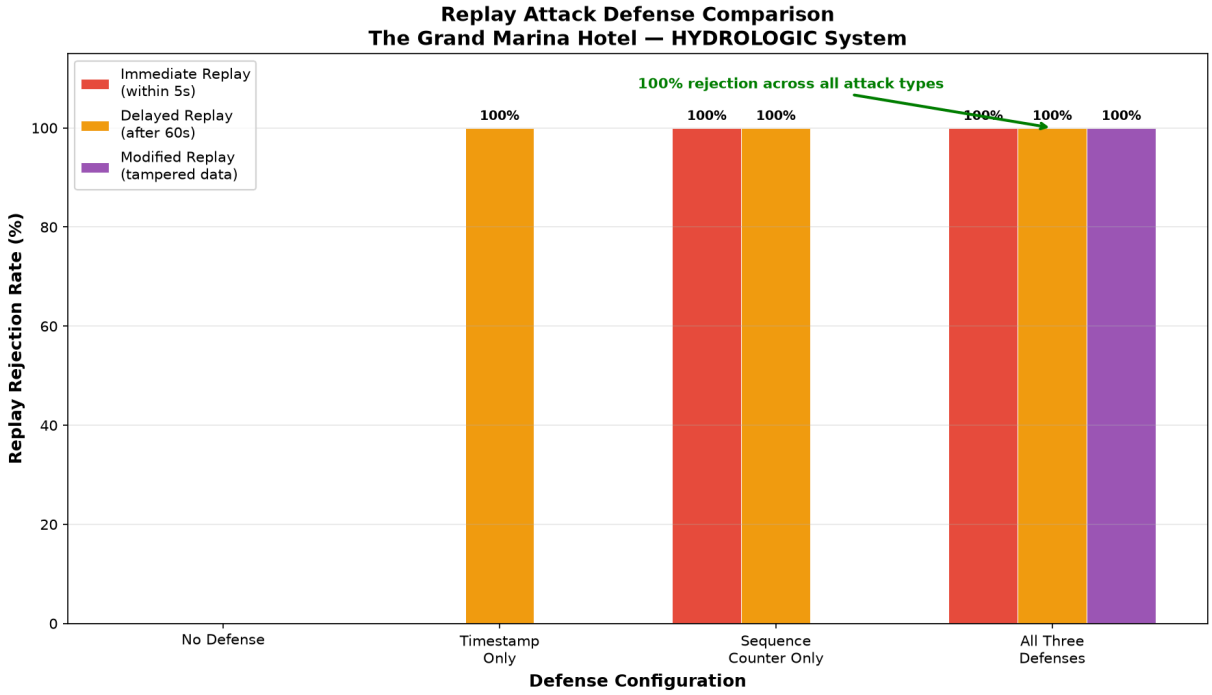


*Figure 1. Replay-attack rejection rate by protection setup.*

**Key finding:** The freshness check missed immediate and altered replays, and message numbering missed altered replays. All three protections together rejected 15 of 15 attempts in that setup - 100% of the tested attacks. This result applies to the replay scenarios tested; it is not a guarantee against every possible cyberattack.

## 5. RECOMMENDATION

**Deploy all three protections on every Grand Marina HYDROLOGIC device.** The evidence supports a layered approach because each check answers a different question: Is this message recent? Has its number already been used? Has its content been changed?

- **Complete tested coverage.** The two single-defense setups left known gaps, but the combined setup rejected all 15 immediate, delayed, and altered replay attempts directed at it.
- **Negligible performance impact.** The three checks together take less than one millisecond per message, compared with the five-second publishing interval. That is less than 0.02% of the time between readings and will not be noticeable in hotel operations.
- **Ready to deploy.** The protected sending and receiving programs (publisher and subscriber) are already built and tested; deployment means replacing the current scripts with the defended versions, followed by a controlled verification test at each location.

## 6. NEXT STEPS

1. **Deploy to all three hotel zones.** Replace the current scripts on the Main Building, Pool/Spa Wing, and Kitchen/Laundry devices, then confirm that normal messages still pass and replayed messages are rejected.
2. **Alert on rejected messages.** Notify the hotel technology or engineering team when messages fail the freshness, numbering, or signing checks because repeated failures may indicate an attack or a device problem.
3. **Create a simple security dashboard.** Show accepted and rejected messages by device and location so management can identify unusual activity without reading technical logs.

## 7. INDUSTRY REFERENCES

- **AWS messaging practice.** AWS IoT Core warns that messages can be delivered more than once, while Amazon SQS FIFO uses a unique tracking number (deduplication ID) to prevent repeat processing. Grand Marina's one-use message numbering applies the same practical idea inside each hotel message. AWS IoT Core guidance
- **IEC 62443.** ISA/IEC 62443-3-3 includes system-integrity and communication-integrity requirements; message signing supports this goal by detecting changed content before it reaches operational equipment.
- **MQTT version 5.** The OASIS MQTT v5 standard lets a publisher set a message-expiry interval, after which the server must discard an undelivered message. This follows the same freshness principle, although Grand Marina still needs application-level numbering and signing to cover the tested replay gaps.
- **Water-sector operating practice.** EPA water cybersecurity guidance recommends collecting protected security logs and maintaining an incident-response plan. Monitoring rejected messages and defining an escalation path align the deployment with those practices.