Under the patronage of HRH Prince Khalid Al-Faisal
Advisor to the Custodian of the Two Holy Mosques & Governor of Makkah Region

المؤتمر الدولي الثاني والعشرون لإدارة الأصول والمرافق والصيانة

The 22nd International Asset, Facility & Maintenance Management Conference

Digitization - Excellence - Sustainability

Zero Trust Architecture Application in Maintenance Operations: A Cybersecurity Perspective

Tamer Hellah
CEO, Happy Life Limited, UK

26-28 January 2025
The Ritz-Carlton Jeddah, Kingdom of Saudi Arabia

www.omaintec.com #OmaintecConf

An Intiative By
OMAINTEC
المجلس العربي لإدارة الأصول والمرافق والصيانة
Arab Asset, Facility and Maintenance Management Council

Organized by
TSG | EXICON.
The Specialist Group • شركة مجموعة المختص

Background

Digitization is a double-edged sword

Digitization brings operational efficiency and sustainability, but it introduces significant cybersecurity risks, especially in maintenance operations

Emerging Technologies in Maintenance

- Internet of Things (IoT)
- Predictive Maintenance & AI
- Digital Twins
- Cloud Computing

Challenges

Increased vulnerabilities in maintenance environments

Need for robust cybersecurity strategies

Understanding Zero Trust Architecture (ZTA)

ZTA is a security framework that requires continuous validation of every access attempt, minimising implicit trust within networks

Core principles of ZTA:

- **Identity verification** (always confirm who is accessing your network)
- **Continuous monitoring** (Keep an eye on the network)
- **Data encryption** (make sure data is protected when it’s stored and shared)

OMAINTEC CONFERENCE EXHIBITION 2025 FM

Why Zero Trust Architecture?

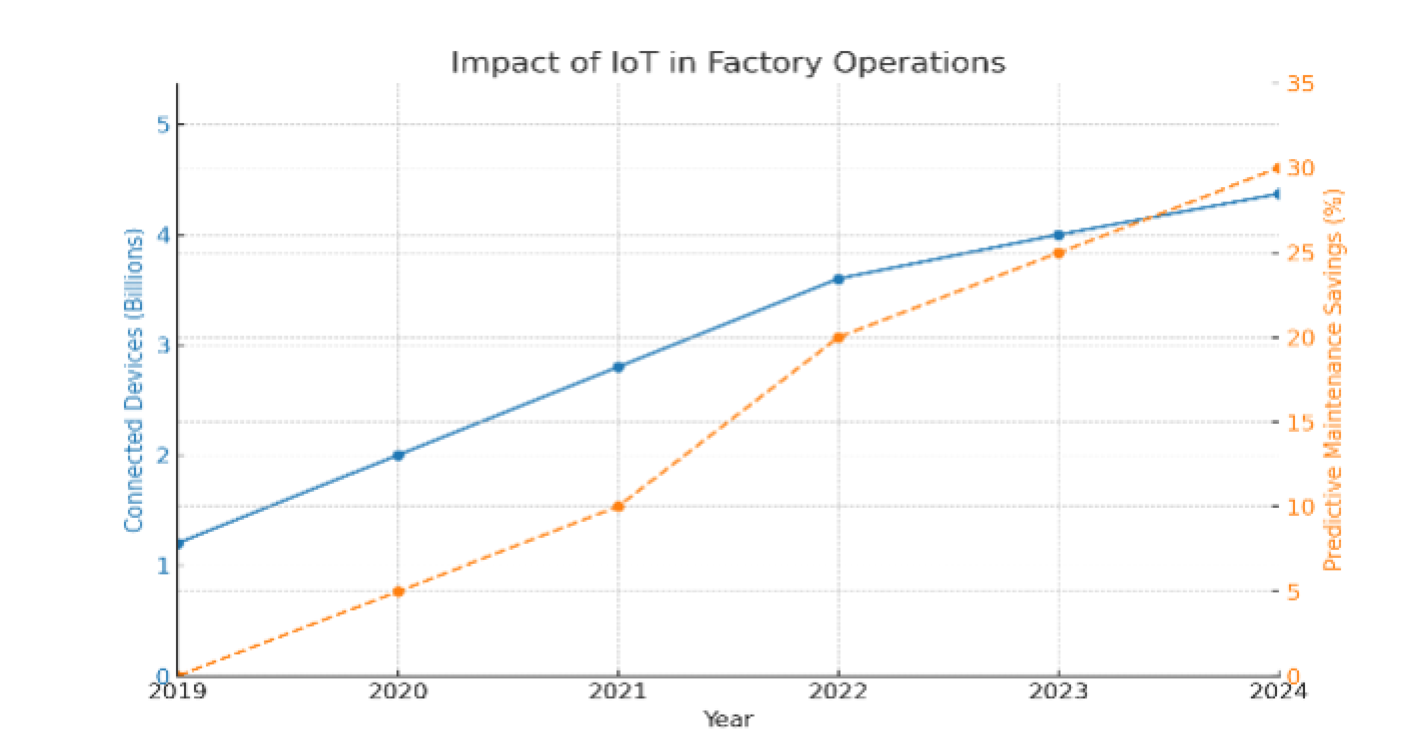
Evolving Threat Landscape
Attackers exploit traditional security gaps and assumptions
A cyber incident is predicted to cause damages exceeding $25 billion by 2025

Remote & Hybrid Work
Organizations need a flexible approach that adapts to users working from anywhere

Data Protection & Compliance
Stricter regulations and privacy requirements demand robust security measures

Reduced Attack Surface
Limiting trust reduces risks at every point of the network

Digitization in Maintenance Operations



IoT in Maintenance

Collects real-time data for critical insights

Uses data analytics to anticipate equipment failures

Used for simulation, monitoring, and optimization

Cybersecurity Risks in Digitized Maintenance

IoT Vulnerabilities

- 98% of IoT traffic is unencrypted
- Devices often lack robust security features

Case Study - Mirai Botnet Attack

- Mirai Botnet exploited vulnerabilities in IoT devices like IP cameras, routers, and DVRs by using their weak security to launch massive Distributed Denial of Service (DDoS) attacks.

Introducing the IBM Maximo Case Study

Happy Life Limited and **Smart System Company** implemented Zero Trust Architecture using IBM Maximo

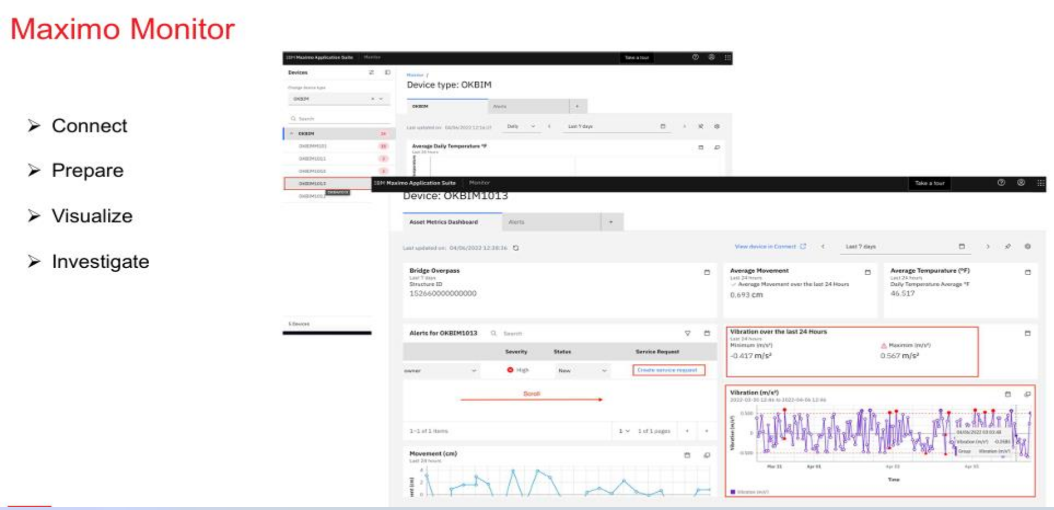
OMAINTEC FM CONFERENCE EXHIBITION 2025

Overview of IBM Maximo Asset Management

An Enterprise Asset Management (EAM) system

Facilitates predictive maintenance and IoT integration

Supports the implementation of Zero Trust principles



Challenges Faced Before Implementation

Legacy Systems Vulnerabilities	Outdated maintenance platforms were prone to cyber threats
Lack of Real-Time Monitoring	Difficulty in promptly detecting unauthorized access
Data Silos	Inefficient data sharing across departments hindered operations
Compliance Issues	Existing systems did not meet new cybersecurity regulations

Need for Change

A robust, secure, and efficient maintenance system was essential

Implementing Zero Trust with IBM Maximo

Identity Verification

Multi-Factor Authentication (MFA)

Implemented for all users accessing IBM Maximo

Role-Based Access Control

Users were granted permissions based on roles and responsibilities

Defined strict firewall rules for traffic

Configured firewalls to allow only specific ports and protocols (e.g., TCP/443 for HTTPS) between segments

Implementing Zero Trust with IBM Maximo

We divided our network into smaller, secure zones

Maximo servers and databases were isolated from other systems (e.g., IoT devices, cloud services)

virtual LANs (VLANs) or software-defined networking (SDN) may be used to create segmented zones

Necessary communication between zones was allowed using strict firewall rules

All communication to and from Maximo was encrypted

TLS encryption was used for all REST API calls and web interfaces

Endpoint security was strengthened

Endpoint protection software was installed

IoT devices and gateways had strong authentication

Endpoint detection and response (EDR) tools were used to monitor and secure edge devices

Lessons Learned and Best Practices

Stakeholder Engagement

Involving all stakeholders early ensured alignment and support

Staff Training and Awareness

Continuous training on new systems and cybersecurity practices was vital

Phased Implementation

Starting with a pilot program allowed for testing and adjustments

Collaboration Between IT and Operations

Bridging the gap between departments enhanced overall effectiveness

Regular System Audits

Ongoing assessments ensured sustained security and performance

HAPPY LIFE
SECURE YOUR DIGITAL LIFE WITH EXPERTS

OMAINTEC 2025 CONFERENCE EXHIBITION FM

Next-Gen EAM+: Innovating Beyond Security

Core Features of Next-Gen EAM+

1. Cognitive Digital Twins

Adaptive Intelligence

Digital twins learn from past actions via reinforcement learning, continuously enhancing performance

Context Awareness

Incorporate external factors (e.g., climate data, market conditions) to optimize operations over time

2. Quantum-Resistant Cryptography

Post-Quantum Security: Employ NIST-approved quantum-resistant algorithms to protect long-term data integrity

Future-Proofing: Ensure secure data and communications against emerging quantum computing threats

Next-Gen EAM+: Innovating Beyond Security

4. Holographic and Spatial Computing Interfaces

Hands-Free Interaction: Manipulate asset models in mid-air using holographic displays.
Spatial Mapping: Integrate with advanced data visualization platforms for easier understanding and action on complex data

5. Bio-Authenticated Access Controls

Continuous Verification: Seamlessly authenticate using biometrics and behavioural cues
Reduced Credential Theft: Minimize unauthorized access, upholding Zero-Trust Architecture principles

6. Intelligent Edge Hardware

Local Inference: Deploy AI chips on-site for immediate anomaly detection
Reduced Latency: Ensure real-time responses without relying on cloud processing

7. Nanotechnology-Based Sensors

Ultra-Sensitive Measurements: Detect micro-level changes in materials, stress, or corrosion
Extended Asset Lifespan: Prevent catastrophic failures through early detection

OMAINTEC CONFERENCE EXHIBITION 2025 FM

Discussion

Contact Information:

Tamer Hellah

Email: cybersec@happylifelimited.co.uk

https://www.linkedin.com/in/tamer-hellah/

HAPPY LIFE
SECURE YOUR DIGITAL LIFE WITH EXPERTS

SmartSystem
PARTNER IN PERFOMANCE

Under the patronage of **HRH Prince Khalid Al-Faisal**
Advisor to the Custodian of the Two Holy Mosques & Governor I of Makkah Region

OMAINTEC CONFERENCE 2025 EXHIBITION FM

المؤتمر الدولي الثاني والعشرون لإدارة الأصول والمرافق والصيانة

The 22nd International Asset, Facility & Maintenance Management Conference

Digitization - Excellence - Sustainability

THANK YOU!

26-28 January 2025
The Ritz-Carlton Jeddah, Kingdom of Saudi Arabia

www.omaintec.com #OmaintecConf

HAPPY LIFE

SmartSystem
PARTNER IN PERFOMANCE

An Intiative By
OMAINTEC
المجلس العربي لإدارة الأصول والمرافق والصيانة
Arab Asset, Facility and Maintenance Management Council

Organized by
TSG | EXICON.
The Specialist Group • شركة مجموعة المختص