# Strategic Analysis of the ICS+ Product Architecture: A Scope of Work Report

## I. Executive Summary: An Integrated Solution for a New Era in Fire Protection

The ICS+ project, also known commercially as Marioff's HI-FOG Smart, represents a strategic evolution in fire protection systems, transitioning from a product-centric business model to one centered on services and data-driven intelligence.1 This initiative positions Marioff and its sister company, Autronica, as pioneers in an increasingly digitized industrial landscape. The solution is designed to deliver "smart alerts, real-time monitoring, and centralized control" by leveraging Internet of Things (IoT) technology to provide continuous visibility into the status and performance of high-pressure water mist and fire detection systems.1

This digital transformation is a significant move in a highly competitive market where major players like Johnson Controls, Carrier, Siemens, and Honeywell dominate the fire protection sector.2 By offering a comprehensive, end-to-end solution that goes beyond a one-time product sale, ICS+ enables a new business model centered on lifetime services and predictive maintenance.3 The foundation of this system is a multi-layered architecture that includes:

* **Perception Layer:** The Marioff HI-FOG pumps (EPU and LPU) and Autronica fire alarm panels (AutroPrime and AutroSafe) serve as the physical data sources.5
* **Edge & Connectivity Layer:** The Advantech ARK-1221L and Teltonika TRB-140 devices act as the Edge and Gateway, respectively, processing data at the source and providing secure connectivity.7
* **Data Processing & Cloud Layer:** The AWS ecosystem, specifically AWS Timestream and DynamoDB, provides the backend infrastructure for data ingestion, storage, and advanced analytics.9
* **Application Layer:** A user-facing web and mobile platform offers a central point for real-time monitoring, user management, and remote device configuration.11

A thorough analysis of this architecture reveals that the development of the Edge and Gateway firmware is a mission-critical component that must not only manage data transmission but also act as a sophisticated protocol converter and security enforcer. Furthermore, the selection of a hybrid cloud database strategy—utilizing both AWS Timestream and DynamoDB—is a deliberate and high-performance architectural choice. Finally, the project's long-term success is intrinsically linked to the strategic use of native device management tools, such as Teltonika's Remote Management System (RMS) and Advantech's WISE-DeviceOn, which are essential for scalable and secure fleet management.

## II. The ICS+ Solution: A Multi-Layered Industrial IoT Architecture

### 2.1. Product Definition and Market Context

The ICS+ solution is a collaborative, unified offering from Marioff Corporation Oy and Autronica, two global leaders in industrial fire safety. Both companies were previously part of Carrier Global's industrial fire business, which was recently acquired by Sentinel Capital Partners for $1.4 billion to form a new platform named Spectrum Safety Solutions.12 This strategic consolidation underscores the importance of an integrated, IoT-enabled product portfolio.

For Marioff's high-pressure water mist systems, the IoT solution is branded as HI-FOG Smart.1 It is described as an "IoT-enabled fire protection upgrade" that enhances the company's decades of innovation by providing real-time visibility, smarter maintenance, and centralized system control.1 The system connects seamlessly to a customer's existing fire protection infrastructure to provide data insights for predictive maintenance and to support remote, centralized management of multiple sites and systems from a single platform.1

This comprehensive, IoT-centric approach aligns with the broader trend of Industrial IoT (IIoT) architecture, which aims to collect vast amounts of data from the factory floor or operational sites to turn it into actionable insights for business decision-making.13

### 2.2. The Layered System Framework

The ICS+ architecture is a classic example of an edge-to-cloud IIoT framework, designed to ensure efficient and secure data collection, transmission, and processing.14 The system is conceptually structured into four distinct, yet interconnected, layers.

* **Layer 1: Industrial Devices (The Perception Layer):** This foundational layer comprises the physical hardware that interacts with the real world, detecting fires and initiating suppression. This includes the Marioff HI-FOG pump units, such as the EPU and LPU models, and the Autronica fire detection panels like AutroSafe.5 These devices generate raw data on their status, events, and performance.
* **Layer 2: Edge & Gateway (The Connectivity Layer):** The Advantech ARK-1221L (Marioff Edge) and Teltonika TRB-140 (Autronica Gateway) act as the intermediary between the industrial devices and the cloud [User Query]. This layer is responsible for collecting data from the physical devices, performing initial processing or filtering at the edge of the network, and establishing a secure communication channel to the cloud infrastructure.13
* **Layer 3: Cloud Infrastructure (The Data Processing Layer):** The AWS cloud serves as the centralized hub for advanced data processing and storage.13 This includes the ingestion of telemetry, events, and logs into purpose-built databases like AWS Timestream and DynamoDB [User Query]. This layer provides the necessary computational power to perform complex analytics, generate reports, and support the application's features.9
* **Layer 4: Monitoring Platform (The Application Layer):** This is the user-facing interface, accessible via a web or mobile platform, that presents the processed data in a clear and concise manner [User Query]. The platform provides real-time monitoring dashboards, visualization tools, and controls for user management and device configuration, enabling end-users to gain a full view of their fire safety systems from anywhere.11

### 2.3. The Industrial IoT Integration Challenge

The core architectural challenge of the ICS+ project is the critical task of bridging the gap between two distinct technology domains: the safety-critical Operational Technology (OT) of industrial fire systems and the flexible, scalable Information Technology (IT) of a public cloud. Traditional fire and suppression systems, such as the AutroSafe and HI-FOG units, are designed to be highly reliable and often operate on proprietary, purpose-built communication protocols and redundant networks, like Autronica's AutroNet and AutroFieldBus.6 This closed-loop design is fundamental to their functionality and to meeting stringent safety and certification requirements.6

The goal of the ICS+ solution, however, is to extract data from these closed systems and transmit it securely to an open, public cloud environment. The Edge and Gateway devices are not merely hardware components; they are the crucial translation layer that makes this possible. The Advantech ARK-1221L and Teltonika TRB-140 devices must be capable of communicating with the industrial systems using their native languages, whether through standard interfaces like RS-232/422/485 or industry-specific protocols such as Modbus and DNP3.7 Simultaneously, they must securely publish this data to the AWS cloud using a protocol like MQTT, which is the industry standard for lightweight, bi-directional IoT communication.18

Consequently, the firmware developed for these devices is far more than a simple data forwarder. It must function as a sophisticated protocol converter, translating data formats and network semantics. It must also perform initial data processing at the edge, a capability that reduces the volume of data sent to the cloud.13 This local processing can include filtering noise, performing anomaly detection, or even pre-analyzing data to accelerate decision-making, which is critical in time-sensitive industrial settings.20 Finally, the firmware is a security enforcer, responsible for authenticating devices and encrypting data before it leaves the on-site network, thus linking the secure world of OT with the broad, open landscape of IT. This multi-faceted role highlights the firmware as a mission-critical component of the entire ICS+ system.

## III. Component-Level Analysis: The Industrial Edge

### 3.1. The Fire Protection and Detection Layer

The ICS+ solution integrates two primary systems at the physical layer: Marioff's HI-FOG water mist fire suppression and Autronica's fire detection panels.

The Marioff HI-FOG system is a well-established fire protection solution that uses high-pressure water mist to control and suppress fires with significantly less water damage compared to conventional sprinkler systems.3 The system's "robust and reliable heart" is its pump units, which are available in models such as the Land Pump Unit (LPU) and Electric Pump Unit (EPU).5 The EPU includes an "advanced control system with frequency converter" that precisely adjusts pressure and flow, while its user-friendly interface allows for the monitoring of system status, alarms, and event logs.5 The EPU is a key source of operational data for the ICS+ system, transmitting information about its status and performance to the Edge device [User Query].

The Autronica fire alarm system, built around the AutroSafe panels, provides the core fire detection functionality [User Query]. The panels act as the "brain" of the fire alarm system, monitoring all inputs and controlling outputs.22 These systems are designed for maximum dependability and are built with redundant communication features to ensure that alarms are never lost.6 Communication is a mix of proprietary protocols, such as AutroCom, AutroFieldBus, and AUTROLON, as well as standard industrial protocols like MODBUS, NMEA-0183, and ESPA 4.4.4.6 The system's ability to communicate with devices across a dual-path, high-speed Ethernet network (AutroNet) and use redundant control units (AutroKeepers) provides a foundation of security and reliability that the ICS+ solution can build upon.6

### 3.2. The Edge and Gateway Hardware

The project is built on two distinct hardware platforms that serve different roles within the architecture.

The **Advantech ARK-1221L** serves as the Marioff Edge device [User Query]. It is a compact, fanless industrial embedded PC designed for demanding environments.7 Its rugged construction, including a wide operating temperature range (-40 to 60 °C), and wide input voltage range (12 to 28 VDC), makes it ideal for installation in industrial cabinets.7 The ARK-1221L is powered by an Intel Atom x6413E quad-core processor and can support up to 32GB of DDR4 memory, providing the necessary processing power for complex applications at the edge.7 With a variety of industrial I/O ports, including two RS-232/422/485 serial ports and two 2.5GbE network ports, it is well-equipped to interface with the Marioff pump units and communicate with the cloud.7

The **Teltonika TRB-140** is the Autronica Gateway device [User Query]. Described as an "ultra-small, lightweight, and energy-efficient industrial gateway," it is designed for projects where a single gadget requires reliable internet connectivity.8 The device features mission-critical LTE Cat 4 connectivity and a Gigabit Ethernet interface.8 It runs on a low-power ARM Cortex-A7 CPU with 128MB of RAM and 512MB of flash storage, which is sufficient for its role as a data-forwarding gateway.8 The TRB-140's compact design, aluminum housing, and wide operating temperature range (-40 to 75 °C) make it suitable for a variety of industrial applications.8 It is also compatible with industrial communication protocols such as Modbus and DNP3, enabling its integration with the Autronica systems.16

A side-by-side comparison of the two devices reveals their complementary roles within the ICS+ architecture. The Advantech ARK-1221L, with its powerful processor and extensive I/O, is suited for more computationally intensive tasks, while the Teltonika TRB-140 is optimized for reliable cellular connectivity in constrained environments.

**Table 1: Edge and Gateway Hardware Comparison**

| Feature | Advantech ARK-1221L (Marioff Edge) | Teltonika TRB-140 (Autronica Gateway) |
| --- | --- | --- |
| **Role in ICS+** | Marioff Edge Device (data processing) | Autronica Gateway (connectivity) |
| **Processor** | Intel Atom x6413E Quad-Core | ARM Cortex-A7 1.2 GHz |
| **Memory (RAM)** | Up to 32 GB DDR4 | 128 MB (50 MB user-space) |
| **Storage (Flash/HDD)** | mSATA, 2.5" SATA | 512 MB (200 MB user-space) |
| **Network Interfaces** | 2x 2.5GbE | LTE Cat 4, 1x GbE |
| **Industrial I/O** | 2x RS-232/422/485, CAN Bus | 1x Digital Input, 1x Digital Output |
| **Operating Temperature** | -40 to 60 °C | -40 to 75 °C |
| **Operating System** | Windows 10, Linux Ubuntu 20.04 | RutOS (OpenWrt-based Linux OS) |

## IV. The Firmware and On-Device Logic

### 4.1. Firmware Architecture

The firmware for the Edge and Gateway devices is described as a "package built of several components inside" [User Query]. The Teltonika TRB-140, for instance, runs on a custom operating system called RutOS, which is based on the OpenWrt Linux distribution.8 This provides a highly customizable Linux environment with support for languages such as Busybox shell, Lua, C, and C++.8 The Advantech ARK-1221L also supports a standard Linux distribution (Ubuntu 20.04), allowing for similar flexibility in software development.7 This open-source foundation is crucial as it enables the development of custom logic to handle data acquisition, protocol conversion, and secure communication with the cloud platform.

### 4.2. Containerization as a Strategic Choice

While the provided documentation does not explicitly mention containerization for these specific devices, the underlying operating systems and the nature of the project suggest that adopting a containerized firmware architecture is a strategic imperative. The modular composition of the firmware package, which consists of multiple components, is a natural fit for container-based solutions such as Docker or Lightweight Linux Containers (LXC).16

Traditional monolithic firmware images are difficult to manage and update, especially in geographically dispersed industrial deployments. A single change or bug fix requires a full firmware rebuild and a potentially lengthy over-the-air (OTA) update process. In contrast, a containerized approach allows the development team to isolate each component of the firmware—for example, the module that communicates with the Marioff EPU, the logic for the Autronica panel, and the AWS IoT Core client—into separate, portable containers.

This architectural decision offers several key benefits. It enhances **portability**, allowing the same logic to be deployed across different devices or environments.26 It improves

**scalability**, as individual components can be managed and updated independently without affecting the entire system.26 Furthermore, containerization significantly improves

**security** by providing inherent isolation between applications and the host operating system, which minimizes the security impact if one component is compromised.26 Finally, it increases

**efficiency and speed**, as only the specific container with updated logic needs to be deployed, greatly reducing the time and bandwidth required for OTA updates.26 This approach represents a modern, robust, and scalable way to manage complex IIoT firmware in mission-critical applications.

### 4.3. Firmware Management and OTA Updates

The long-term operational viability of the ICS+ solution depends on a robust remote management strategy. The Edge and Gateway devices come with native management systems that are crucial for simplified operations.

Teltonika's **Remote Management System (RMS)** provides a centralized, cloud-based platform for monitoring, configuring, and maintaining devices without the need for a public IP address.27 RMS supports Firmware Over-the-Air (FOTA) updates, allowing for a single device or an entire fleet to be updated simultaneously with minimal effort.8 New devices can be configured to automatically update to the latest firmware version as soon as they connect, which streamlines the onboarding process.29 The system also enables remote configuration, real-time device status monitoring, and event alerts, providing a single point of control for the entire network.27

Similarly, the Advantech ARK-1221L is compatible with Advantech's **WISE-DeviceOn** platform, which is designed for centralized device management.7 WISE-DeviceOn provides features such as zero-touch onboarding, real-time monitoring through a visualized dashboard, and remote control of device settings.32 It also enables OTA updates for firmware, drivers, and software, a critical capability for maintaining security and functionality in the field.32

The following table provides a comparison of the key features of these two systems.

**Table 2: Firmware Management Capabilities**

| Feature | Teltonika Remote Management System (RMS) | Advantech WISE-DeviceOn |
| --- | --- | --- |
| **Core Function** | Remote monitoring, configuration, and OTA updates for Teltonika and third-party devices | Centralized device management with zero-touch onboarding and OTA updates |
| **OTA Updates** | Supports FOTA, bulk updates, and automatic updates for new devices | Enables OTA updates for firmware, drivers, and software |
| **Remote Configuration** | Centralized control via a web platform, with remote access via CLI and WebUI | Remote control of power, watchdog timers, and other device settings |
| **Real-Time Monitoring** | Real-time device status (online/offline) and activity reports | Visualized dashboards and real-time alerts for abnormal events |
| **Security** | Supports secure VPN tunnels, firewalls, and encrypted communication | Provides a comprehensive cybersecurity solution from edge to cloud |

## V. The Cloud Platform: Data and Monitoring

### 5.1. The Data Flow

The data journey begins at the Edge and Gateway devices, which acquire data from the Marioff and Autronica systems. This information, including events, logs, and device statuses, is then published to the AWS cloud [User Query]. The primary communication protocol used for this is MQTT, a lightweight and widely adopted messaging protocol optimized for constrained devices.18 AWS IoT Core acts as the central message broker, providing a secure, bi-directional channel that connects the devices to the rest of the AWS ecosystem.18 This managed service handles secure device authentication, message brokering, and routing, which eliminates the need for the development team to manage complex infrastructure.19

### 5.2. Data Storage and Analysis: AWS Timestream vs. DynamoDB

The user query specifies that data processed by the Edge and Gateway devices are stored in AWS databases, specifically AWS Timestream or DynamoDB [User Query]. A detailed analysis indicates that the optimal solution is not a choice between the two, but a synergistic combination that leverages the unique strengths of each service.

**AWS Timestream** is a purpose-built time-series database designed for high-volume, continuous measurements.9 It is highly efficient for ingesting millions of data points per second, making it ideal for storing the stream of events, logs, and telemetry from the fire safety devices.9 Timestream excels at running analytical queries on large datasets, allowing for the easy identification of trends and patterns over time.9 Its tiered storage model, which separates a high-speed memory store from a cost-effective magnetic store, is optimized for both rapid querying of recent data and long-term, low-cost storage for historical analysis.9

**AWS DynamoDB**, a high-performance NoSQL database, is optimized for low-latency, targeted lookups.34 While it can handle high-volume data, its design is centered on fast key-value queries, not large-scale, ad-hoc analytics.34 In the context of the ICS+ platform, DynamoDB's ideal use case is for storing data that requires frequent, single-record access, such as user management profiles, device configuration settings, and current device statuses [User Query]. This type of data does not fit the time-series model and requires the kind of blazing-fast, targeted access that DynamoDB provides.34

The architectural decision to use both databases is a strategic one. Attempting to use a single database for both time-series analytics and real-time lookups would inevitably lead to performance bottlenecks and inflated costs. For example, using Timestream for user management would result in slower query times for a simple user login, while using DynamoDB for historical trend analysis would be prohibitively expensive due to the large volume of data and the nature of the queries required.34

The hybrid approach is a best-practice solution that allows the ICS+ platform to provide both a near-real-time view of device status and comprehensive historical analytics for predictive maintenance. The back-end logic will intelligently route data to the appropriate database, and the front-end application will query from both to provide a complete, performant user experience.

**Table 3: AWS Database Comparison**

| Feature | AWS Timestream | AWS DynamoDB |
| --- | --- | --- |
| **Primary Use Case** | Time-series data, Event Logs, IoT telemetry, DevOps monitoring 9 | User management, Device configuration, Key-value lookups, Real-time data access 34 |
| **Data Model** | Time-stamped measures and dimensions 9 | Flexible attributes with unique keys 34 |
| **Querying** | SQL-based queries with built-in time-series functions 9 | Targeted queries by key/index, limited ad-hoc analytics 34 |
| **Performance** | Sub-second analytical queries on terabytes; fast ingestion 9 | Micro-second latency for targeted reads/writes 35 |
| **Scalability** | Automated ingestion and query scaling based on workload 35 | Seamless scaling to handle 20 million+ requests/sec 35 |

### 5.3. The Real-Time Monitoring Platform

The ultimate purpose of the ICS+ system is to provide a user-friendly, real-time monitoring platform for Marioff and Autronica device statuses [User Query]. The application layer is a web and mobile platform that serves as a visual interface for the data collected and stored in the cloud. This aligns with industry standards for IIoT dashboards, which are designed to support smart factory transformation by collecting live data from IoT sensors and presenting it in interactive charts, graphs, and tables.11

The platform's features, including real-time data monitoring, user management, and device configuration, are consistent with best practices for industrial remote access solutions.36 These platforms enable users to monitor system health, receive alerts, and even troubleshoot and program devices remotely, reducing travel costs and increasing operational efficiency.36

## VI. Strategic and Competitive Context

### 6.1. Competitive Landscape and Market Position

Marioff and Autronica are operating within a global fire protection market dominated by large, diversified companies.2 The major players include Johnson Controls, Carrier, Honeywell, Siemens, and Robert Bosch GmbH.2 Many of these competitors offer comprehensive fire detection, suppression, and monitoring solutions, with some, like Bosch, also providing remote services through smart IoT technology.2

Despite the competition, Marioff has a strong market position, particularly in the marine sector, where it has extended service agreements with major cruise lines such as Royal Caribbean and Norwegian Cruise Line.4 The company's proprietary HI-FOG water mist technology provides a competitive advantage, as it is a highly effective suppression method that causes minimal water damage.3 By introducing an IoT-enabled solution like ICS+, the company differentiates itself by being among the first to bring this level of digital intelligence to high-pressure water mist fire protection.1

### 6.2. The Business Model Shift

The ICS+ project signifies a fundamental shift in the business model from selling products to selling ongoing services and insights. Traditionally, fire protection has been a capital expenditure involving a one-time product sale followed by a maintenance contract for scheduled checks. The introduction of real-time monitoring and predictive analytics fundamentally changes this paradigm.

The HI-FOG Smart solution provides "real-time visibility," "smarter maintenance," and "centralized system control".1 This allows Marioff and Autronica to move from reactive maintenance, where they respond to an issue after it has occurred, to proactive, predictive maintenance. By analyzing continuous streams of data from the Edge devices, the company can identify potential issues before they cause a system failure, schedule maintenance at optimal times, and maximize asset lifespan.1 The research confirms that Marioff already has service agreements for "preventive maintenance" with clients, and the ICS+ platform is the technological enabler for scaling and enhancing this service.4

This new model allows for the creation of a stable, recurring revenue stream through long-term service contracts that are centered on the value of insights and uptime, rather than just the physical product. This strategic approach aligns the company with modern market expectations and positions it as a technology leader in the fire safety industry.

### 6.3. Recommendations and Key Considerations for Scope of Work

Based on the detailed analysis of the ICS+ architecture, the following recommendations are provided to inform the project's scope of work:

* **Firmware Architecture:** The firmware for the Advantech ARK-1221L and Teltonika TRB-140 should be developed with a containerized architecture to provide a flexible, secure, and highly manageable solution for the long term. This approach will simplify component updates, improve security by isolating individual services, and streamline development processes.
* **Protocol Translation:** A primary focus of the firmware development must be the robust and reliable translation of proprietary industrial protocols from the Marioff and Autronica systems into a standardized format for transmission to the cloud. This protocol conversion layer is the critical bridge between the OT and IT worlds.
* **Cloud Data Strategy:** The project should adopt a hybrid AWS Timestream and DynamoDB data strategy. AWS Timestream should be used for all time-series data, including events, logs, and telemetry, due to its cost-effectiveness and optimization for large-scale analytics. AWS DynamoDB should be used for all real-time lookups, such as user profiles, device configurations, and current device statuses, to ensure a low-latency and performant user experience.
* **Operational Readiness:** The scope of work should explicitly leverage the native remote management capabilities of the selected hardware. Integrating the development and operational processes with Teltonika's RMS and Advantech's WISE-DeviceOn will provide centralized control, simplified onboarding, and efficient OTA firmware updates, which are essential for managing a global fleet of deployed devices.

#### Works cited

1. HI-FOG Smart - Marioff HI-FOG®, accessed September 10, 2025, <https://www.marioff.com/en/lifecycle-services/smart/>
2. Top Companies List of Fire Protection System Industry - MarketsandMarkets, accessed September 10, 2025, <https://www.marketsandmarkets.com/ResearchInsight/fire-protection-systems-market.asp>
3. Fire protection on Land - Marioff HI-FOG®, accessed September 10, 2025, <https://www.marioff.com/en/fire-protection-on-land/>
4. Marioff Company Overview, Contact Details & Competitors - LeadIQ, accessed September 10, 2025, <https://leadiq.com/c/marioff/5a1d982c2300005a0086d131>
5. Marioff HI-FOG fire suppression system pump units, accessed September 10, 2025, <https://www.marioff.com/en/water-mist/system-components/pump-units/>
6. AUTROSAFE 4, accessed September 10, 2025, <https://www.sealab.pl/img/autrosafe%204/pdf/p-asafe_exp_agb.pdf>
7. ARK-1221L - Tempel Group, accessed September 10, 2025, <https://www.tempelgroup.com/en/productos-ingenieria/informatica-industrial/embedded-advantech/ark-1221l/>
8. Teltonika TRB140 4G (LTE) Gateway - Mouser Electronics, accessed September 10, 2025, <https://www.mouser.com/new/teltonika/teltonika-trb140-gateway/>
9. An Overview and Lessons learned from Storing and Analysing IoT Data in AWS Timestream, accessed September 10, 2025, <https://superluminar.io/2025/03/21/an-overview-and-lessons-learned-from-storing-and-analysing-iot-data-in-aws-timestream/>
10. How to Audit AWS DynamoDB Table Access | Stratusphere™ - StratusGrid, accessed September 10, 2025, <https://stratusgrid.com/knowledge-base/how-to-audit-dynamodb-table-access-stratusphere>
11. Industrial IoT Dashboards - Synergy Codes - data visualization agency for data products, accessed September 10, 2025, <https://www.synergycodes.com/our-work/industrial-iot-dashboards>
12. Sentinel Carves Industrial Fire Business from Carrier - Private Equity Professional, accessed September 10, 2025, <https://peprofessional.com/2024/07/sentinel-carves-industrial-fire-business-from-carrier/>
13. Revolutionizing Industries with IIoT Architecture: Maximum Impact - Cyber Infrastructure, CIS, accessed September 10, 2025, <https://www.cisin.com/coffee-break/iiot-architecture-explained-with-benefits-and-examples.html>
14. IoT Architecture: Six Levels, Core Components and Use Cases - Itransition, accessed September 10, 2025, <https://www.itransition.com/iot/architecture>
15. AutroSafe communication - Fire and gas detection system units ..., accessed September 10, 2025, <https://product.autronicafire.com/products/fire-and-gas-detection-systems/fg-system-units/autrosafe-communication/>
16. TRB140 4G IoT Gateway - Teltonika Networks, accessed September 10, 2025, <https://teltonika-networks.com/products/gateways/trb140>
17. TRB140 - The Kenton Group, accessed September 10, 2025, <https://www.thekentongroup.com/wp-content/uploads/2023/07/trb140-flyer-2022-v10.pdf>
18. Building Smart Industrial Machines with AWS: A Comprehensive Guide - Amazon.com, accessed September 10, 2025, <https://aws.amazon.com/blogs/iot/building-smart-industrial-machines-with-aws-iot-a-comprehensive-guide/>
19. AWS IoT Core Features - Amazon Web Services, accessed September 10, 2025, <https://aws.amazon.com/iot-core/features/>
20. Remote Monitoring and Notifications - Fire Safety IoT - GAO Tek, accessed September 10, 2025, <https://gaotek.com/remote-monitoring-and-notifications-fire-safety-iot/>
21. Marioff HI-FOG® Land Pump Unit (LPU) - adipec, accessed September 10, 2025, <https://marketingmanual.adipec.com/Exhibitors/ADIPEC25-IT-14-18/PressReleases/20250805-104043-ADIPEC25-IT-14-18-press.pdf>
22. A Guide to Fire Alarm Basics - NFPA, accessed September 10, 2025, <https://www.nfpa.org/news-blogs-and-articles/blogs/2021/03/03/a-guide-to-fire-alarm-basics>
23. Advantech ARK-1221L-S5A1 Industrial Computer - Intel Atom x6413E - Fanless Embedded System - CDW, accessed September 10, 2025, <https://www.cdw.com/product/advantech-ark-1221l-s5a1-industrial-computer-intel-atom-x6413e-fanless/8111142>
24. ARK-1221L - Advantech, accessed September 10, 2025, <https://www.advantech.com/en-us/products/1-2jkbyz/ark-1221l/mod_06c34358-87b6-4f11-97af-be1a1dd885dd>
25. Teltonika TRB140 LTE Router - Getic, accessed September 10, 2025, <https://www.getic.com/product/teltonika-trb140-lte-router-housing>
26. Digi Containers, accessed September 10, 2025, <https://www.digi.com/products/iot-software-services/value-added-services/digi-containers>
27. Teltonika Remote Management System - Westward Sales, accessed September 10, 2025, <https://www.westwardsales.com/blog/teltonika-remote-management-systems/>
28. Managing Your Fleet, Your Way: RMS Packages Explained - Teltonika Networks, accessed September 10, 2025, <https://teltonika-networks.com/newsroom/managing-your-fleet-your-way-rms-packages-explained>
29. How to Download & Update Firmware | Teltonika Networking - YouTube, accessed September 10, 2025, <https://www.youtube.com/watch?v=6mS8HRnFubA>
30. How to upgrade a router's firmware version via RMS? - Teltonika Networks Wiki, accessed September 10, 2025, <https://wiki.teltonika-networks.com/view/How_to_upgrade_a_router%27s_firmware_version_via_RMS%3F>
31. How can I configure devices from RMS? - Teltonika Networks Wiki, accessed September 10, 2025, <https://wiki.teltonika-networks.com/view/How_can_I_configure_devices_from_RMS%3F>
32. AIoT Software, Distribution & Services - Advantech, accessed September 10, 2025, <https://www.advantech.com/en-us/products/aiot-software-distribution-services/sub_1-2jkj9e>
33. MQTT - AWS IoT Core, accessed September 10, 2025, <https://docs.aws.amazon.com/iot/latest/developerguide/mqtt.html>
34. Amazon Timestream vs DynamoDB for Timeseries Data - bahr.dev, accessed September 10, 2025, <https://bahr.dev/2020/10/29/timestream/>
35. DynamoDB vs Amazon Timestream - The Ultimate Comparison - Dynobase, accessed September 10, 2025, <https://dynobase.dev/dynamodb-vs-amazon-timestream/>
36. Secure industrial remote access for machines - IXON, accessed September 10, 2025, <https://www.ixon.cloud/iiot-platform/industrial-remote-access>
37. Industrial Remote Access - HMS Networks, accessed September 10, 2025, <https://www.hms-networks.com/industrial-remote-access>
38. Fire detection solutions for industrial applications - Bosch Security, accessed September 10, 2025, <https://www.boschsecurity.com/en/industries/fire-alarm-systems-industrial-applications/>
39. Opinion - United front for shipboard technology - Riviera, accessed September 10, 2025, <https://www.rivieramm.com/opinion/opinion/united-front-for-shipboard-technology-35610>
40. Industrial IoT | Digital Transformation - AWS, accessed September 10, 2025, <https://aws.amazon.com/iot/solutions/industrial-iot/>
41. Marioff HI-FOG system upgrades and extensions for Marine, accessed September 10, 2025, <https://www.marioff.com/en/fire-protection-for-marine/lifecycle-service-platform-for-marine/system-upgrades-extensions/>