

DATASHEET

Remote Monitoring

See Every System. Catch Issues Early. Prove Alarm Compliance.

Modern manufacturing runs on a growing fleet of OT systems including SCADA & edge nodes, historians, databases, network devices and MES applications which are often spread across multiple sites, time zones and support teams. Most failures announce themselves in advance such as a disk filling up, a backup that stopped running, a certificate approaching expiry, a store-and-forward buffer quietly growing. Yet without dedicated monitoring, the first sign of trouble is usually an operator calling because screens went blank or when data has stopped flowing.

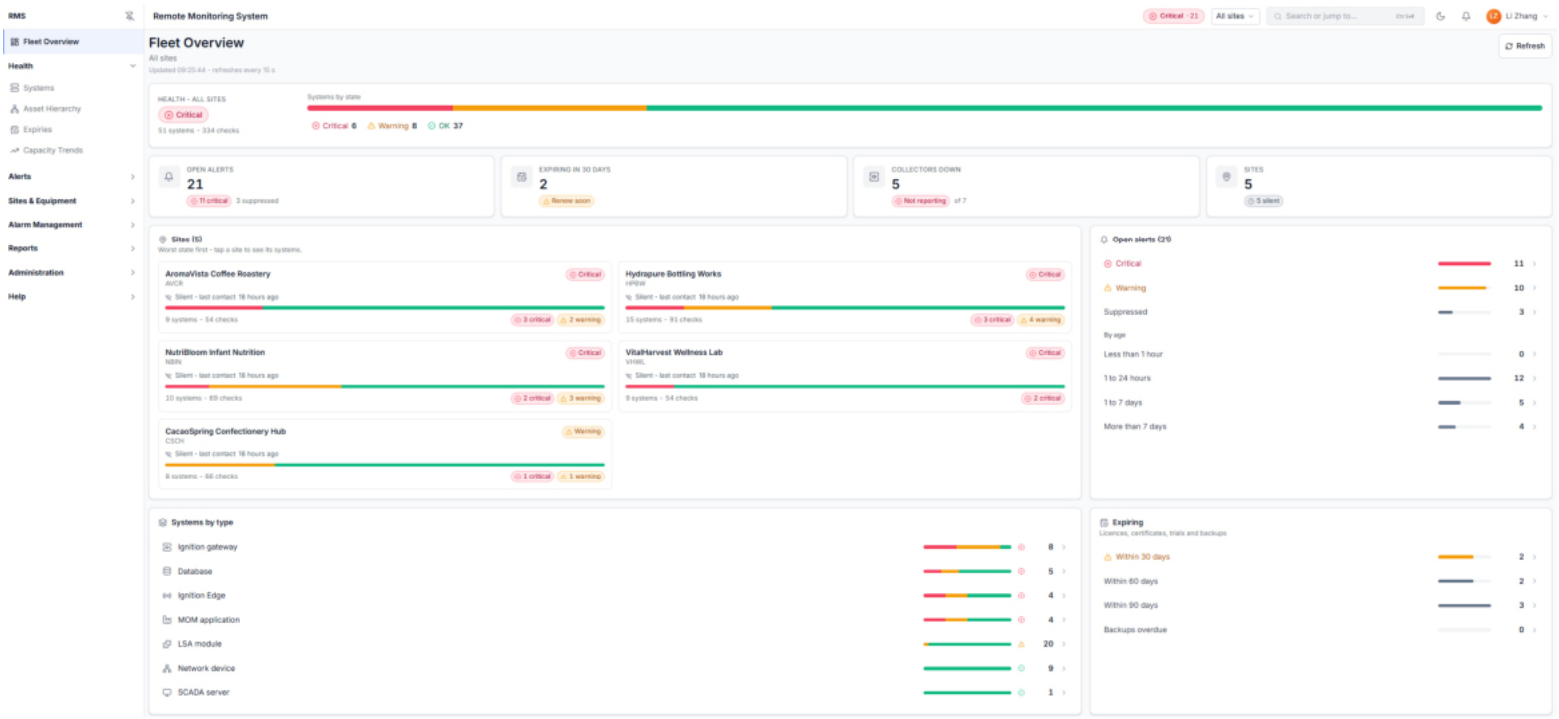
The LOGICAL SYSTEMS Remote Monitoring System (RMS) gives you a single pane of glass over your entire automation infrastructure. Running natively on the Ignition® platform, RMS continuously checks the health of every gateway, edge node, database, host, network link and application in your fleet completely agentless, with no software to install on the monitored systems. Health states roll up from individual checks through systems, areas and sites to a fleet-wide overview, so one glance tells you what needs attention and where. When a check crosses its threshold, RMS raises an alert with full context, routes it to the right people, and tracks it through acknowledgement, assignment and resolution with a complete timeline.

RMS goes beyond infrastructure health: it is also a complete alarm management application built around ISA-18.2 / IEC 62682. It reads alarm activity directly from your Ignition systems, assesses KPIs per operator position against your alarm philosophy, identifies floods, chatter and bad actors, and takes you through structured rationalization from candidate-alarm testing to documented consequence, response and approved attributes in a Master Alarm Database with electronic signatures, management of change and a full audit trail.

Whether you operate a single plant or a global fleet, RMS scales with you: site instances keep monitoring and alerting autonomously even when the WAN is down, and synchronize with the Global instance over the Ignition Gateway Network the moment the link returns. The result is fewer surprises, faster response, and documented control over your alarm system.

Complete Fleet Visibility

One Pane of Glass for Your Entire OT Infrastructure



Comprehensive Infrastructure Coverage

RMS monitors every layer of the automation stack behind your operations.

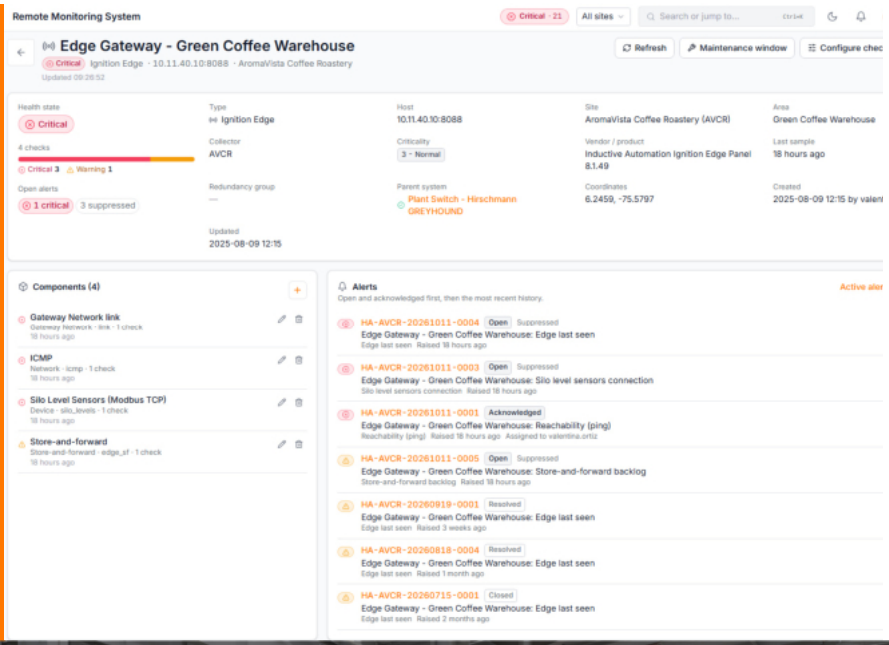
Ignition Gateways CPU, JVM heap, memory, disk and disk-full forecast, license state, faulted modules, data sources, OPC connections and tag providers, Gateway Network links, store-and-forward quarantine, Perspective sessions, backup age and TLS certificate - including redundant pairs with standby synchronization checks.

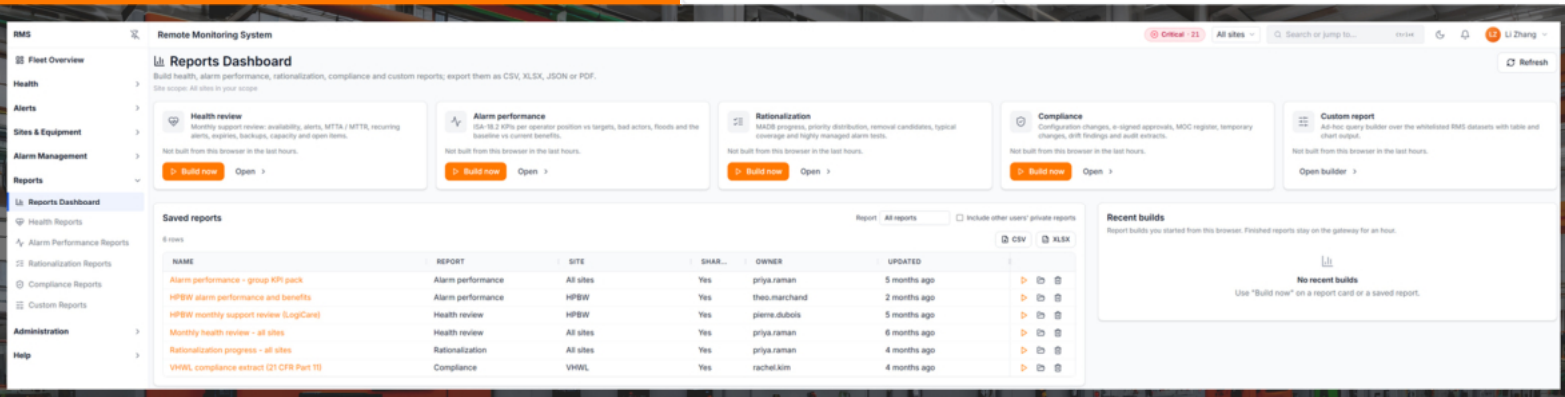
Edge Nodes watched agentless from their parent gateway last-seen heartbeat, device connections and reachability, with store-and-forward backlog visibility.

Databases SQL Server monitored through existing Ignition data sources (SELECT-only) - connection, query latency, Agent job failures, full and log backup age, data and log free space.

Networked Devices & Hosts reachability, latency and port checks for switches, firewalls, routers, servers, PLCs, VSDs, etc.

Applications such as LS MES modules (OEE, TMS, WMS, SPC and more) with Enterprise Sync health, plus applications such as MQTT brokers, LIMS and warehouse systems via HTTP, TCP, tag and SQL checks.





One system, every layer of your OT estate :

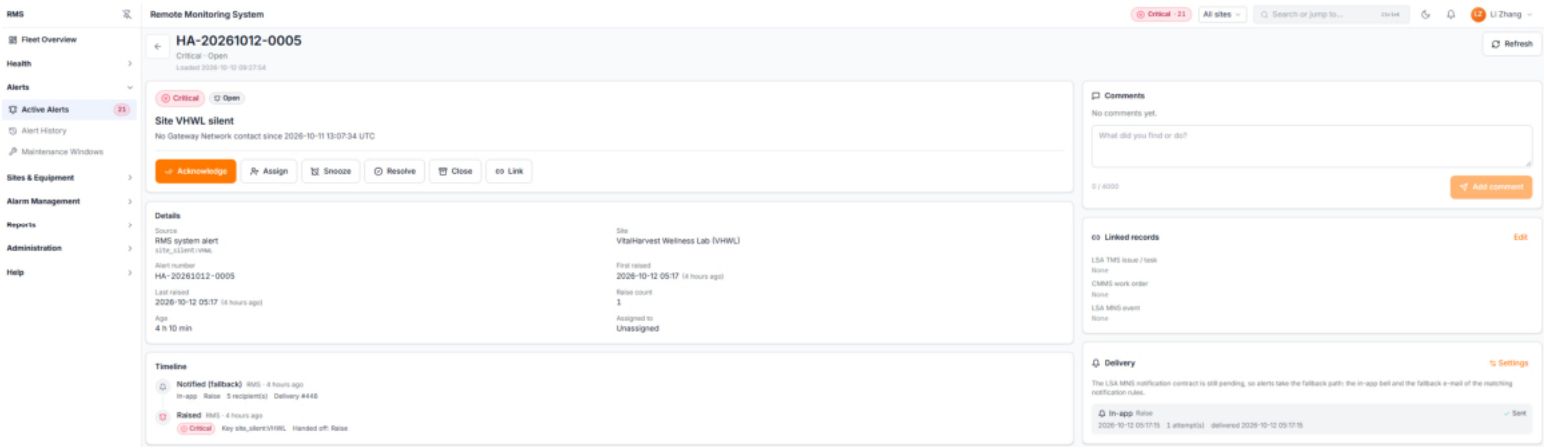
- Health rolled up from check → system → area → site → fleet.
- Agentless monitoring - nothing to install on monitored systems.
- Sites keep alerting autonomously when the WAN link is down.
- Certificates, licenses, backups and trials tracked before they expire.
- Full alarm management built on ISA-18.2 / IEC 62682.

Proactive, Not Reactive

Infrastructure Health and ISA-18.2 Alarm Management in One Application

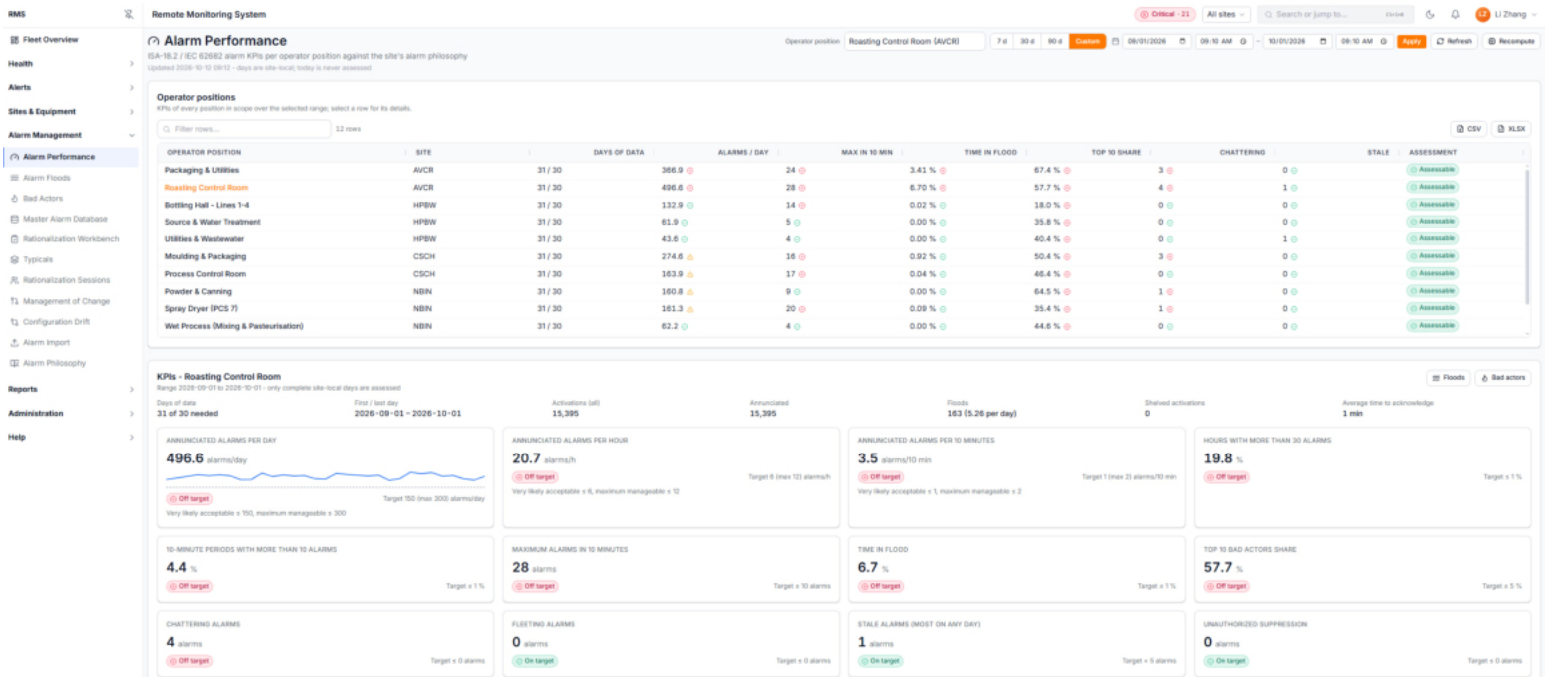
RMS runs a library of built-in check types including gateway self-diagnostics, host metrics, SQL queries, tag values, ICMP ping, TCP port, HTTP endpoints, TLS certificates, backup file age and edge heartbeats - scheduled by a collector service across the fleet. Check templates apply a proven monitoring pack to a new system in seconds, complete with warning and critical thresholds, deadband and on/off delays that suppress nuisance alerts.

When a threshold is crossed, RMS raises an alert with the exact reading and message, routes it by site, system type and severity, and tracks it through acknowledgement, assignment and resolution - with maintenance windows for planned work, flap detection, auto-resolve, and measured time-to-acknowledge and time-to-resolve. Trend-based checks forecast when a disk will fill or a license will lapse days in advance, and the Expiries view counts down every certificate, license, trial and backup across the fleet. Notifications reach the right people in-app and by e-mail through your existing Ignition SMTP profiles, with outbound webhooks to channels such as Microsoft Teams and hand-off to the LOGICAL SYSTEMS Message Notification System (MNS) for managed escalations.



RMS is also a complete alarm management application built around ISA-18.2 / IEC 62682. It reads alarm activity directly from your Ignition gateways and assesses the KPIs per operator position - annunciated alarms per day and per hour, peak 10-minute rates, time in flood, bad-actor share, chattering, fleeting and stale alarms - against the targets in your approved alarm philosophy. Flood episodes are reconstructed with their alarm sequences and top contributors, and bad actors are ranked by the attention they cost your operators - ready to send straight to the rationalization workbench.

The Master Alarm Database holds every alarm in scope, imported from a tag export, a live gateway browse or CSV or XLSX, and takes each one through structured rationalization: candidate-alarm test, consequence and priority from your philosophy matrix, documented cause and operator action, and proposed attributes - approved with electronic signatures, covered by management of change, and checked for configuration drift against the running system.



Whether you run one plant or a global fleet, every site instance evaluates, alerts and notifies autonomously even with the WAN link down and synchronizes with the Global instance over the standard Ignition Gateway Network when the connection returns, with silent-site detection at the Global.

Every decision leaves a record: a full audit trail, versioned alarm philosophies, per-position Alarm Response Manuals in the operator's own language, and reports including KPI packs, rationalization progress, health reviews and compliance extracts that can be exported to CSV, XLSX, JSON or PDF reports.



Key Features and Benefits

Features

- Fleet-wide health overview with roll-up from check to site to enterprise
- Agentless monitoring of gateways, edge nodes, databases, hosts, network devices and applications
- 11 built-in check types with templates, thresholds, deadbands and on/off delays
- Full alert lifecycle: acknowledge, assign, snooze, resolve, with comments and timeline
- Maintenance windows, flap detection and auto-resolve to eliminate nuisance alerts
- Disk-full and threshold forecasting; expiry tracking for certificates, licenses, trials and backups
- ISA-18.2 / IEC 62682 alarm KPIs per operator position with philosophy targets
- Flood reconstruction, bad-actor ranking and alarm rate analytics
- Master Alarm Database with rationalization workbench, typicals for UDT-based alarms, and team sessions
- Management of change with electronic signatures and temporary-change expiry
- Configuration drift detection and write-back to Ignition

Benefits

- Find failing infrastructure before operations does
- Cut unplanned SCADA/MES downtime through early-warning forecasts
- One support view across all sites, vendors and system types
- Faster response with measured time-to-acknowledge and time-to-resolve
- Reduced alarm load per operator and fewer floods
- Audit-ready alarm rationalization and change records
- No agents, no extra servers - runs on your existing Ignition infrastructure
- Remote sites stay protected even when the WAN is down

Technical Requirements

System Requirements

Ignition® (8.1.+) Core Modules, Quad-core processor, 16 GB RAM, 10 GB free disk space

Supported Operating Systems

Windows Server 2019/2022/2025, Windows 10/11, macOS (X, 10.16+), Linux (Ubuntu, CentOS, RHEL)

Supported Protocols

MQTT, OPC UA / OPC DA, REST API (JSON Payloads)
Kafka (via connector), Snowflake (via pipeline, data bridge)

Supported Databases

Microsoft SQL Server, Oracle, MySQL, MariaDB, PostgreSQL, any database with JDBC driver

Supported Browsers

Chrome, Firefox, Safari, Microsoft Edge

LOGICAL SYSTEMS

RMS

Know Your Fleet. Validate Your Alarms.

Your automation infrastructure is the backbone of your production and it deserves the same monitoring discipline as the process itself.

LOGICAL SYSTEMS RMS gives you the visibility, early warnings and alarm management control to run a reliable, compliant operation at one site or across the world.

LOGICAL SYSTEMS
AUTOMATION & INTEGRATION SERVICES
Specialists in Automation & Digitalization for Manufacturing Industries

Copyright © 2026 LOGICAL SYSTEMS and its subsidiaries. All rights reserved.
All product names mentioned are the trademarks of their respective holders.

www.logicalsystems.io | info@logicalsystems.io