White paper

Cybersecurity for the Monitoring Box including FieldEdge IXA71 edge gateway

Author
Dr. Sören Geffken, Research & Development - Endress+Hauser SICK GmbH+Co. KG
Falko Kraus, Product Manager - Endress+Hauser SICK GmbH+Co. KG

Endress+Hauser
People for Process Automation

1. Introduction

The Monitoring Box is the Endress+Hauser condition monitoring solution for gas analyzers. It combines an edge device and cloud-based software to collect, process, and visualize status-related device information. Continuous monitoring of analyzer health and diagnostic information helps increase device availability, reduce service effort, and supports data-driven services such as predictive maintenance.
The Monitoring Box has been designed to provide these services while maintaining a clear separation from the analyzer's primary measurement and control functions. Security measures have been implemented to protect connected assets, transmitted data, and supporting backend systems throughout the solution lifecycle. These measures are intended to minimize cybersecurity risks and support secure operation of the solution.
This document provides an overview of the cybersecurity measures implemented in a standard Monitoring Box deployment. Additional measures may be required depending on customer-specific requirements and IT infrastructures.
A typical Monitoring Box architecture is illustrated in Figure 1.

2. Components

The Monitoring Box solution consists of hardware and software components working together to collect analyzer data, provide condition monitoring services, and securely visualize the resulting information.
The following sections describe the individual components and the measures implemented to protect them.

2.1. Monitoring Box edge device

The FieldEdge IXA71 shown in Figure 2 is the edge device used to collect data from analyzers, perform data processing, and transfer processed data to the backend using authenticated and encrypted communication.
The device is equipped with two LAN ports to segregate data acquisition and external communication traffic. To collect data from connected analyzers, the first LAN port uses existing analyzer communication interfaces to retrieve the required information. Communication with the analyzers is limited to the functions required for data acquisition.

The second LAN port is used to connect the device to the internet to transfer the processed data to the backend server. Communication between the device and backend

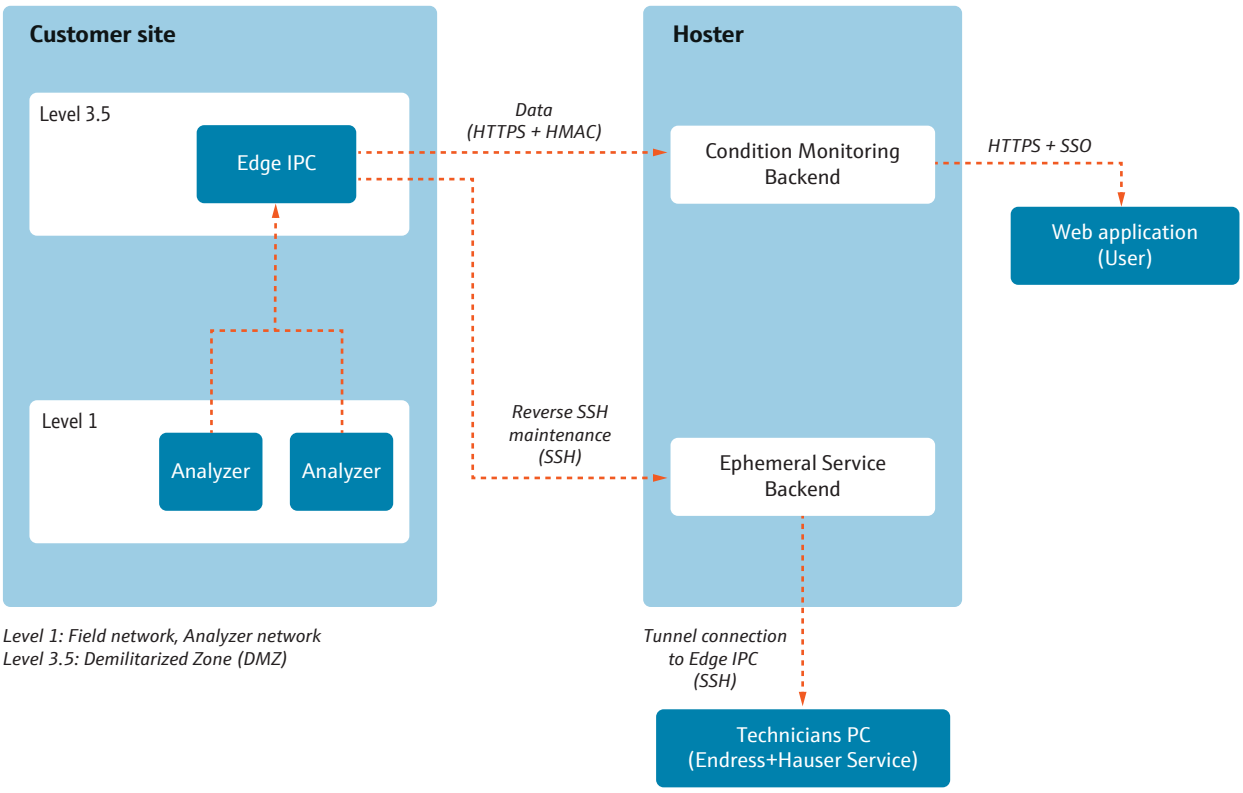

Fig.1: Schematic illustration of Monitoring Box connections

is authenticated and encrypted using device-specific certificates trusted by the backend system, ensuring confidentiality, integrity, and authenticity of transmitted data.
In the default configuration, the device provides a secure maintenance channel through this connection, allowing Endress+Hauser to deploy software and security updates remotely.
The device enforces network separation through a built-in firewall.

Fig.2: Monitoring Box gateway - FieldEdge IXA71

2.2. Condition Monitoring Backend

The condition monitoring backend infrastructure is hosted in Germany and operated in accordance with applicable German and European legal and regulatory requirements.
Independent certifications of the hosting provider, including ISO 27001 certification and PCI DSS compliance, demonstrate established information security and operational controls.
The solution primarily processes technical monitoring and diagnostic information. Personal data required for user authentication and access management is limited to the minimum necessary and is processed in accordance with applicable data protection regulations, including the General Data Protection Regulation (GDPR).
Access to system functions and customer data is controlled through role-based access control (RBAC). Users are granted access only to the assets and information required for their assigned responsibilities.
Additional technical and organizational measures, including authentication controls, system monitoring, vulnerability management processes, and secure operational procedures, are implemented to reduce the risk of unauthorized access, data manipulation, or service disruption.

2.3. Analyzers

The edge device retrieves diagnostic and condition monitoring data from connected analyzers using existing communication interfaces and protocols, including TCP/IP-based and RS485-based communication.
Data acquisition is implemented using existing analyzer communication interfaces and does not require modifications to the analyzer's measurement or control functions.
Condition monitoring operates independently of the analyzer's primary process functions. The analyzer continues to perform its measurement tasks even in the event of a failure of the monitoring infrastructure.
This separation helps ensure that condition monitoring activities do not interfere with the analyzer's operational functionality.

2.4. Web application

The Monitoring Box web application provides authorized users with access to condition monitoring information, diagnostics, and analysis functions.
Users are authenticated through the Endress+Hauser identity management system using individual user accounts.
Access to assets and associated information is restricted according to assigned permissions, ensuring that users can only view information for which they have been authorized.
To support accountability, traceability, and auditing of user activities, shared or group accounts are not permitted.
All access is performed using individually assigned user identities.

3. General principles and measures

The Monitoring Box has been developed and is maintained according to established cybersecurity principles.
The following measures support the security of the overall solution.

3.1. Security risk analysis

The system was developed following the Security by Design principle. During the design phase of the systems architecture, security risks were systematically assessed. Based on the identified risks, appropriate technical and organizational controls were defined and implemented to reduce the associated risks to an acceptable level.

3.2. Repeated external security testing

Prior to market introduction, the solution underwent an independent external penetration test.
Subsequently, additional external security assessments covering different parts of the solution have been conducted at regular intervals. Findings from these assessments are reviewed and addressed as part of the continuous improvement process.

3.3. Vulnerability management

Endress+Hauser maintains a structured vulnerability management process in alignment with the principles of the Cyber Resilience Act.
Software components used within the solution are continuously monitored through a Software Bill of Materials (SBOM) approach. Automated processes compare incorporated software components against known vulnerability databases to support timely identification, assessment, and remediation of security vulnerabilities.

3.4. Product Security Incident Response Team (PSIRT)

The Endress+Hauser Product Security Incident Response Team (PSIRT) serves as a central contact for customers, suppliers, security researchers, government agencies, and other stakeholders regarding cybersecurity-related topics.
PSIRT coordinates the handling of reported vulnerabilities and cybersecurity incidents through a company-wide vulnerability and incident management process, supporting a consistent and coordinated response to cybersecurity issues.
Further information and security advisories are available at:
https://www.endress.com/en/pages/security

Headquarters

Endress+Hauser
Instruments International AG
Kaegenstraße 2
4153 Reinach
Switzerland

Tel +41 61 715 8100
Fax +41 61 715 2500
info@ii.endress.com
www.ii.endress.com

WP01285K/90/EN/01.26-00
(8026574 / EN / V1-0)

Endress+Hauser

People for Process Automation