White paper

Cybersecurity for the Monitoring Box including gateway

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

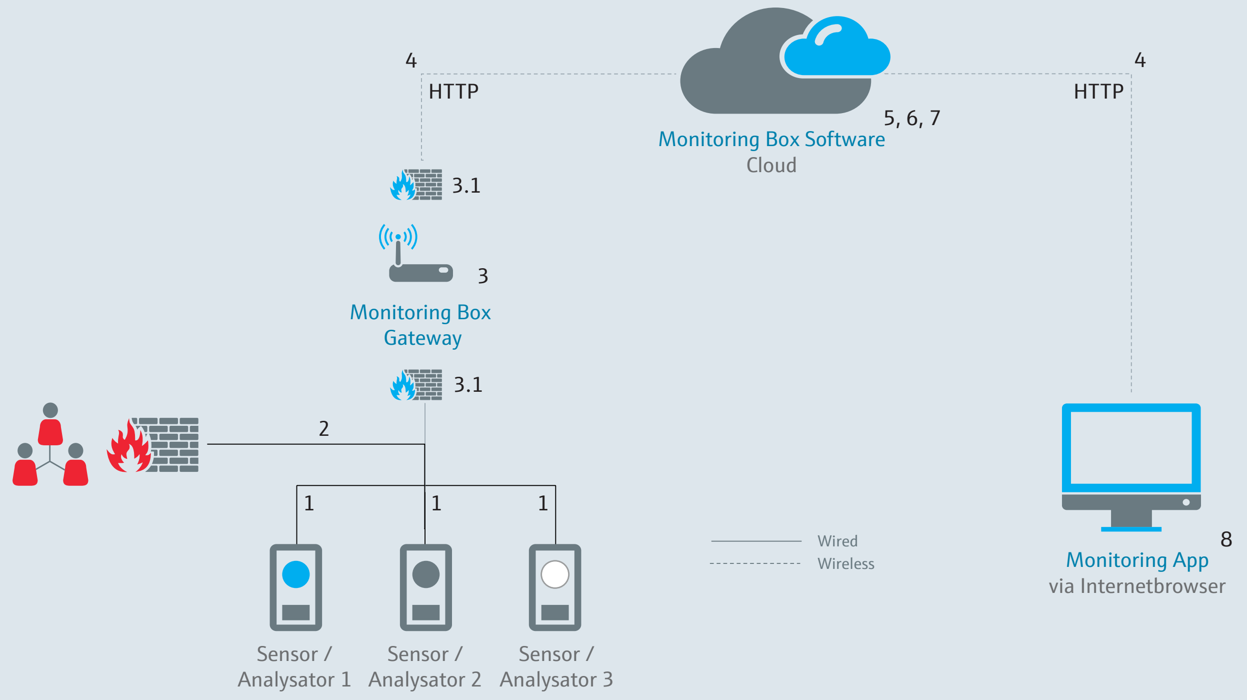
Endress+Hauser
People for Process Automation

1. Introduction and background

As part of its service products, Endress+Hauser has developed a new system comprising software and hardware: the Monitoring Box. This system allows you to visualize status-related data from analyzers and sensors in an online dashboard by using a combination of a gateway and a cloud application (condition monitoring). By permanently monitoring and evaluating status-related parameters, Endress+Hauser helps customers to increase the availability of their devices, reduce service costs and provides the basis for data analytic services such as predictive maintenance. Endress+Hauser has taken various measures to protect the system (Monitoring Box), data and the associated customer devices and to minimize IT security risks. The following pages are aimed at Monitoring Box stakeholders and provide an initial overview of the cybersecurity measures as provided with a standard installation of the Monitoring Box. Customized installations and individual IT infrastructures may require further measures or adjustments to existing measures.

2. Hardware components

In order to implement condition monitoring for sensors using the Monitoring Box, various hardware and software components must work together. The following system overview describes these components and provides detailed information on each component and the measures taken to ensure IT security.



(1) Unidirectional data traffic (read-only access to sensor data)
(2) Independent data transmission, as it is not part of the customer network
(3) Firewall integrated in the Monitoring Box gateway
(4) SSL/TLS encryption via HTTPS
(5) Validation of input data at all interfaces
(6) Brute-force protection measures
(7) Continuous monitoring of the software packages used for vulnerabilities
(8) Role-based access

Fig.1: The system overview shows which protective measures Endress+Hauser has implemented at which points in the system to protect communication and transmitted data from attacks and manipulation.

2.1. Monitoring Box gateway

The Monitoring Box gateway (SSG-E) in Fig. 2 acts as a gateway to collect data from analyzers and sensors directly from Edge and transfer it to the cloud as smart data.
The Monitoring Box uses one-way communication from the gateway to the cloud as standard. The sensor data is transferred to the gateway and sent to the Endress+Hauser cloud. There is no provision for configuring the sensors or for communicating the sensor data in the other direction.
In the standard configuration, the gateway is equipped with a maintenance channel via a secure connection, allowing Endress+Hauser to easily install security updates.

Fig.2: Monitoring Box gateway

2.2. Server

To protect the data during transmission from the Monitoring Box to the server and during transmission from the server to the dashboard or front end, encryption, authentication, and identification are implemented using TLS.
The servers on which the Monitoring Box data is processed are located in Germany and are therefore subject to German and European law, and in particular to the GDPR. The implementation of and compliance with various security measures prevent access and manipulation by unauthorized persons. All data communication is protected by authentication and authorization, ensuring that permissions for reading and writing data are checked, secured, and complied with at all communication levels.

2.3. Sensors

Endress+Hauser implements data transmission from the sensor to the Monitoring Box gateway using various protocols and plug-ins (e.g. TCP/IP or RS485). The transfer of data from the analyzer or sensor to the Monitoring Box gateway and from there to the server can be carried out independently of the customer's network via dedicated interfaces. The physical or virtual separation of the networks involved prevents interference with the local customer network. The sensor transmits data via cable using industry-standard protocols such as TCP/IP, serial interfaces such as Modbus RS485, or USB. Thanks to the aforementioned unidirectional connection between the analyzer or sensor and the gateway, it is not possible to access the analyzer or sensor via the Monitoring Box.

3. Software components

From the user's perspective, the most important software component of the Monitoring Box is the browser application (also known as the dashboard or front end). The dashboard can be accessed at https://monitoringbox.endress.com. Authentication takes place via Endress+Hauser's single sign-on system – Entra-ID. Authorization for access to stored data is verified using role-based access control.
The following sections describe the environment required for the safe use of the browser application at Endress+Hauser and the protective measures to ensure safe use and data protection.

3.1. Browser application

The browser application gives users access to the Monitoring Box functions and, in particular, insights into the recorded sensor data.
Each user has a unique user ID, an Endress+Hauser identification number. After logging in to the dashboard, each user account will only display the assets that belong to them. To ensure that server accesses can be clearly assigned, group accounts may not be used. This serves to ensure the traceability of the requested data, enabling any errors that occur and failed access attempts to be checked.

3.2. Protocols used

Common protocols are used for data transmission between the gateway and the cloud, as well as between the cloud and the frontend or browser. Endress+Hauser has implemented generally accepted security measures in the implementation of the software. The most important protocols and standards are described below by way of example.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a communication protocol that enables data to be transmitted securely over the Internet. It represents transport encryption via TLS. HTTPS communication between the dashboard and server is configured in accordance with standard security requirements, meaning that known attack scenarios cannot be implemented on the communication.

TLS

TLS is a hybrid encryption protocol and is an integral part of HTTPS encryption. It is used to authenticate clients and servers during data transmission on the Internet. Endress+Hauser uses new TLS versions. The use of older versions to support older browser versions is constantly reviewed and reevaluated.

SSH
Secure Shell (SSH) refers to both a network protocol and programs that can be used to securely establish an encrypted network connection with a remote device. Endress+Hauser uses SSH for remote maintenance of the Monitoring Box gateway. The services used for remote maintenance are not directly accessible from the Internet or from the local area network.

TCP
The standard transmission control protocol (TCP) is used for data transfer from the analyzer or sensor to the gateway.

Serial protocols
Sensors and analyzers that do not have a TCP interface can be connected to the Monitoring Box via serial protocols such as Modbus RTU.

4. Cybersecurity

Endress+Hauser has implemented various cybersecurity measures to protect the system against malware and other IT security threats. The initial focus here was on an independent external security audit. Based on the results, relevant issues relating to data security and data integrity were then identified and specific measures were derived for addressing them.

External security audit
Endress+Hauser has commissioned an independent company to carry out the security audit. During this audit, various aspects of the Monitoring Box relating to cybersecurity were tested extensively and comprehensively.

4.1. General checks

The starting point for the external audit was a thorough analysis of the dashboard application. As part of this measure, the authentication and authorization mechanisms used were tested in the first step. The focus here was particularly on the following: It had to be ensured that individual users could only perform the actions for which they had previously been authorized.

Another focus of this analysis was a comprehensive investigation of the encryption technologies used during data communication.

4.2. Penetration test

In the next step, the external service provider performed a penetration test using the open interfaces of the Monitoring Box. The service provider analyzed in detail the communication between the gateway and the server, as well as between the dashboard and the server. Any vulnerabilities revealed during testing were subsequently revised and remedied.

4.3. Weak point analysis

Finally, as part of the audit, a detailed vulnerability analysis was carried out between the development team at Endress+Hauser and the auditors from the external service provider. This analysis forms the basis for the derived follow-up measures in particular. During this analysis, the planned further developments of the Monitoring Box were also discussed and the associated new attack scenarios identified.

4.4. Continuous development

After completion of the audit, the findings were used to firmly anchor them in the continuous development of the Monitoring Box. For example, the software packages used on both the gateway and the server are regularly and automatically checked against known vulnerability lists from various providers to enable a timely and rapid response if necessary.

5. Attack scenarios and countermeasures

Endress+Hauser's focus is on information security for the Monitoring Box. When it comes to information security, a distinction can be made between data security and data integrity. Both will be discussed in more detail below.

5.1. Data security

Data security is ensured in a system or transmission when data is not lost and unauthorized persons cannot copy or read it. Communication between the gateway and server, and between the server and dashboard, is encrypted at all times and secured by the role-based authorization concept. A cache on the gateway prevents data loss. Theoretical attack scenarios for interrupting encrypted communication usually require physical access to the gateway. Restricting access to the site of operation can prevent such attacks from the outset.
As another example, targeted denial-of-service attacks could compromise data integrity. This is because during the attack, it is – at least temporarily – impossible to retrieve or save new data. One variant of such an attack is, for example, a distributed denial-of-service attack. This involves using a network of computers to overload the system with requests. This can lead to server failure and, as a result, failure of data transmission from the server to the frontend. The server infrastructure used is secured with standard mechanisms to protect against such attacks. Furthermore, the underlying authorization mechanism provides an additional layer of protection, as access is only possible for logged-in users, who can be easily identified in the event of such an attack and then blocked immediately.

5.2. Data integrity

Data integrity describes the correctness of the data. With regard to condition monitoring, manipulation of a sensor's status data could mean that the operator of a plant does not notice the failure of a sensor, which could lead to damage and problems in the process. To prevent such manipulation, it is necessary to ensure that the transmitted data cannot be manipulated and that no artificial data can be transmitted.

Here too, the above-mentioned access restrictions to the Monitoring Box gateway offer protection against manipulation of the gateway. As an additional measure, communication between the gateways is also equipped with an authorization concept. It ensures that third parties are unable to feed false data into other devices.

We use the principle of key rotation for this purpose.

5.3. Conclusion

With the help of the numerous measures and protective precautions mentioned, Endress+Hauser offers a secure solution for condition monitoring. By way of an externally conducted audit, the protection was verified by an independent body and improved for the application. The introduction of continuous monitoring mechanisms for the software and applications used means that the cloud's security system is constantly checked, improved, and kept up to date with the latest technology.

Due to the security risk posed by humans, an external attack can never be completely ruled out, but the risk of an attack on the Endress+Hauser Monitoring Box is considered low, and the effort required to do so is significantly increased for potential attackers due to the precautions that have been taken.

Due to the unidirectional connection between the gateway and the sensor, it is difficult for the Monitoring Box system to access the sensor. The risk of damage to the sensor or customer network is considered to be virtually non-existent.

5.4. Endress+Hauser PSIRT

Endress+Hauser PSIRT is part of Endress+Hauser's company-wide cybersecurity policy and serves as a point of contact and information for customers, government agencies, suppliers, security researchers, and other stakeholders regarding the cybersecurity of Endress+Hauser solutions.

To ensure a consistent and coordinated approach to cybersecurity vulnerabilities, Endress+Hauser PSIRT operates a central vulnerability and incident management system.

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

Endress+Hauser
People for Process Automation