Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

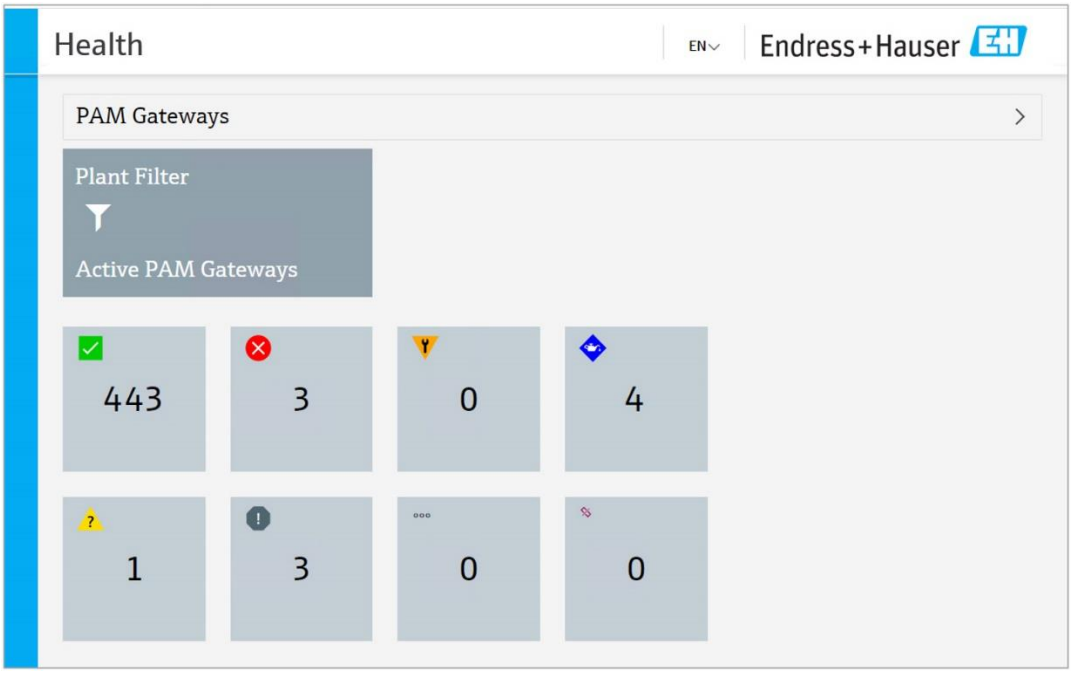
Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser SE+Co. KG.

Sonderdokumentation

Security-Handbuch
Asset Health Monitoring Solution SAH70

Asset Health Monitoring Software



Anmerkungen: / /		Projekt: 12230013 Asset Health Monitoring Solution SAH70	
Status: Released	Datum: 21.07.2023	Autor: Andreas Ernst	
Version: 1.00	Dokumentennummer: D055-1	Dateiname: AHM Solution SAH70 - Security_Handbuch D055_DE.docx	Seite: 1 von 22

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Inhaltsverzeichnis

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

1 Meldung von Sicherheitslücken und Advisories

Auf der folgenden Internetseite stellt Endress+Hauser Informationen zur Cybersicherheit

sowie zur Security bereit: https://www.endress.com/cybersecurity

Diese Internetseite enthält beispielsweise folgende Informationen:

- Aktuelle Sicherheitswarnungen (Security Alerts), die Endress+Hauser Produkte betreffen
- Kontakt-Mailadresse, um Sicherheitslücken von Endress+Hauser Produkten zu melden. Über PGP besteht die Möglichkeit zur vertraulichen Kommunikation. Sie können den öffentlichen Schlüssel von der Internetseite herunterladen.
- Abonnement des E-Maildienstes für neue Advisories für Endress+Hauser Produkte
- Endress+Hauser Kontakt: PSIRT@endress.com

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

2 Hinweise zum Dokument

2.1 Dokumentfunktion

Dieses Security-Handbuch gilt ergänzend zu der mitgeltenden Produktdokumentation wie z.B. Betriebsanleitung, Technischen Information und ATEX-Sicherheitshinweisen. Die mitgeltende Produktdokumentation ist während des gesamten Lebenszyklus des Produkts zu beachten. Die für den Bereich Security zusätzlichen Anforderungen sind in diesem Security-Handbuch beschrieben.

2.2 Verwendete Symbole

2.2.1 Warnhinweissymbole

⚠ GEFAHR
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen wird.

⚠ WARNUNG
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen kann.

⚠ VORSICHT
Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu leichter oder mittelschwerer Körperverletzung führen kann.

HINWEIS
Dieser Hinweis enthält Informationen zu Vorgehensweisen und weiterführenden Sachverhalten, die keine Körperverletzung nach sich ziehen.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

2.2.2 Symbole für Informationstypen und Grafiken

Tipp
Kennzeichnet zusätzliche Informationen

Verweis auf Dokumentation

Verweis auf Abbildung

▶
Zu beachtender Hinweis oder einzelner Handlungsschritt

1., 2., 3.
Handlungsschritte

Ergebnis eines Handlungsschritts

1, 2, 3, ...
Positionsnummern

A, B, C, ...
Ansichten

2.3 Dokumentation

2.3.1 Mitgeltende Dokumente

Eine Übersicht über die zugehörige Dokumentation erhalten Sie wie folgt:
- *W@M Device Viewer* (www.endress.com/deviceviewer): Seriennummer vom Typenschild eingeben
- Downloadbereich der Endress+Hauser Internetseite (www.endress.com/download)

Mitgeltende Dokumente AHM Solution

- Technische Information TI01544S
- Betriebsanleitung BA01682S
- Installationsanleitung
- FieldCare SFE500 Betriebsanleitung BA00065S

2.3.2 Zweck und Inhalte der Dokumentationstypen

Technische Information (TI)

Planungshilfe
Das Dokument liefert alle technischen Daten zum Gerät und gibt einen Überblick, was rund um das Gerät bestellt werden kann.

Kurzanleitung (KA)

Schnell zum 1. Messwert
Die Anleitung liefert alle wesentlichen Informationen von der Warenannahme bis zur Erstinbetriebnahme.

Betriebsanleitung (BA)

Ihr Nachschlagewerk
Die Anleitung liefert alle Informationen, die in den verschiedenen Phasen des Lebenszyklus vom Gerät benötigt werden: Von der Produktidentifizierung, Warenannahme und Lagerung über Montage, Anschluss, Bedienungsgrundlagen und Inbetriebnahme bis hin zur Störungsbeseitigung, Wartung und Entsorgung.

Sicherheitshinweise (XA)

Sicherheitshinweise (XA)

Abhängig von der Zulassung liegen dem Produkt bei Auslieferung Sicherheitshinweise (XA) bei. Diese Sicherheitshinweise sind integraler Bestandteil der Betriebsanleitung.

Auf dem Typenschild ist angegeben, welche Sicherheitshinweise (XA) für das jeweilige Produkt relevant sind.

Sonderdokumentation (SD)

Sonderdokumentation (SD)

Weitere Informationen
Eine Sonderdokumentation liefert weitere Informationen zu dem Produkt. Weitere Informationen können z.B. die Inbetriebnahme grafisch dargestellt oder Informationen zu einer App sein.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

3 System-Design

3.1 Zielgruppe

Dieses Kapitel richtet sich an Planer und Systemintegratoren

3.2 Systemüberblick

3.2.1 Allgemeine Informationen

Die Inbetriebnahme der AHM Solution erfolgt durch den Service von Endress+Hauser.

Das Produkt wird auf einem Microsoft Windows Betriebssystem ausgeführt und das System verfügt dementsprechend über eine Bedienoberfläche, Eingabemöglichkeiten und Benutzerverwaltung.

Zusätzlich nutzt die AHM Solution folgende Schnittstellen:

- HTTP (empfohlen HTTPS)
- WCF
- EtherNet/IP
- HART

3.2.2 Systemaufbau und Systemgrenzen

In diesem Security-Handbuch wird die AHM Solution, bestehend aus dem AHM Server, PAM Gateways, PAM Clients und deren Verbindung zu Gateways und Feldgeräten betrachtet. Die weiteren Komponenten wie Bedientools sind keine Bestandteile dieses Security-Handbuches. In der folgenden Abbildung sind die Systemgrenzen farblich markiert.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

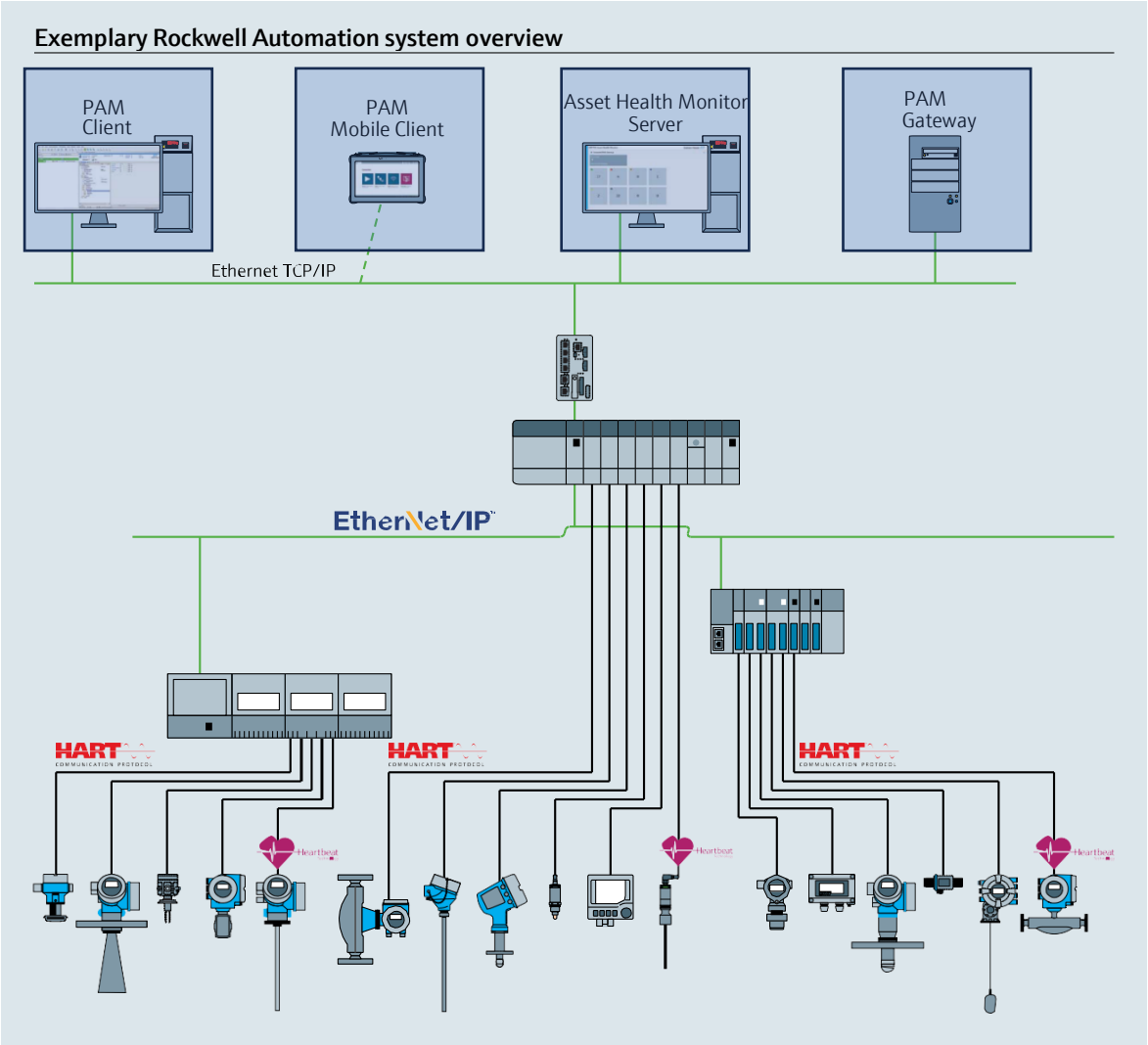


Abbildung 1 Beispielhafter Systemaufbau

Die AHM Solution wird in diesem Dokument in den allgemeinen Texten abhängig vom Zusammenhang als Produkt bezeichnet.

Im Folgenden werden PAM Client und PAM Mobile Client nicht unterschieden und generell als PAM Client bezeichnet.

Der AHM Server und das PAM Gateway werden auf Microsoft Windows ausgeführt, welches im folgenden als Hostsystem bezeichnet wird. Dies kann nativ auf einem PC oder in einer virtuellen Umgebung installiert sein.

3.3 Security-Level festlegen

Abhängig vom angestrebten Security-Level müssen das System und die darin installierten Produkte unterschiedlich hohe Anforderungen erfüllen. Als erstes müssen Sie den erforderlichen **Security-Level** SL1 bis SL4 für das System festgelegen. Abhängig von dem Security-Level leiten Sie gemäß DIN IEC 62443-3-3 die Anforderungen an das System und gemäß DIN EN 62443-4-2 die Anforderungen an die Produkte ab.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

3.4 Typische Einsatzumgebung des Produktes

Wir empfehlen für die Festlegung der Security-relevanten Eigenschaften des Produkts die typische Einsatzumgebung zu definieren.

Die Betrachtung der Einsatzumgebung soll zu den Anforderungen durch die Umgebung führen. Beispielsweise können Sie einen Denial-of-Service-Angriff betrachten.

Für eine typische Einsatzumgebung könnten z.B. folgende Punkte zutreffen:

- Das Produkt ist eine Systemkomponente.
- Das Produkt wird in einer industriellen Umgebung betrieben.
- Der Zugang zum Hostsystem, auf dem das Produkt installiert ist, ist reglementiert. Nur autorisierte Personen haben Zugang zum Hostsystem.
- Das Personal ist in dem Gebrauch des Produkts und in die Security-Risiken unterwiesen.
- Das Produkt wird in einem Ethernet-Netzwerk, das nur für industrielle Zwecke vorgesehen ist, betrieben. Das Netzwerk ist entweder vollständig vom restlichen Unternehmensnetzwerk getrennt oder durch Firewalls geschützt.
- Das Produkt verfügt optional über eine durch HTTPS geschützte Datenverbindung, die den Produktionsbereich verlässt. Die Authentifizierung für den Zugriff wird vom Betreiber sichergestellt.
- Das Automatisierungsnetz ist über einen Perimeterschutz gegen Angriffe von außen wie z.B. einen Denial-of-Service-Angriff geschützt.
- Das Produkt ist in einer Umgebung installiert, die nach dem Defense-in-Depth-Konzept abgesichert ist.
- Passworte für das Produkt sind nur autorisierten Personen bekannt.
- Nur autorisierten Personen können über das zugehörige Human Machine Interface (HMI) auf das Produkt zugreifen.
- Da die Rechenleistung des Hostsystems begrenzt ist, können bestimmte Angriffe nur in begrenztem Umfang abgewehrt werden.

3.5 Maßnahmen, falls erforderliche Einsatzumgebung nicht erfüllbar ist

Sofern die spezifizierten Anforderungen an die Einsatzumgebung nicht eingehalten werden können, sind ggf. Ersatzmaßnahme vorzusehen. Dabei kann es sich z.B. um einen mechanischen Schutz des Produkts gegen Manipulation, einen mechanischen Schutz der Verkabelung oder auch um organisatorische Maßnahmen handeln.

3.6 Bedrohungsanalyse und Risikobeurteilung durchführen

Bei der Planung einer Anlage müssen Sie für die gesamte Anlage eine Risikobeurteilung in einem gesamtheitlichen Ansatz durchführen. Für die Risikobeurteilung von Anlagen können Sie sich an der VDI 2182 orientieren.

Im Zuge der Risikobeurteilung führen Sie eine Risikoanalyse / Bedrohungsanalyse durch.

Beachten Sie für die Risikoanalyse folgende Aspekte:

- Schnittstellen des Produkts, über die eine Kommunikation mit dem Produkt möglich ist oder über die auf das Produkt zugegriffen werden kann.
- Datenflüsse des Produkts innerhalb der Anlage

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

- Zum Produkt eingehende Daten
- Vom Produkt ausgehende Daten

- Datenflüsse des Produkts, die den Bereich der Anlage verlassen und ggf. Firewalls überwinden

Aus der Risikoanalyse können Sie risikomindernde Maßnahmen ableiten.

Neben der Risikobeurteilung sollten im Planungsprozess auch Festlegungen getroffen werden, wie das Produkt während der Inbetriebnahme zu konfigurieren ist. Hierzu gehören z.B. das Abschalten nicht benötigter Schnittstellen und/oder Dienste. Das Abändern von Standardpassworten usw. Diese Maßnahmen werden in den folgenden Kapiteln vorgestellt.

3.7 Empfehlung für risikomindernde Maßnahmen

3.7.1 Gesamtsystem betrachten

Die AHM Solution ist eine Anwendung, die in einem Produktionssystem eingesetzt wird.

Ein Produktionssystem kann schnell zu einem Stückwerk aus verschiedenen Endgeräten werden. Jedes abweichende Produkt stellt bei solchen heterogenen Gesamtlösungen eine neue Gefahrenquelle dar, die Brüche an den Schnittstellen erzeugt und zu unsicheren Übertragungswegen führen kann.

In diesem Handbuch wird die AHM Solution von Endress+Hauser betrachtet. Für das Gesamtsystem sind zusätzliche Analysen erforderlich.

Netzwerk

Besondere Beachtung sollte den eingesetzten Netzwerkkomponenten (z.B. Router und Switches) gelten. Die Integrität der Komponenten sowie der Zugriff auf das Netzwerk muss vom Betreiber sichergestellt bzw. eingeschränkt werden. Daher, dass im aktuellen Stand der AHM Solution der PAM Client, der AHM Server und das PAM Gateway nicht verschlüsselt miteinander kommunizieren, kann ansonsten ein Angreifer vollständigen Zugriff auf Komponenten des Steuerungssystems (z.B. Feldgeräte) erlangen.

DTMs

Für die Konfiguration von Feldgeräten werden in der AHM Solution DTMs verwendet. Diese dürfen nur aus vertrauenswürdigen Quellen stammen und die Herkunft muss vor der Installation über digitale Signaturen validiert werden.

3.7.2 Anwender schulen

Je nach Anwendungsszenario können auch fachfremde Anwender mit dem System in Berührung kommen. Wir empfehlen, diese Anwender für den sicheren Gebrauch mit den entsprechenden Endgeräten und / oder Schnittstellen zu schulen und für die Security zu sensibilisieren (siehe Kapitel 5.3)

3.7.3 Zugriffsmanagement optimieren

Im aktuellen Stand der AHM Solution findet in der Web Anwendung sowie der Konfiguration mittels PAM Client kein Zugriffsmanagement statt. Das bedeutet das jede Person, die die Möglichkeit hat über das Netzwerk mit dem Produkt zu kommunizieren, Zugriffe auf alle vom Produkt angebotenen Schnittstellen und Daten hat. Deswegen empfehlen wir die in Kapitel 4.4.3 und 4.4.4 empfohlenen Maßnahmen umzusetzen.

Host- und Clientsysteme

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Wir empfehlen, für den Zugriff auf das Hostsystem die gleichen Regeln für das Identitäts- und Zugriffsmanagement wie für die anderen Unternehmensbereiche anzusetzen.

- Mitarbeitern nur die Zugriffsrechte geben, die der Mitarbeiter zur Erfüllung seiner Aufgaben benötigt
- Benutzerkonten (Accounts) nur mit starken Passwörtern vergeben
- Passwörter über einen Passwort-Manager generieren, sichern und verwalten
- Für verschiedene Dienste verschiedene Passwörter verwenden
- Automatisches Sperren, wenn das System nicht mehr verwendet wird

Wir empfehlen das Hostsystem (AHM Server und PAM Gateway) dediziert für das Produkt zu verwenden und keine weiteren Anwendungen dort zu installieren. Auch sollten keine weiteren User auf dem Hostsystem arbeiten dürfen, da diese die Möglichkeit haben auf die Konfiguration oder die Daten des Produktes zuzugreifen.

3.7.4 Gerätedaten und Gerätestatus überwachen

Viele Angriffe auf ein Produkt in einem System erzeugen Anomalien im Netzwerkverkehr. Wenn ein Produkt plötzlich unrealistische Werte liefert, kann das ein Indiz für einen Angriff sein.

Da ein Echtzeit-Monitoring für die meisten Anwender nicht in Frage kommt, muss dieser Vorgang automatisiert werden. Wir empfehlen eine Monitoring-Software einzusetzen, die bestimmte Parameter und den Zustand des Produkts und des Netzwerks überwacht und bei Abweichungen informiert.

Die AHM Solution ist eine Software im Produktionssystem und die Erkennung von Anomalien ist eine Aufgabe des übergeordneten Systems

Überwachung über EtherNet/IP oder HART

Die AHM Solution ist über EtherNet/IP und HART an ein Steuerungssystem angebunden sein. Die Kommunikation mit den Geräten erfolgt meistens unverschlüsselt. Der physikalische Schutz, eine Erkennung und die Behebung von Anomalien ist Aufgabe des Betreibers des Steuerungssystems.

3.7.5 Produkt-Software updaten

Aufgrund der Dynamik in der IT, wachsenden Anforderungen in der Vernetzung und dem Einsatz von Softwarebibliotheken sind Updates erforderlich.

Wir empfehlen, regelmäßig zu prüfen, ob neue Updates zur Verfügung stehen und die Updates zu installieren. Versäumte Updates sind ein akutes Security-Risiko, da auch Angreifer über die zu behebenden Schwachstellen informiert sein könnten.

3.7.6 Anwendungen und Apps schützen

Software und insbesondere eine heterogene Software-Landschaft stellen ein weiteres Security-Risiko dar, wie z.B. Einsatz von Android-Apps auf einem Tablet und Windows-Lösungen auf einem PC.

Zur Sicherung der Anwendungen sollte auch der Schutz der mobilen und stationären Endgeräte gewährleistet sein, die auf die AHM Solution Zugriff haben. Dies beinhaltet regelmäßiges Installieren von Betriebssystem- und Anwendungsupdates sowie der Einsatz eines Virenscanners.

Zum Schutz des Kundensystems und der Kundendaten sollte auch der Schutz der Zugangsdaten der Endgeräte gewährleistet sein. Zugangsdaten und Zertifikate sollten sicher aufbewahrt werden.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

4 Inbetriebnahme (Installation und Konfiguration)

4.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

4.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:

- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

4.3 Installation

Produkt gemäß zugehöriger Kurzanleitung / Betriebsanleitung montieren und elektrisch anschließen.

4.4 Konfiguration

4.4.1 Produkt in Betrieb nehmen und konfigurieren

Produkt gemäß zugehöriger Kurzanleitung / Betriebsanleitung in Betrieb nehmen und konfigurieren. Für den Bereich "Security" zusätzlich dieses Kapitel und die weiteren Kapitel beachten.

Die Inbetriebnahme der AHM Solution erfolgt durch den Service von Endress+Hauser.

Eine Integritäts- und Authentizitätsprüfung der Installationsdateien muss durch die Person, die das Produkt installiert, durchgeführt werden. Die Installationsdateien sind dafür digital signiert.

Klicken Sie hierfür mit der rechten Maustaste auf die Installationsdateien und wählen Sie die Eigenschaften der Datei aus.

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

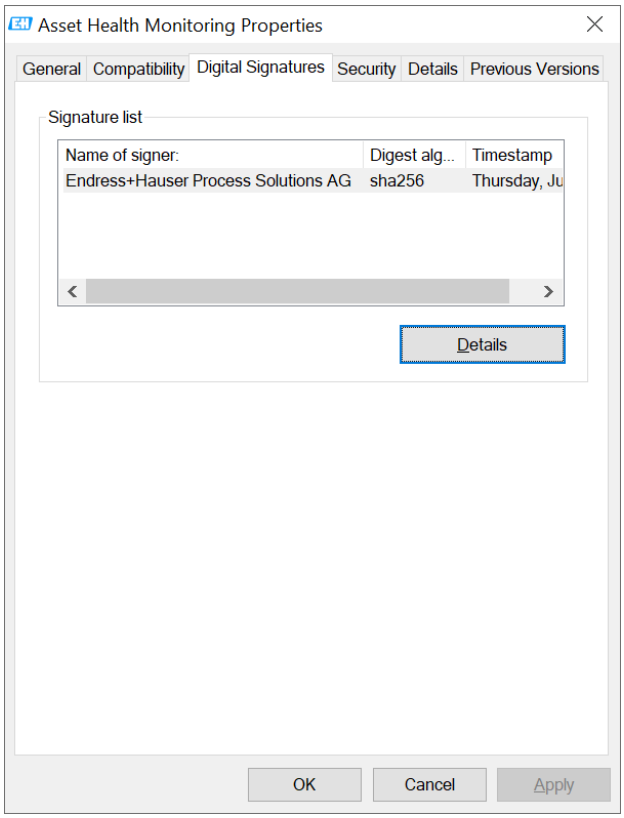


Abbildung 2 Prüfung der digitalen Signatur

Wechseln Sie hier auf den Tab „Digital Signatures“ und verifizieren Sie, dass der „Name of Signer“ „Endress+Hauser Process Solutions AG“ enthält. Wenn hier der Reiter "Digital Signatures“ nicht vorhanden ist oder der „Name of Signer“ abweicht, dürfen Sie die Datei unter keinen Umständen ausführen. Die Datei stammt dann nicht von Endress+Hauser und enthält möglicherweise Schadsoftware.

Es wird empfohlen den AHM Server und das PAM Gateway auf einem Host zu betreiben und nicht auf getrennten Hosts zu installieren. Die Kommunikation untereinander findet im aktuellen Stand der Lösung über einen nicht verschlüsselten Kanal statt. Sollte aus technischen Gründen die Installation auf einem Host nicht möglich sein, empfehlen wir die in Kapitel 3.7.1 beschriebenen Maßnahmen besonders zu betrachten.

Systemüberblick AHM Solution: → 3.2

4.4.2 Erforderliche Security-Schritte während der Inbetriebnahme

Aktivieren von HTTPS für die Web Anwendung

Damit die Web Anwendung verschlüsselt kommuniziert und der Nutzer die Authentizität der Anwendung sicherstellen kann, muss HTTPS aktiviert werden. Darüber hinaus empfehlen wir ein speziell für den Server generiertes Zertifikat zu verwenden.

Deaktivieren des PAM Services auf dem PAM Gateway

Der PAM Service ist ein Hintergrunddienst der Services anbietet, die in der AHM Solution nicht verwendet werden. Daher wird die Deinstallation des PAM Services und des PAM Agents auf dem PAM Gateway empfohlen. Öffnen sie dazu die Windows Einstellungen und deinstallieren sie dort die beiden Anwendungen, wie in Abbildung 3 Deinstallation nicht benötigter Software zu sehen.

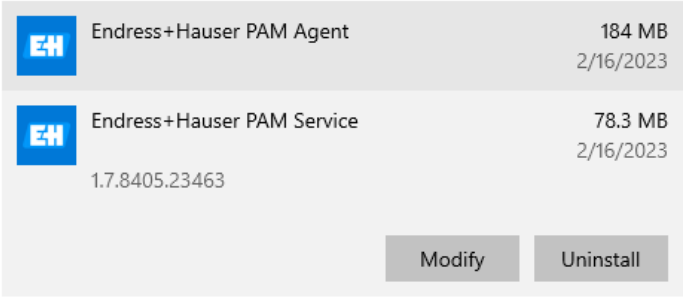


Abbildung 3 Deinstallation nicht benötigter Software

4.4.3 Firewall konfigurieren

Es dürfen nur folgende Ports für den Betrieb der AHM Solution in der Windows Firewall freigegeben werden:

- TCP 443 (HTTPS für den Zugriff auf die Web Anwendung)
  Auf der Schnittstelle findet in der aktuellen Version der AHM Solution keine Autorisierung statt. Deswegen empfehlen wir, wenn möglich den Scope einzuschränken, indem nur Verbindungen von bestimmten IP-Adressen angenommen werden (IP Whitelisting).

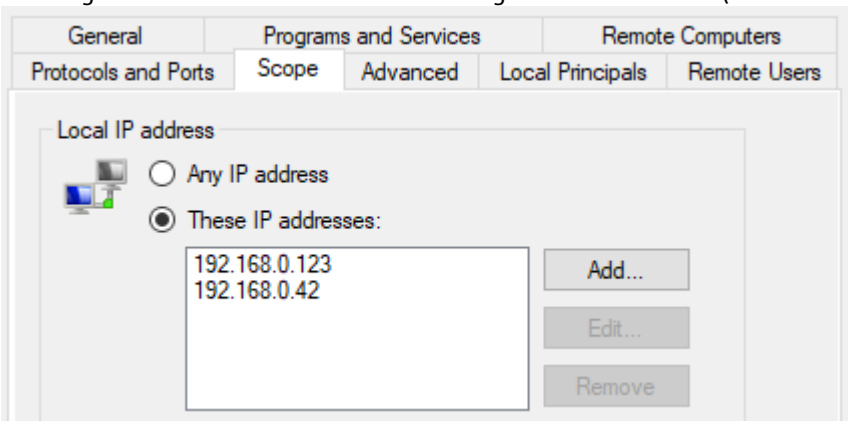


Abbildung 4 Festlegen des Scopes in einer Firewall Regel

- TCP 8302 (Port für die Verbindung von PAM Clients)
  Nicht gesicherte Verbindung, die nur zugelassen werden sollte wenn die Konfiguration über PAM Clients verwendet wird.
  Wir empfehlen beim Anlegen der Firewall Freigaben auch den Scope zu konfigurieren und nur die Verbindung von IP-Adressen zuzulassen, bei denen es sich um zugelassen PAM Clients handelt.

- TCP 1433, UDP 1434 (Port für die Kommunikation zwischen AHM Server und PAM Gateway)
  Nur auf dem PAM Gateway, wenn der AHM Server auf einem anderen Host betrieben wird.
  Wir empfehlen auch hier beim Anlegen der Firewall Freigaben den Scope zu konfigurieren und nur die Verbindung des AHM Servers zuzulassen.

4.4.4 Produkt härten

Im Bereich Security bedeutet "Härten", dass nur die Dienste freigeschaltet werden, die für den ordentlichen Betrieb des Produkts für den vorliegenden Anwendungsfall erforderlich sind.

Web Reporter

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Der Web Reporter ist eine mit der AHM Solution ausgeliefertes Modul von FieldCare 2. Der Web Reporter wird nicht mehr gepflegt und wir empfehlen daher diesen zu deaktivieren.

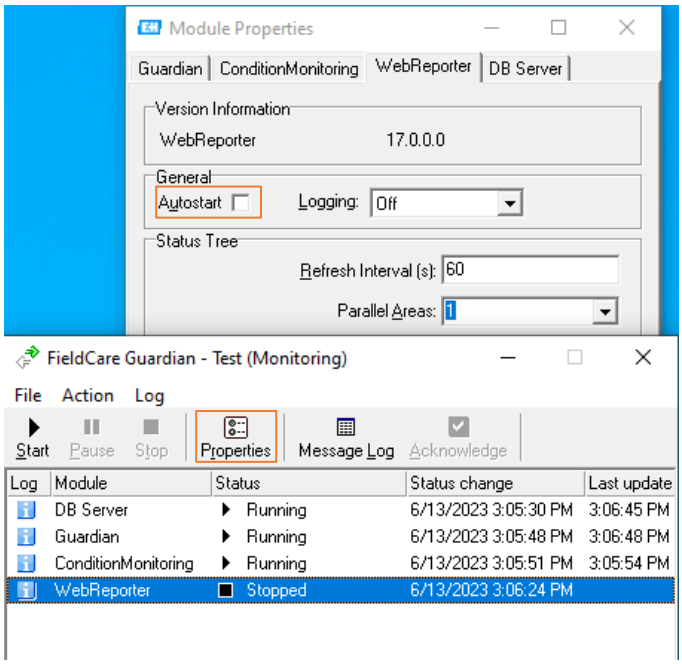


Abbildung 5 Ausschalten des Web Reporters

Communication Service

Wenn die Konfiguration über PAM Clients nicht verwendet wird, sollte in der FieldCare Administration auf dem PAM Gateway der Communication Server deaktiviert werden. Für die entsprechende Konfiguration siehe Installationsanleitung 2.3.5

Soll die Konfiguration über PAM Clients verwendet werden, sind die in Abschnitt 3.7.1 beschriebenen Maßnahmen zwingend erforderlich.

Wenn möglich empfehlen wir den Communication Service nur vorübergehend zu aktivieren.

4.4.5 Anwenderdaten konfigurieren

Anwenderdaten sind z.B. Login-Daten, Benutzer, Messstellenbezeichnung (TAG), Passwörter, IDs usw.

siehe FieldCare Betriebsanleitung Kapitel 3.1.2

4.4.6 Security-relevante Einstellung des Produktes

Log Level

Das Produkt wird mit einem sicheren Log Level installiert. Niedrigere Log Level wie Trace oder Debug können Informationen über Feldgeräte enthalten und sollten nur für die Diagnose von Problemen vorübergehend eingestellt werden. Log Files müssen grundsätzlich vertraulich behandelt werden.

4.4.7 User-Management und Auswirkungen auf die Security

siehe FieldCare Betriebsanleitung: → 2.3.1

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

5 Betrieb

5.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

5.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:

- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

5.3 Aufgaben während des Betriebs

Produkt gemäß zugehöriger Betriebsanleitung betreiben. Für den Bereich "Security" zusätzlich dieses Kapitel und die folgenden Kapitel beachten.

Während der Eingabe von Passwörtern muss darauf geachtet werden, dass niemand die Eingaben beobachten kann. Wenn ein Passwort nicht mehr vertrauenswürdig ist, muss das entsprechende Benutzerkonto umgehend gesperrt oder das Passwort geändert werden.

Im Browser muss der Anwender beim Zugriff auf den AHM Server die sichere Verbindung zum AHM Server validieren, die meistens über ein Schloss neben der Adresszeile symbolisiert wird.

Beim Verlassen des Arbeitsplatzes muss der Anwender seinen Arbeitsplatz sperren, um unbefugten Zugriff auf das Produkt auszuschließen.

5.4 Security Aspekte während des Betriebs

Windows Updates

Windows Updates für das Hostsystem auf denen die AHM Solution installiert ist müssen regelmäßig installiert werden.

HTTPS Zertifikate

Die Zertifikate für die HTTPS Verbindung haben eine begrenzte Laufzeit und müssen regelmäßig erneuert werden.

5.5 Update-Management

Endress+Hauser stellt Updates für die AHM Solution bereit. Updates werden vom Endress+Hauser Service installiert.

Endress+Hauser stellt Updates für folgende Fälle bereit:

- Security-Updates
- Bugfixes: Fehlerbehebungen bestehender Funktionen

- Funktionale Erweiterungen des Produkts

Endress+Hauser stellt durch Prüfsummen und Signaturen in der Software die Integrität und Authentizität der Updates sicher. Eine Integritäts- und Authentizitätsprüfung der Updates muss durch die Person, die das Update installiert durchgeführt werden. Wie die Signatur geprüft werden kann ist in Kapitel 4.4.1 beschrieben.

Updates werden im Endress+Hauser Software Portal veröffentlicht:

https://software-products.endress.com/

5.6 Wiederholung der Bedrohungsanalyse

Die Bedrohungssituation von Anlagen kann sich durch externe Ereignisse wie z.B. durch Auftreten bisher unbekannter Angriffsmuster, ändern. Gemäß der VDI/VDE 2182-1-2011, Kapitel 4.4 muss die Bedrohungsanalyse in regelmäßigen Abständen oder bei Änderungen der Anlage, die Einfluss auf die Bedrohungsanalyse haben können, wiederholt und aktualisiert werden.

5.7 Reparatur und Entsorgung

/

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

6 Außerbetriebnahme

6.1 Zielgruppe

Dieses Kapitel richtet sich an das Betriebspersonal.

6.2 Anforderungen an das Personal

Das Personal muss folgende Bedingungen erfüllen:

- Über eine fachliche Qualifikation verfügen, die dieser Funktion und Tätigkeit entspricht.
- Vom Anlagenbetreiber autorisiert.
- Mit den nationalen Vorschriften vertraut.
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen.
- Anweisungen und Rahmenbedingungen befolgen.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

6.3 Produkt außer Betrieb nehmen

Für eine Außerbetriebnahme des Produkts gibt es verschiedene Gründe. Abhängig von dem Grund der Außerbetriebnahme sind entsprechende Handlungen erforderlich.

Grund der Außerbetriebnahme	Erforderliche Handlungen
Das Produkt wird für längere Zeit nicht genutzt.	Ausschalten der Hostsysteme, oder wenn nicht möglich zu mindestens Beenden der Prozesse
Das Produkt hat eine Störung und Sie können die Störung nicht beheben.	Endress+Hauser kontaktieren
Das Produkt soll entsorgt werden.	Wir empfehlen vor der Entsorgung oder Verschrottung der physikalischen Medien, auf denen das Produkt installiert war gemäß folgender Richtlinie vorzugehen: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Alle Rechte vorbehalten. Das Kopieren dieses Dokuments und die Verwendung von Teilen aus diesem Dokument ist ohne schriftliche Genehmigung der Endress+Hauser Solutions AG nicht erlaubt.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

7 Anhang

7.1 Security Checkliste für den Produktlebenszyklus

Lebenszyklus	Tätigkeit	Geprüft
Planung	Typische Einsatzumgebung des Produkts definiert und bei der Planung berücksichtigt. → 3.4 Falls erforderlich, Ersatzmaßnahmen berücksichtigt. →3.5	❑
	Planungsarbeiten in der Engineering-Phase beachtet. Bedrohungsanalyse und Risikobeurteilung durchgeführt. → 3.6	❑
	Sofern möglich, risikomindernde Maßnahmen berücksichtigt. → 3.7	❑
Wareneingang / Transport	Geprüft, dass die Signatur der gelieferten Dateien Endress+Hauser als Hersteller identifiziert	❑
Inbetriebnahme	Produkt für den Anwendungsfall gehärtet. → 4.4	❑
Betrieb	Vorgaben zum Betrieb beachtet. → 5.3, 5.4	❑
	Vorgaben zum Update-Management beachtet. → 5.5	❑
	Planung der wiederkehrenden Bedrohungsanalyse vorgenommen. → 5.6	❑
Außerbetriebnahme	Produkt außer Betrieb nehmen. → 6	❑

7.2 Versionshistorie

Dokumentenversion	Softwareversion	Änderungen
01.00	Ab 02.00.00	Erste Version