DE

Softwarehandbuch (Ergänzung)

Cyber-Security

moneo|edgeGateway

AE2100
AE2400

11621108 / 00 09 / 2024

Inhaltsverzeichnis

1 Vorbemerkung

1.1 Zweck des Dokuments

Dieses Dokument gibt einen Überblick über die Cyber-Security-Mechanismen für das moneo|edgeGateway von ifm.

Dieses Dokument stellt Informationen für Systemintegratoren und Maschinenbauer zur Verfügung, damit das moneo|edgeGateway in ein umfassendes Sicherheitskonzept integriert werden und zu einer robusten Sicherheitsarchitektur beitragen kann.

1.2 Verwendete Symbole

✓	Voraussetzung
▶	Handlungsanweisung
▷	Reaktion, Ergebnis
[...]	Bezeichnung von Tasten, Schaltflächen oder Anzeigen
→	Querverweis
	Wichtiger Hinweis Fehlfunktionen oder Störungen sind bei Nichtbeachtung möglich
	Information Ergänzender Hinweis

1.3 Mitgeltende Dokumente

- Datenblatt
- Kurzanleitung
- Betriebsanleitung
- Softwarehandbuch moneo|Appliance Management System (AMS)
- ifm moneo Online-Hilfe

2 Sicherheitshinweise

2.1 Cyber-Sicherheit

Installation

Das Gerät ist für den Betrieb in einer sicheren Umgebung gemäß IEC 62443-1-1 geeignet.

Das Gerät ist für den Betrieb hinter einer Firewall konzipiert.

- ▶ Eine Risikobeurteilung der Anlage nach IEC 62443-1-1 durchführen.
- ▶ Maßnahmen zur Sicherstellung der physikalischen Sicherheit ergreifen.

Benutzer- und Rechtemanagement

- ▶ Nur die entsprechend der Risikobeurteilung notwendigen Nutzerrechte vergeben.
- ▶ Bei der Einrichtung der Benutzerkonten die Vorgaben der Sicherheitsrichtlinie des Unternehmens beachten.
- ▶ Werkseitig eingestellte Passwörter sofort bei der Installation / Ersteinrichtung ändern.

Betrieb

- ▶ Nur Kommunikationsprotokolle mit ausreichend sicheren Verschlüsselungstechnologien verwenden.
- ▶ Die in der Gerätedokumentation beschriebenen Security-Funktionen und die Empfehlungen für deren Anwendung beachten.

Wartung

- ▶ Regelmäßig prüfen, ob Softwareaktualisierungen für das Gerät verfügbar sind.
- ▶ Systemkonfiguration und Systemdaten gemäß den Change-Management-Prozessen des Unternehmens sichern.

Außerbetriebnahme

- ▶ Vor der Außerbetriebnahme des Geräts die Systemeinstellungen immer auf die Werkseinstellungen zurücksetzen.
- ▶ Darauf achten, dass keine schützenswerten Informationen in unberechtigte Hände gelangen können.

3 Systemübersicht

Das moneo|edgeGateway ist ein Embedded-Gerät für den Schaltschrankeinbau oder Feldeinsatz.

Das moneo|edgeGateway dient als Endpunkt für die Bereitstellung von Daten aus der Produktionsumgebung zur Weiterverarbeitung in der moneo|cloud oder in anderen kundeneigenen Datenplattformen.

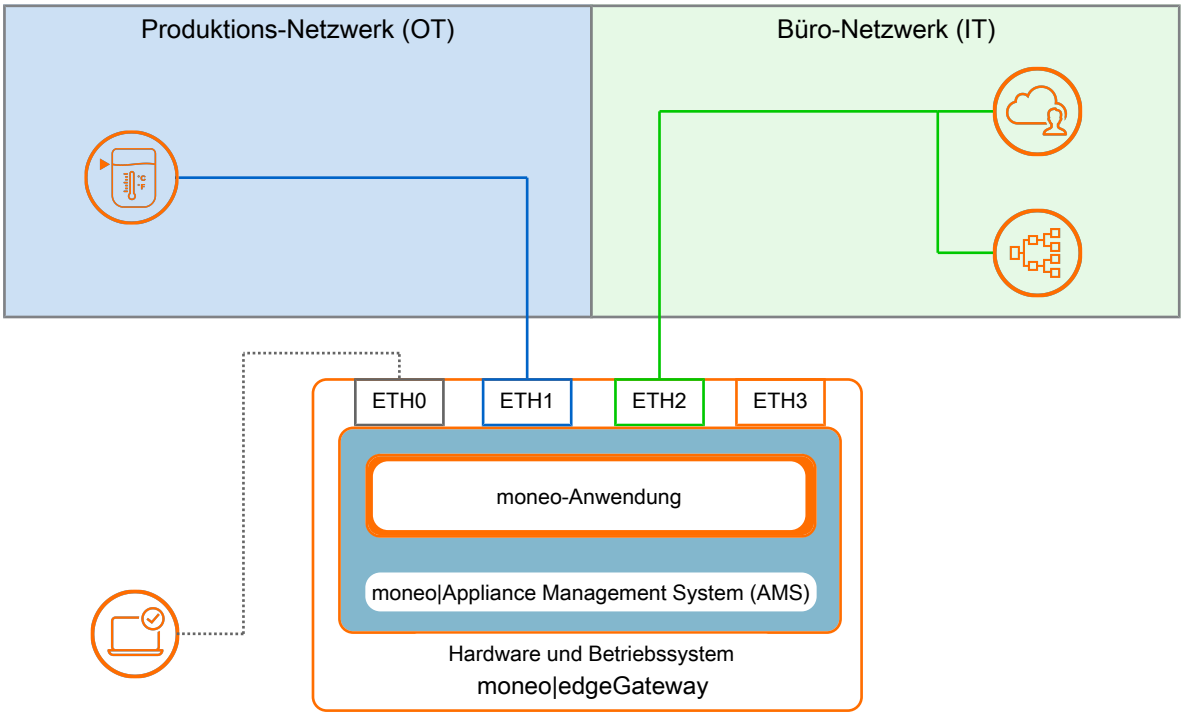

Abb. 1: moneo|edgeGateway Systemübersicht

Die folgende Tabelle beschreibt die einzelnen Bestandteile des moneo|edgeGateway und deren Funktion:

Bestandteil	Funktionalität
Hardware und Betriebssystem	Lüfterlose Embedded-Hardware für den Betrieb des gehärteten Debian Linux Betriebssystems.
Appliance Management System (AMS)	Webbasierte Management-Plattform für die Verwaltung des moneo|edgeGateway. Das AMS stellt alle notwendigen Verwaltungsschnittstellen für Administratoren bereit.
moneo-Anwendung	Die moneo-Applikation mit den einzelnen Modulen und Softwareschnittstellen wie MQTT, UPC-UA.
Ethernet-Port ETH0	Service-Schnittstelle Ausschließlich für die Inbetriebnahme des Geräts.
Ethernet-Port ETH1	OT-Schnittstelle Zur Verbindung des Geräts mit der OT-Netzwerkstruktur. Die Verbindung wird für die Kommunikation mit Geräten mit ifm IoT-Core (z. B. IO-Link Master) und den angeschlossenen Sensoren genutzt.
Ethernet-Port ETH2	IT-Schnittstelle Zur Verbindung des Geräts mit der IT-Netzwerkstruktur. Die Verbindung wird für die Kommunikation mit Cloud-Systemen genutzt.
Ethernet-Port ETH3	Deaktiviert und funktionslos

4 Netzwerkkommunikation

4.1 Segmentierung der Netzwerkschnittstellen

Das moneo|edgeGateway ermöglicht den gleichzeitigen Betrieb im Büro-Netzwerk (IT) und im Produktions-Netzwerk (OT).

IT- und OT-Netzwerk sind getrennt. Es ist sichergestellt, dass keine Kommunikation zwischen den Netzwerken über die Netzwerkschnittstellen des moneo|edgeGateways stattfinden kann.

IT-Sicherheitskonzepte werden dadurch nicht beeinträchtigt.

5 Anforderungen an die Netzinfrastruktur

Das moneo|edgeGateway ist für den Betrieb innerhalb einer sicheren Zone gemäß IEC 62443-1-1 vorgesehen.

Es werden keine Funktionalitäten bereitgestellt, die einen sicheren Zonenübergang gewährleisten bzw. reglementieren.

Nachfolgend werden Anforderungen an die Netzwerkumgebung beschrieben.

5.1 Standard-Netzwerkkommunikation

Je nach Einsatzgebiet und Nutzung des moneo|edgeGateway werden folgende Zugriffe auf entfernte Systeme benötigt, die aus dem Netzwerk erreichbar sein müssen.

Nicht in jedem Fall wird jede Freigabe benötigt.

- ▶ Prüfen, welche Freigaben für die Nutzung erforderlich sind.
- ▶ Die benötigten Freigaben in der Firewall einrichten.

Verwendung	Richtung	Quelle	Ziel-Adresse (URL)	Ports	Proto-koll	Beschreibung
OPC UA	Eingehend	Client	moneo OPC UA Server	4840	TCP	Kommunikation zwischen OPC UA Client und moneo OPC UA Server.
Web UI	Eingehend	Client	moneo	80, 443	TCP	Erforderlich für den Zugriff auf die moneo-Website über den Internetbrowser auf einem Linux-System
Web UI	Eingehend	Client	moneo	5000	TCP	Erforderlich für den Zugriff auf die moneo-Website über den Internetbrowser auf einem Windows-System
SFI /SAP	Eingehend	Client	moneo SfiHub (Graph-QL Server)	5050	TCP	Erforderlich für eine SFI/SAP Connection zur Bereitstellung von API-Informationen über Topology, ProcessData und moneo Tickets.
Namensauflö-sung	Ausgehend	System	DNS-Server	53	UDP/ TCP	Übersetzen von Domainnamen in IP-Adressen. Erforderlich, wenn mit Hostnamen anstelle von IP-Adressen auf moneo zugegriffen werden soll.
Zeitsynchronisation	Ausgehend	System	NTP-Server	123	UDP/ TCP	Erforderlich, um die Zeit systemübergreifend in einem Netzwerk zu synchronisieren und so genaue und konsistente Zeitstempel für Protokolle, Transaktionen und geplante Aufgaben zu gewährleisten (AMS Setup Wizard bezieht sich auf {0... 3}.pool.ntp.org)
EdgeConnect	Ausgehend	moneo	Azure IoT Hub	5671, 5672	TCP (AM-QP)	Erforderlich für die Nutzung eines Azure IoT Hubs zum Empfangen von Prozessdaten aus moneo.
EdgeConnect	Ausgehend	moneo	MQTT (default)	1883, 8883	TCP	Für die Nutzung eines MQTT Brokers zum Empfang von Prozessdaten aus moneo.
EdgeConnect	Ausgehend	moneo	AWS IoT Core	8883	TCP	Für die Nutzung eines AWS IoT Core zum Empfangen von Prozessdaten von moneo.

Verwendung	Richtung	Quelle	Ziel-Adresse (URL)	Ports	Protokoll	Beschreibung
remoteConnect	Ausgehend	remoteConnect client	global.azure-devices-provisioning.net	443	TCP	Device Onboarding und Konfiguration
remoteConnect	Ausgehend	remoteConnect client	rc-c-us-prod-iothub.azure-devices.net	8883	TCP	Device Onboarding und Konfiguration
remoteConnect	Ausgehend	remoteConnect client	relay0.remoteconnect-c-us-prod.moneo.ifm relay1.remoteconnect-c-us-prod.moneo.ifm	443	TCP	Remote Access Rendezvous Server in c-us
remoteConnect	Ausgehend	remoteConnect client	stun0.remoteconnect-c-us-prod.moneo.ifm stun1.remoteconnect-c-us-prod.moneo.ifm	3478	UDP	Remote Access Rendezvous Server für eine direkte P2P-Verbindung in c-us
remoteConnect	Ausgehend	remoteConnect client	relay0.remoteconnect-w-eu-prod.moneo.ifm relay1.remoteconnect-w-eu-prod.moneo.ifm	443	TCP	Remote Access Rendezvous Server in w-eu
remoteConnect	Ausgehend	remoteConnect client	stun0.remoteconnect-w-eu-prod.moneo.ifm stun1.remoteconnect-w-eu-prod.moneo.ifm	3478	UDP	Remote Access Rendezvous Server für eine direkte P2P-Verbindung in w-eu
Remote access	Ausgehend	ifm remote support	gm01-emea.ifm.com	443	TCP	Erforderlich, wenn ifm aus der Ferne auf das System zugreift, um Kundensupport zu leisten.
moneo cloud	Ausgehend	moneo	mqtt.w-eu.moneo.cloud mqtt.e-us.moneo.cloud	8883	TCP	Erforderlich für eine aktive Verbindung von einem Edge-Client zum entsprechenden Cloud-Cluster für den Prozessdatentransfer.
moneo cloud	Ausgehend	AMS	mqtt.moon-w-eu.moneo.cloud	8883	TCP	Erforderlich für das Cloud-Onboarding eines Edge-Clients in den entsprechenden Cloud-Cluster.
moneo cloud	Ausgehend	AMS	ifm-mobileiot-services-prod.azurewebsites.net	443	TCP	Erforderlich für das Cloud-Onboarding eines Edge-Clients in den entsprechenden Cloud-Cluster.
IODD descriptions	Ausgehend	moneo	https://ioddfinder.io-link.com	443	TCP	Erforderlich, um IODD-Dateien bei Bedarf zu laden. IODD-Dateien (IO Device Description Files) werden für die Konfiguration und Integration von IO-Link-Geräten benötigt.
moneo notification	Ausgehend	moneo	MS Teams	je nach Konfiguration	HTTP	Erforderlich, um Benachrichtigungen von moneo zu erhalten, die an diesen Kommunikationskanal gesendet werden.
moneo notification	Ausgehend	moneo	SMS Gateway	je nach Konfiguration	SMS gateway	Erforderlich, um Benachrichtigungen von moneo zu erhalten, die an diesen Kommunikationskanal gesendet werden.
moneo notification	Ausgehend	moneo	Discord	je nach Konfiguration	HTTP	Erforderlich, um Benachrichtigungen von moneo zu erhalten, die an diesen Kommunikationskanal gesendet werden.

Verwendung	Richtung	Quelle	Ziel-Adresse (URL)	Ports	Protokoll	Beschreibung
moneo notification	Ausgehend	moneo	Slack	je nach Konfiguration	HTTP	Erforderlich, um Benachrichtigungen von moneo zu erhalten, die an diesen Kommunikationskanal gesendet werden.
Online Update	Ausgehend	AMS	system.update.ifm	443	HTTP	Erforderlich, um Onlineupdates für EdgeGateways oder (v)Appliances zu erhalten.
Sensor-Daten	Ausgehend	moneo	VSE	3321	TCP	Erforderlich, um Daten von einem VSE-Gerät anzufordern.
Sensor-Daten	Ausgehend	moneo	IoTCore	je nach Gerät	TCP	Erforderlich, um Daten von einem IoT-Core-Gerät anzufordern.
Sensor-Daten	Ausgehend	moneo	LRAgent	je nach Konfiguration	TCP	Erforderlich, um Daten von einem LRAgenten anzufordern.

6 Security-Funktionalitäten

6.1 Verschlüsselung und Integritätssicherheit

▶ Kommunikationsprotokolle mit Verschlüsselungstechnologien verwenden.

Beim Zugriff über den Browser ist die gesamte Kommunikation zwischen Client und dem moneo|edgeGateway TLS-verschlüsselt (4096 Bit RSA oder 256 Bit AES). Standardmäßig stellt das moneo|edgeGateway ein selbstsigniertes Zertifikat zur Verfügung.

Die verschlüsselte Kommunikation zwischen Client und moneo ist gewährleistet.

Aufgrund des inhärenten Verhaltens von selbstsignierten Zertifikaten kann die Authentizität nicht überprüft werden, was zu Warnmeldungen in einigen Browsern führt.

Für die Sicherstellung der Endpunkt-Integrität hat der Kunde die Möglichkeit, eigene vertrauenswürdige Zertifikate für das Web-Frontend einzuspielen.

Die Sicherheit der Verbindung zwischen dem moneo|edgeGateway und Cloud-Plattform wird ebenfalls per TLS gesichert. Zusätzlich verfügt jedes moneo|edgeGateway über eine mehrstufige zertifikatsbasierende Authentifizierungsmethode für den gesicherten und eindeutigen Zugriff auf die moneo Cloud-Instanz.

6.2 Fernwirkzugriff über moneo|cloud

Das moneo|edgeGateway beinhaltet für den Fernwirkzugriff den moneo|remoteConnect-Dienst von ifm.

Der Dienst moneo|remoteConnect muss über das AMS explizit freigegeben werden.

Bei Inbetriebnahme des Gerätes ist der Dienst nicht aktiv.

6.3 Datensicherung und Wiederherstellung

▶ Die Systemkonfiguration und Systemdaten gemäß den unternehmenseigenen Change-Management-Prozessen sichern.

Zum Sichern der moneo-Konfiguration verfügt das moneo|edgeGateway über eine Sicherungs- und Wiederherstellungsoption.

Als Speicherziel können lokale USB-Geräte oder Netzwerkspeicher verwendet werden. Die Sicherung kann bei Bedarf manuell oder automatisch nach Zeitplan erfolgen.

Durch die Verwendung eines Netzwerkspeicherorts können die erstellten Datensicherungen in das bestehende Datensicherungskonzept des Kunden eingebunden werden.

Die Datensicherungen werden verschlüsselt.

▶ Empfehlung: Um Desaster-Recovery-Möglichkeiten zu gewährleisten, die Datensicherung vom Betrieb des moneo|edgeGateway physisch trennen.

6.4 Ausführungsschutz auf Betriebssystemebene

Da das moneo|edgeGateway keinen direkten Zugriff auf die Betriebssystemebene zulässt, kann kein bösartiger Code auf das System übertragen werden.

6.5 Gesichertes Update-Verfahren über dedizierte und signierte Update-Pakete

▶ Regelmäßig prüfen, ob Softwareaktualisierungen für das Produkt verfügbar sind.

Über das AMS kann ein Online-Update für das moneo|edgeGateway durchgeführt werden.

Alternativ kann das Update-Paket von www.ifm.com heruntergeladen und über das AMS installiert werden. Wird das moneo|edgeGateway in Verbindung mit der moneo|cloud genutzt ist es außerdem möglich ein Update direkt aus der Cloud anzustoßen. Die Aktualisierung wird dann umgehend durchgeführt.

Da das moneo|edgeGateway ausschließlich über ifm-Server aktualisiert wird, ist eine Kompromittierung durch Updates ausgeschlossen. Die Update-Pakete werden von der ifm-Entwicklung verschlüsselt und signiert.

Alle bereitgestellten Updates beinhalten:

- moneo Betriebssystem-Plattform
- Appliance Management System
- Sicherheitsupdates

Die Updates können durch den Kunden entsprechend dem Change-Management-Prozess installiert werden.

7 Benutzerzugriff und Benutzerrollen

moneo und das Appliance Management System (AMS) sind Anwendungen, die per Webbrowser aufgerufen werden können.

Der Zugriff auf das AMS oder auf moneo ist über separate Benutzerauthentifizierungsmechanismen gesichert. Die Trennung der Applikationen ermöglicht es, dass die Zugriffe auf unterschiedliche Benutzergruppen aufgeteilt werden können.

Für die moneo Applikation und das AMS werden verschiedene Benutzerkonten breitgestellt. Hierdurch wird eine Trennung der Verantwortlichkeiten ermöglicht.

Der Zugriff auf die Kommandozeile (CLI) über SSH muss für die Nutzung explizit freigegeben werden. Die Kommandozeile kann für die Erstinstallation und ggf. für den ifm-Support genutzt werden.

Die Standardbenutzer und Standardbenutzergruppen mit ihren Berechtigungen sind unten aufgeführt.

7.1 Standardbenutzer

System	Name	Berechtigung	Beschreibung
AMS & AMS-Konsole	Administrator	Vollzugriff	Zentraler Administrator für die Grundkonfiguration der Appliance
OS	Maintenance	Vollzugriff	ifm Wartungsbenutzer. Der Benutzer-"Maintenance" steht nur nach erfolgreicher Aktivierung und nur für den Zugriff über SSH CLI zur Verfügung.
moneo	Administrator	Vollzugriff	Der Benutzer wird automatisch angelegt. Bei der Ersteinrichtung des Systems wird ein gemeinsames Passwort für das moneo-Administratorkonto und das AMS-Administratorkonto festgelegt. Eine nachträgliche Passwortänderung in moneo oder im AMS führt dazu, dass das Passwort nicht mehr gleich ist. Das Programm, bei dem das Passwort geändert wurde, verwendet fortan das neue Passwort, das andere Programm nicht.
moneo	Wird während des initialen Setups erstellt.	Vollzugriff	Mindestens ein Administrator ist erforderlich. Der Administrator hat die Möglichkeit, zusätzliche Benutzer in verschiedenen Berechtigungsgruppen anzulegen.

7.2 Standardbenutzergruppen

- ▶ Entsprechend der Risikobeurteilung die notwendigen Nutzerrechte vergeben.
- ▶ Passwörter entsprechend der Unternehmens-Sicherheitsrichtlinie verwenden.

System	Gruppe	Berechtigung	Beschreibung
moneo	Administrator	Vollzugriff	Benutzergruppe für die grundlegende Inbetriebnahme von moneo. Zusätzlich haben Benutzer dieser Gruppe Zugriff auf die Benutzerkontenverwaltung
moneo	User	Default-Benutzergruppe	Benutzer dieser Gruppe können Elemente innerhalb der Module bearbeiten und verwenden (→ Benutzerrechte in der moneo Hilfe). Benutzer dieser Gruppe können Tickets bearbeiten.
moneo	Visitor	Lesezugriff	Benutzer dieser Gruppe können Informationen in den moneo-Modulen anzeigen. Benutzer dieser Gruppe können Tickets bearbeiten.

8 Außerbetriebnahme

- ▶ Sicherstellen, dass bei der Außerbetriebnahme keine schützenswerten Informationen in unberechtigte Hände gelangen können.
- ▶ Vor der Außerbetriebnahme des Geräts die Systemeinstellungen immer auf die Werkseinstellungen zurücksetzen.

9 Cyber-Security-Schwachstellen melden / Fragen

▶ Bei Fragen zum Thema Cyber-Security bei ifm-Produkten und zum Melden von Cyber-Security-Schwachstellen in ifm-Produkten bitte an das „Product Security Incident Response Team“ (PSIRT) der ifm-Unternehmensgruppe wenden: psirt@ifm.com