Sicherheitshandbuch

Honeywell

Touchpoint Pro

Revisionsprotokoll

Revision	Kommentar	Datum
Ausgabe 01	A04815	Nov 2016

RECHTLICHE HINWEISE

Haftungsausschluss

Honeywell ist in keinem Fall, unabhängig von deren Entstehung, haftbar für Schäden oder Verletzungen jeglicher Art, die auf die Nutzung dieses Geräts, auf das sich diese Bedienungsanleitung bezieht, zurückzuführen sind.

Eine strenge Einhaltung der in dieser Bedienungsanleitung dargelegten und besprochenen Sicherheitsverfahren und äußerste Sorgfalt bei der Nutzung des Geräts sind von entscheidender Bedeutung, um Verletzungen oder Schäden am Gerät zu verhindern oder deren Wahrscheinlichkeit zu minimieren.

Die Informationen, Zahlen, Abbildungen, Tabellen, Spezifikationen und Schemas in dieser Bedienungsanleitung gelten zum Zeitpunkt der Veröffentlichung oder Überarbeitung als korrekt und genau. Im Hinblick auf die Richtigkeit und Genauigkeit wird jedoch keine Haftung und Gewährleistung gewährt oder impliziert. Honeywell wird unter keinen Umständen gegenüber Personen oder Unternehmen für Verluste oder Schäden haften, die in Verbindung mit der Nutzung dieser Bedienungsanleitung entstanden sind.

Die Informationen, Zahlen, Abbildungen, Tabellen, Spezifikationen und Schemas in dieser Bedienungsanleitung können ohne Vorankündigung geändert werden.

Nicht autorisierte Änderungen am Gaswarnsystem oder seiner Installation sind nicht zulässig, da diese zu einem Anstieg inakzeptabler Gesundheits- und Sicherheitsrisiken führen.

Jegliche Software, die Teil dieses Geräts ist, darf nur zu den Zwecken verwendet werden, zu denen sie von Honeywell bereitgestellt wurde. Der Benutzer darf keine Änderungen, Modifikationen, Konvertierungen, Übersetzungen in andere Computersprachen oder Kopien (außer zu den erforderlichen Sicherungszwecken) vornehmen.

Honeywell ist in keinem Fall haftbar für Gerätestörungen oder -schäden jeglicher Art, einschließlich (aber nicht beschränkt auf) zufällige, direkte, indirekte, konkrete und Folgeschäden oder Folgeverluste durch entgangene Gewinne, Unterbrechung der Geschäftstätigkeit, Verlust von geschäftlichen Informationen oder andere Vermögensschäden, die auf Verstöße gegen die Verbote oben zurückzuführen sind.

Garantie

Honeywell Analytics gewährt für das Touchpoint Pro-System (nach eigenem Ermessen) eine Garantie für den Ersatz oder die Reparatur von Komponenten im Falle von Material- und Fertigungsfehlern, die bei korrekter Verwendung innerhalb von 12 Monaten ab Inbetriebnahme durch einen von Honeywell Analytics zugelassenen Vertreter* oder innerhalb von 18 Monaten ab dem Versand durch Honeywell Analytics auftreten, wobei das frühere Datum gilt.

Von der Garantie ausgeschlossen sind Verbrauchsmaterialien, Batterien, Sicherungen, normaler Verschleiß sowie Schäden, die durch Gewalteinwirkung, missbräuchliche Verwendung, unsachgemäße Installation, nicht autorisierte Verwendung, Änderungen oder Reparaturen, die Betriebsumgebung, Giftstoffe, Schadstoffe oder Einsatzbedingungen außerhalb der Spezifikationen entstehen.

Diese Garantie gilt nicht für Sensoren oder Komponenten, die durch separate Garantien abgedeckt werden, oder für Kabel und Komponenten von Drittanbietern.

Jegliche Ansprüche gemäß der Honeywell Analytics Produktgarantie sind innerhalb der Garantiezeit und innerhalb einer angemessenen Frist nach Auftreten eines Defekts geltend zu machen. Wenden Sie sich im Fall eines Garantieanspruchs an Ihren Honeywell Analytics Servicemitarbeiter vor Ort.

Dieser Abschnitt stellt lediglich eine Übersicht über die Garantie dar. Die vollständigen Garantiebedingungen sind im Dokument General Statement of Limited Product Warranty (Beschränkte Garantie) von Honeywell Analytics enthalten, das auf Anfrage erhältlich ist.

* Bei einem von Honeywell Analytics zugelassenen Vertreter handelt es sich um eine qualifizierte Person, die von Honeywell Analytics geschult wurde oder dort angestellt ist, oder um eine qualifizierte Person, die im Einklang mit dieser Bedienungsanleitung geschult wurde.

Urheberrechtshinweis

Weitere Informationen erhalten Sie unter www.honeywellanalytics.com

INHALTSVERZEICHNIS

1 Inhalt

EINLEITUNG

2 Einleitung

Dieses Handbuch wurde zur Verwendung durch autorisierte Personen und IT-Mitarbeiter von Kunden entwickelt, die ein Honeywell Touchpoint Pro (TPPR)-System verwenden.

Es ist für die Planung der Konfiguration und Wartung der Netzwerkinfrastruktur des TPPR-Systems vorgesehen.

Es stellt Informationen zur Verfügung, die die Erkennung und Linderung von Sicherheitsrisiken unterstützen, die mit der täglichen Verwendung des Systems in vernetzten IT-Infrastrukturen in Verbindung stehen.

2.1 Umfang

Dieses Dokument gilt für Touchpoint Pro-Systeme in Netzwerkumgebungen, zugeordneten Computern und Datenspeichermedien.

2.2 Annahmen und Voraussetzungen

Dieses Handbuch setzt ein hohes Maß an technischen Kenntnissen und Vertrautheit mit folgenden Elementen voraus:

- PC-Verwaltung und Betriebssysteme
- Netzwerksysteme und -konzepte
- Sicherheitsprobleme und -konzepte

2.3 Zugehörige Dokumente

Dieses Handbuch sollte in Verbindung mit den folgenden Dokumenten gelesen werden:

Dokument	Teilenummer
Technisches Handbuch zum Touchpoint Pro	2400M2501
Webserver-Benutzerhandbuch	2400M2563
Bedienungsanleitung zur PC-Konfigurationssoftware	2400M2564

Tabelle 1. Zugehörige Dokumente

2.4 Steuerelemente für die Sicherheit

Das Touchpoint Pro-System weist eine Reihe von integrierten Zugriffsrechten für die Sicherheit auf. Dazu zählen:

- Einschränkung des Zugriffs für designierte Benutzer
- Kennwortschutz für Benutzerkonten
- Sichere Webserververbindung (https)
- Webserver-Gerätezertifikat
- Reduzierung vertraulicher Daten

2.4.1 Zusätzliche Benutzerrechte

Dieses Handbuch konzentriert sich auf zusätzliche Zugriffsrechte für die Sicherheit, die von Benutzern implementiert werden sollten.

2.4.2 Weitere Informationen

Wenden Sie sich an Ihren Honeywell-Vertreter, wenn Sie weitere Informationen zur Sicherheit Ihres TPPR-Systems benötigen.

IT-ARCHITEKTUR

3 IT-Systemarchitektur

Touchpoint Pro kann in einer Vielzahl an Netzwerktopologien konfiguriert werden. Dazu zählen einfache Peer-to-Peer- oder isolierte LAN und auch Unternehmensnetzwerke mit Internetzugang.

Dieses Handbuch befasst sich hauptsächlich mit Systemen, die mit einem WAN oder Unternehmensnetzwerk mit möglichem Internetzugang vernetzt sind.

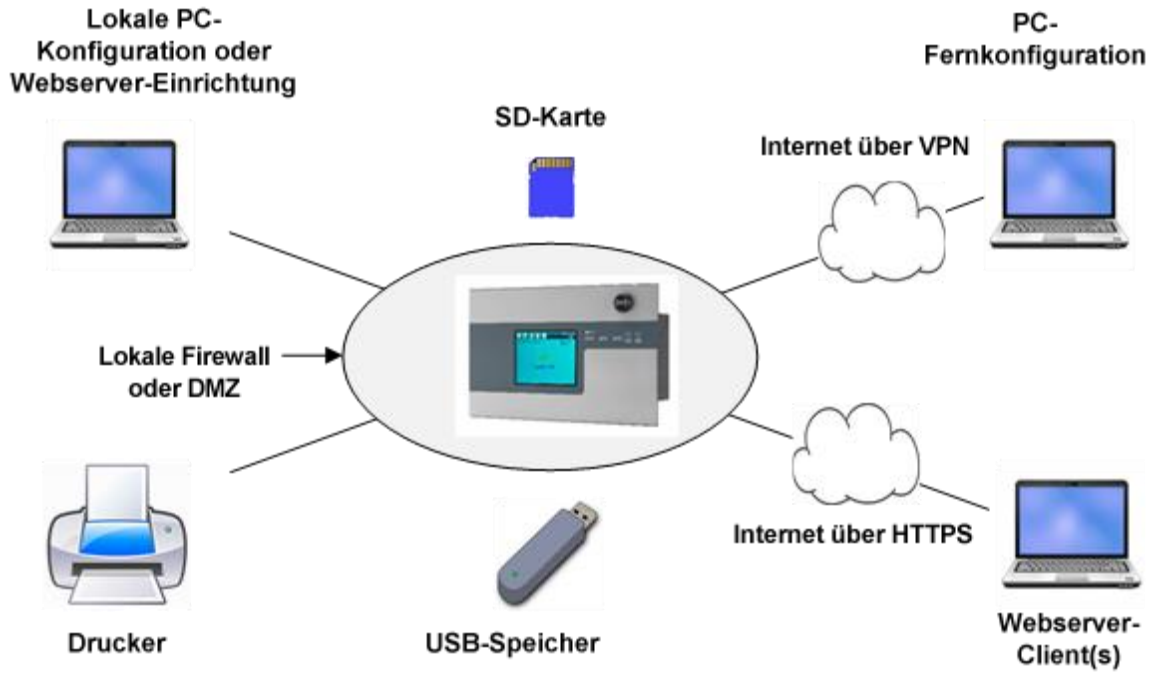

Abbildung 1. Systemarchitektur-Optionen

3.1 Ethernet-Fernverbindungen

Mögliche Ethernet-Verbindungen:

Verbindung	Umfang	Anmerkung
PC-Konfigurationstool	Intranet oder Internet	Einzelbenutzer erlaubt
Webserver-Clients	Intranet oder Internet	Mehrere Clients
Ethernet-Drucker	Intranet oder Internet. In der Regel Intranet.	Einzeldrucker unterstützt
Webserver-Einrichtung	Intranet oder Internet. In der Regel Intranet.	Kurzfristiger Einzelbenutzerzugang

Tabelle 2. Verbindungen über Ethernet

3.2 Physische und lokale Verbindungen

Physische Verbindungen:

- Touchscreen/Bedienfeld
- USB-Speichergerät
- SD-Speichergerät

BEDROHUNGEN

4 Bedrohungen

Sicherheitsbedrohungen für Netzwerksysteme:

- Nicht autorisierter Zugriff
- Kommunikationsüberwachung
- Viren und andere böswillige Software-Agents

4.1 Nicht autorisierter Zugriff

Diese Bedrohung umfasst physischen Zugriff auf den Controller und Eindringen in das Netzwerk, mit dem das TPPR-System verbunden ist, vom Unternehmensnetzwerk/Intranet oder Internet aus.

Nicht autorisierter externer Zugriff führt möglicherweise zu:

- Verlust der Systemverfügbarkeit
- Fehlerhafte Ausführung von Prozessen, die zu Schäden am Gebäude, fehlerhaften Vorgängen oder unechten Alarmen führt
- Diebstahl oder Schäden an den Inhalten
- Erfassung, Änderung oder Löschung von Daten
- Ansehensverlust, falls der externe Zugriff öffentlich bekannt wird

Ein nicht autorisierter Zugriff auf das System kann folgende Ursachen haben:

- Mangelnde Sicherheit von Benutzername und Kennwort
- Unkontrollierter Zugriff auf den Controller
- Unkontrollierter Zugriff auf das Netzwerk und den Netzwerkdatenverkehr

4.2 Kommunikationsüberwachung

Diese Bedrohung umfasst die Überwachung oder Manipulation der Ethernet-Kommunikationsschnittstelle auf Port 4000 (Fernkonfigurationsport), während der Port aktiv ist, mithilfe von Man-in-the-middle, Packet Replay oder ähnlichen Methoden.

Die Manipulation der Kommunikationsschnittstelle hat möglicherweise folgende Konsequenzen:

- Verlust der Systemverfügbarkeit
- Fehlerhafte Konfiguration und damit fehlerhafte Ausführung der TPPR-Sicherheitsfunktion
- Erfassung, Änderung oder Löschung von Daten

Der Konfigurationsport ist offen, wenn das PC-Konfigurationstool verwendet wird, und für die anfängliche Einrichtung und Wartung des Webserver-Dienstprogramms.

Der Konfigurationsport kann nur von Benutzern mit physischem Zugang zum Controller und entsprechenden Anmeldeinformationen geöffnet werden. Der Konfigurationsport ist zeitlich beschränkt und kann nicht offen gelassen werden, wenn er nicht verwendet wird.

4.3 Viren und andere böswillige Software-Agents

Diese Bedrohung beinhaltet böswillige Software-Agents, wie etwa Viren, Spyware (Trojaner) und Computerwürmer. Sie sind möglicherweise vorhanden:

- Auf einem PC, der für die PC-Konfigurationssoftware verwendet wird
- Auf PCs, von denen aus die TPPR-Webschnittstelle mit Webclients aufgerufen wird
- Auf beliebigen anderen Knoten des Netzwerks, mit dem das TPPR-System verbunden ist

Das Eindringen böswilliger Software-Agents führt möglicherweise zu:

- Leistungsabfall
- Verlust der Systemverfügbarkeit
- Erfassung, Änderung oder Löschung von Daten, einschließlich Konfigurationsdaten und Geräteprotokolle

Viren können anhand von Medien wie etwa USB-Speichergeräten und SD-Karten, anderen infizierten Systemen im Netzwerk und infizierten oder böswilligen Websites im Internet übertragen werden.

5 Strategien zur Minderung

Die folgenden Strategien zur Minderung sollten beachtet werden:

5.1 Touchpoint Pro System

5.1.1 Zugriff auf Überwachungssystem

Zusätzlich zu den Zugriffsrechten für die Sicherheit, die im Absatz 2.4 aufgelistet sind, verfügt TPPR über die folgenden Möglichkeiten zur Erkennung unerwarteter Konfigurationsänderungen:

1. Bildschirmwarnung

   Das TPPR-System zeigt eine Bildschirmwarnung an, wenn sich die Konfiguration seit der letzten Sicherung geändert hat. Die Warnung kann nur von einem Benutzer gelöscht werden, der über ausreichende Berechtigungen zum Sichern des Systems oder zum Wiederherstellen eines vorherigen Systems verfügt. Diese Vorgänge können nur lokal am TPPR-Controller durchgeführt werden.

2. Konfigurationszähler

   TPPR betreibt einen Konfigurationszähler, der jede Konfigurationsänderung erfasst. Die Erhöhung ist variabel. Jede Änderung steht für eine Konfigurationsänderung.

   Der Konfigurationszähler kann über **Toolbox, Help** aufgerufen werden.

3. Letzte Anmeldung

   Der Anmeldename des zuletzt angemeldeten Benutzers kann angezeigt und überprüft werden, wenn Änderungen vorgenommen wurden.

   Der Name des zuletzt angemeldeten Benutzers kann über **Toolbox, Help** aufgerufen werden.

4. Ereignisverlauf und -protokoll

   Alle Benutzeranmeldungen und Systemvorgänge werden im Ereignisprotokoll erfasst und können auf dem Bildschirm „Ereignisverlauf“ oder durch Erstellen eines Ereignisberichts angezeigt werden.

Die Elemente oben müssen im Rahmen der Systemwartung routinemäßig überwacht und überprüft werden.

5.1.2 Benutzerzugang und Kennwörter

Touchpoint Pro weist drei Benutzerebenen auf. Benutzer verfügen auf jeder Ebene über eigene Benutzernamen und Kennwörter. Beachten Sie die folgende empfohlene Vorgehensweise:

1. Gewährleisten Sie die physische Sicherheit der Kennwörter. Schreiben Sie keine Benutzernamen und Kennwörter an Orten auf, wo sie von nicht autorisiertem Personal gesehen werden können.
2. Legen Sie die minimale Zugriffsebene für jeden Benutzer fest. Verleihen Sie Benutzern keine Rechte, die sie nicht benötigen.
3. Erstellen Sie separate Benutzernamen und Kennwörter für alle Benutzer. Geben Sie die Benutzernamen und Kennwörter nicht an mehrere Benutzer weiter.
4. Stellen Sie sicher, dass sich Benutzer nur anhand ihrer eigenen Anmeldeinformationen anmelden.
5. Überprüfen Sie die Benutzerkonten regelmäßig und entfernen Sie alle, die nicht mehr benötigt werden.
6. Stellen Sie sicher, dass Kennwörter und Anmeldeinformationen regelmäßig geändert werden.
7. Erstellen Sie ein neues Administratorkonto mit neuen Anmeldeinformationen und löschen Sie den standardmäßigen Administratorbenutzer.
8. Minimieren Sie die Anzahl der Benutzer auf Administratorebene. Die empfohlene Anzahl ist zwei.

STRATEGIEN ZUR MINDERUNG

5.1.3 Software und ungewöhnliche Vorgänge

Touchpoint Pro isoliert das Gasüberwachungssystem von der Benutzeroberfläche. Falls ungewöhnliche Vorgänge auf der Benutzeroberfläche bemerkt werden, können folgende Maßnahmen ergriffen werden:

1. Starten Sie die Benutzeroberfläche neu, um die Software neu zu laden. Dadurch wird der Betrieb des Gasüberwachungssystems nicht unterbrochen, auch wenn die Berichtübermittlung an den Touchscreen kurzzeitig unterbrochen wird:

   Halten Sie die Tasten „Accept“ und „Reset“ auf dem Bedienfeld etwa zehn Sekunden gedrückt, bis die Software der Benutzeroberfläche neu gestartet wurde. Dieser Vorgang kann nur lokal am Controller durchgeführt werden. Das System zeigt mehrere Sekunden lang einen Fehler an. Möglicherweise müssen Schnittstellen von Geräten einer höheren Ebene isoliert werden.

2. Schalten Sie das Gerät aus und wieder ein. Die Software für Gasüberwachung und Benutzeroberfläche wird neu geladen. Das Gasüberwachungssystem ist mehrere Minuten lang nicht verfügbar. Es wird allerdings ein Ausgangssignal erzeugt. Möglicherweise müssen Schnittstellen von Geräten einer höheren Ebene isoliert werden. Die Stromversorgung von Modulen, die separat versorgt werden, muss nicht getrennt werden.

Ein ungewöhnlicher Vorgang an einem TPPR-Controller muss Ihrem Servicemitarbeiter vor Ort gemeldet werden.

5.1.4 Speichermedien

Touchpoint Pro verwendet SD-Karte und USB-Speichermedien:

1. Verwenden Sie nur autorisierte, entnehmbare Medien, die mit aktueller Antivirensoftware auf Viren und Malware gescannt und überprüft wurden.
2. Stellen Sie sicher, dass für Touchpoint Pro verwendete Speichermedien nicht für andere Zwecke verwendet werden, um das Infektionsrisiko zu minimieren.
3. Steuern Sie den Zugang zu Medien, die Sicherungen enthalten, um das Manipulationsrisiko zu minimieren.

5.1.5 Konfigurationsport

Der Konfigurationsport bietet Zugang für die PC-Konfigurationssoftware und für das Einrichten und Lizenzieren des Webservers. Der Port darf nur von einem Benutzer mit entsprechender Autorisierung am Controller geöffnet werden und wird nach einem bestimmten Zeitraum oder bei Zeitüberschreitung aufgrund von Inaktivität automatisch geschlossen.

1. Der Konfigurationsport darf nur in einer vertrauenswürdigen, sicheren Umgebung in einem sicheren Netzwerk verwendet werden.
2. Der Port muss manuell über den Controllerbildschirm „IP-Konfiguration“ geschlossen werden, wenn kein Zugriff mehr erforderlich ist.

5.1.6 Software- und Firmware-Updates

Von Zeit zu Zeit werden Updates und Upgrades von Systemsoftware- und -firmware angeboten, die möglicherweise zusätzliche oder aktualisierte Sicherheitsfunktionen enthalten. Informationen zu Updates:

1. Stellen Sie sicher, dass Ihr Vertreter vor Ort aktuelle Kontaktdetails besitzt.
2. Besuchen Sie regelmäßig die Touchpoint Pro-Website unter www.honeywellanalytics.com.

5.2 Computer und Zugriff

Bewährte Sicherheitspraktiken müssen auf Computern und Netzwerken beachtet werden, mit denen TPPR-Systeme verbunden werden können, einschließlich Peer-to-Peer- und LAN-Verbindungen.

5.2.1 Betriebssoftware

Betriebssysteme und Browser müssen auf dem neuesten Stand gehalten werden, indem die Updates des Herstellers installiert werden.

5.2.2 Virenschutz

Unterhalten Sie aktuelle Antivirensoftware auf allen Computern, die direkt oder über ein Netzwerk mit TPPR-Systemen verbunden werden können. Stellen Sie sicher, dass die Computer regelmäßig gescannt werden.

5.2.3 Dateien und Medien

Erlauben Sie die Installation und Verwendung auf zugeordneten Computern nur für Dateien und Software von vertrauenswürdigen Quellen.

Verwenden Sie nur autorisierte entnehmbare Medien, z. B. CD/DVD, externe Festplatten, USB-Sticks, die mit aktueller Antivirensoftware gescannt wurden.

5.2.4 Benutzerzugang und Kennwörter

Bewährte Praktiken zum Kennwortschutz müssen beachtet werden.

1. Verlangen Sie die Verwendung starker Kennwörter und Benutzerkonto-Steuerelemente.
2. Gewährleisten Sie die physische Sicherheit der Kennwörter. Schreiben Sie keine Benutzernamen und Kennwörter an Orten auf, wo sie von nicht autorisiertem Personal gesehen werden können.

Computer, die mit TPPR-Systemen verbunden sind, dürfen nicht unbeaufsichtigt gelassen werden, wenn eine Konfigurationssitzung geöffnet ist. Der Zugriff muss auf autorisierte Benutzer beschränkt sein.

5.2.4.1 TPPR-Kennwörter

TPPR-Kennwörter werden auf keinen Computern aufbewahrt oder gespeichert, auf denen PC-Konfigurationssoftware und Webserver-Clients ausgeführt werden. Fernbenutzer müssen sich nach Verbindungsherstellung anmelden. Die physische Sicherheit von TPPR-Kennwörtern muss auf Computern bewahrt werden, die für Fernverbindung verwendet werden.

5.3 Netzwerke, Firewalls und VPN-Verbindungen

5.3.1 Physischer Zugriff

Der physische Zugriff auf Netzwerkknoten und -infrastruktur muss auf autorisiertes Personal beschränkt sein, um Manipulationen zu vermeiden.

5.3.2 Firewall und DMZ

Das Netzwerkdesign muss den Zugriff auf das TPPR-System vom größeren Netzwerk aus einschränken, beispielsweise durch Verwendung lokaler Firewalls oder eines DMZ-Bereichs. Die Anzahl der Komponenten im selben Bereich wie TPPR muss auf ein Minimum begrenzt werden, insbesondere wenn der Konfigurationsport verwendet wird.

5.3.3 Internet und VPN

Wenn Zugriff von nicht vertrauenswürdigen Netzwerken erforderlich ist, wie etwa Internetzugriff, muss ein VPN verwendet werden, um die Sicherheit der Verbindung zu gewährleisten.

GLOSSAR

6 Glossar

6.1 Abkürzungen

Die folgenden Abkürzungen werden verwendet:

Abkürzung	Bedeutung
DMZ	De-Militarized Zone (entmilitarisierte Zone): wird verwendet, um den Zugang von Teilen eines Netzwerks einzuschränken
https	Hypertext Transfer Protocol Secure-Version
LAN	Local Area Network (lokales Netzwerk)
PC	Personal Computer
SD	Secure Digital-Speicherkarte
TPPR	Touchpoint Pro-Gasüberwachungssystem
USB	Universal Serial Bus-Speichergeräte
VPN	Virtual Private Network

Weitere Informationen erhalten Sie unter

www.honeywellanalytics.com

Kontaktieren Sie Honeywell Analytics:

Europa, Naher Osten, Afrika

Life Safety Distribution GMBH

Javastrasse 2

8604 Hegnau

Schweiz

Tel.: +41 (0)44 943 4300

Fax: +41 (0)44 943 4398

gasdetection@honeywell.com

Kundendienst

Tel.: 00800 333 222 44 (gebührenfreie Telefonnummer)

Tel.: +41 44 943 4380 (alternative Telefonnummer)

Fax: 00800 333 222 55

Tel. Naher Osten: +971 4 450 5800 (fest montierte Gasdetektionssysteme)

Tel. Naher Osten: +971 4 450 5852 (tragbare Gasdetektionssysteme)

Amerika

Honeywell Analytics Inc.

405 Barclay Blvd.

Lincolnshire, IL 60069

USA

Tel.: +1 847 955 8200

Gebührenfrei: +1 800 538 0363

Fax: +1 847 955 8210

detectgas@honeywell.com

Asien-Pazifik-Raum

Honeywell Analytics Asia Pacific

7F SangAm IT Tower,

434 Worldcup Buk-ro, Mapo-gu,

Seoul 03922,

Korea

Tel.: +82 2 6909 0300

Fax: +82 2 2025 0328

Indien Tel.: +91 124 4752700

analytics.ap@honeywell.com

Technischer Service

EMEA: HAexpert@honeywell.com

USA: ha.us.service@honeywell.com

AP: ha.ap.service@honeywell.com

www.honeywell.com

Teilenummer 2400M2567

Ausgabe 1