Panasonic
INDUSTRY

TOUCH-TERMINALS

Sicherheitsleitfaden

HM-Serie

Version 1.0

2024.07 | https://industry.panasonic.eu/

Copyright und Haftung

Copyright- und Haftungshinweise zu dieser Dokumentation.

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Deutschland

Letzte Änderung am: 2024-07-23

Panasonic Industry Europe verbessert das Design und die Leistung seiner Produkte kontinuierlich. Aus diesem Grund behalten wir uns das Recht vor, die Dokumentation/das Produkt ohne Hinweis zu ändern. In keinem Fall ist Panasonic Industry Europe für direkte, spezielle, zufällige oder Folgeschäden jeglicher Art haftbar, die aufgrund eines eventuellen Mangels oder Fehlers des Produkts oder der Dokumentation entstanden sind, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Wenn Sie technischen Support benötigen, wenden Sie sich bitte an die Panasonic Hotline.

Inhaltsverzeichnis

1 Zu diesem Dokument....4
2 Sicherheitskonzept für Produkte von Panasonic....5
3 Standardkonfiguration der Touch-Terminals der HM-Serie....6
4 Mögliche Bedrohungsszenarien....8
5 Allgemeine Sicherheitsvorkehrungen....10
6 Bewährte Verfahren zur Absicherung Ihrer Touch-Terminals....11
6.1 Systemeinstellungen....11
6.1.1 Passwortschutz....11
6.1.2 Firewall-Einstellungen....11
6.1.3 Protokolldateien und SSH-Debugging-Funktionen....12
7 FAQ....13
8 Checkliste für die Sicherheitskonfiguration....14
9 Panasonic Hotline....16
10 Änderungsverzeichnis....18

1 Zu diesem Dokument

Interne und externe Cybersicherheitsrisiken entwickeln sich mit der zunehmenden Digitalisierung und der steigenden Vernetzung weiter.

So veröffentlichte das BSI (Bundesamt für Sicherheit in der Informationstechnik) einen Bericht mit den zehn häufigsten Bedrohungen und definierte Regeln und Empfehlungen für Netzwerkprodukte in industriellen Steuerungssystemen (ICS):

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- DDoS-Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld

Quelle: https://www.bsi.bund.de/ICS

Dieses Dokument enthält die Geräteinformationen, die Sie für Ihr Netzwerkmanagement benötigen, und unterstützt Sie dabei, die Touch-Terminals der HM-Serie vor Sicherheitsrisiken zu schützen.

2 Sicherheitskonzept für Produkte von Panasonic

Produkte und Dienstleistungen von Panasonic unterliegen einem kontinuierlichem Verbesserungsprozess. Die Produkte werden unter strenger Beachtung von Sicherheitsrichtlinien entwickelt und vor Auslieferung ausführlich getestet. Das Sicherheitskonzept von Panasonic basiert auf internationalen Richtlinien entsprechend IEC 62443 und ISO/IEC 27001.

Das Panasonic Product Security Incident Response Team (Panasonic PSIRT) ist das zentrale Koordinationsteam, an das Sicherheitsrisiken im Zusammenhang mit Produkten von Panasonic gemeldet werden können.

3 Standardkonfiguration der Touch-Terminals der HM-Serie

Die integrierten Netzwerkfunktionen der Touch-Terminals der HM-Serie stellen ein potenzielles Sicherheitsrisiko dar. Achten Sie darauf, die Standardeinstellungen anzupassen, um dieses Risiko zu beseitigen oder zu minimieren.

- Ab Mai 2024 hergestellte Produkte haben kein voreingestelltes Passwort. Bei der ersten Verbindung mit dem Gerät muss ein Passwort eingegeben werden, das den Mindestanforderungen entspricht. Bei älteren Versionen wurde werkseitig ein Standardpasswort eingestellt, das Sie so bald wie möglich ändern sollten.
- Die Ethernet-Schnittstellen sind als DHCP-Client konfiguriert.
- Standardmäßig sind die folgenden Ports geöffnet und befinden sich im Listening-Modus:

Port-Nr.	Protokoll	Funktion
80, 8000, 443	TCP	Für die Browserkonfiguration und für Benutzer-Webseiten verwendet
53	TCP	Für den DNS-Dienst verwendet
990- 991	UDP	Für Geräteerkennung über Broadcast verwendet
21 (BSP 1.0 vor 05/2024)	TCP	FTP-Datenports (passiver FTP-Modus: 16384-17407/TCP)
18756- 18759	TCP	FTP-Datenports, gesichert
990 (ab BSP 1.3 05/2024)	TCP	Laufzeit- und Projektmanagement

- Alle Funktionen und Dienste der Touch-Terminals der HM-Serie, die ein Sicherheitsrisiko darstellen könnten, wurden mit Ausnahme der Autorun-Script-Funktion werkseitig deaktiviert. Die Dienste sind unter IP/machine_config/#/services aufgeführt.

Dienst	Sicherheitsrisiko
Autorun-Skripte	Anwendungen, die von einem externen Speichermedium, z. B. einem USB-Stick, gestartet werden
Avahi-Dämon	Öffnet Port 5353 (zum Erfassen von Informationen und zur Suche nach Funktionen)
Cloud-Dienst	Beispiel: eine OpenVPN-Serverkonfiguration aus einer früheren Nutzung
DHCP-Server	Öffnet Port 67, 68
SNMP-Server	Öffnet Port 161, 10161 (zum Erfassen von Informationen)
SSH-Server	Öffnet Port 22 (Anmeldung mit Administratorrechten und Ausführung von Befehlen)
VNC-Server	Öffnet Port 5900 (Webseite und Gerätesteuerung)

- Standardmäßig ist die in den Touch-Terminals der HM-Serie implementierte Firewall (IP/machine_config/#/services) deaktiviert.

- Die Touch-Terminals der HM-Serie schreiben Protokolldaten und untypische Nutzungsinformationen in Protokolldateien. Diese Dateien werden auf dem Gerät gespeichert und können mit Administratorrechten heruntergeladen werden.

Anmerkung

Verwenden Sie die Firewall, um ungenutzte Ports zu schließen, stellen Sie jedoch sicher, dass Ethernet-Port 443 geöffnet und in der Firewall-Konfiguration enthalten ist (für BSP 1.0 muss auch Port 80 geöffnet sein). Andernfalls wird der Zugriff auf die Systemeinstellungsseite dauerhaft verweigert.

Verwandte Themen

Firewall-Einstellungen (Seite 11)

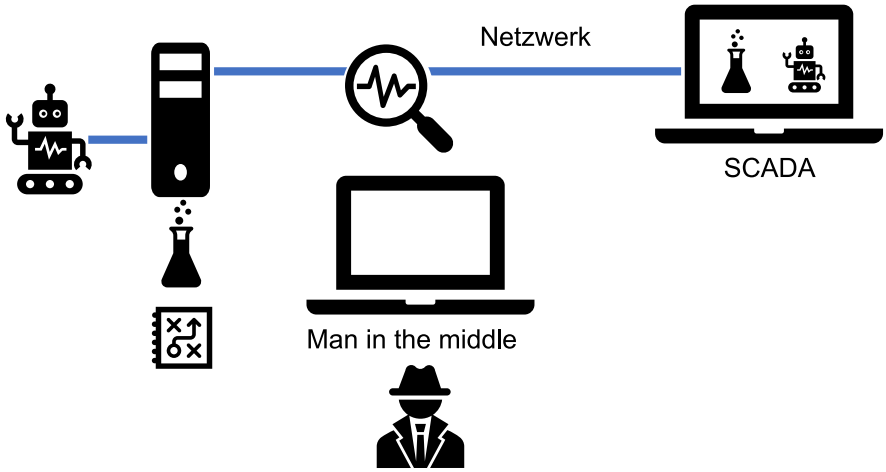
4 Mögliche Bedrohungsszenarien

Damit Sie sich möglicher Cyber-Bedrohungen bewusst werden und diese besser verstehen, sind im Folgenden einige typische Beispiele aufgeführt.

- Abfangen von Daten

  Es gibt viele Tools, mit denen der Datenverkehr im Netz ausgelesen werden kann, einschließlich Benutzernamen, Passwörtern und anderen sensiblen Daten wie Rezepturen oder Prozessdaten.

  Besonders wenn Ihr Datenverkehr im Netz nicht verschlüsselt ist, wird es Spionen sehr leicht gemacht, nach auslesbaren Informationen zu suchen.

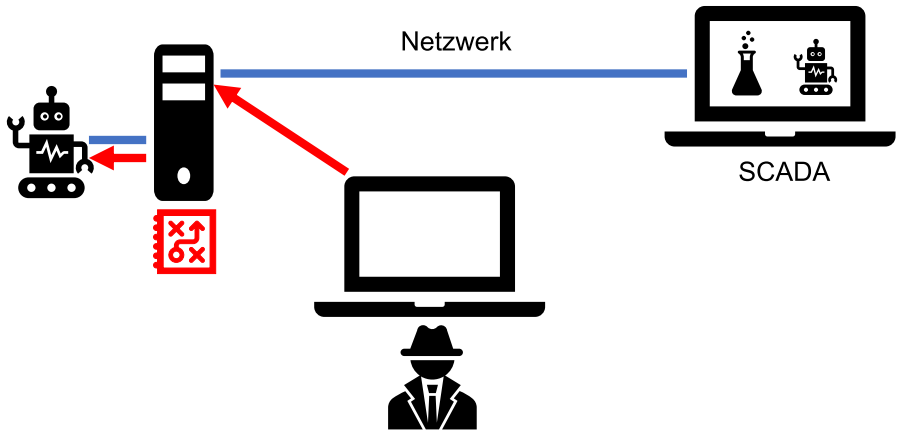


  Gegenmaßnahmen:

  Verwenden Sie die FTP- oder Telnet-Protokolle nicht außerhalb eines gekapselten Netzwerks, um sensible Daten zu übertragen. Diese Protokolle stellen ein hohes Sicherheitsrisiko dar, da Benutzernamen und Kennwörter in Klartext (unverschlüsselt) übertragen werden.

- Eingriff in Steuerungssysteme

  Wenn Zugangsdaten oder das verwendete Protokoll bekannt sind, können unter Umständen Störungen oder Schäden an Maschinen verursacht werden, und Geräte können in Botnets abgefangen oder so manipuliert werden, dass sie andere Geräte angreifen.

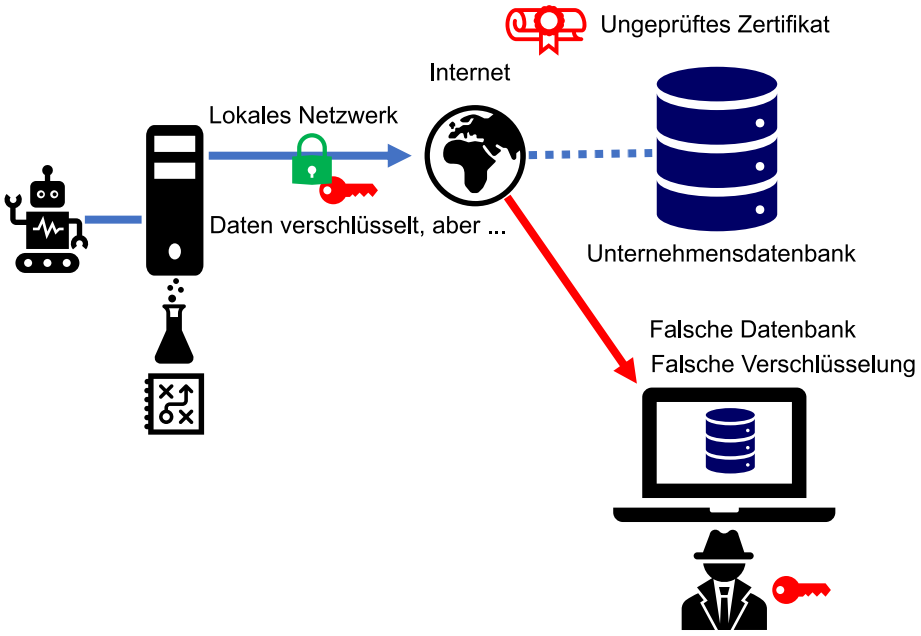


Gegenmaßnahmen:

Stellen Sie sicher, dass fremde Computer keinen Zugriff bzw. keine Kontrolle erhalten.

- Identitätsdiebstahl

  Verbindungen zu Webseiten, die nicht von einer Zertifizierungsstelle überprüft werden, können gefährlich sein, da sie Identitätsdiebstahl und die Umleitung der Kommunikation erleichtern. Dies gibt Angreifern die Möglichkeit, sensible Informationen (z. B. Benutzernamen, Kennwörter, Prozessdaten oder Rezepturen) zu erlangen und durch die Manipulation von Maschinen Schaden anzurichten.



Gegenmaßnahmen:

Stellen Sie sicher, dass Sie Zertifikate verwenden, um die Identität des Zielservers zu authentifizieren.

5 Allgemeine Sicherheitsvorkehrungen

Die Implementierung von Maßnahmen zum Schutz Ihres Netzwerks ist entscheidend, damit Ihr Netzwerk und der zugehörige Datenverkehr sicher sind.

Da Sie dieses Produkt in einem Netzwerk verwenden, wird auf folgende Sicherheitsrisiken hingewiesen:

- Datenlecks oder Datendiebstahl mithilfe dieses Produkts
- Verwendung dieses Produkts für illegale Aktivitäten durch Personen mit böswilligen Absichten
- Störung oder Abschaltung dieses Produkts durch Personen mit böswilligen Absichten
- Es liegt in Ihrer Verantwortung, Sicherheitsvorkehrungen, beispielsweise die im Folgenden beschriebenen Maßnahmen, zu ergreifen, um sich vor den oben genannten Netzwerksicherheitsrisiken zu schützen.
- Wenn dieses Produkt zusammen mit PCs in einem Netzwerk verwendet wird, sorgen Sie dafür, dass das System nicht mit Computerviren oder anderen bösartigen Entitäten infiziert ist (durch Verwendung eines regelmäßig aktualisierten Antivirenprogramms, Anti-Spyware-Programms usw.).
- Verwenden Sie dieses Produkt in einer Umgebung, die über ein LAN, ein VPN (virtuelles privates Netzwerk) oder ein Standleitungsnetzwerk verfügt.
- Verwenden Sie dieses Produkt in einer Umgebung, in der nur Personen mit kontrollierten Zugriffsrechten Zugang haben.
- Verwenden Sie dieses Produkt und andere über ein Netzwerk angeschlossene Geräte wie PCs und Tablets nur, wenn Sie Schutzmaßnahmen getroffen haben, um die Sicherheit zu gewährleisten.
- Installieren Sie dieses Produkt nicht an Orten, an denen das Produkt oder die Kabel von Personen mit böswilligen Absichten zerstört oder beschädigt werden können.

Beachten Sie, dass eine falsche Anschlusseinstellung zum bestehenden LAN zu Fehlfunktionen bei den Geräten im Netzwerk führen kann. Wenden Sie sich vor dem Anschluss an Ihren Netzwerkadministrator.

Im Internet finden Sie hierzu hilfreiche Informationen: MITRE ATT&CK® ist eine kuratierte Wissensdatenbank für die Modellierung von Cyberangriffen.

6 Bewährte Verfahren zur Absicherung Ihrer Touch-Terminals

Sie können Sicherheitsrisiken minimieren, indem Sie vorbeugende Maßnahmen ergreifen und die richtigen System- und Anwendungseinstellungen vornehmen. Verwenden Sie die in diesem Leitfaden enthaltene Checkliste, um sicherzustellen, dass Sie alle erforderlichen Maßnahmen zur Absicherung Touch-Terminals der HM-Serie ergreifen.

Verwandte Themen

Checklist für die Sicherheitskonfiguration (Seite 14)

6.1 Systemeinstellungen

Wechseln Sie zu “Systemeinstellungen” (IP/machine_config), um Passwort- und Firewall-Einstellungen vorzunehmen, auf Protokolldateien zuzugreifen und die SSH-Debugging-Funktionen zu nutzen.

6.1.1 Passwortschutz

Legen Sie ein sicheres Passwort fest, das Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (außer Leerzeichen) enthält.

Verwenden Sie unterschiedliche Passwörter für HMWIN Studio-Anwendungen und die Haupteinstellungen der Touch-Terminals der HM-Serie. Beim ersten Einschalten eines Terminals werden Sie zur Vergabe eines neuen sicheren Passworts aufgefordert. Sie können das Passwort direkt am Display oder in einem Browser eingeben, der mit dem Gerät über dessen IP-Adresse (IP/machine_config) verbunden ist.

6.1.2 Firewall-Einstellungen

Verwenden Sie die Firewall (IP/machine_config/#/services), um alle nicht verwendeten Ports zu schließen.

Wenn Sie den “Firewall Service” (IP/machine_config/#/services) aktivieren, werden alle verwendeten Funktionen mit den angegebenen Einstellungen und Ports aktiviert. Deaktivieren Sie ungenutzte Dienste und Ports oder verweigern Sie den Zugriff auf dedizierte Schnittstellen (ETH0, ETH1 und ETH2).

Anmerkung

Vergewissern Sie sich, dass “Web Server – HTTP” und “Web Server – HTTPS” aktiviert sind und Ethernet-Port 443 geöffnet ist (für BSP 1.0 auch Port 80). Andernfalls wird der Zugriff auf die Systemeinstellungsseite dauerhaft verweigert.

Beispiel für die Firewall-Einstellungen:

Name	Quell-Schnittstelle	Port oder Bereich	Protokoll	Erforderlich
Webserver - HTTP (für die Konfiguration erforderlich)	Beliebige	80	TCP	✓ (BSP 1.0)
Webserver - HTTPS (für die Konfiguration erforderlich)	Beliebige	443	TCP	✓
Geräteerkennung	Beliebige	990–991	UDP	✓
FTP-Befehls-Port, erforderlich für HMWIN Studio-Betrieb	Beliebige	21	TCP	✓ (BSP 1.0)
Passiver FTP-Modus, erforderlich für HMWIN Studio-Betrieb	Beliebige	18756–18759	TCP	
SSH-Server	Beliebige	22	TCP	
VNC-Server	Beliebige	5900	TCP	
DHCP-Server	Beliebige	67	UDP	
SNMP-Server	Beliebige	161	UDP	
SPS-Verbindungsports	Beliebige	9094–9097	TCP	
HMWIN Studio-Betrieb	Beliebige	990	TCP	

6.1.3 Protokolldateien und SSH-Debugging-Funktionen

Diese Funktionen können verwendet werden, um eine untypische Nutzung zu erkennen. Sie können nur mit Administratorrechten verwendet werden.

7 FAQ

1. Kann ich Software-Patches und Firmware-Updates erhalten?

   Kostenlose Downloads der neuesten Versionen sind auf der Panasonic-Website verfügbar: Panasonic Downloadcenter oder InfoHub

2. Ist eine Hintertür auf dem Gerät installiert?

   Es ist keine Hintertür auf dem Gerät installiert. Wenn Sie Ihr Passwort verlieren, gibt es keine Möglichkeit, um Ihre Einstellungen wiederherzustellen.

3. Ruft das Gerät Panasonic-Server auf?

   Mit den Werkseinstellungen gibt es keinen Prozess, um automatisch einen Panasonic-Server aufzurufen.

4. Wo kann ich eine neue Sicherheitslücke melden?

   Kontaktieren Sie das Panasonic Product Security Incident Response Team (Panasonic PSIRT), das zentrale Koordinationsteam für Sicherheitsrisiken im Zusammenhang mit Produkten von Panasonic.

8 Checklist für die Sicherheitskonfiguration

Verwenden Sie diese Checkliste, um sicherzustellen, dass Sie alle erforderlichen Maßnahmen zur Absicherung der Touch-Terminals der HM-Serie ergriffen haben. Haken Sie alle Punkte ab, die Sie erledigt haben. Am Ende der Liste ist Platz für zusätzliche Punkte.

Erledigt	Risiko[1)]	Bereich	Konfigurationsseite	Zu erledigen
	Hoch	Passwörter (admin, user)	IP/machine_config/#/ authentication	Sichere Administrator- und Benutzerpasswörter einrichten
	Hoch	Dienst: Autorun-Skripte	IP/machine_config/#/services	Deaktivieren
	Hoch	Dienst: SSH-Server	IP/machine_config/#/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Avahi-Dämon	IP/machine_config/#/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Cloud-Dienst	IP/machine_config/#/services	Deaktivieren, wenn nicht benötigt
	Niedrig	DHCP-Server	IP/machine_config/#/services	Deaktivieren, wenn nicht benötigt
	Niedrig	VNC-Dienst	IP/machine_config/#/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Firewall	IP/machine_config/#/services	Aktivieren und Einstellungen anpassen
	Hoch	HMWIN-Passwörter (mindestens admin, user, log)	HMWIN Studio Project/Configuration/Security	Standard-Administrator- und Benutzerpasswörter ändern
	Hoch	Protokollkonfiguration	HMWIN Studio Project/Configuration/ Protocols	Nicht benötigte Passthrough-Funktionen und Serverprotokolle deaktivieren Verschlüsselte Varianten der verwendeten Feldbusprotokolle bevorzugen
	Mittel	HMWIN-OPC-UA-Funktion	HMWIN Studio Project/Configuration/Interface	Serverzugriff prüfen
	Mittel	HMWIN-MQTT-Funktion	HMWIN Studio Project/Configuration/Interface	Verschlüsselung und Zertifikate verwenden

Erledigt	Risiko[1)]	Bereich	Konfigurationsseite	Zu erledigen
	Mittel	SMTP- und FTP-Javascript-Funktionen	HMWIN Studio Prüfen Sie Ihre konfigurierten Ereignisse (z.B. Email, FTP, Web-Kamera)	Verschlüsselung und Zertifikate verwenden

1) Das Risikoniveau hängt von Ihrer Anwendung ab.

9 Panasonic Hotline

Sollten Sie Fragen haben, die sich nicht mit Hilfe des Handbuchs oder der Online-Hilfe klären lassen, kontaktieren Sie bitte eines unserer Vertriebsbüros.

Folgende Informationen sind bei einem Kontakt wichtig:

- Die Seriennummer und/oder die Versionsnummer Ihres Produkts.
- Die Versions- und Service-Pack-Nummer von MS-Windows, das auf Ihrem PC installiert ist.
- Der verwendete Hardwaretyp.
- Der genaue Wortlaut der am Bildschirm angezeigten Fehlermeldung.
- Welches Problem ist aufgetreten und was haben Sie unternommen, um es zu beheben?
- Wie haben Sie versucht, das Problem zu lösen?

Kontaktieren Sie uns über eine der Hotline-Nummern oder senden Sie uns Ihre Anfrage über unser Kontaktformular.

Kunden außerhalb Europas erreichen den technischen Support über unsere globale Webseite.

Panasonic Industry Europe GmbH

- Deutschland und alle europäischen Ländern, die nicht auf dieser Seite aufgeführt sind:
  +49 89 45354-2748 (SPS, FP-I4C, Touch-Terminals)
  +49 89 45354-2737 (Sensoren)
  +49 89 45354-2750 (Servoantriebe)
- Frankreich:
  +33 160 135757

Panasonic Industry Austria GmbH

Bosnien und Herzogowinien, Bulgarien, Kroatien, Montenegro, Österreich, Schweiz, Serbien, Slowenien:

+43 2236 26846

Panasonic Industry Benelux B.V.

Belgien, Dänemark, Luxemburg, Niederlande, Norwegen, Schweden:

+31 499 372727

Panasonic Industry Italia srl

Italien:

+39 045 6752711, support.piit@eu.panasonic.com

Panasonic Industry Poland sp. z o.o.

Baltische Staaten, Finnland, Polen, Rumänien, Tschechische Republik, Slowakei, Ungarn:

+48 42 2309633

Panasonic Industry Iberia S.A.

Portugal, Spanien:

+34 91 3293875

Panasonic Industry UK Ltd.

Vereinigtes Königreich Großbritannien und Irland:

+44 1908 231555

10 Änderungsverzeichnis

Sicherheitsleitfaden Version 1.0, 2024.07

Erste Ausgabe