Kennzeichnung

Direct Monitor DM-320P-* Personal Computer PC-320P-* Remote Monitor RM-320P-* Operator Workstation (PC)PC-GXP1100-*, PC-GXP1200-* Operator Workstation (RM)RM-GXP1100-*, RM-GXP1200-* Industrieller Box Thin Client BTC22-*, BTC24-*
Betriebssystem IGEL OS 11, IGEL OS 12

Die mit * markierten Stellen sind Platzhalter für Varianten des Geräts.

Pepperl+Fuchs-Gruppe Lilienthalstraße 200, 68307 Mannheim, Deutschland
Internet: www.pepperl-fuchs.com

Verweis auf weitere Dokumentation

Die entsprechenden Datenblätter, Betriebsanleitungen, Handbücher, Konformitätserklärungen, EU-Baumusterprüfbescheinigungen, Zertifikate und Control Drawings soweit zutreffend ergänzen dieses Dokument. Diese Dokumente finden Sie unter www.pepperl-fuchs.com.

Sie finden spezifische Geräteinformationen wie z. B. das Baujahr, indem Sie den QR-Code auf dem Gerät scannen. Alternativ geben Sie die Seriennummer in der Seriennummernsuche unter www.pepperl-fuchs.com ein.

Bestimmungsgemäße Verwendung

Das Gerät ist nur für eine sachgerechte und bestimmungsgemäße Verwendung zugelassen. Bei Zuwiderhandlung erlöschen jegliche Garantie und Herstellerverantwortung.

Verwenden Sie das Gerät nur im Industriebereich.

Bestimmungswidrige Verwendung

Der Schutz von Personal und Anlage ist nicht gewährleistet, wenn das Gerät nicht entsprechend seiner bestimmungsgemäßen Verwendung eingesetzt wird.

Security-Kontext

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen umzusetzen.

Setzen Sie Defense-in-Depth-Mechanismen ein, die mehrere, aufeinander abgestimmte und koordinierte Maßnahmen beinhalten.

Betreiben Sie das Gerät nur in den folgenden Netzwerken:

- **Off-Plant**-Netzwerk
- **Automation**-Netzwerk
- **Intranet**-Netzwerk
- **Enterprise**-Netzwerk

Bei diesen Netzwerken handelt es sich um sichere und überwachte Netzwerke mit bekannten und vertrauenswürdigen Teilnehmern, welche physisch oder logisch vom Internet getrennt sind.

Das Gerät wird mit einem vorinstallierten Betriebssystem geliefert: IGEL OS 11 oder IGEL OS 12.

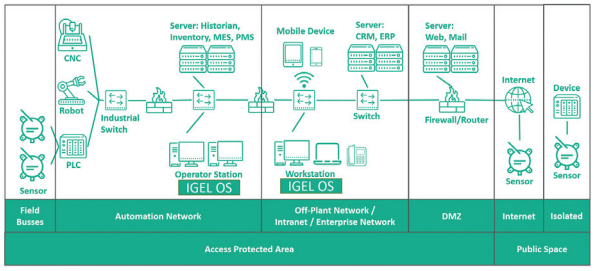

Abbildung 1 Beispiel für die Integration von Geräten und Software in einer Anlage

Schnittstellen

Das Gerät besitzt die folgenden Schnittstellen.

Informationen zu den Schnittstellen finden Sie im Datenblatt.

Inbetriebnahme

Befolgen Sie die Installationsanweisungen und die bewährten Methoden der IGEL-Wissensdatenbank unter kb.igel.com

Härtung des Geräts

Ändern Sie vordefinierte Benutzerkonten, Zugangsdaten und Rechte.

Ändern Sie das voreingestellte BIOS-Passwort.

Deaktivieren Sie alle nicht genutzten Benutzerkonten, Zugangsdaten und Rechte.

Deaktivieren Sie alle nicht genutzten Dienste.

Deaktivieren Sie alle nicht genutzten Funktionen.

Deinstallieren Sie nicht genutzte Software.

Verwenden Sie eine Firewall zur Beschränkung des Zugriffs.

Aktivieren Sie die Firewall.

Schützen Sie wichtige Verzeichnisse und Daten gegen ungewollte Veränderungen.

Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung nach der Security-Richtlinie und den gesetzlichen Bestimmungen zum Datenschutz.

Aktivieren Sie den Aktualisierungsmechanismus nach der Security-Richtlinie.

Aktivieren Sie nach einer bestimmten Zeit der Inaktivität den automatischen Sperrbildschirm und die Benutzerabmeldung.

Verwenden Sie nur Daten und Software aus zugelassenen Quellen.

Öffnen Sie keine Hyperlinks aus unbekannten Quellen, z. B. aus E-Mails.

Empfohlene security-bezogene Werkzeuge

Konfigurieren Sie Benutzerkonten, Zugangsdaten und Rechte mit starken Passwörtern.

Verwenden Sie z. B. den Passwortmanager KeePass, um Passwörter zu erstellen und zu speichern.

Betrieb

Sperren Sie das Gerät gegen Hardware-Manipulation. Stellen Sie sicher, dass nur autorisierte Benutzer Zugang haben.

Beschränken Sie den Zugang zu den externen Schnittstellen des Geräts auf autorisierte Benutzer.

Erneuern Sie Zertifikate in regelmäßigen Abständen.

Ändern Sie Passwörter in regelmäßigen Abständen.

Führen Sie regelmäßige Backups durch.

Instandhaltung und Verwaltung

Prüfen Sie regelmäßig die IGEL-Internetseite auf die Veröffentlichung der aktuellsten Software und von Security Advisories: https://www.igel.com.

Umgang mit Sicherheitsvorfällen

Melden Sie Vorfälle an den Hersteller.

Nutzen Sie die Internetseite, um Vorfälle zu melden, RSS-Feed: https://www.pepperl-fuchs.com/cybersecurity.

Auf dieser Internetseite erhalten Sie Informationen, wie Sie mit Pepperl+Fuchs in Kontakt treten.

Sicherheitsexperten – Computer Emergency Response Team (CERT)

Ziel des Expertenteams ist es, dass Anwender und Hersteller zusammenarbeiten, um vermutete Sicherheitslücken bezüglich der Produkte, Lösungen und Dienste von Pepperl+Fuchs zu schließen.

Außerbetriebnahme und Entsorgung

Außerbetriebnahme

Befolgen Sie die Anweisungen in der IGEL-Dokumentation, um das Gerät auf die Werkseinstellung zurückzusetzen: kb.igel.com

Entsorgung

Verwenden Sie ein Datenlöschprogramm eines Drittanbieters, um die Festplatte sicher zu löschen oder zerstören Sie die Festplatte.

Löschen Sie folgende Daten über die Funktion **Zurücksetzen auf Werkseinstellung**.

- Zugangsdaten
- Konfigurationseinstellungen
- Logdaten
  - Historie
  - Ereignisdaten
  - Fehlerdaten
- Weitere Betriebsdaten, die auf dem Gerät gespeichert sind
  - Personenbezogene Daten (DSGVO)