Marking

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-* Industrial Box Thin Client BTC22-*, BTC24-*
Operating System IGEL OS 11, IGEL OS 12

The *-marked letters of the type code are placeholders for versions of the device.

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

Reference to Further Documentation

The corresponding datasheets, instruction manuals, manuals, declarations of conformity, EU-type examination certificates, certificates, and control drawings if applicable supplement this document. You can find this information under www.pepperl-fuchs.com.

For specific device information such as the year of construction, scan the QR code on the device. As an alternative, enter the serial number in the serial number search at www.pepperl-fuchs.com.

Intended Use

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

Only use the device in the industrial location.

Improper Use

Protection of the personnel and the plant is not ensured if the device is not used according to its intended use.

Security Context

To protect your components, networks, and systems, it is not enough to implement standalone measures.

Use defense-in-depth mechanisms that include several coordinated measures designed to work together.

Only operate the device in the following networks:

- **Off-Plant** network
- **Automation** network
- **Intranet** network
- **Enterprise** network

These networks are secure and monitored networks with known and trusted participants that are physically or logically separated from the internet.

The device is supplied with a pre-installed operating system: IGEL OS 11 or IGEL OS 12.

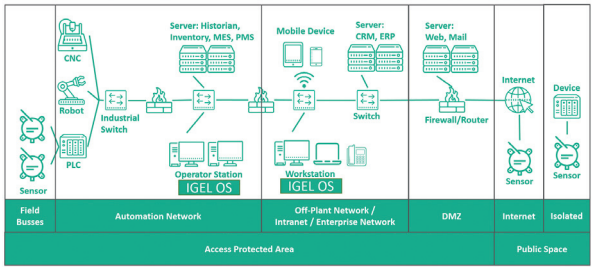

Figure 1 Example of the integration of the devices and software in a plant

Interfaces

The device features the following interfaces.

Refer to datasheet for information regarding the interfaces.

Commissioning

Follow the installation instructions and best practices from the IGEL knowledge base at kb.igel.com.

Hardening of the Device

Change predefined user accounts, access data and rights.

Change the default BIOS password.

Disable any unused user accounts, access data and rights.

Disable any unused services.

Disable any unused functions.

Uninstall any unused software.

Use a firewall to restrict access.

Enable the firewall.

Prevent unintentional changes to important directories and data.

Enable the security-relevant event logging according to the security policy and the legal provisions in relation to data protection.

Enable the updates procedure according to the security policy.

Enable the automatic lock screen and user logout after a specified period of inactivity.

Only use data and software from approved sources.

Do not open hyperlinks from unknown sources, e. g. in e-mails.

Recommended Security-Related Tools

Configure user accounts, access data and rights with strong passwords.

Use a password manager such as KeePass to create and store passwords.

Operation

Lock the device to prevent hardware tampering. Ensure that only authorized users have access.

Restrict the access to the external interfaces on the device to authorized users only.

Renew certificates at regular intervals.

Change passwords at regular intervals.

Make regular backups.

Maintenance and Management

Check the IGEL website regularly for latest software and security advisories: https://www.igel.com.

Handling Security Incidents

Report incidents to the manufacturer.

Use the website to any report incidents, RSS feed: https://www.pepperl-fuchs.com/cybersecurity.

This website contains information about how to contact Pepperl+Fuchs.

Security Experts – Computer Emergency Response Team (CERT)

Establish and coordinate a team of experts including security experts from the user, manufacturer, and other stakeholders.

The objective of the team of experts is for users and manufacturers to work together to resolve suspected vulnerabilities regarding Pepperl+Fuchs products, solutions, and services.

Decommissioning and Disposal

Decommissioning

Follow the instructions in the IGEL documentation to perform a factory reset of the device: kb.igel.com.

Disposal

Use a third-party data wiping tool to securely wipe the hard drive or destroy the hard drive.

Delete the following data using the **Reset to Factory Defaults** function.

- Access data
- Configuration settings
- Log data
  - History
  - Event data
  - Fault data
- Additional operating data stored on the device
  - Personal data