CONTAINERIZED DEVICE AND APPLICATION MANAGEMENT

FASTER AND SAFER THAN THE MANUAL VERSION



Everyone is talking about the IoT (Internet of Things): networking objects and digitizing information from a wide variety of devices.

In professional and industrial contexts, the IoT concept appears in various guises in different industries. For instance, the term “smart grid” is used for the energy sector, “smart building” for building technology and “smart factory” for the digitization of manufacturing, where the term “IIoT,” the industrial IoT, has also become established.

In all applications, the devices themselves and the applications on them need to be managed. Why? Digitization and automation in a professional context are nothing new.

In the past decades, machines, buildings and other applications have already been automated and digitized. However, these applications were often local and spatially limited. In terms of the technology and workflow, the natural approach to management was local, involving a laptop and direct cable connection. Given the number of devices involved, that was economically feasible. However, the IIoT aims to network many hundreds, if not thousands, of devices. Locally updating the operating system/firmware, as well as its security settings and applications, is not economically feasible. Many industrial IoT gateways come from automation technology and were never designed for bulk handling of OSs and apps.

This professional article contains basic technical information; it is not contractually binding and may contain errors or omissions.

Since as far back as the mid 2000s, WAGO has used Linux® as the OS for its higher-end controllers. This allows IoT and security innovations to be incorporated and Docker® technology to be utilized fully. This approach has traditionally been used for services, i.e. containerized apps. However, Docker® can also be used to execute scripts and other programs on the devices. Doing so allows clearly organized, traceable management of all network settings and security settings – a huge advantage in terms not only of speed, but also of reliability.

Imagine a manual step in which the protocol ports have to be set for many devices – perhaps even just 20; can anyone really claim they can carry this out 20 times with zero errors and uniform quality? In contrast, a script for a Docker® container can be created once and then distributed and executed automatically 20, 200, 2000 times or more. Two separate pairs of eyes can even check it in advance for double verification. And if an error occurs nonetheless, it can be quickly corrected for all the devices – and that's it!

Different tools are available on the market for orchestrating and managing software containers. These tools – for example, Docker Swarm or Portainer – can be used to handle thousands of containers. With some WAGO controllers that are typically used in digitization environments, the firmware or the entire operating system can be swapped out via Docker® containers, allowing uniform bulk handling of devices and applications in all applications around the world.

For instance, assume a device is accessible via Portainer; then all that's required is a suitable Docker® image containing the desired firmware. As soon as the Docker® container is started on the desired device, the firmware is swapped out. It is possible to set error handling parameters like the number of attempts. If the process terminates in an error state, the original firmware version is retained.



If, for example, you want to load firmware version 19 onto one or many WAGO PFC200s, the corresponding image is located here:
https://hub.docker.com/r/wagoautomation/fw-update

Images for higher firmware versions are available upon request: **iot@wago.com**

Are you looking for a supplemental solution for managing and distributing containers?
You can find it here: **iot@wago.com**

In Summary:

- ✓ The bulk handling required for large IoT products is possible.
- ✓ Familiar IT technologies are used.
- ✓ Firmware, applications, network settings and security settings can be managed centrally and automatically.
- ✓ Errors that could creep in during manual steps are reduced to the absolute minimum, making troubleshooting as fast as possible.

Executive Example

In conclusion, let's make a time comparison: local update via laptop (A) vs. container roll-out/deployment and start (B).

- Assume the laptop and, in the second case, a repository with container management software, are ready for use.
- For (B), software is started and executed – that's it.
- For (A), the notebook needs to be connected to the device; in industrial environments, that requires first finding a safe location to set up the laptop in the immediate vicinity of the control cabinet.

Here we see the advantage of the container solution even with just a single device. Imagine adding in the amount of time a trained electrician needs in order to get to the device. And multiply that travel time by 20, 200 or 2000 devices.

For the error prevention and savings this offers, also see the "Network Settings and Security Settings" example described and marked above.

MM-41 8120 - 08/2023 - Printed in Germany - Subject to design changes

WAGO GmbH & Co. KG
Postfach 2880 · 32385 Minden
Hansastraße 27 · 32423 Minden
info@wago.com
www.wago.com

Headquarters	+49 571/ 887 - 0
Sales	+49 571/ 887 - 44 222
Orders	+49 571/ 887 - 44 333

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.
"Copyright – WAGO GmbH & Co. KG – All rights reserved. The content and structure of the WAGO websites, catalogs, videos and other WAGO media are subject to copyright. Distribution or modification of the contents of these pages and videos is prohibited. Furthermore, the content may not be copied or made available to third parties for commercial purposes. Also subject to copyright are the images and videos that were made available to WAGO GmbH & Co. KG by third parties."