Kontron AIS GmbH

KontronGrid

From Manual to Mandatory

The Evolution of Device Management Strategies and How to Future-Proof Your Fleet

Thomas Dreyer, Director R & D at Kontron AIS GmbH

Understand the transition from manual to automated device management and learn strategies for managing legacy devices, integrating IT, OT and IoT, and complying with EU security regulations. Navigate the complexity of the digital landscape, enhance operational efficiency, and safeguard your devices.

August, 2024

Table of Contents

Imagine your fleet running like a well-oiled machine with real-time visibility into device locations, predictive maintenance that minimizes downtime, and safety measures that leave nothing to chance. Whether you have thousands of vehicles on the road or cameras in a smart factory – in the age of the Internet of Things (IoT), managing thousands of devices isn't science fiction – it's the new reality. With more than 15 billion IoT devices already in the field and another 14 billion on the horizon by 2030[1], fleet management has become a data-driven, technologically advanced field. This White Paper explores the evolution from manual to mandatory device management and offers insights on how to future-proof your fleet in today's IoT-powered world.

Managing thousands of devices isn't science fiction – it's the new reality.

What is device management for IoT edge devices and why it is important in today's interconnected world?

An edge device is a piece of hardware that controls data flow between local networks and broader systems. Edge devices can range from simple sensors to complex industrial systems, including scanners, smartphones, medical devices, vehicles, and automated machines. They are an integral part of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT), collecting, analyzing, and using data where it originates before sending insights to the cloud.

Device management for IoT edge devices refers to the processes of provisioning, deploying, monitoring, controlling, and updating IoT devices. IoT technology has revolutionized device management by providing benefits such as real-time tracking, predictive maintenance, and enhanced safety measures.

The existing technology that has formed the core of industrial processes for decades cannot be easily or safely transferred to the connected world. Legacy devices are generally unsupported and in some cases 20, 30, or more years old. However, this equipment still works and is seldomly replaced, often due to the huge capital expenditure required to upgrade. Sometimes this equipment does not even understand IP (Internet Protocol) as a communication protocol, making it incompatible with modern IoT devices. Upgrading this legacy technology will take device management to new heights, enabling organizations to operate more efficiently, reduce costs, and improve compliance and safety standards.

Today's IoT gateways can connect legacy devices to a cloud platform by translating their communication protocols into a unified format. This allows organizations to integrate new IoT devices into their existing »

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 28th Nov 2023

infrastructure, providing scalability and flexibility. IoT devices, which are becoming increasingly powerful, compact and robust, have emerged as essential tools in this transformation. Their ability to be installed anywhere, their resilience for multiple use cases, and their emphasis on data security have made them a must.

Real-world examples of successful device management strategies:

- **Roll out updates and remote support to public transit ticket validators:** Device Management can be used to remotely update the software on ticket validators to ensure they have the latest features and security patches. If a ticket validator is not functioning properly, engineers can use device management to remotely diagnose and fix the problem without requiring a technician to physically visit the device.
- **Global monitoring of electric car charging stations:** Device management is a critical aspect of managing a fleet of charging stations, especially when those stations are distributed around the world. It makes it much easier to manage, monitor and operate your fleet of charging stations, regardless of their geographic distribution.
- **Simplified handling of multiple Docker containers for artificial intelligence (AI) inference of industrial seals in ATEX environments:** In critical environments such as ATEX, where mechanical seals, seal supply systems, magnetic couplings, carbon floating ring seals, expansion joints or flat gaskets are difficult to access but widely used, safety and reliability are paramount. That's why a complex predictive monitoring and analysis system was implemented using OpenTreat Routers and AI interference, which not only streamlined the configuration, management and deployment of multiple Docker containers in a fleet management solution, but also optimized the bandwidth, data volume and roaming costs required for updates to a minimum.

Organizations have different options for device management – they can embed IoT edge devices into older machines, manually manage devices, or take an integrated approach to information technology (IT), operational technology (OT), and IoT.

Challenges at the edge of security

IoT devices are often designed to be inexpensive and compact, reduced to bare minimum regarding components and size, while providing as much functionality, flexibility, and performance as possible[2]. In addition to this, global dispersion and the need for uninterrupted connection leaves them vulnerable to threats and makes security one of the biggest challenges »

[2] https://www.techtarget.com/searchsecurity/tip/Use-IoT-hardening-to-secure-vulnerable-connected-devices

in the world of edge device management. This is especially true when these IoT edge devices are embedded in older machines that were not designed with today's threats in mind, leaving them susceptible to:

Malware infections:
Outdated operating systems lack the latest security updates and patches, leaving them vulnerable to malware infections. These infections can lead to data breaches and system compromise.

Data theft:
Attackers can exploit vulnerabilities in outdated operating systems to steal sensitive data. This can lead to data breaches, financial loss, and damage to an organization's reputation.

Lack of compatibility with new security technologies:
New security features aren't compatible with older operating systems, leaving them vulnerable to attack. Modern security solutions and protocols may not work as intended on legacy systems.

Regular automatic updates:
Updates are designed to keep devices up-to-date with the latest security patches, bug fixes, and new features. However, these automatic updates can also pose a threat to the operation of critical applications because the compatibility of new updates cannot always be ensured. This is especially true for applications that are highly customized or have specific hardware requirements.

Exploitable backdoors:
Older hardware systems may have security flaws that no longer meet modern standards, such as default passwords that many organizations have failed to update.

Loopholes or flaws in operating systems:
Cybercriminals can exploit vulnerabilities in outdated operating systems to gain unauthorized access to a computer system. This unauthorized access can lead to data breaches and system compromise.

Denial of Service (DoS) attacks:
Attackers can exploit vulnerabilities in operating systems to launch DoS attacks. These attacks involve sending repeated bogus requests to overload the system, causing service disruptions and potential financial loss. »

The Mirai botnet attack

The Mirai malware incident is a strong reminder of the consequences of not managing devices properly.

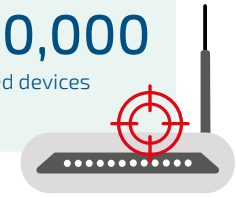
The incident in 2016, involved the Mirai botnet, which targeted consumer devices such as smart cameras, home routers and refrigerators, transforming them into a vast network of remotely controlled bots.

Mirai attacked by scanning for vulnerable IoT devices with open ports or default usernames and passwords. Once it found these vulnerable devices, it used exploits to gain access and infect the devices with its malicious code. The infected devices became part of the Mirai botnet, allowing attackers to remotely control them.

The malware was designed to perform unauthorized activities such as intercepting messages, remotely turning on a device's camera and microphone, and stealing personal information such as financial data, passwords, and contacts.

With a peak of 600,000 infected devices, this incident highlights the critical importance of effective device management, especially in the context of IoT and edge device security, to mitigate such risks and prevent large-scale network disruptions.

600,000
infected devices



The limitations of manual device management

Similar to the vulnerability challenges associated with adding a simple IoT solution to legacy machines, the security risks of manually managing devices are significant. Manual management increases security risks by making it difficult to ensure all devices are up to date with the latest security patches and firmware updates. In addition other challenges of manual device management are:

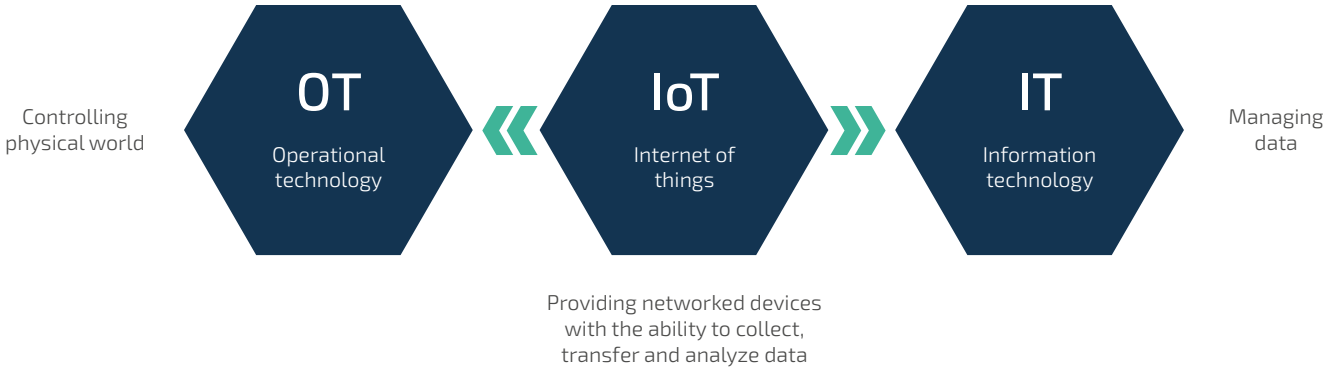
- Time-consuming: Manually managing many IoT devices can be time-consuming and inefficient. It can take a lot of time to diagnose and manage each device individually, especially if they are in different locations.
- Difficult to scale: As the number of devices grows, it becomes increasingly difficult to manage them manually. The manual management of hundreds or thousands of devices is nearly impossible and can lead to errors and oversights.
- Limited visibility: Manual management can limit visibility into the health and performance of IoT devices. It can be difficult to monitor and keep all devices updated, especially if they are in remote or inaccessible locations. »

› Data overload: As the number of devices and the data they generate increases, it can be difficult to manage and analyze all the data manually. This can lead to inefficiencies and limitations in IoT system functionality.

The mandated need for an automated device management

As the device management landscape continues to evolve, the need for automation becomes more apparent. While it may be possible to manage devices manually, complexity escalates when there are hundreds or even thousands of devices involved or when they are in constant motion. Even when organizations develop a proprietary solution, controlling and monitoring these devices can quickly become a daunting task.

The integration of IT, OT and IoT is a key consideration in device management. This convergence offers many benefits that are critical to overcoming device management challenges and ensuring efficiency and security:



› Data collection and analysis: IoT devices can collect data from OT devices and transmit it to IT departments where it can be processed, analyzed, and acted upon. This real-time flow of data enables organizations to monitor their operations, make data-driven adjustments, and respond quickly to emerging opportunities or challenges.

› Improved automation: The convergence of IT and OT enables connected devices and real-time data to inform and automate operations. For example, IoT tags and sensors deployed in a warehouse for tracking and navigation enable intelligent automation with the help of robots. »

- Enhanced security: In an age where devices connected to the Internet or cloud are at risk of being accessed by malicious actors, security is paramount. IoT device management provides a solution, enabling organizations to better monitor and control their critical IoT devices. The insights gained from IoT data improve decision making and strategy development, further strengthening security measures.

- Seamless connectivity: Achieving integration between OT and IT domains is a mandatory requirement in the modern business landscape. IoT serves as a bridge between isolated OT devices and IT software and resources. This connectivity enables organizations to gain valuable insights, implement process improvements, and realize the full potential of their operations.

- Efficient device management: IT serves as the technological backbone of an enterprise, while OT is the linchpin that connects, monitors, manages, and secures industrial operations. By integrating IT, OT, and IoT, organizations can efficiently and effectively manage their devices and ultimately improve their overall operations.

The integration of IT, OT and IoT is the fundamental step towards automated device management. By seamlessly connecting these three critical areas, organizations create the framework that enables the wide range of benefits of automated device management to come to life.

For those who have yet to decide on a device management solution, it's crucial to recognize that the landscape is evolving rapidly. New security standards are emerging, and the urgency of addressing device management cannot be underestimated. The European Commission has imposed minimum security requirements for Internet of Things (IoT) products, also known as smart devices, starting in 2024. If they do not meet these standards, the product will be banned from the EU market. »

Are you already aware of these security standards?

› **EU Data Act (formally adopted on January 11th 2024, will become enforceable in 2025)**
The EU Data Act is a set of rules governing the use of and access to data generated by internet-connected devices in the European Union. It regulates who can access and share data generated by internet-connected devices and makes more data available for use across all sectors of the EU economy. The law gives consumers the right to access all this data, free of charge and in real time, and may require manufacturers to share this data with other repair or service providers, thereby promoting competition in the after-sales market.[3]

What does this mean for component and equipment manufacturers?
The Act seeks to bring greater fairness to the use of IoT data by giving consumers and businesses access to the data generated by their devices and enabling them to use it for subsequent value-added services, such as predictive maintenance. The law also poses significant challenges for the IoT industry in terms of how data is handled. In particular, it will require significant design changes to ensure that the data generated by IoT devices is accessible, by default, free of charge and, where applicable, continuously and in real time.

Therefore, manufacturers of IoT devices and providers of IoT services marketed or offered on the EU market will need to comply with the relevant requirements of the Data Act to avoid penalties and ensure that they are not left behind in the data-driven society.

› **Cyber Resilience Act (still in draft stage)**
The Cyber Resilience Act (CRA) is a proposed regulation on cybersecurity requirements for products with digital elements marketed in the European Union (EU). It will be the first IoT legislation in the world. The CRA aims to establish minimum standards and ongoing updates to strengthen cybersecurity and protect digital products, such as Internet of Things (IoT) devices.[4]

What will this mean for component and equipment manufacturers?
For component and device manufacturers, the introduction of the CRA means a profound change in how they develop and bring digital products to market. It will oblige manufacturers to improve the security of products with digital components from the design and development phase through the entire life cycle, including hardware and software updates and new versions on the market. In addition, it will create a uniform framework for cybersecurity, increase the transparency of the security properties of products and enable companies and consumers to safely use products featuring digital components.

Failure to comply with the requirements of the act can result in severe penalties of up to EUR 15 million or 2.5 % of annual revenue.[5]

»

[3] https://www.politico.eu/article/europe-new-data-act-explained/, 28th Nov 2023
[4] https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act, 28th Nov 2023
[5] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet, 9th Jan 2024

› **NIS2 (Network and Information Security) Directive**

The NIS2 directive is an EU-wide piece of legislation that provides legal measures to improve the overall level of cybersecurity in the EU by ensuring readiness and cooperation between member states and requiring the most important players in key industries to implement security measures and report incidents.

The NIS2 directive came into force on January 16, 2023. The member states must adopt and publish the necessary measures to comply with the NIS2 directive by 17 October 2024 and apply these measures from 18 October 2024.9 In Germany, a draft bill from the Federal Ministry of the Interior on the NIS2 Implementation Act (NIS2umsuCG) has already been drawn up.[6]

What does this mean for component and equipment manufacturers?

› Prioritizing supply chain security:
Manufacturers must assess the security of their supply chain and mitigate risks. This includes measures to secure suppliers, partners and contractors.

› Focus on risk management:
Manufacturers who are classified as "important" must introduce mandatory risk management processes. This may require investment in new tools and additional specialist staff.

› Increased collaboration with IT service providers:
To meet NIS2 requirements, manufacturing companies must work more closely with IT service providers. This can lead to higher costs and changes in business models.[7]

Companies in critical infrastructures in particular need to take NIS2 compliance seriously. Failure to comply may result in significant fines, which can amount to EUR 10 million or 2 % of revenue. »

[6] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, 9th Jan 2023
[7] https://nis2directive.eu/, 9th Jan 2024

› IEC63442 Cyber security in industrial automation

EC63442 Cybersecurity in Industrial Automation is a program that focuses on securing industrial control systems (ICS) from cyber threats. ICS are specialized industrial computers that control critical infrastructure and process automation systems such as power grids, water and wastewater management, transportation, natural gas, nuclear power plants, oil refineries, steel mills, and most types of factories. The program is designed to ensure that manufacturers consider cybersecurity in the design and development of their products with digital elements.[8]

What does IEC 62443 come into force?

The IEC 62443 series of standards has been developed over time and the individual sections have been published and introduced step by step at different times. For example, the IEC 62443-4-1 standard, which sets process requirements for the safe development of products for industrial automation and control systems (IACS), was published in February 2018.

IEC 62443 is divided into four parts:

1. General:
   The first part describes the basic nomenclature, concepts, models and guidelines that apply to the complete series of standards.

2. Policies and Procedures:
   The second part focuses on methods and processes related to IEC security. The requirements for security training for various roles in the industry, such as operators, integrators and service providers, are defined her.

3. System:
   The third part deals specifically with the assessment of security risks for system design and risk management and provides a systematic approach for preventing and managing security risks in industrial automation and control systems.

4. Component and system requirements:
   This last part describes the detailed requirements for secure product development and the security-related features of IEC components.[9]

[8] https://www.tuv.com/usa/en/cyber-security-in-industrial-automation.html, 28th Nov 2023
[9] https://www.iec.ch/blog/understanding-iec-62443, 9th Jan 2024

Modern device management strategies

The technical intricacies of modern device management take an integrated approach to IT, OT, and IoT. By focusing on the benefits of virtual private networks (VPNs), remoting, Docker, and templates. Together, these tools minimize technical issues, improve security, and enable proactive health monitoring. This enables centralized management, efficient deployment, and secure connectivity in the complex device management landscape.

What is Docker and why does it matter?

Docker is an open platform that is revolutionizing the way applications are built, shipped, and run. Imagine a world where your applications exist independent of the underlying infrastructure, enabling rapid and consistent deployment. Docker accomplishes this through containers – lightweight, self-contained packages that contain everything an application needs to run. Code, libraries, and system tools are all neatly packaged.

Why is this separation of application and infrastructure so important?

Traditional device management methods often involve complicated processes, such as updating operating systems with a new partition, which risks losing important files. Docker eliminates this complexity by isolating applications from the operating system, creating a standardized environment for developers. This is a big step that makes things easier in a fast-changing world.

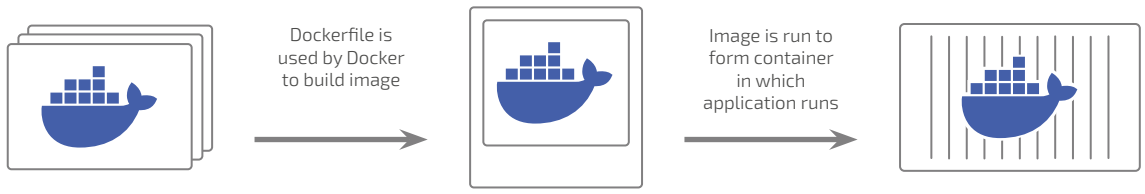
The importance of Docker in a device management strategy

Consider this scenario: a new operating system update flips the switch to a different partition, temporarily wiping out critical files stored on the system. Docker, with its containerized approach, avoids this challenge by keeping applications in a separate environment. There is no need to juggle system settings or worry about lost files during updates. Docker allows smooth transitions, ensuring that your applications remain intact and operational.

In addition, Docker containers provide a streamlined alternative to traditional application installation. They can be easily moved from one device to another, simplifying the deployment process. It's a practical solution that addresses the need for simplicity in managing diverse device fleets. »

How Docker works

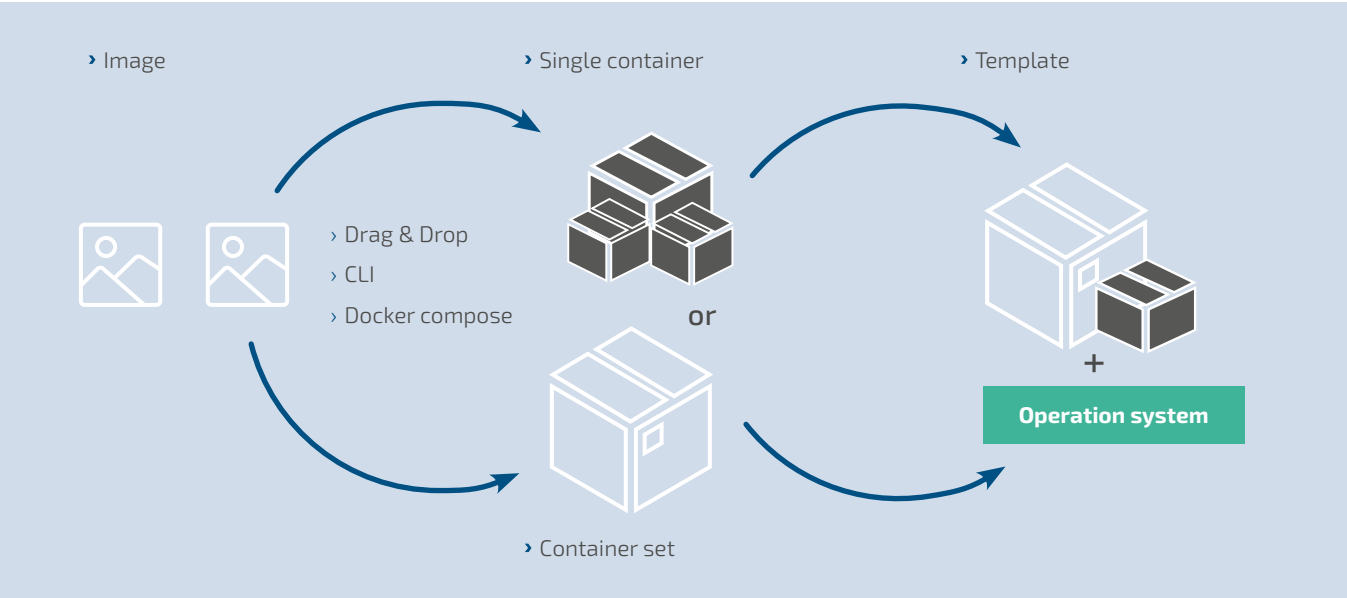
At the heart of Docker's functionality are images: packed files that serve as templates for creating applications (containers). These images, similar to blueprints, are managed in a registry. While public options like Docker Hub exist, the need for security and control led to the creation of a proprietary registry.



Dockerfile, image and container

Imagine this: you want to install an application on a device. You provide the Docker environment with the image link and a few startup parameters. The Docker environment, controlled through the cloud by an embedded agent in the operating system, seamlessly loads the image onto the device. Voila! The container is created, housing your application.

This process mirrors the simplicity of a smartphone experience. Your operating system is iOS 17, and applications are installed independently of the registry – think of it as your own personal AppStore. The registry is the gatekeeper, the container is the app, and everything works in a harmonious, separate way. »



Automated build process, from image to template via CLI and Docker Compose integration

Docker registry and automated image deployment

The easiest way to populate a Docker image to a registry is to use the drag-and-drop interface available through the web UI. This method provides a quick way to upload images directly to the registry. However, in the fast-paced world of development, relying solely on manual processes can lead to errors and inefficiencies. Imagine having to repeat the drag-and-drop routine every time you make a code change – it's not only time-consuming, it's a recipe for oversight and frustration.

That's where the Command Line Interface (CLI) comes in. Unlike the manual approach, the CLI allows developers to seamlessly integrate image deployment into their build scripts. This means that as part of the build process, the resulting Docker image can be automatically sent to the cloud without any manual intervention. By adding a simple line of code to the build script, developers can effortlessly initiate the deployment process. This not only saves time, but also eliminates the risk of forgetting critical steps in the deployment pipeline. The automated CLI approach ensures that any code change triggers the necessary actions to update the Docker registry, making the entire development workflow smoother and more reliable. By allowing developers to focus on coding rather than manual tasks, you're laying the foundation for agility and adaptability in the face of changing technology landscapes.

The Docker Compose advantage in containerized environments

Containers are convenient, but unfortunately, solutions often consist not of a single application, but of a series. This is where service-oriented architecture (SOA) comes in. This strategy involves breaking down systems into smaller, manageable services that work together to achieve common goals. Think of it as assembling disparate components to work together seamlessly.

Consider an IoT scenario: Connect a machine to NodeRed for data storage and create a user interface for operational purposes. Instead of handling each application independently, Docker Compose steps in to streamline the process. In this setup, you have three containers:

- **NodeRed container:** Manages the connection to the machine and data storage in the database.
- **Database container:** Stores the generated machine data.
- **UserUI container:** Provides an interface for users to analyse the data. »

For CTOs and IT managers navigating this evolving landscape, Docker Compose is the ally that simplifies the intricacies of container management.

While it is possible to configure these containers individually, Docker Compose simplifies orchestration. With Compose, you describe the entire setup in a single configuration file. It's a convenient solution – no need for scattered configurations; everything is neatly organized in one place.

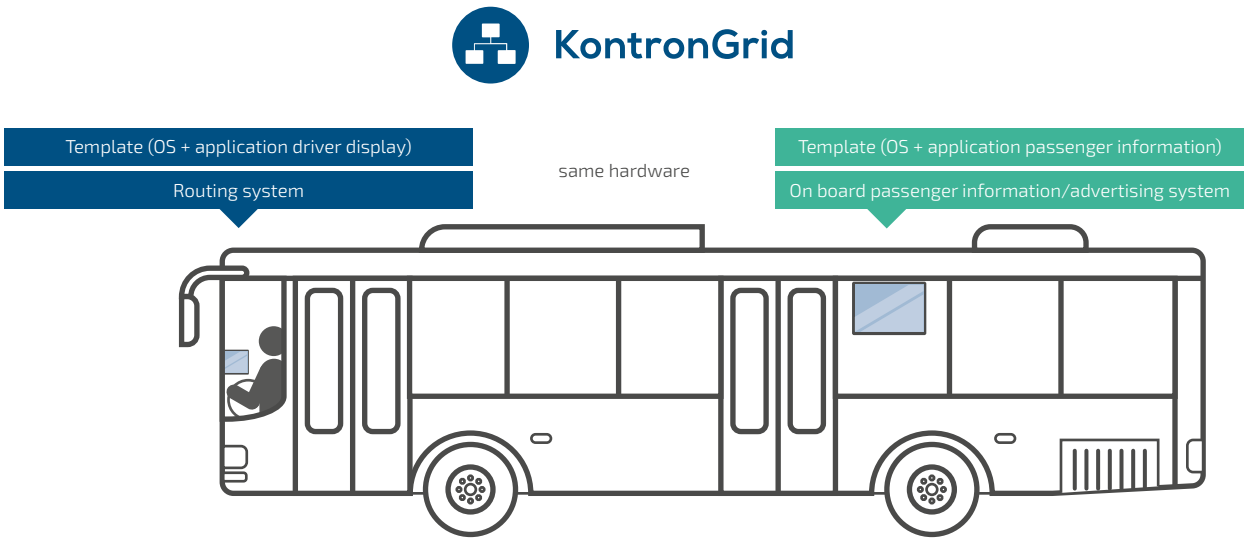
Docker Compose is a tool that simplifies container management without imposing complex deployment strategies. It's not about complicated roll-outs; it's about laying the foundation for efficient container management. For CTOs and IT managers navigating this evolving landscape, Docker Compose is the ally that simplifies the intricacies of container management.

Streamlining device management with templates

In the vast landscape of device management, the challenge grows as the number of devices increases. Imagine a fleet of buses with identical pieces of hardware, each serving a specific purpose – one for the directional sign at the front, another for displaying advertisements in the passenger compartment, and so on. Managing each device individually becomes impractical. This is where templates come in.

A **template** is a bundled configuration of an operating system and associated Docker containers or Compose specifications, neatly packaged and given a unique name. These templates become the building blocks for deploying specific configurations across devices.

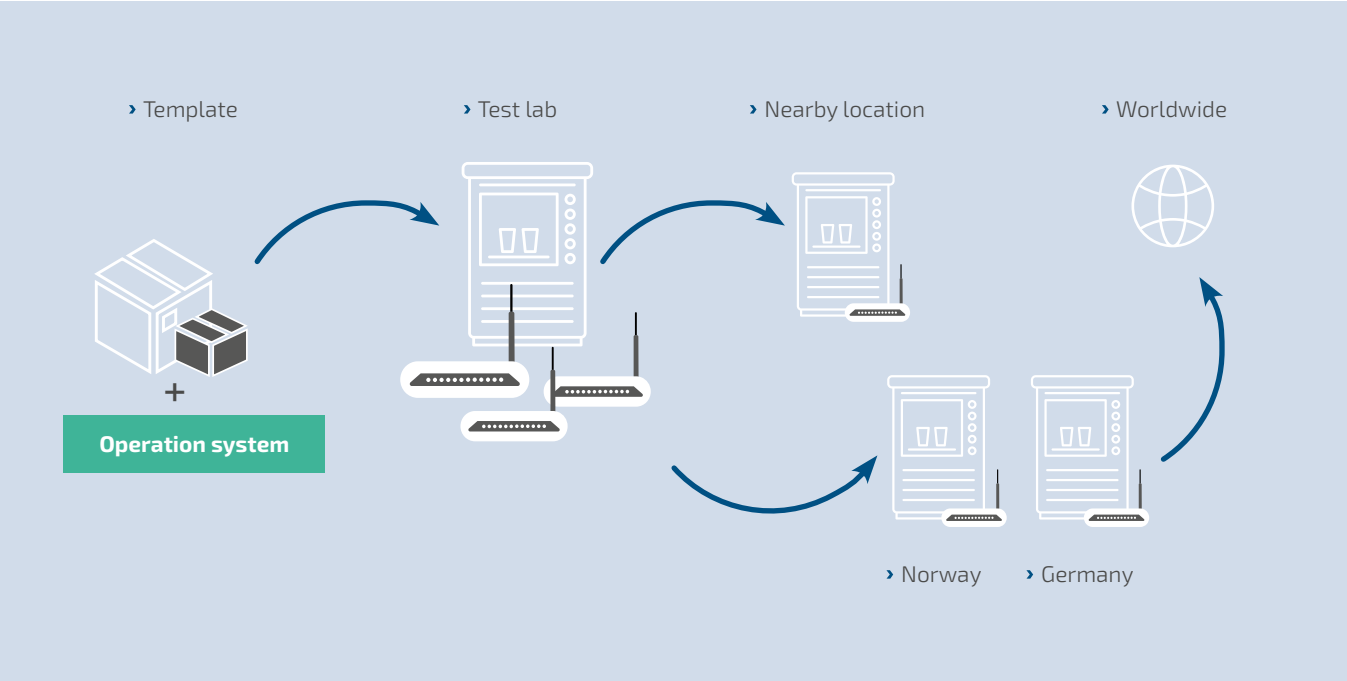
With modern device management, administrators can specify which template should be installed on a particular device, tailored to its unique use case. For example, one template is created for the routing system and another for the advertising system. The computer at the top of the bus gets the signage template, while the other computer gets the advertising template. The Kontron AIS KontronGrid ensures that all three devices are working with the intended operating system and that applications are running as Docker. »



Ideally, organizations can load designated devices with the operating system and applications run seamlessly as Docker containers. When hardware is later replaced, the transition to a new device is as simple as assigning the appropriate template, ready to fulfill its intended role.

But in the dynamic landscape of technology, change is inevitable. Updates, whether to the operating system or applications, are part of the evolution. The beauty lies in the simplicity of managing these updates through templates rather than on a device-by-device basis. For example, upgrading the OS version on a template from „1.0“ to „1.1“ triggers the system to propagate this change to all devices associated with that template.

This centralized approach allows administrators to update all devices at once or select a specific subset to update. This flexibility extends beyond the operating system to include Docker containers or Compose configurations. It's a streamlined process that unifies device management and ensures your fleet evolves effortlessly as technology advances. »



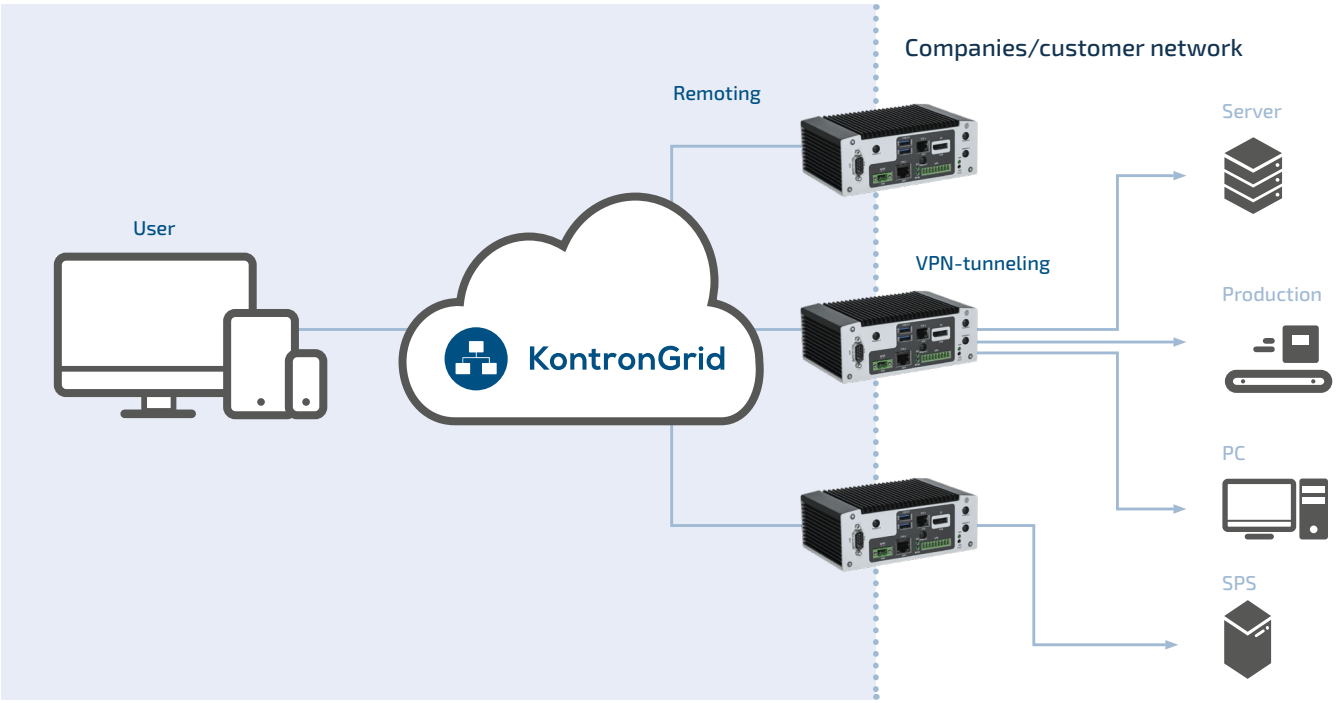
Automated update cycle: plan rollout scenarios strategically

Remote Support – Securely access devices in the field and increase service depth

Accessing IoT devices shouldn't be a maze of complexity, and with cloud remoting, simplicity is at the forefront. In this approach, devices autonomously tunnel to the cloud, creating a direct line for remote access without the need for VPN configurations. Organizations need a secure path, allowing users to effortlessly open a browser-based command line where the cloud handles the security settings, making device maintenance and troubleshooting a simple task. This seamless connection to IoT devices via the cloud transforms accessibility and troubleshooting, simplifying the entire process for efficient device management.

Improve Device Connectivity with VPN

Virtual Private Network (VPN) technology transforms device connectivity by creating secure virtual networks through encrypted tunnels. While commonly associated with remote access, our device management system uses VPNs for more than just remote connectivity. VPNs serve as a conduit for additional device connections, such as seamlessly integrating a device with an IoT gateway. This means that a programmer can interact with the machine as if it were physically connected, running, updating, »



Quickly and efficiently access machines remotely for service with KontronGrid

and analyzing software securely over the VPN network. The key is that the data travels securely over the Internet, ensuring confidentiality and facilitating remote interactions without compromising security. VPNs become the silent enablers, navigating the complexities of the Internet to create a secure bridge between devices and programmers. This makes it possible for multiple service technicians to work together remotely on a single machine from anywhere in the world.

Securing IoT devices with hardened operating systems

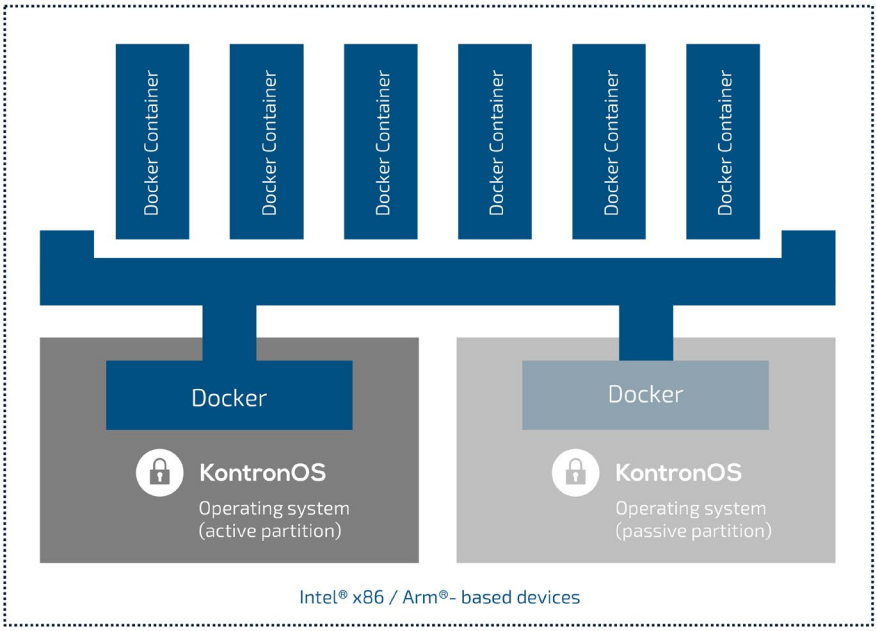
Hardening IoT devices and the platform they run on is necessary to prevent unauthorized devices from accessing a network and acting as an attack entry point. Many IoT devices lack built-in security, and the biggest security risk with IoT devices is that they are often designed and built without security as a priority or even a consideration.[2] Hardening IoT devices can help prevent security issues, and using automated responses can help minimize the amount of time exposed.

The time to act is now

As the number of connected devices continues to grow and the threat environment becomes more dynamic, organizations must take proactive measures to ensure the security and efficiency of their operations. In this evolving context, staying ahead of the curve in device management and adhering to the latest security standards is not only smart, but necessary to protect both your business and your customers.

For those managing existing fleets, incorporating effective device management becomes a critical aspect of adapting to the evolving regulatory environment. The challenge is to adapt a secure operating system, such as KontronOS, to the diverse hardware within the fleet. At the same time, the required agent to facilitate communication with the cloud, Docker environment and CLI must be seamlessly integrated. »

[2] https://www.techtarget.com/searchsecurity/tip/Use-IoT-hardening-to-secure-vulnerable-connected-devices



KontronOS is a hardened Linux-based operating system for the reliable operation of Docker Containers on edge devices, that protects IoT solutions in critical environments from compromise, external access and uncontrolled updates, so that containerized and native applications can run securely and without interruption.

When deploying new hardware, particularly the streamlined Kontron hardware, the onboarding process is significantly easier. It comes pre-installed with all the necessary software packages, making onboarding a simple and efficient process.

A core component of the KontronGrid fleet management solution is the hardened Yocto Linux-based KontronOS operating system, which comes preinstalled for enhanced security and optimal operation of Docker containers and can be used flexibly for Intel® x86 and Arm based devices.

Future-proofing your fleet

Managing devices can be challenging, with tasks such as operating system management, identifying security vulnerabilities, and ensuring connectivity. Our goal is to simplify this process for you. KontronGrid is the complete fleet management solution for edge devices that has been specially developed to make management easy and simplify the rollout of docker containers.

This complete hardware and software solution lays the foundation for the development of your custom IoT solutions to automate tasks such as securely carrying out fleet updates at operating system and application level with just a few clicks. It facilitates the seamless monitoring of devices in the field and provides fast remote support to minimize downtimes. »

How KontronGrid supports tool grinding machine manufacturer VOLLMER Maschinenfabrik

As a technology leader for grinding, eroding and processing machines for rotary tools and circular saws in the woodworking, metalworking and metal band sawing industries, we wanted to create a clear platform for our customers to manage and update their machines and IoT gateways themselves.

To achieve this goal, we integrated KontronGrid with the KontronOS secure operating system and used Docker to create and configure Docker containers. We used KontronGrid to efficiently manage and deploy Docker images, enabling easy device management and software updates. It allows us to respond quickly to critical security vulnerabilities and provide necessary security updates that can be easily and quickly installed by the customer. In addition, the existing rights management offers sufficient flexibility to manage the rights and access of developers, commissioning, service and customers and to adapt them very quickly if necessary.

An important success factor for the switch from the old management platform to KontronGrid was the very good support and cooperation with Kontron AIS, which enabled us to adapt our internal processes and maintain our existing deployment by using Docker container technology.

Overall, KontronGrid has helped us to improve the efficiency of our production processes.

Patrick Bauer, Design & Development, VOLLMER Werke Maschinenfabrik GmbH

Combined device and Docker Management

Our KontronGrid solution is the ideal solution for seamless device and Docker management. It's a powerful combination that simplifies operations and increases efficiency. But it's important to note that it can stand alone, especially in a Docker environment. This versatility ensures that you have the freedom to choose the setup that best suits your unique needs.

Securing devices with KontronOS

Security is at the core of everything we do. Our devices are fortified with the hardened KontronOS operating system, a robust shield against the ever-evolving threat landscape. With security as a top priority, our customers can rest assured that their devices are protected against potential vulnerabilities.

An expert partner

When it comes to device management, we get down to the details at Kontron. We diligently examine and maintain the operating system, leaving nothing to chance in our search for security vulnerabilities. »

Our commitment to keeping the OS up to date ensures that your devices always perform at their best. By relieving you of the responsibility of OS maintenance, we allow you to focus on what really matters – your applications. Our team partners with clients to establish and optimize these important connections.

Flexible product portfolio

We understand that no two organizations are alike. That's why our product portfolio is designed to be flexible and adaptable. Whether you're looking for an out-of-the-box standard IoT stack, a modified stack tailored to your specific needs, or a fully customized solution, we have you covered. Our range of products ensures that you can find the perfect fit for your device management needs, if you wish.

Standard IoT stack	Modified standard	Fully customized
  i.MX8M Mini (Arm®) KBox A-151-EKL	  Modified hardware: Arm®-based to x86-based	   Custom hardware
KontronOS	KontronOS Windows IoT	Customized OS
KontronGrid	KontronGrid	KontronGrid
Licenses	Licenses + project costs	Licenses + project costs
get started right away	get started in weeks	get started in months

User management allows flexible adding and deleting of users, so management can be done internally or assigned to an external partner, or even define which tasks can be done by whom. We provide you with an intuitive tool that combines all the tasks in one place, so you can manage them the way you want.

As part of our commitment to providing comprehensive solutions, we offer an IoT bundle that includes hardware, software, and connectivity. This all-inclusive package simplifies the device management process, making it more accessible and efficient for our customers. »

From manual to mandatory: Staying ahead in the IoT age

Edge device management solutions are not yet mandatory, but make no mistake, the winds of change are blowing. The rapid expansion of the IoT and the emergence of new security standards are shaping a landscape where device management will become an essential component of success. The status quo is changing, and it is not a question of if, but when you will need to adapt, because in the near future, there will be no way around device management solutions. So embrace the change, stay ahead of the curve, and future-proof your fleet. We not only empower OT and IT integration, but also automate the management of thousands of device connections. Our solution works seamlessly on a global scale and provides a bird's eye view of your device network. With our ISO 27001-certified development process, you can meet the highest security and compliance standards and benefit from easy access to IEC 62443 certifications to secure your projects at the highest level. This level of automation and security enables organizations to stay ahead in an increasingly connected world.

Are you ready to future-proof your fleet with KontronGrid device management?
Get started now!

Download our
FREE KontronGrid factsheet

Book a guided demo session
with one of our sales experts

About Kontron AIS GmbH

Kontron AIS GmbH sets the benchmark in industrial software – for more than 30 years and with an experienced team of over 250 employees. The proven software products and customized digitalization solutions enable machine and equipment builders as well as factory operators to break new ground in automation and secure long-term competitive advantages. Together with its customers, Kontron AIS implements worldwide cross-industry, intelligent digitalization strategies and solutions for the smart manufacturing of tomorrow.

As a subsidiary of the Kontron AG, Kontron AIS offers integrated, end-to-end IoT concepts consisting of hardware and software as well as worldwide project management, service, and support thanks to a global network.

Further information: **www.kontron-ais.com**

Company contact
Kontron AIS GmbH | Otto-Mohr-Str. 6 | 01237 Dresden | +49 (0) 351 2166 0 | sales@kontron-ais.com