BOSCH
Invented for life

Frequently asked questions

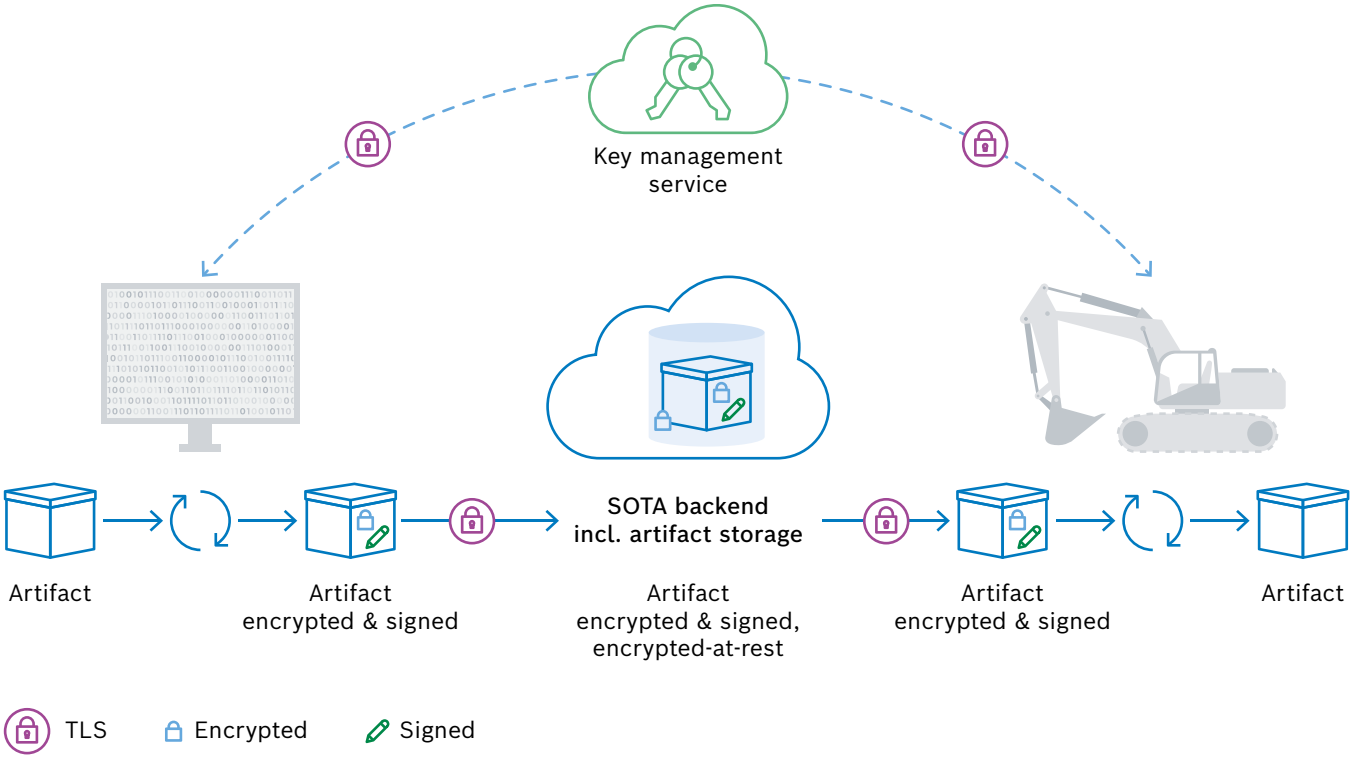
Software updates over the air (SOTA)

Centrally controlled remote software updates are a common tool to quickly resolve software issues, push new features, and thus extend the product life cycle. Digging deeper into the topic often leads to a lot of additional questions. With the experience gained from many SOTA projects, we have compiled the most frequently asked questions and provided answers by our experts to help you overcome the first hurdles when getting acquainted with software updates over the air.

Contents

1. How is SOTA handled in projects with customers? Which key aspects do you need to consider?

Security is a multifaceted topic in the IoT, which is why companies must adopt a holistic approach to ensure a secure software rollout from start to finish, from edge to cloud. By drawing on key principles, companies are able to cope with this complexity, reach a high degree of security, and minimize the risk of security threats that can result in breaches and data leaks.



There are three key points to consider for companies when preparing for SOTA updates:

1. Security during the artifact life cycle, from development through to deployment. This includes encryption to guarantee communication confidentiality, a digital signature to verify the integrity of the artifacts the devices receive, and transport layer security (TLS) to ensure in-transit security.

2. Secure communication and authentication between devices and the SOTA back end. The technical implementation includes a public key infrastructure and key management system, TLS for secure communication, and a trusted server with certificate pinning and device authentication as well as communication with a content delivery network (CDN).

3. Access management to protect the backend against unauthorized access. A fine-grain permission scheme with role-based access control is a key enabler.

Expert insights:
Over-the-air updates

How do companies ensure a secure software rollout from start to finish? Learn more about the three key points to keep an eye on.

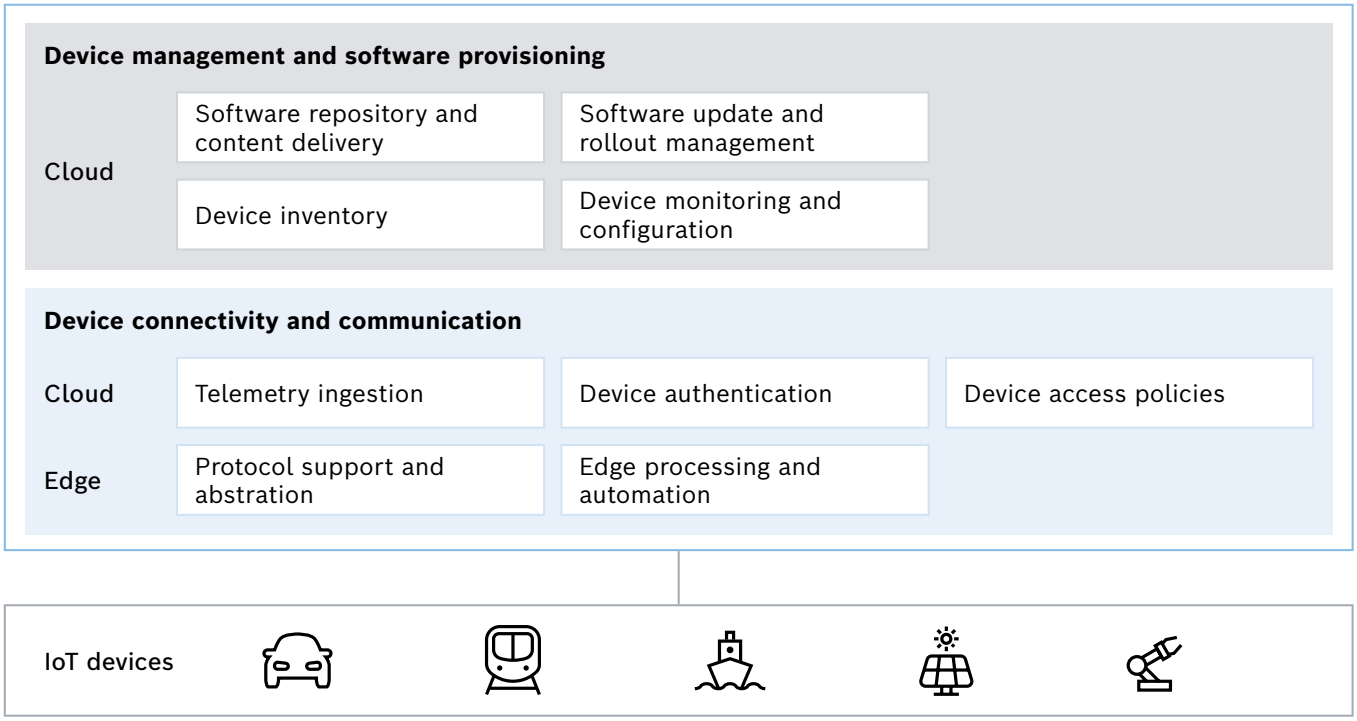
Download now

2. Does your SOTA project require device management functionalities as a foundation?

With the growing number of connected devices and the more widespread use of edge computing components, it is crucial to ensure that the software running on these devices is up to date. This includes adding new product features and rolling out necessary security updates as well. These are major functional blocks needed to enable updating software/firmware over the air:

Device connectivity and communication: with a common protocol abstraction layer at the edge, edge processing and automation in the cloud and on-premise, telemetry data ingestion, device authentication, and device access policies.

Device management and software provisioning: including a device inventory (with all the necessary parameters), device monitoring and configuration, a software repository and content delivery (CDN), and software update and rollout management.



From edge to cloud: principal building blocks for device connectivity in the IoT

3. What do you need to consider before you start your SOTA initiative?

Managing software updates of thousands of devices can be quite a challenge. Finding the right means to handle software rollout processes in a reliable and secure way can be a difficult decision. You can either build your own solution, use existing open source software, or rely on a managed service. To guide you through the requirements of software/firmware updates over the air (SOTA/FOTA) solutions, there are five things you need to consider:

- Team, time, costs: for example, does your company have the know-how to develop or implement over-the-air (OTA) functionalities?
- Business case: is your solution scalable in line with your business demands?
- Device connectivity: do you have a solution to provision your devices?
- Security: are you aware of state-of-the-art security mechanisms such as certificate-based authentication?
- Features: software artifact management, campaign management, user management, etc.

Checklist:
Five things to consider before realizing a SOTA use case

With this checklist, we want to guide you through the requirements of SOTA solutions and find the solution that best suits your needs.

Download now

4. What are typical campaign sizes in big SOTA infrastructure implementations?

It depends on what is defined as a device. We have customers with up to 8 million assets updated in a single campaign, each asset in turn comprising up to 100 control units (CCU, ECU, etc.). More widespread update campaigns consist of up to 600,000 assets in the field globally. Those campaigns can be scheduled by region and other parameters (asset type, manufacturer's date, serial number, etc.).

5. What are typical challenges, update frequencies, update package sizes, campaign sizes ...?

Typical challenges of SOTA use cases lie in the variety of devices, software artifacts, and the scope of the rollout process.

Different types of devices

- Gateways, car-ECU, PLCs, etc.
- Large variety of software environments, e.g. OS
- Management agent on the device required

Different types of software artifacts

- Software artifacts may come from different suppliers
- Ensure software artifacts work with corresponding CPU architecture and OS
- Management dependencies between software artifacts
- Management of system capabilities

Worldwide rollouts

- Scalability to support a fleet of millions of devices
- Campaign management ensures delivery of software updates under certain conditions
- Report about successful/ unsuccessfu updates
- Rollback in case of malfunction

- The wealth of different types of devices with their different requirements can be met with a management agent on the device.
- Different types of software artifacts from different vendors require the compiling of a manifest containing all dependencies for the target device for each artifact.
- Worldwide rollouts pose a challenge for the global availability and scalability of services.
- Reducing the update package size with delta updates enhances the efficiency of updates.
- The frequency of the updates depends on type of device, type of software updates, legal boundaries, etc.
- Different device management solutions for different types of devices should be avoided.

6. What are the biggest pain points that companies address with a SOTA initiative?

- Software is no longer static, and this also holds true for IoT devices, smartphone apps, and desktop computers.
- There are various reasons for performing software updates such as operating system updates, security-related improvements, bug fixes, and deployment of new features.
- Various types of assets, such as cars, industrial machinery, off-road equipment, can additionally benefit from software updates by reducing expensive recalls and minimizing the sending of service personnel to remote locations to carry out manual software updates.

7. Is SOTA offered as a standard solution today? Which cases warrant an individual solution?

It depends ...

Do you bring your own CCU to be connected? Is it already connected via Bosch IoT Suite? Or are you already using Bosch's iTrams? We can implement your project based on standard off-the-shelf components.

With Bosch IoT Edge as the basis of our SOTA solution, software can be updated on a wide range of devices, from microcontrollers to powerful hardware platforms. These solutions are to a large extent standard, needing only individualization efforts.

8. What happens if the assets to be updated are not online?

Devices that are off-line will remain in the queue of the software update campaign until they are brought back online to carry out the software update.

9. What happens if the update fails?

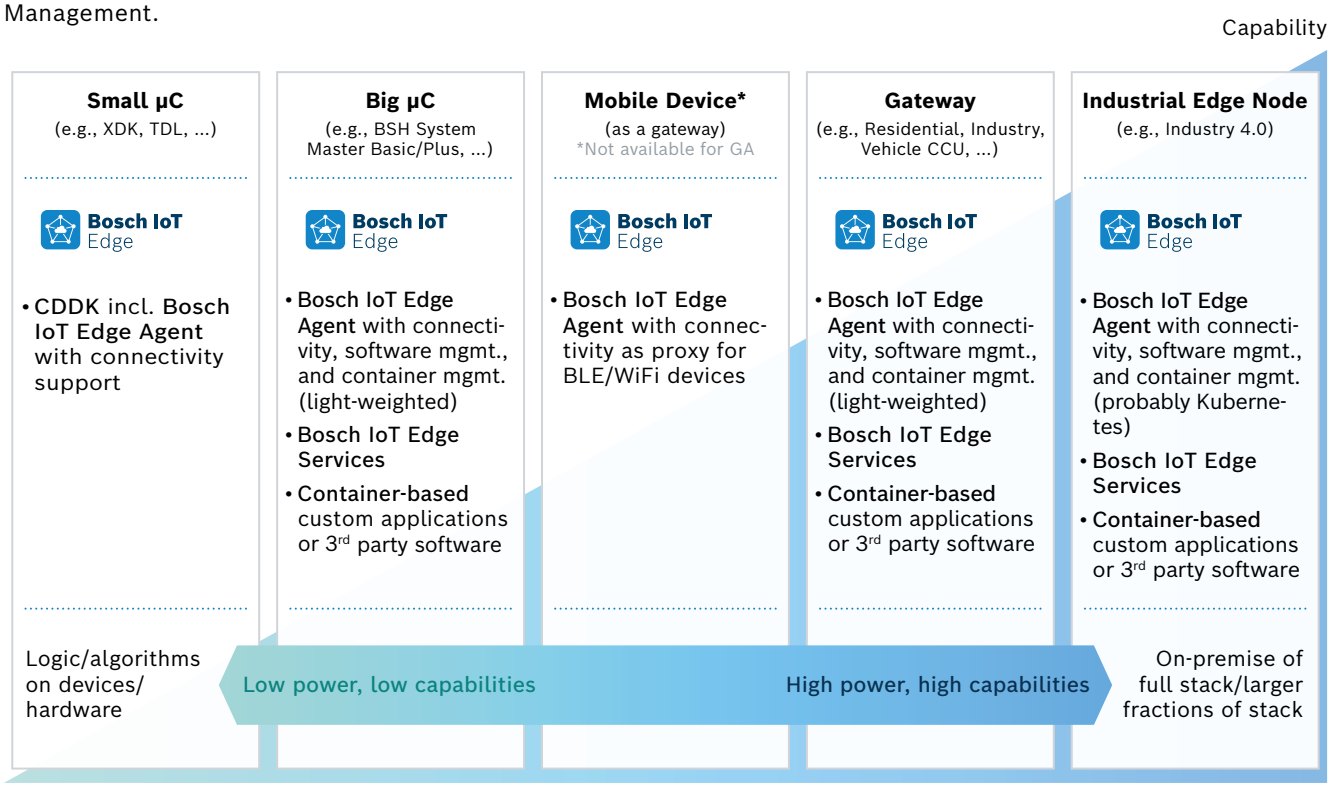
There could be several reasons why the update on the device fails. It might be specifically related to device configuration, for example, insufficient memory or firmware corruption during transfer. These are, however, individual cases that affect only a few devices. In such an event, the device firmware should be rolled back to the latest working firmware.

Another reason for rollback to a previous software version might be a bug in the software that was updated, which could potentially affect all connected devices. The management system retains a history of performed software updates in order to launch another rollout campaign to distribute the previous working version.

In case of a connectivity interruption during the software update process of a device, the update is logged as faulty and restarted at the next suitable update campaign.

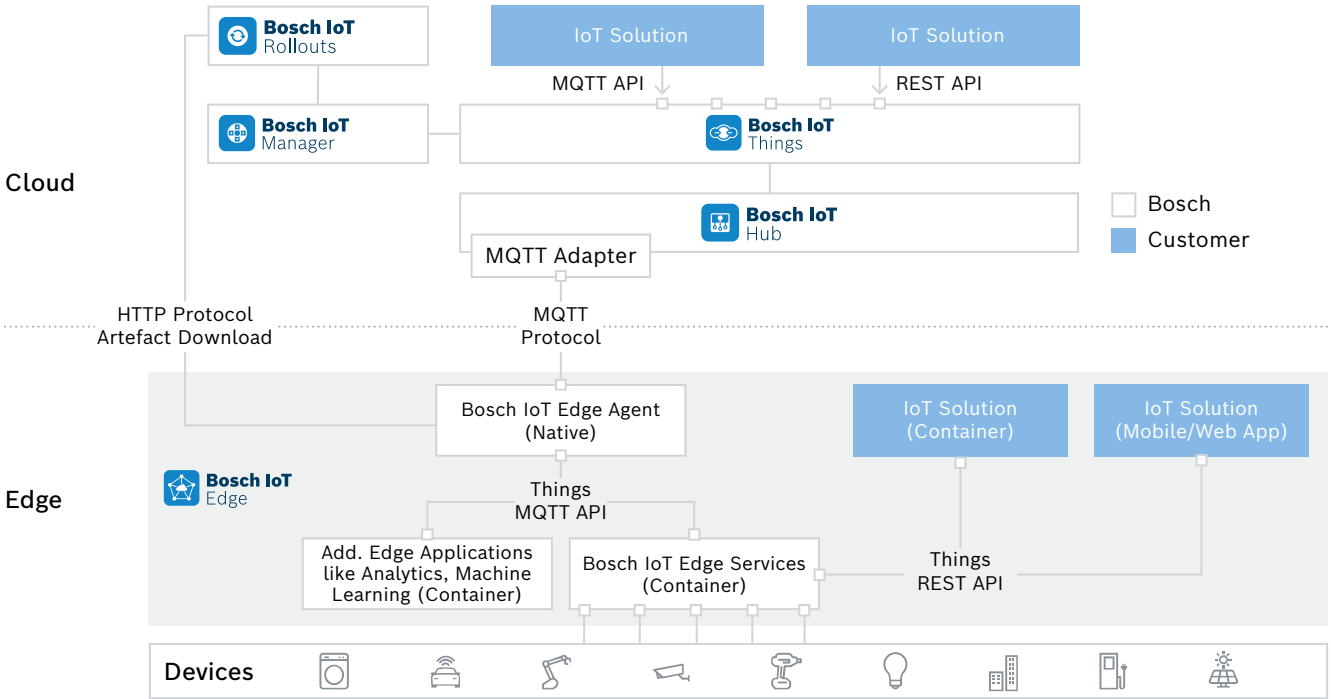
10. What requirements do the target devices / ECUs have to fulfill?

The Bosch IoT Edge Agent has been designed to run on different types of devices: by cross-compiling it for the corresponding target device architecture (CPU/OS), it can be used for resource-constrained microcontrollers and very powerful edge nodes as well. The Bosch IoT Edge Agent is free of charge for customers of Bosch IoT Device Management.



11. How are IoT edge agents used to update devices in the field?

The use of edge agents may vary on the type of device and the exact use case it is intended for. In the simplest case, for example, a microcontroller, the edge agent connects via MQTT to a device management backend and/or cloud service in order to receive/deploy software/firmware updates. In case of more complex devices and software stacks, the edge agent can also orchestrate the deployment and management of containers.



12. Is SOTA a push or pull process from the edge point of view?

While the process itself is triggered via the software management service (this could be either Bosch IoT Rollouts or Bosch IoT Remote Manager), the edge device receives information on the destination from which the corresponding software artifact can be downloaded. This means that the edge device “pulls” the new software, but the trigger to do so is “pushed”.

Even if an edge device proactively asks if a new software version is available, the trigger to perform an update is pushed to the device. This helps to prevent updates being pulled by unauthorized devices or those that are not part of a scheduled update campaign.

The whole process is accomplished by applying the security principles described in answer 1 to ensure a secure software rollout from start to finish, from edge to cloud.

13. What mechanism is provided to prevent software from being deployed to noncompatible hardware?

The device management platform knows all the relevant information (e.g. CPU, OS version, deployed applications, etc.) of all connected devices. Additionally, software artifacts (e.g. firmware versions) should come with a manifest that describes certain aspects such as compatibility with CPU types and operating systems as well as dependencies to other software components. The operator of a software update campaign can only perform software updates where the software artifact matches the criteria defined in the manifest.

Europe

Bosch Global Software Technologies
GmbHLöwentorstr. 72-76, 70376 Stuttgart,
Germany
www.bosch-softwaretechnologies.com