BOSCH
Invented for life

Industrial IoT: how companies increase transparency and optimize operational efficiency

Benefits of remote device management for high-value assets

White paper | October 2021

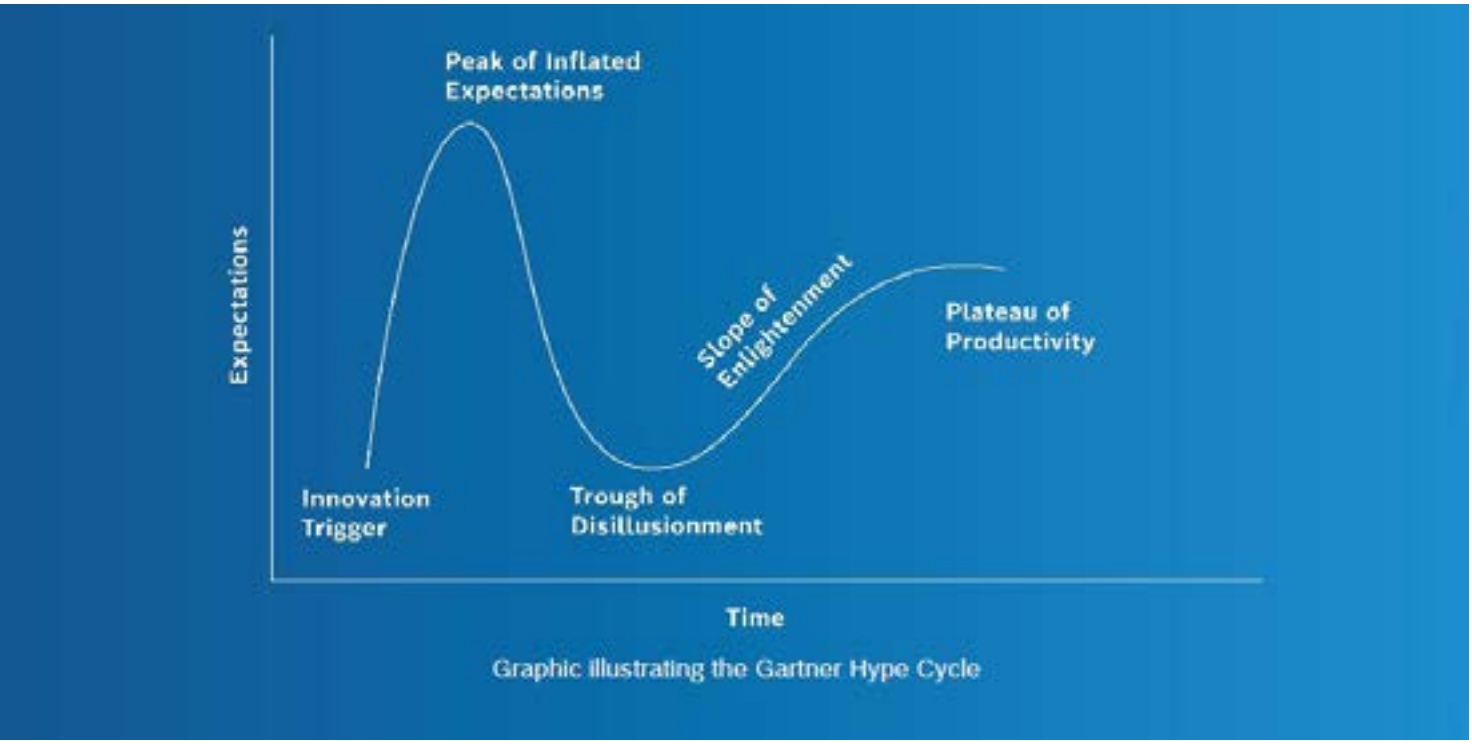
Content

1. IoT and connectivity: from hype to productive usage

Over the past few years, we have seen a huge hype surrounding topics such as digitization, the Internet of Things (IoT), and device connectivity – whether it is the automotive industry, the manufacturing sector, or consumer goods, companies have invested heavily in new technologies and new skills to advance their digital transformation.

Many of these initiatives have been successfully implemented from a technological standpoint, providing companies with useful insights into their operational processes and business models. However, only a few use cases so far have been able to provide sustainable business value and a positive return on investment (ROI) to the companies driving these projects.

Looking at technology trends in the past, it is evident that this is not a problem unique to the IoT; rather, it is indicative of the typical maturity cycle that every major advancement in technology goes through. The Gartner Hype Cycle illustrates this concept perfectly: it starts with a growing hype, which leads to inflated expectations. A phase of disillusionment follows once it becomes apparent that the new technology might not make good on all its promises. Over time, however, a more realistic view sets in as more companies put the technology to productive use.



Graphic illustrating the Gartner Hype Cycle

In our experience, the remote management and software update management of high-value industrial assets is an IoT use case that is approaching the stage of productivity and profitability. These assets are characterized by long-term investments, complex engineering, high capital investment (CAPEX), and a long service and maintenance life cycle.

Some examples of these assets are:

Industrial installations and facilities

Large engines for vessels and commercial vehicles

Power plants and turbines

Large drives, compressors, and gears

Definition: remote management and software update management

The ability to remotely manage heterogeneous devices is the foundation of any IoT solution. It enables companies to remotely access globally distributed devices and gain information on e.g. their status or usage. Additionally, they are able to deploy software updates over the air, which are convenient for their customers. This allows manufacturers to address security issues or provide new features.

What is the best way for industrial companies to go about implementing IoT solutions? In the following chapters, we will draw upon the use case of managing and updating devices to illustrate key considerations. To this end, we take an in-depth look at both the technological perspective as well as the business as a whole.

2. Strategic considerations: business impact and return on investment

Defining a clear strategy is important before starting any IoT project. For an original equipment manufacturer (OEM) of high-value industrial assets, it is essential to not just define an approach that meets the technical challenges of an IoT solution but also consider the business perspective and use as many synergies as possible for a faster amortization and a positive return on investment (ROI). At the risk of sounding obvious, focusing on a functioning business plan and a well-thought-out business model is fundamental to the success of digitization activities. All relevant stakeholders – both within and outside the company – should be involved in developing and realizing the strategy.

2.1 Business benefits of remote management and software update management

Implementing an IoT solution is a complex endeavor – software development, the time and effort needed to connect the devices, and the cost of ownership of the solution are just some of the aspects to consider. Companies should therefore invest wisely and set a realistic ROI. Going back to the Gartner Hype Cycle, companies should not let the hype around a new technology cloud their judgment as this often leads to solutions that create no real business value.
A positive ROI is about compensating for planned investments – either through cost savings or by creating new revenue streams. But what are the benefits of managing and updating devices remotely? Since generating new revenue potential is only indirectly possible and depends on several factors, companies should focus on the cost savings potential initially. With regard to this use case, the following effects can contribute to the savings potential:

- **Reduce downtime**, which lowers work and travel expenses and prevents long-term damage to the system, contractual penalties, and opportunity costs.
- **Reduce software update and configuration efforts** by switching from a manual process to an automated system.
- **Reduce average asset connection efforts** for engines by using standard tools and methods.
- **Reduce individual software operation and maintenance costs** by using managed cloud services.

In the long run, companies can of course also consider creating new revenue streams and business models e.g. via pay-per-use service contracts or additional device features.

2.2 Taking a closer look: reducing downtime and costs

To illustrate the savings potential for industrial companies, let us consider the impact of reducing downtime. There are many cost drivers in play in this context. Costs for travel and spare parts may accrue in addition to labor costs for carrying out maintenance

Time is of the essence: the maintenance and support division of the manufacturer must react quickly in order to reduce financial damage for the customer and itself. In a best-case scenario, the maintenance staff is already on-site and able to respond quickly. In a worst-case scenario, the asset is located far away or even offshore with no maintenance staff on hand. This leads to hours, if not days, where the asset is not in operation. Depending on the agreed service level between the customer and the asset manufacturer/maintenance provider, downtime costs are either shared between the two parties or carried by one side alone.
A solution for remote device management enables maintenance providers to monitor the status of devices and change their configuration remotely. This helps maintenance providers save time when it comes to finding the fault and solving the issue. In the end, this leads to significantly lower downtime costs.

Business impacts of downtime
Unplanned downtime can significantly affect direct and indirect costs as well as lead to contractual penalties. The following examples illustrate the potential impact of reducing downtime on key performance indicators (KPIs):

Example 1: Bosch plant, Germany – connecting and analyzing data from industrial assets

Annual cost savings of 260,000 euros due to fewer line stoppages (from four malfunctions to zero per year).

Example 2: Spindle monitoring customer project – data collection and alert system

Shorter periods of downtime resulted in savings of 500 euros per machine per month.

Undoubtedly, the investment in an IoT solution that covers all relevant security, scaling, and technical aspects can easily reach six-digit or seven-digit figures. Therefore, it is crucial to start with a strong business plan. A realistic consideration of all relevant costs (total cost of ownership) and the possible benefits is the first step to success.

We see a huge savings potential in reducing downtime and automating device management processes – savings per year can easily reach between 150,000 euros and one million euros. This savings potential can usually be realized a year after implementation (short-term potential) and increase further with an increase in the number of devices.

Follow this link to visit our training: IoT & Platform Business Model Innovation

Automating software updates and device management processes pays off even more in the long run. Having an IoT solution in place allows companies to collect data from their devices, which in turn can be used for product improvements or even data-based business models.

3. IoT deployment challenges for high-value industrial assets

High-value assets are long-term investments for companies. Rather than replacing their equipment periodically, companies mostly rely on long maintenance cycles to keep them operational. Some even use their assets for over 50 years and, as a result, deal with a very heterogeneous device landscape. Consequently, this leads to various technical challenges when implementing an IoT solution.

3.1 Connecting a heterogeneous and distributed device landscape

Be it the machines in a manufacturing plant or the fleet of vessels and commercial vehicles of a logistics provider, gathering data and managing the devices in the field poses a major challenge. Most of the legacy assets in use today are not able to communicate with modern cloud applications. This leads to expensive retrofit projects and varying approaches to connectivity. Deciding on suitable communication protocols and connectivity technologies is a skill in itself and matures with experience in practice. Moreover, industrial assets are very complex in nature, making the traditional connectivity approach of most IoT platforms redundant and a one-size-fits-all approach rarely feasible.

The global distribution of devices compounds this complexity. It is not just about devices located in different countries and regions but also in areas, for instance, with weak mobile connectivity, offshore, off-road, or in rural areas.

3.2 Keeping assets operational and up to date

Considering the global distribution of devices and the many legacy devices in the field, it is hard for companies to stay on top of the state of their assets. This can have far-reaching consequences, as exemplified by the maintenance process. Ideally, companies want to become aware of a problem as early as possible and intervene in due course to prevent downtime. A lack of insight makes a quick turnaround difficult – locating a fault and fixing it after the problem has already occurred takes considerable time and effort. It also means the asset is not in use until the issue is resolved.

Click here to find out more about edge computing

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. Manually updating software can be an extremely costly and complex process: for example, take a security issue with the software embedded in the engines of marine vessels. An issue such as this limits functionality or even leads to malfunctions. Sending service technicians to vessels strewn across the world is a very inefficient approach. Addressing this challenge therefore calls for a fast and reliable update process, ideally supported by technology that reduces manual efforts to a minimum.

3.3 Commissioning and managing devices in the field

Keeping software up to date during the entire product life cycle is not the only challenge; the initial commissioning of devices and systems in the field can also prove to be difficult. As with rolling out software updates, the main challenge here arises from devices that are hard to access across the world, in remote locations, or offshore.

Manually commissioning an engine, for example, calls for technical experts to be on-site. If there is no technician on hand, the company then has to send someone, making it a time-consuming and expensive exercise. And that might not be all – political restrictions or world events outside of a company's control can make it harder or even prevent technicians from accessing a device.

However, an automated and digital solution enables companies to commission and manage their devices with far less hassle. They also benefit from a huge cost savings potential through reduced on-site assignments of service technicians.

4. A technological approach to IoT deployments for high-value industrial assets

An IoT solution for connecting high-value assets needs to be both easy to implement and easy to use. In addition, it must cover all relevant technological and security requirements. As mentioned before, a one-size-fits-all approach by using a single Software-as-a-Service (SaaS) application is rarely feasible. Analysts from IoT Analytics found that it takes a considerable amount of time to connect even the first device to an IoT platform – on average, it takes about 113 days.

“Connecting assets is a lengthy process. On average, connecting the first asset takes ~ 4 months (113 man-days)”

Industry 4.0 & Smart Manufacturing Adoption Report 2020, IoT Analytics

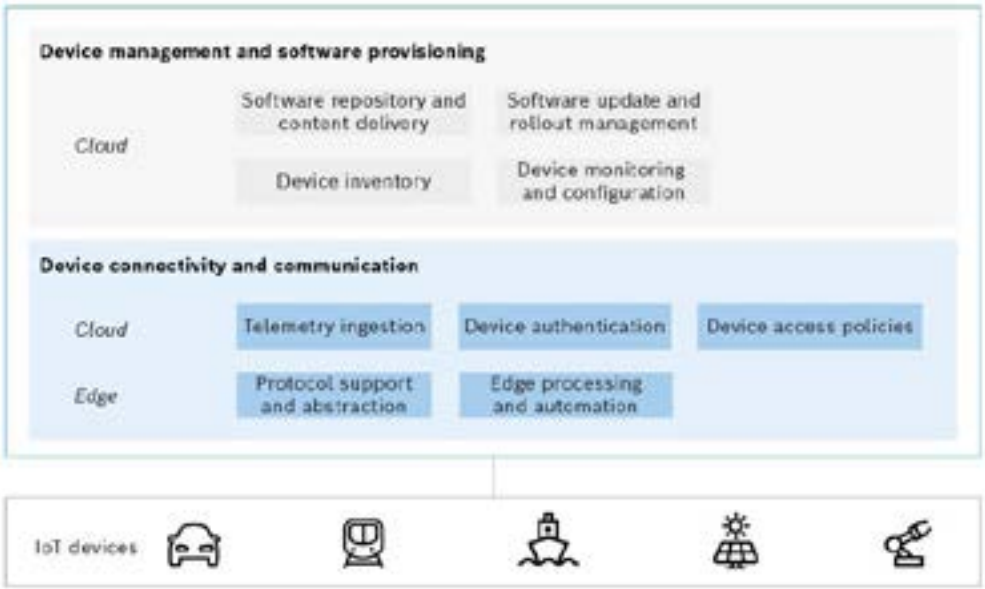
In order to tackle the high complexity of the abovementioned challenges with reasonable effort, a solution architecture is required that is not only flexible but also uses as many standard components as possible.

4.1 Major function blocks: device connectivity and communication

As regards the challenge of connecting a heterogeneous device landscape (see chapter 3.1), it is important that the system is able to understand the language of the devices or gateways. In technical terms, the solution must support the right communication protocols or at least have the right adapters to do so. The protocols used vary from industry to industry, mostly due to domain-specific technical challenges. Companies should choose an efficient connectivity method and flexible connectivity tools right from the start. That way, they are prepared for the future and can implement use cases that are industry agnostic.

Currently, most IoT platforms provide a tool for device connectivity: a so-called hub, which represents the interface between the devices and the platform. The more relevant protocol adapters the system offers, the easier it is to connect devices to the solution.

Furthermore, it is important that granting access rights and the entire device authentication process are automated as far as possible – especially if several thousand devices need to be connected.



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

Protocol support and abstraction

In order to manage the variety of protocols, a common protocol abstraction layer at the edge is necessary. In many cases, the abstraction includes a data transformation into a unified format (e.g. JSON). A unified interface reduces the complexity for developers and applications by providing a common way to interact with the devices.

Similar to the variety that exists at the local level, an IoT solution also needs to handle multiple device-to-cloud communication protocols. Depending on the use case, selecting the appropriate protocol will have an impact on the costs and capabilities of the solution.

Edge processing and automation

Many industrial applications do not handle latency as well as IoT applications in other domains. Particularly, when the task is critical and it has to be ensured that there are no delayed responses due to poor connection. This is why edge software may not rely on the cloud alone. It has to process telemetry data and events sent from devices with an automation engine that executes predefined monitoring and control rules on its own. An operator or developer should be able to write these rules and deploy them remotely to edge devices. As an added bonus, processing at the edge slashes the costs of data traffic.

Telemetry ingestion

After receiving telemetry data from the devices and processing it at the edge, it needs to be ingested into the cloud. For that to happen, an industrial IoT solution needs to be able to process the message with its specific protocol adapter, and then send it to the addressed application or service via its internal messaging network. The messaging network should distinguish between different types of delivery according to the type of message or the recipient. Delivery has to be guaranteed for the operator or application to respond swiftly to critical events or alerts sent from devices. Request or response schemes can offer that assurance by providing a receipt to confirm delivery, without which the message is classed as undelivered. One-way schemes can handle less critical messages, for example, frequently taken sensor readings that do not have not be re-sent when one message goes astray.

Device authentication

Security breaches and cyberattacks pose a great threat to industrial IoT applications, so protecting the platform's vulnerabilities is a top priority. This requires many safeguards, one being the ability to authenticate devices. It is important that applications can rely on the fact that the message stems from nowhere else but the device indicated in its source address. This is why the IoT platform needs to distinguish between an identity associated with the authentication credentials and an identity to act as. A device may present an authentication identity as part of its credentials during the authentication process, which is then resolved to a device identity on successful verification of the credentials. The IoT platform should also support different types of authentication, e.g. certificate-based authentication and username or password based authentication on a per-device level.

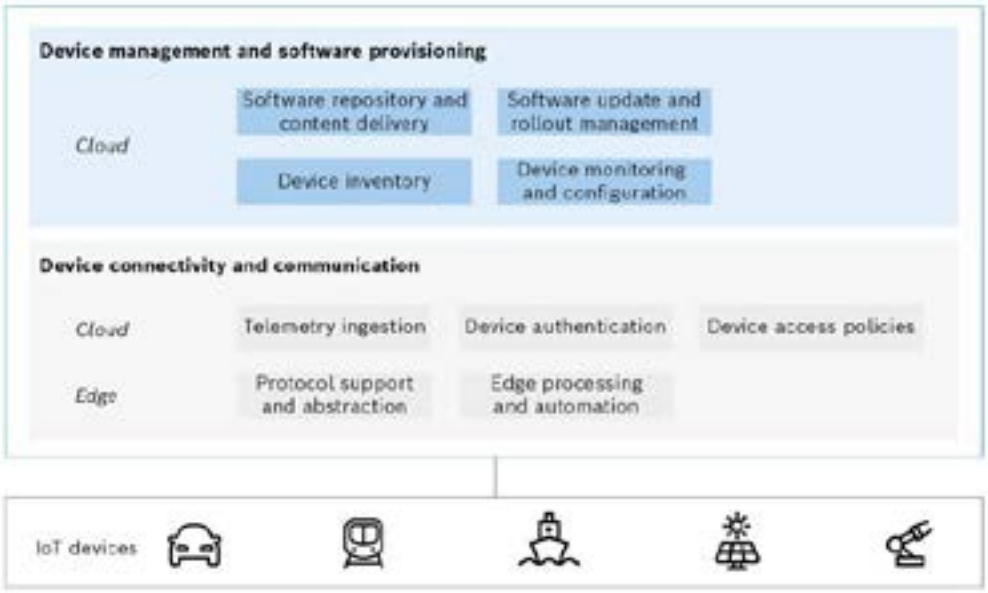
Devices access policies

The ability to manage the access of users and applications for a fleet of devices, a particular device, or even just one feature is also important. This can be achieved by using policies that are attached to the digital twin of a device and handle the link towards the identity management service.

These policies enable developers to define and control access to a device's twin and other entities, with rules as to who can view or edit designated areas of the digital twin.

4.2 Major function blocks: device management and software provisioning

The second and third challenge of managing software updates and devices are closely related and therefore addressed together in the following analysis. We abstracted the functional components of the solution into four functional blocks that are required to manage and update devices effectively and efficiently.



The main functions for device management and software update provisioning

Device inventory

In order to serve a large and heterogeneous device landscape, the device management system needs to have detailed information about remotely connected devices. Among others, this information concerns various technical parameters such as the central processing unit (CPU) type, operating system, installed software versions, and their current configuration. Ideally, devices are commissioned automatically when they are connected for the first time, thus directly providing all the necessary parameters. The device inventory then stores all this information. It is possible to create groups of devices in the inventory according to different parameters such as devices located in specific regions or specific device models. This not only facilitates device management operations but also the rollout of software updates on a large scale.

Device monitoring and configuration

Companies can monitor certain device parameters such as the connection status, CPU temperature, and available disc space, in order to keep track of the status/health of their connected devices. Depending on the use case, this can be done permanently, in specific time intervals, or triggered by an event. In case of anomalies or malfunctions, the device management system helps with troubleshooting. For instance, it sends alert notifications or disables certain functionalities to prevent damage.

Changing device configurations such as network settings and permissions and the configuration of software components and application settings – which come into play when onboarding new devices – are also critical requirements. The system can automatically configure these devices according to customer requirements (initial provisioning). It is also able to adapt, should there be changes in the technical setup at a later stage.

Software repository and content delivery

A repository collects all the software artifacts, e.g. firmware versions or security patches. Each software artifact comes with a set of meta-information that describes attributes such as the type of software, vendor, version, target platform, and other specific requirements.

For software update operations to scale to possibly millions of devices in different regions, companies can draw upon content delivery networks (CDN). A CDN is a geographically distributed network of proxy servers that executes software updates close to the location of the connected devices.

Software update and rollout management

Software update operations can be performed on a single device, a group of devices, or on devices that match specific parameters. The software update process must ensure that software artifacts are distributed in accordance with individual, device-specific parameters. For large-scale software rollouts, the use of a campaign management tool allows conditions under which the updates are performed to be defined. Companies can thus execute software update operations manually or at a scheduled time. Software updates should always be monitored in order to keep an eye on successful, failed, and pending updates.

4.3 Bosch IoT Suite: an open toolbox to build sustainable IoT solutions

Summed up, the major function blocks described above define the technical architecture used to implement IoT solutions for industrial assets. Companies do not need to develop these components by themselves – the market has plenty of IoT platform offerings and solutions that help decrease individual efforts and operation costs.

A prominent representative in this field is the Bosch IoT Suite that is based on the experience and expertise of the Bosch Group and the open-source community working together as part of the Eclipse IoT Working Group. The Bosch IoT Suite is an industry-proven platform that covers all the above mentioned function blocks and provides companies with all the necessary tools to address these challenges.

Bosch IoT Suite balances both flexibility and standardization. The platform not only provides several deployment options and is interoperable with various enterprise and IoT systems, but it also offers managed cloud services and packages that reduce implementation and operation costs.

4.4 Example: rolling out software updates to large engines

How can the Bosch IoT Suite be used in practice? Let us take a look at a project we realized together with a manufacturer of engines for commercial vehicles. The manufacturer was already updating the software of its engines, but the process required a high degree of manual work and was therefore extremely inefficient.

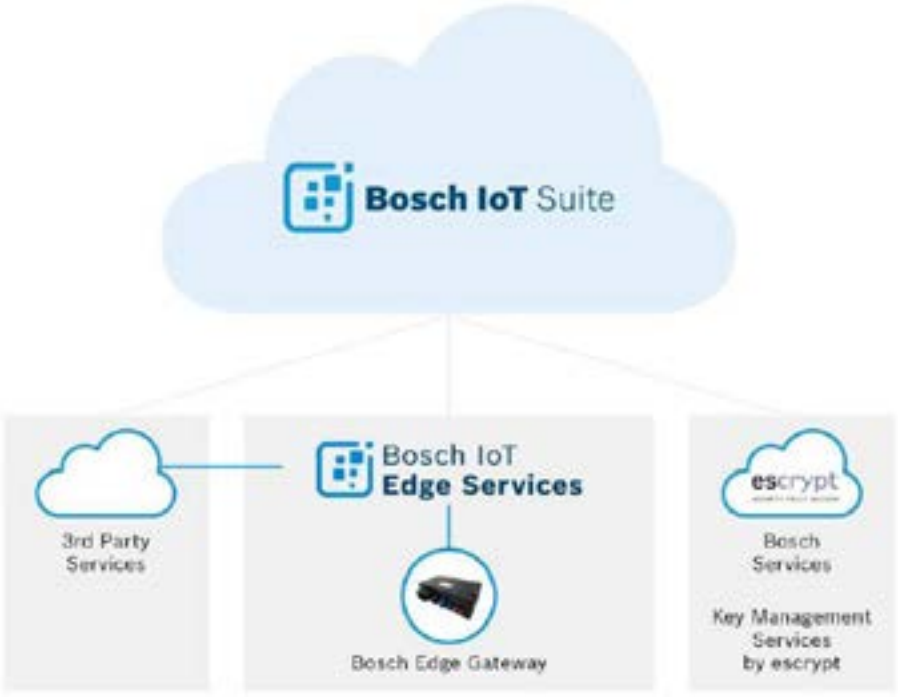
This is where we came into the picture. We provided the manufacturer with a solution comprising hardware, edge software, and cloud components to carry out software updates over the air. The manufacturer was thus able to automate the process of updating the edge software on the gateway and also the software in the vehicles. In addition, our customer is now able to manage large-scale software update campaigns in various markets and across a variety of different vehicle models.

Request a live demo to learn how to manage software updates with the Bosch IoT Suite

Did you know?

Another example for rolling out over-the-air firmware updates is the project we realized together with Daimler. The Bosch IoT Suite is a key component in the car manufacturer's system as it enables communication with the vehicles. Some four million car owners already receive new versions of vehicle software – for example, infotainment system updates – conveniently and securely via the cellular network.

Learn more about our customer projects >



Exemplary technical set-up for a SOTA solution with the Bosch IoT Suite.

The solution consists of several components of the Bosch IoT portfolio that are integrated with third-party services and the customer's public cloud provider of choice. Connecting the engines requires a connectivity device that communicates with the electronic control system of the vehicle. In this case, Bosch provides the connectivity unit and its Key Management Services. They are used to encrypt update packages and ensure that each device receives valid certificates.

The edge computing software (Bosch IoT Edge Services) is deployed on this gateway. It abstracts the connection protocols and executes commands on the device. The edge software is connected to the back end, which is based on the Bosch IoT Suite. There, the cloud services are used to manage large-scale software updates and the configuration of the engines.

5. Conclusion

There are many challenges in the field of industrial assets which, until recently, have made it difficult to advance the digitization of maintenance processes and product life cycle management. Global distribution and the complex technical characteristics of long-lasting devices pose additional challenges to the automation process.

However, the number of standard components and solutions on the market is growing, which makes it easier for industrial companies to address these challenges. IoT platforms such as the Bosch IoT Suite provide feature-rich tools to manage and update out-of-the-box devices. Combined with an edge computing solution that reduces cloud traffic and executes logic closer to the devices, companies have all the base technology at hand to create IoT solutions for their assets.

Nevertheless, it is important to note that a one-size-fits-all approach is rarely feasible. Industrial IoT solutions often need to be adapted and implemented according to the specific requirements of a project. Companies often have to invest considerable time, effort, and resources before the first device is even connected. Therefore, a well-thought-out and, above all, well-executed business plan is essential. It ensures that these expenses are amortized within the first year after implementation, forming the basis for long-term business success.

Apart from building on their own know-how, a key to successful industrial IoT use cases is also drawing upon the expertise of partners (e.g. software partners or hardware suppliers) who accompany you in the long term.

At Bosch.IO, we are proud to be a partner that industrial companies can rely on. We not only provide the functional solution modules of the Bosch IoT Suite but also have wide-ranging experience based on more than 250 successfully completed IoT projects in industrial IoT, energy, mobility, manufacturing, and more.

Free plans: **Test** Bosch IoT Suite for free

Request a live demo

Bosch Global Software Technologies GmbH
Löwentorstr. 72-76
70376 Stuttgart
Germany