Whitepaper

PostBus Technology for Industrial Progress...

...or How Industry Can Learn from Public Transport

Every day, several thousand vehicles transport PostBus passengers from A to B. These are, in essence, machines on wheels that continuously generate and require data. This includes information such as driving behavior, payment transactions, passenger data, or maintenance notifications. Some of these data should only be accessible to PostBus Ltd as the operator, others exclusively to the bus manufacturer, and still others must be transmitted to the payment service provider.

Challenges: Networking and Data Sovereignty

Industry faces similar challenges. The networking of people, machines, products, systems, and companies has been a central topic for years and is often referred to as the "Fourth Industrial Revolution" or Industry 4.0. Critics, however, see this less as a revolution and more as an evolution. The idea that certain data should be exchanged across company boundaries – between machine users, manufacturers, and other stakeholders—continues to be met with great skepticism. As a result, machine manufacturers today often have no access to the operating data of their delivered machines.

Barriers to Data Exchange

There are two main reasons why the exchange of machine data has not yet become established across company boundaries:

- Machines in manufacturing companies often process business-critical data such as formulas, bills of materials, or construction plans. These data must not fall into the hands of third parties – not even into those of machine manufacturers. For this reason, data exchange with external parties is often completely blocked, or only released manually and selectively.
- In addition, the different operating environments in which machines are deployed worldwide are considered a technical barrier. Each environment differs in terms of network topology, system

architecture, and security standards. This wide range of variables makes it difficult to develop a uniform and at the same time scalable solution for cross-company networking.

Multiple Benefits

The benefits are clear:

- Machine manufacturers who gain access to selected operational data could plan service interventions proactively, based on real-time and historical data, before a breakdown occurs. The further development of machines could also be based on real operational data.
- New business models, such as Machine-as-a-Service or uptime guarantees, could be established, while also improving customer service.
- With the EU Data Act, which enters into force on September 12, 2025, it will be legally defined who may derive value from data under which conditions. Companies will gain the right to access data generated through their use of connected devices, machines, or systems. At the same time, it will also be defined when a company is obliged to share data with other companies.

To achieve this, however, companies require technical solutions that allow precise control over who may access which data..

Solution Concept:

What if technological advances in IT already provided solutions today that could overcome exactly these obstacles?

Since the term "Industry 4.0" first emerged, computer science has evolved significantly. In particular, the development of Software-Defined Wide Area Networks (SD-WAN) has opened up new opportunities for mechanical engineering.

Originally designed to flexibly and securely connect decentralized company locations over the internet, SD-WAN today provides enormous added value in public transport: It enables simple, secure, and scalable connections between vehicles and various data stakeholders (e.g. public transport companies, vehicle manufacturers, suppliers). The challenge: vehicles such as buses, trains, or trams are constantly in motion and regularly lose their internet connection. The "software-defined" aspect of SD-WAN compensates for these interruptions by continuously analyzing connection quality and adapting data transmission accordingly.

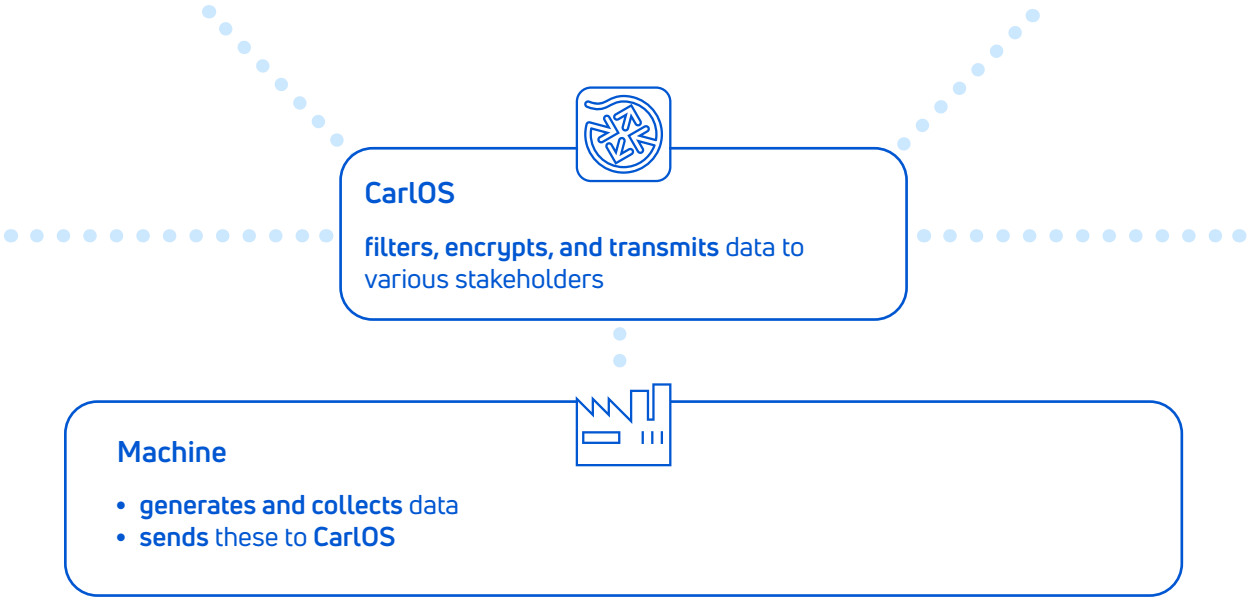
These advantages can be directly transferred to industry—ensuring that all stakeholders benefit equally from machine data. Data must be collected directly on the machine and then forwarded. If there are multiple recipients, the data must be filtered in advance—so that each party only receives the data intended for them.
In IT, this task is handled by a firewall. It decides, based on predefined rules, which data may be sent to which recipient, as the following example shows:

Content of Data	**Transmission:**	
	Machine User	Machine Manufacturer
Formula Part A	Yes	No
Vibration Value Part B	No	Yes
Temperature Value Main Unit	Yes	Yes

If the filter rules are set correctly, all data are transmitted only to their authorized recipients. Transmission to the machine manufacturer takes place via the internet. For this reason, all data must be encrypted (VPN) during transfer.

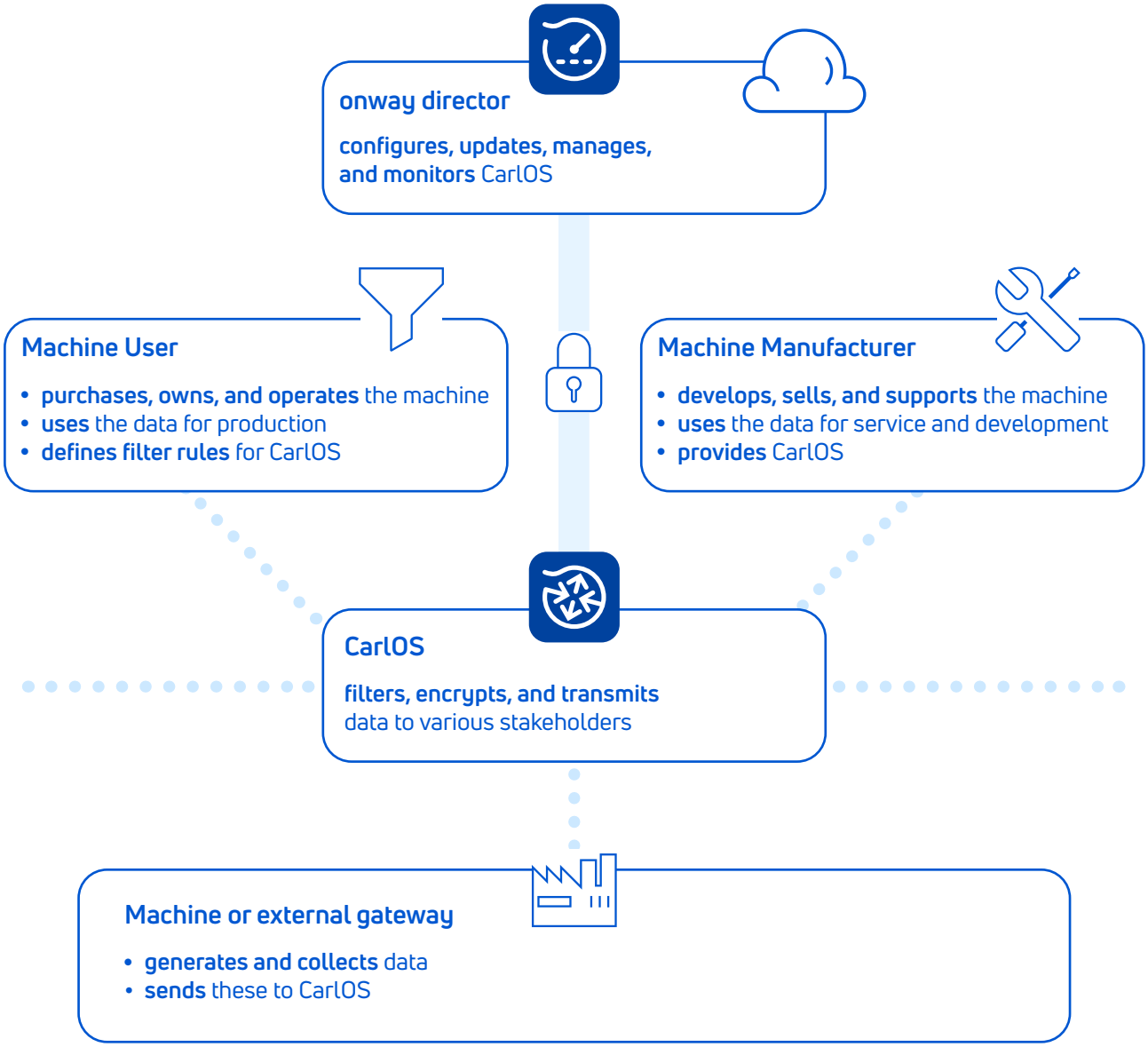
Concrete Solution

Our software, which can filter, encrypt, and transmit data, is called **CarlOS**. CarlOS can be operated on any hardware gateway that meets the software requirements. One option is for CarlOS to run directly on the machine, controlling all incoming and outgoing **data traffic**:



The filter rules are defined by the so-called data owner, i.e. the device user or machine operator. The machine manufacturer delivers CarlOS preconfigured. The user then determines which data may be sent to whom.

With potentially thousands of machines worldwide, manual configuration would not be practical. For this reason, CarlOS is managed centrally via a cloud solution called the **onway director**. All communication between CarlOS and the onway director is, of course, end-to-end encrypted.



The **onway director** can be operated on the servers of the customer, the machine manufacturer, or the onway cloud. Together, **CarlOS** and **onway director** form a secure, simple, and scalable **SD-WAN** networking solution.

The central cloud logic is the key to scalability. Commissioning, updates, monitoring, error diagnosis, or reassignments of machines to other machine users are all carried out centrally.

The solution is also multi-tenant capable. Machine users receive their own areas for management. The manufacturer, in turn, can assign specific access rights to different departments (e.g. service, development) in order to stay informed about current customer installations.

Linking Back to Public Transport

Back to public transport and how it can help industry: simply replace the word "machine" with "vehicle" in the diagram on the previous page, and you will see how public transport providers securely, easily, and scalably network their vehicles. With this knowledge, you as a machine manufacturer can extend your own machines with exactly these functions – or you can talk to us.

We are happy to support you in quickly and easily implementing a proof of concept (PoC) with our proven public transport system.

Who We Are – onway (Switzerland) ag

onway is the leading provider of customized communication solutions for all areas of modern network infrastructures. We support more than 100 customers across various industries with the design, implementation, operation, and support of secure ICT infrastructures. Our own products include a multi-tenant smart access solution, public hotspots, and mobile solutions for public transport vehicles. In addition, we integrate communication solutions from established manufacturers, creating seamless, future-proof networks. The onway Group is fully certified according to ISO 9001:2015, ISO 14001:2015, and ISO/IEC 27001:2022.

onway (Schweiz) ag | Stauffacherstrasse 16 | 8004 Zurich | Switzerland | phone +41 58 404 45 40 | sales@onway.ch | www.onway.ch