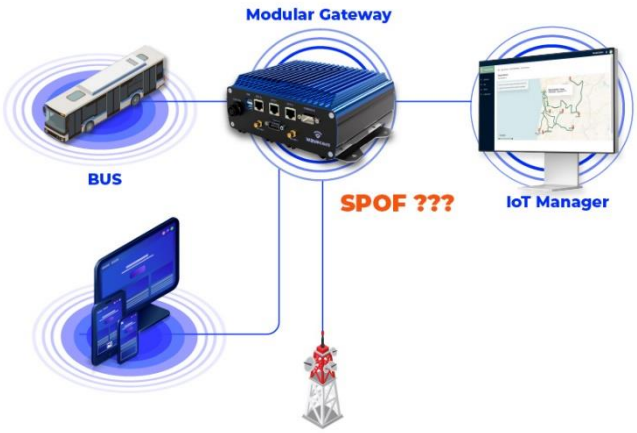
wavecom
Technologies

White Paper

Connected Bus by Wavecom

Minimizing the effects of modular Gateway as a SPOF



A SPOF (Single Point of Failure) is any non-redundant component or equipment of a system architecture that, if dysfunctional, would cause the entire system to fail, leading to its downtime.

In **Connected Bus** solution architecture, the **modular Gateway** is sometimes seen as a SPOF. The reliability and resilience of the **Connected Bus** are critical issues since **modular Gateways** relies on constant connectivity and data exchange with **IoT Manager/Multi-Tenant Platform**.

To minimize the effects of a **modular Gateway** as a SPOF, network access and data at all levels are secured. The software is regularly updated and maintained properly for **modular Gateways**. A VPN is used to protect network access from unauthorized users or devices. SD-WAN (Software Defined - Wide Area Network) makes a **Connected Bus** solution more flexible, automatable, resilient, and reliable. This solution is cloud managed by **IoT Manager/Multi-Tenant Platform** and supports ZTP (Zero-Touch Provisioning).

However, the main strategy is focused on using two **modular Gateways** in a balanced mode, to create redundancy in connectivity.

Date: 01st February 2024
Version 1.0.

White Paper

Connected Bus by Wavecom
Minimizing the effects of modular Gateway as a SPOF

Introduction

A SPOF (Single Point of Failure) is any non-redundant component or equipment of a system architecture that, if dysfunctional, would cause the entire system to fail, leading to its downtime.

In **Connected Bus** solution architecture, the **modular Gateway** is sometimes seen as a SPOF. The reliability and resilience of the **Connected Bus** are critical issues since **modular Gateways** relies on constant connectivity and data exchange with **IoT Manager/Multi-Tenant Platform**.

To minimize the effects of a **modular Gateway** as a SPOF in a **Connected Bus** solution, network access and data at all levels are secured. The software is regularly updated and maintained properly for **modular Gateways**. Additionally, using preventive maintenance, diagnostics, or troubleshooting allows us to detect and solve errors before they affect network functionality of the **Connected Bus.** A VPN is used to protect network access from unauthorized users or devices. SD-WAN (Software Defined - Wide Area Network) makes a **Connected Bus** solution more flexible, automatable, resilient, and reliable. This solution is cloud managed by **IoT Manager/Multi-Tenant Platform** (Figure 1) and supports ZTP (Zero-Touch Provisioning).

However, the main strategy is focused on using two **modular Gateways** in a balanced mode, to create redundancy in connectivity, as depicted in Figure 4.

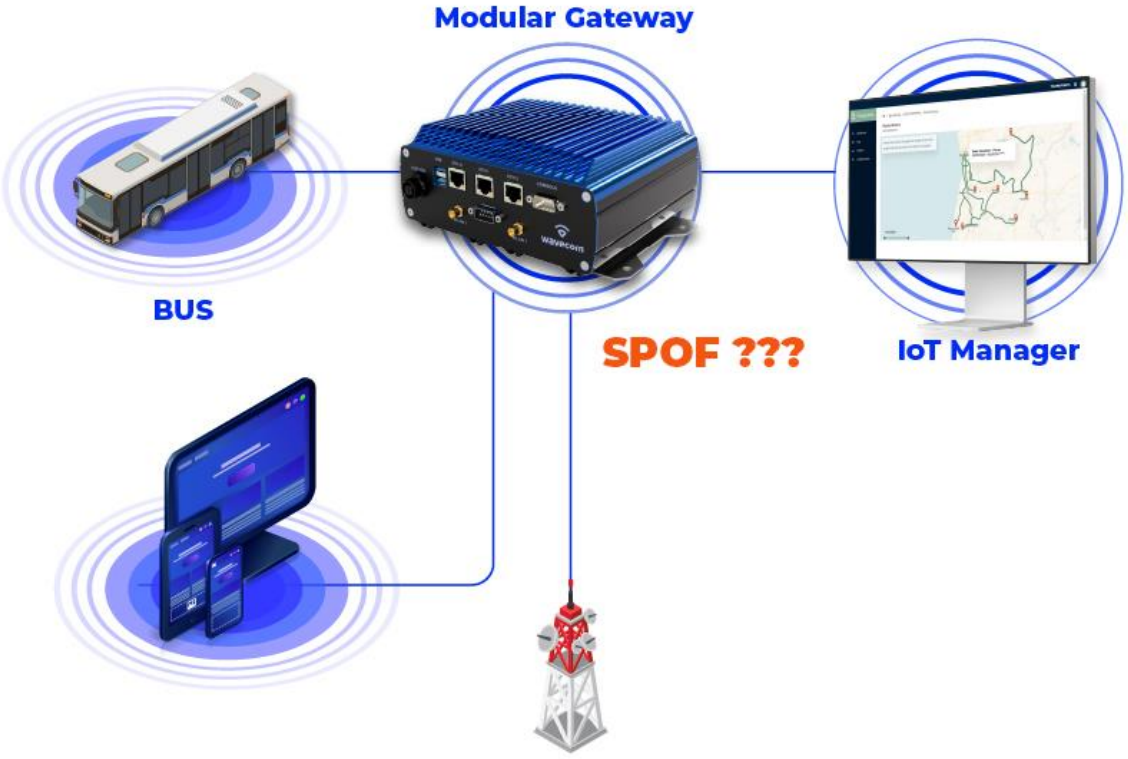


Figure 1 – Modular Gateway | SPOF - Single Point of Failure???

Connected Bus Solution

Connected Bus solution is designed for Bus Operators to significantly improve their business efficiency and profitability.

Through a complete onboard Wi-Fi connectivity solution, **Connected Bus** provides access to internet and communication to passengers, Real-Time FMS (Fleet Management Service) | Tracking | GPS positioning | CAD – AVL (Computer-Aided Dispatch / Automatic Vehicle Location) and APC (Automatic Passenger Counting). Seamlessly. It also enables integration with CCTV | surveillance video streaming and Ticketing systems through APIs.

The elementary **Connected Bus** solution's components comprise a **Wavecom Technologies** **modular Gateway** (5G Native) installed in each bus vehicle, which is cloud managed by **IoT Manager/Multi-Tenant Platform** (5G WAN Manager | SD-WAN) as shown in Figure 2.

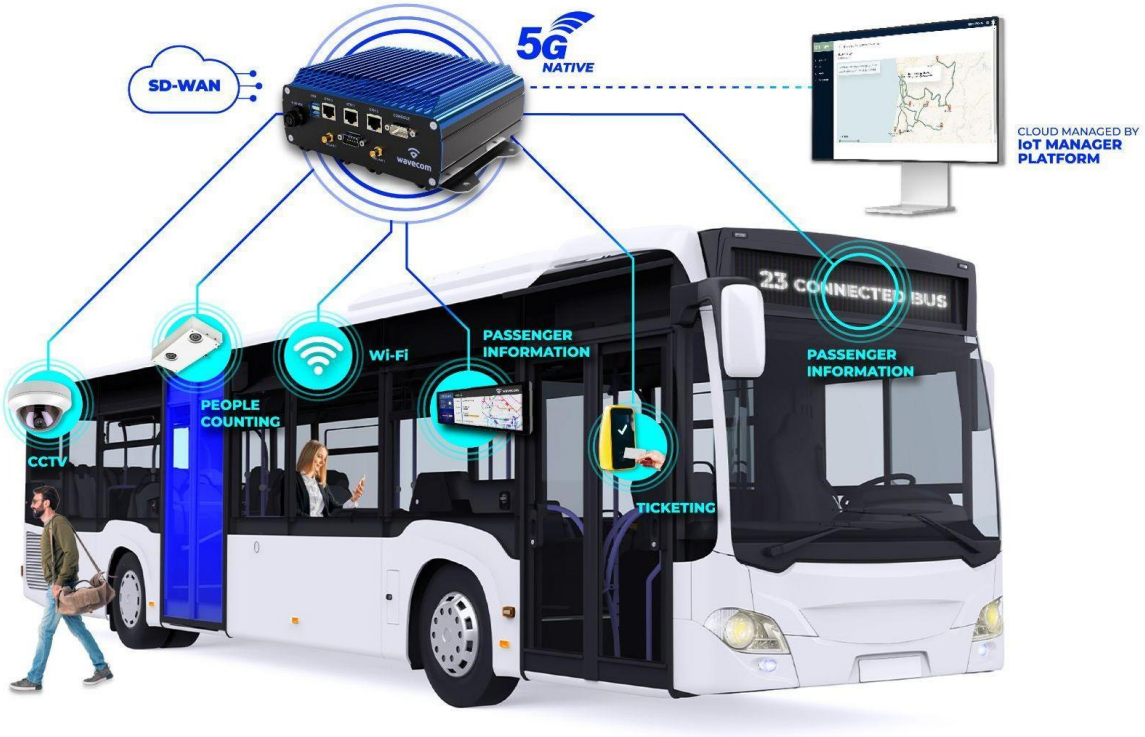


Figure 2 – Connected Bus Architecture and functionalities

- **Modular Gateway (5G Native)**

Bus onboard equipment refers to single **modular Gateway** (5G Native) offering the following features:

- 2 x Independent 4G-LTE/5G modules
- 2 x separated dual band Wi-Fi Access Points
- 1 x integrated GPS
- Possibility of providing information in IoT Manager Platform or via API
- Network resources (OSPF, STP, DHCP Server/Client, NAT, DNS, Link Aggregation, VPN Server/Client, QoS, VLAN …)
- Ethernet and serial interfaces for local connectivity
- VPN over WWAN (4G-LTE/5G) for centralized real-time monitoring and management
- Certified for automotive environment

Modular Gateway has up two 4G-LTE/5G interfaces, which provides redundancy since it uses SIMs from two different Cellular Operators.

- **IoT Manager/Multi-Tenant Platform**

IoT Manager/Multi-Tenant Platform (5G WAN Manager | SD-WAN | Virtual Networks | Link aggregation | Security) provides a cloud managed ZTP system multi-tenant approach, as it allows a System Integrator to manage multiple **modular Gateways**.

IoT Manager /Multi-Tenant Platform (5G WAN Manager | SD-WAN | Virtual Networks | Link aggregation | Security) is able of centralizing all provided functionalities such as:

- Wi-Fi User Access Control
- Network Access Control
- Gateways/Device management
- Real Time equipment's' monitoring
- Customizable Captive Portal
- Real Time Fleet Visibility with Route Optimization
- Ability to create CSAT (Customer Satisfaction Surveys)

Minimizing the effects of modular Gateway as a SPOF

A SPOF (Single Point of Failure) is any non-redundant component or equipment of a system architecture that, if dysfunctional, would cause the entire system to fail, leading to its downtime. The SPOFs are undesirable to systems that demand high availability, reliability and resilience, such as on an onboard connectivity architecture.

In **Connected Bus** Architecture, the **modular Gateway** is sometimes seen as a SPOF, as shown in Figure 1. In a **Connected Bus** solution, to ensure reliability and resilience for **modular Gateways** in order to minimize the effects of SPOF, some procedures are implemented.

- **Secure network access and data**

In **Connected Bus** solution, a VPN is used to secure network access and data at all levels from unauthorized or malicious users or devices (Figure 3).

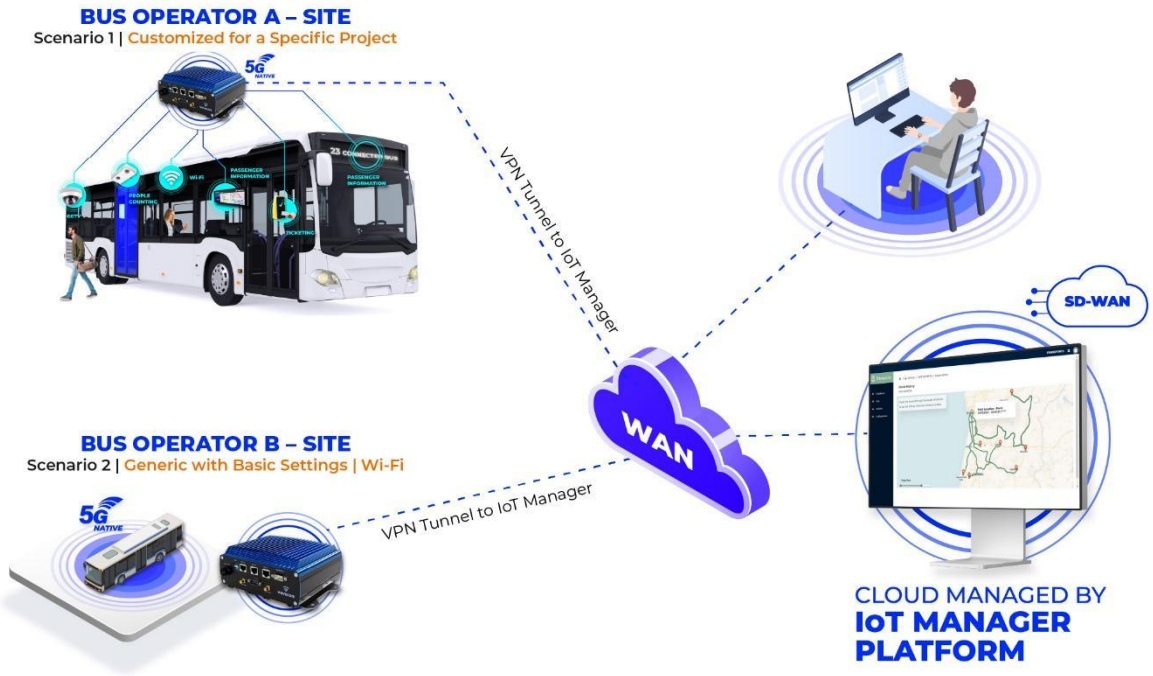


Figure 3 – Cloud Managed Architecture

SD-WAN virtualizes network functions so that the network can be used over a variety of heterogeneous physical and logical network connections and protocols, such as Wi-Fi and 5G.

In terms of security issues, tunnel protocols (SD-WAN), security policies and other mechanisms are used to prevent possible attacks to the network, as depicted in Figure 3.

- **Architecture with two modular Gateways in a balanced mode**

The main strategy is focused on using two modular Gateway in a balanced mode, to create redundancy in connectivity, as depicted in Figure 4 . If the **modular Gateway** is a SPOF, then we can add another one in Bus vehicle. If the first one crashes, the second one will be used. Or we can distribute load across both the **modular Gateways**.

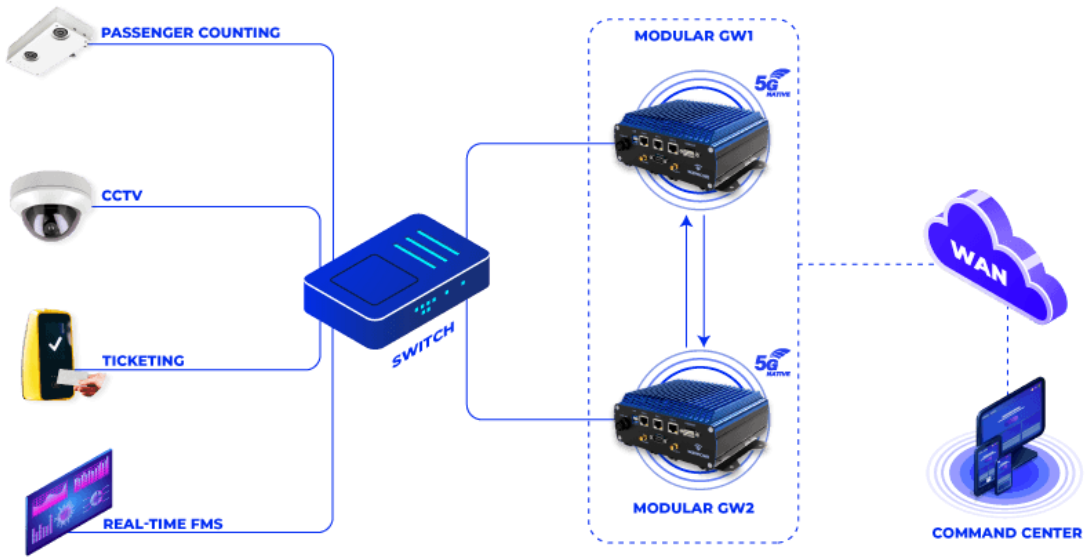


Figure 4 – Two modular Gateways in a balanced mode | Architecture

The architecture presented (Figure 4) involves placing a switch that communicates with 2 **modular Gateways**, each with two modems. This architecture allows the two **modular Gateways** to be configured via ZTP and communicate with each other, allowing them to operate in load balanced and/or failover mode.

This is because the two routers constantly exchange messages with each other and if one stops working, the second will take over communications for all internal systems. This means that critical internal services do not suffer from failures in communications with central systems. Thus, we are able to combat the effects of SPOF in a resilient and simple way to implement.

It should be noted that this way is very transparent for internal systems and that it is easily put into service, always maintaining the focus on ensuring flawless communications.

Conclusion

The SPOFs are undesirable to systems that demand high availability, reliability and resilience, such as on an onboard connectivity architecture.

In order to minimize the effects of SPOF due **modular Gateway, Wavecom Technologies** provides a cloud managed **IoT Manager/Multi-Tenant Platform** that improves the reliability and efficiency, when deploying a **Connected Bus** solution.

In terms of security issues, tunnel protocols (SD-WAN), security policies and other mechanisms are used to prevent possible attacks to the network, minimizing the effect of the **modular Gateway** as a SPOF.

However, the main strategy is focused on using two modular Gateway in a balanced mode, to create redundancy in connectivity. If the **modular Gateway** is a SPOF, then we can add another one in Bus vehicle. If the first one crashes, the second one will be used. Or we can distribute load across both the **modular Gateways**.

This architecture allows the two **modular Gateways** to be configured via ZTP and communicate with each other, allowing them to operate in load balanced and/or failover mode. This way of minimizing the effects of a SPOF, is very transparent for internal systems and it is easy to put into service, always maintaining the focus on ensuring flawless communications.

Acronyms

4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network
API	Application Programming Interface
APC	Automatic Passenger Counting
AVMS	Audio Visual Media Services
CAD – AVL	Computer-Aided Dispatch / Automatic Vehicle Location
FMS	Fleet Management System
GNSS	Global Navigation Satellite Systems
IP	Internet Protocol
ITxPT	Information Technology for Public Transport
LTE	Long Term Evolution
SD-WAN	Software Defined – Wide Area Network
SDN	Software Defined Network
SPOF	Single Point of Failure
VPN	Virtual Private Network
WWAN	Wireless Wide Area Network
ZTP	Zero Touch Provisioning

Contacts

For more information about the **Connected Bus** solution, feel free to contact us.

Phone: +351 234 919 190
Web: https://www.wavecom.com