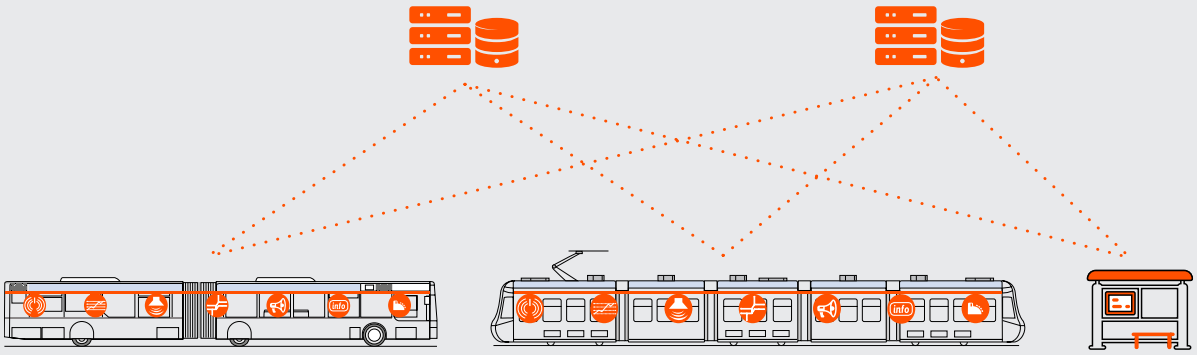

INTEGRATED COMMUNICATION SYSTEM FOR PUBLIC TRANSPORT

With the ongoing digitalization and the emerging „Internet of Things (IoT)“ applications, the quality of operational processes can be significantly increased. Nowadays, a great number of isolated applications can still be found in rolling stock and busses. However, in the era of IoT communication systems no longer work in isolation. They share their information and states with other applications via secured interfaces. The strategy of isolated solutions has definitely reached its limits. **In future, (current) separate applications, such as customer information systems, fleet management solutions, ticketing systems, passenger counters, sensors, cameras, etc. , will share their data in real-time, thus offering unimaginable possibilities for new applications.** Examples to be mentioned are a better registration and influence on passenger streams (-> customer analytics), supply of real-time information for staff, supply of personalized passenger information such as information on their journey or new services like the introduction of a dynamic ticket prizing.

The integration of manifold applications into one communication system means ever increasing requirements in terms of availability. Smooth network connectivity, however, is required at all times. The intelligent management of dead spots, for instance, is key and can be achieved by connecting to several mobile networks in parallel. Moreover, different safety requirements need a strict separation of traffic flows. And, Quality-of-Services mechanisms have to prioritize important applications over less critical ones.

Our network engineering know-how combined with the intelligent software components of CloudGuard guarantee a safe, performant and highly available communication infrastructure with and within vehicles. **Transportation companies benefit from reduced administrational efforts and less configuration tasks regarding communication devices and profit from a central data storage and real-time monitoring.** Hence, a significant reduction of expenses can be achieved when operating a vehicle fleet.

ARCHITECTURE

The architecture of the integrated communication systems is based on the standard hardware components of the common manufacturers and enhances them with intelligent software components:

Backend

- RMS
- macman – Network Access-Control
- mpp – Captive Portal Marketing
- Internet

Value added Software

Device Management
- Auto-Provisioning
- Monitoring
- Alarming
- SW-Updates
- Security Updates

Firewall VPN
- Access-Control
- Network Partitioning
- VLANs / ACL
- Perimeter FW

Routing QoS
- Routing per Application
- Bandwidth Control
- QoS
- NAT/PAT

Uplink-Control
- Multiprovider
- Uplink Management
- Load Sharing
- Cost Control

Guest WiFi Lawful Intercept
- Landing-Page
- SMS Auth.
- Webfilter
- Lawful Intercept

GPS
- Localization
- Measurements Mobile Network Coverage
- Statistics

Certified Hardware



THE MOST IMPORTANT FUNCTIONS AT A GLANCE:

Our integrated communication systems enhance your standard hardware in a straightforward way and empower you to successfully cope with the following challenges:

- Automatic Lifecycle Management of the communication infrastructure
- Uplink Management for mobile networks
- Security Management
- Dynamic Routing
- Firewall
- Quality of Services
- URL Filtering
- Data Recording / Monitoring
- VPN Management

DEVICE MANAGEMENT

Auto-provisioning and auto-configuration allow for dynamically downloading configuration changes, software and security updates. Thus, on-site interventions are no longer required and communication devices are automatically configured and initialized. Additionally, status information and logging data of the different system components and applications are continually transmitted to the backend during running operations. Should a problem occur, an alert is sent immediately.

FIREWALL

It is vital that different traffic flows are strictly separated. For safety reasons, internal applications and traffic flows should always be connected with a different backend than the passenger WiFi. Moreover, all systems need to be protected against hacking, malware or DDOS attacks.

ROUTING QOS

A multi-functional environment is faced with a great number of communicating devices (e.g. board computers, passenger information, surveillance cameras, passenger WiFi, etc.). Their different traffic flows need to be individually routed (VLAN/VR). Quality-of-Service (QoS) mechanisms allocate the available bandwidths, as mobile network capacity can vary significantly depending on the location.

UPLINK-CONTROL

The dynamic control of several mobile connections is a highly challenging task. Not only do the modules in vehicles need to be controlled, but also the tunnel endpoints at the backends. Our Traffic Control ensures that only as much traffic is sent from the backend to the different mobile networks as the vehicle can receive. It precisely takes the signal strength, the technology and available throughput of the radio cell. Moreover, the intelligent use of different mobile networks results in lower roaming costs.

GUEST WIFI

There are many transportation companies that presently offer Public WLAN access in vehicles for their customers. Innovative firms use this new communication channel even for the individual passenger information, targeted advertising or data collection on passenger flows. However, legal requirements regarding traceability and real-time monitoring have to be strictly fulfilled. Content filters, for instance, prevent users from consuming inappropriate contents.

GPS

GPS data relate all real-time information, such as current data throughput, system load, reception quality of mobile networks as well as logs and alarms to the present vehicle location. Consequently, companies benefit from a better overview and easier troubleshooting.

WLAN-PARTNER

In 2004, WLAN-Partner.com was originally founded as a startup company of the University of Applied Sciences Rapperswil. Ever since, the company has offered professional client support regarding the evaluation, planning, implementation, operation and support of complex WLAN and Network Access Control (NAC) solutions. We are specialized on the integrated networking of trains, busses, stations and airports.

CLOUDGUARD

CloudGuard Software AG offers telecommunication solutions for private and public companies. The product range includes Network Access Control (NAC) solutions, Bring-Your-Own-Device (BYOD) access, public WLAN guest access and sophisticated communication facilities in public transport. By now, more than 100 institutions rely on the software products of CloudGuard.

EXTRACT FROM OUR CUSTOMER LIST

- **Flughafen Zürich Skymetro**
- **PostAuto**
- **ARL Autolinee Regionali Luganesi**
- **Bieler Schifffahrt**
- **Jungfraubahnen**
- **Verkehrsbetriebe Leuk-Leukerbad und Umgebung**
- **Verkehrsverbund Vorarlberg**

WLAN PARTNER

WLAN-Partner.com AG
Zurich
Switzerland

Phone +41 58 404 45 40
info@wlan-partner.com
www.wlan-partner.com