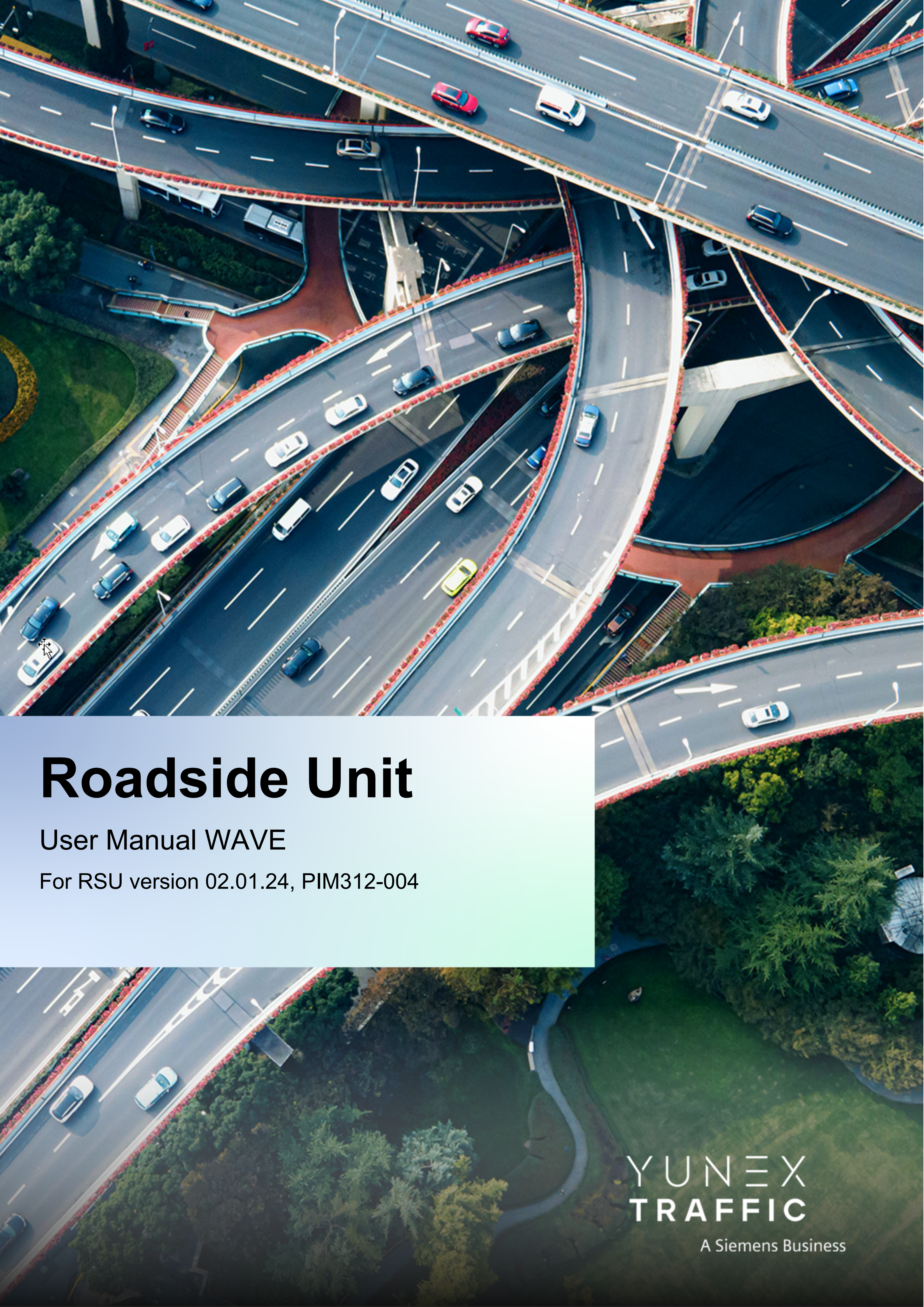


Roadside Unit

User Manual WAVE

For RSU version 02.01.24, PIM312-004

YUNEX TRAFFIC

A Siemens Business

Contents

List of Tables

List of Figures

References

Change History

Date	Modifications	Editor
2019-02-01	Initial draft	Jiri Ohnheiser
2021-08-01	RSU2.0 and RSU2X update	Jiri Ohnheiser

Abbreviations and Definitions

Abbreviation	Comment
APU	Application Unit
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
CA	Certificate Authority
CAM	Cooperative Awareness Message
CCH	Control Channel (ITS-G5 communication channel)
C-ITS	Cooperative Intelligent Transport/Traffic Systems
C-ITS-S	Central ITS Station
C-V2X / PC5 / LTE-V2X	Cellular Vehicle To X
CMS	Central Management System
CPU	Central Processing Unit
DENM	Decentralized Environmental Notification Message
DHCP	Dynamic Host Configuration Protocol
DSRC	Dedicated Short Range Communications
ESCoS	Ecosystem for Cooperative Systems
FW	Firmware
FQDN	Fully qualified domain name
GN	GeoNetworking
GPS	Global Positioning System
GUI	Graphical User Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ITS	Intelligent Transport/Traffic Systems
ITS-G5	European 802.11p protocol stack for Cooperative Intelligent Transport/Traffic Systems, enhanced for supporting European frequency regulatory requirements
IVIM	In-vehicle Information Message
MAPEM	MAP extended message. Detailed topological description of street
JSON	JavaScript Object Notation
LTE	Long Term Evolution
OCIT-C	Open Communication Interface for Road Traffic Control Systems
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PUK	Personal Unblocking Key
RSU	Roadside Unit
RWW	Road Works Warning
SBAS	Satellite-based augmentation system
SCH	Service Channel (ITS-G5 communication channel)
SPATEM	Signal Phase and Timing (e.g. traffic light) extended message
SRK	Super Root Key

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol,
UPER	ASN.1 Unaligned Packed Encoding Rules
VPN	Virtual Private Network
V2x	Vehicle to vehicle - , vehicle to infrastructure- , infrastructure to vehicle - communication
Wifi AP	IEEE802.11 WLAN Access Point
WLAN	Wireless Local Area Network
XER	ASN.1 XML Encoding Rules

Preface

Notes on safety and environmental protection

Safety notice

The devices/systems are only to be employed for their intended use in accordance with the product documentation; the warning labels and product documentation are to be adhered to. The installation and initial startup of the devices may only be performed by authorized professional personnel (electrically qualified persons with the appropriate training for these devices/systems through the Yunex Academy, Traffic Systems Segment).

If not sufficiently trained personnel are working on the devices, substantial bodily damage and property damage can come as a consequence.

The devices/systems are to be tested regularly by authorized professional personnel. The test intervals and the checks to be performed can be found in the specifications of the product standards. If there are no product standards with information about regular checks for the devices, then the tests are to be performed in accordance with the standards VDE 0100-600, VDE 0105-100 and BGV A3.

Occupational safety, environmental protection

All legal regulations regarding occupational safety and environmental protection are to be complied with during the course of production. We design our products (parts, devices, systems) in such a way that these present no health hazards to the user or hazards the environment according to the current state of information if properly and predictably used.

Recycling, disposal

The information above makes it possible to assess to a large extent the possible potential for hazards to people and the environment, even at the end of the product’s life cycle. The regulations for recycling and disposal procedures must be observed here.

All information has been given to the best of our knowledge and belief. It is in accordance with the current state of the art. The information does not constitute a guarantee in the legal sense of a warranty.

1. Introduction

This document gives an overview of the system integration and usage of the Yunex ESCoS Roadside Unit.

2. Overview

This section shall give a step by step guide on how to initially setup an ESCoS RSU with factory default settings. Mounting shall not be part of this section, please see the “ESCoS RSU Installation Manual” for information on this topic.

2.1. Part numbers

- RSU2X incl. WAVE software: RSU2X US, PoE, LTE
  - SAP No. L24707-E200-A2
- Power supply: ESCoS RSU PoE+ Injector
  - SAP No. V24707-Z103-A6
- Optional external antennas: Toplink 5.9GHz antenna OMNI
  - SAP No. V24707-Z100-A1

2.2. Connectors (RSU1)

The ESCoS RSU provides several wired and wireless interfaces. All antenna connectors are Female N-Type connectors.

All connectors for wired connections (Ethernet, RS232) are on the bottom of the enclosure. The Ethernet (RJ45) and RS232 connectors are IP67 rated connectors, which require suitable cable assemblies to keep the IP sealing. On the ETH0 port the RSU is powered via a PoE+ power supply.

Additionally the status LED’s and the two LTE antenna connectors are located on the bottom side. The PG M16 gland is a general purpose connector, which might be used to connect currently only internally (not accessible from outside the enclosure) available interfaces in the future and thus not used at the moment.

> The ESCoS RSU must not be powered up without all antennas connected to otherwise the transceiver units might be damaged!

Please refer to the *ESCoS RSU Installation Manual* for further details.

2.3. Connectors (RSU2X)

The RSU2X provides several wired and wireless interfaces. All external antenna connectors are Female N-Type connectors.

Ethernet connectors are on the bottom of the enclosure. The Ethernet (RJ45) connectors are IP67 rated connectors, which require suitable cable assemblies to keep the IP sealing. On the ETH0 port the RSU is powered via a PoE+ power supply.

Additionally the status LED’s and the pass-through connector for RS485 cable are located on the bottom side.

Please refer to the *RSU2X Datasheet* for further details.

2.4. Status LEDs

- Power LED
  - Off - No power
  - Solid green - Device is powered on
- Status LED
  - Off - No power
  - Blinking Green - Device start-up

- Solid Green - Device operational
- Amber - Firmware upgrade in progress
- Red - At least one of the services is in error state

2.5. Interfaces

2.5.1. Physical interfaces - common for RSU1 and RSU2X

- ETH0
  - Default settings: 172.24.5.254/24 and DHCP client running
  - Used for PoE+, Service UI, CMS interface, XFER interface, etc.
- ETH1
  - Default is in bridged mode (with WIFI if that is enabled) + DHCP server
  - Default IP settings is 10.0.0.1/24
  - Used for Service UI, Traffic controller connection
- GPS
  - Satellite positioning and time synchronization
- Standard WLAN (WiFi AP)
  - Disabled by default
  - Used for service UI, XFER interface, etc.
- Bluetooth
  - Disabled by default
  - Used for service UI, XFER interface, etc.
- LTE
  - Disabled by default
  - Can be used for connection to central server, PKI connection

2.5.2. Physical interfaces - RSU1 specific

- DSRC1
  - cw-llc:0 - continuous approach: SCH1 (172) - BSM, SPAT, MAP, WSA
  - cw-llc:1 - timeslot0: CCH (178), timeslot1: SCH3 (176) - SSM, SRM, TIM, PSM
- C-V2X (for dual mode RSUs)
  - C-V2X interface
- RS232
  - Disabled by default
  - Proprietary interface

2.5.3. Physical interfaces - RSU2X specific

RSU2X has internal antennas and can be optionally equipped with various configurations of external antennas (See more in RSU2X Datasheet).

These antennas are used for DSRC or C-V2X communication.

RSU2X has various user accessible ports hidden behind the circular opening in its enclosure:

- RS485 (RSU2X)
  - Disabled by default
  - Proprietary interface
- Rotary switch
  - 0 - normal operation
  - F - factory reset
    - set to rotary switch to F
    - power cycle the RSU
    - After web UI is reachable, set it back to 0
    - RSU should now be in factory default settings
    - This will erase all settings, data and enrollments
- SIM card holder
- SD card holder
- USB connector

> Never open the RSU enclosure, if you have hardware problem with the RSU, approach your service contact person.

2.5.4. Logical interfaces

The ESCoS RSU provides several applications and interfaces. Depending on the configuration and connection of external components different data flows are possible. External components interfacing the RSU include:

- Service Web GUI
  - This is the main configuration and diagnostic interface. A connection to the Service GUI can be established from any of the available IP interfaces.
- XFER
  - The XFER interface is a lightweight secure websocket based application unit interface. It provides both communication and device management functions.
- OCIT-C
  - OCIT-C is the default interface for connecting an RSU to an ESCoS CMS. Main functionalities provided are ETSI communication (DENM, IVIM, CAM Aggregation) as well as RSU device management functionality (SW update, monitoring, configuration). The communication channel between CMS and RSU shall always be protected via a VPN tunnel.
- WAVE
  - The communication to V2x equipped vehicles is done via the DSRC or C-V2X WAVE protocol. The RSU provides two radio modules, both capable of running in alternating mode. Thus in total a maximum of four channels can be used in parallel.
- SNMP
  - SNMP interface based on USDOT requirements. It provides both communication and device management functions.
- Traffic Controller - SPAT (V2I Hub)
  - A traffic controller sending SPAT UDP data packets according to the V2I Hub specification can be connected to the RSU via one of the Ethernet interfaces. The data is used to send residual time information on the current phases to vehicles via the SPAT and MAP messages.

- Traffic Controller - NTCIP
  - Additionally to the SPAT data the RSU can also interface via NTCIP with the traffic controller. The RSU can access the detector values and issue priority requests via this interface.
- SSH
  - For diagnostic and debugging purposes an SSH access is provided. However per default the interface is deactivated to provide a higher security.

3. Quick start

The following section shall provide a step by step guide on how to configure the ESCoS RSU for first time use. In general each of the following sections and the described steps should be performed in the order shown here.

3.1. Assembly and Power up

Please refer to the “ESCoS RSU Installation Manual” for details on physical requirements, mounting and antenna connections.

> Make sure that no power is applied to the unit before all antennas are installed!

1. Connect all antennas as described in “ESCoS RSU Installation Manual”.
2. Connect the PoE+ output of the PoE injector via a standard Ethernet cable (Cat5e or higher) to ETH0 port of the RSU.
3. The RSU should boot up now (Power LED green, Status LED flashing green). Wait until both LEDs are statically on. The boot up is finished.

> Colors of LEDs don’t matter in terms of booting. Status LED may be even red for various reasons (e.g. not sufficient GPS signal). Boot up is finished when they are not flashing anymore.

3.2. Accessing the service UI

1. Connect your PC to the RSU, either to ETH0 via the PoE+ injector/switch or directly to ETH1 on the RSU.
2. Make sure your PC is in the same IP subnet as the RSU, depending on the Ethernet connector you are using on RSU side, the configuration should be following:
   - ETH0
     - Set static IP address of PC in range 172.24.5.1 - 172.24.5.253
     - RSU has IP address 172.24.5.254 by default
   - ETH1
     - PC will be in role of DHCP client, don’t assign static address
     - RSU has IP address 10.0.0.1 by default and work as DHCP Server
3. Open the web UI in the web browser
   - ETH0: 172.24.5.254
   - ETH1: 10.0.0.1
   - Note that internet explorer is not supported
4. Login with the default credentials
   - Login: **admin**
   - Password: **admin**
5. You will be asked to change the default password to a different password.
6. Inspect the options that the service interface presents

3.3. Installing firmware

New firmware can be installed in the Maintenance - System overview page (see 4.5.1).

3.4. Updating the RSU firmware

When installing new release following order should be respected:

- Bootloader image - if provided for particular release, most often this will not be the case.
- Firwmare image - if provided
- Application image - if provided
- Configuration reset for particular version if it is needed to reset configuration for the RSU (RSU2X HW has configuration reset built in the web UI - see the Maintenance, System overview)

3.4.1. Supported firmware update paths

- 1.0 -> 1.1
- 1.1 -> 1.2
- 1.2 -> 1.3
- 1.3 -> 1.4
- 1.4 -> 2.0

Although downgrade is possible, it is not recommended. For best results consider resetting configuration on the RSU after downgrade.

4. Web UI and configuration

Web UI is separated into these main sections:

- Status - general status reporting of the RSU, logging viewer, V2X traffic viewer
- Configuration - general configuration (e.g. IP settings, CMS connection)
- Application - application specific configuration (e.g. zones, traffic controller connection, message sender)
- Maintenance - FW update, general maintenance tools

The RSU web user interface is only available over **https** (TLS) on 443 port. Depending on the configuration this might require valid client certificate installed in the browser.

4.1. Status

4.1.1. Operating state

In this screen general state of the RSU can be checked. Internal components are listed together with their state (OK, Warning, Error, Off).

To further investigate you can navigate into the corresponding settings in the other parts of the UI.

4.1.2. Monitor

Monitor is used to inspect what messages are being received/transmitted by the RSU in the V2X environment. The switches can be used to select which messages should be reported. For dropped messages the RSU also tells reason on why they were dropped.

Filter logs feature can be used to filter only lines containing certain strings in the real time. This can be used for example to see messages coming only from certain OBU with filtering for MAC address.

4.1.3. Statistics

On the statistics page the RSU displays message counters per channel and network layer.

Network layers description:

- DRV - driver level
- MAC - 80211 level
- NET - ieee1609 level
- APP - messages that are being processed by the internal components in the RSU

Column description:

- Tx - packet was processed by the layer and forwarded to next layer (for DRV layer the packet was sent over radio)
- Tx Errors - there was a problem with a packet and it was discarded on this layer - it will not be forwarded further.
- Rx - packet was processed by the layer (for DRV layer the counter can be read as received packets)
- Rx Errors - there was a problem with a packet (for example it was malformed or signature was not corrects) and it was dropped on this layer - it will not be forwarded further.

On the *Rx* the packet flows from DRV into the APP layer, for the *Tx* the other way around. Note that if no application inside of RSU is interested in certain types of packet, they might not be accounted for in APP level, since they are not forwarded to improve performance of the system.

More detailed inspection of the communication on the V2X network can be conducted on the *Status-Monitor* page in the Web UI.

4.1.4. Logger

Logger page is used for inspecting general logs on the RSU. **Filter logs** functionality can be used to filter the logs on the fly to inspect only lines containing (or lines not containing) certain strings.

With the settings button logging levels for specific components can be changed.

The **Clear** button will clean in-browser cache and does not affect the logs stored on the RSU.

For exporting the logs use the **Export logs** feature that can be found in Maintenance section of the UI. The **Export logs** functionality will provide with an archive with logs and parts of the configuration that is helpful with investigation when irregular behavior is detected on the RSU.

4.2. Live Map

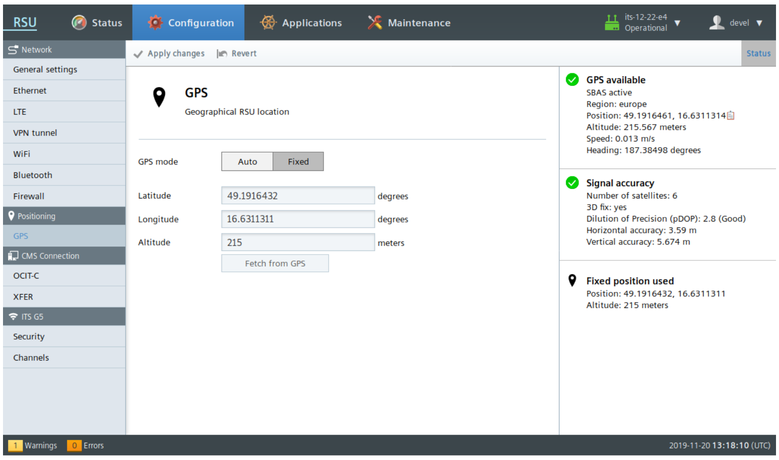
Live Map page will show you the realtime situation of the RSU. This can be used to troubleshoot RSU use cases and verify the range from which RSU is receiving messages from OBUs.

Available layers:

- RSU position
  - Blue RSU icon - GPS position
  - Gray RSU icon - fixed position (if defined)
- RSSI heatmap
  - Shows the areas from which has the RSU received CAM messages
  - Can be used to determine the coverage from which the RSU receives messages
  - The are where messages from RSU are received by OBUs will be similar based on the performance of the antennas of OBUs
- Zones
  - Shows the zones defined on the RSU
- Vehicles
  - Displays incoming CAM/BSMs in the realtime
- MAP
  - Displays the MAP topology as is being sent to the OBUs
- SPAT
  - Displays the outgoing SPAT messages

4.3. Configuration

Generally the configuration screens are separated into configuration part (left) and status part (right).



GPS

Geographical RSU location

GPS mode: Auto [✓ Fixed]

Latitude: 49.1916432 degrees

Longitude: 16.6311311 degrees

Altitude: 215 meters

GPS available
SBAS active
Region: europe
Position: 49.1916461, 16.6311314
Altitude: 215.567 meters
Speed: 0.013 m/s
Heading: 187.38498 degrees

Signal accuracy
Number of satellites: 6
3D fix: yes
Dilution of Precision (pDOP): 2.8 (Good)
Horizontal accuracy: 3.59 m
Vertical accuracy: 5.674 m

Fixed position used
Position: 49.1916432, 16.6311311
Altitude: 215 meters

2019-11-20 13:18:10 (UTC)

Figure 1: Configuration page example

4.3.1. Network

- ETH0
  - Default settings: 172.24.5.254/24 and DHCP client running
- ETH1
  - Default is in bridged mode (with WIFI if that is enabled) + DHCP server
- Bridge
  - Default IP settings is 10.0.0.1/24
  - DHCP server is running

By default the ETH1 and WIFI are in bridged mode and DHCP server where is enabled.

> Subnet 192.168.1.0/24 shall not be used as it is dedicated to the communication with modem.

4.3.1.1. General settings

In this page you can configure general network settings such as hostname, time server address, bridge settings and DNS settings.

DNS settings can be used to specify which DNS servers should be used to subdomains (for example you can specify that for custom.city.com based domains 192.168.0.1 DNS server should be used, for others the default one will be used).

In DNS settings you can also set static DNS records.

> In case that RSU is using LTE modem, subnet 192.168.1.0/24 shall not be used by any other network interface.

4.3.1.2. Ethernet

In Ethernet settings you can change the settings for two network interfaces. RSU allows you to configure IP or enable DHCP client.

4.3.1.3. LTE

If RSU is equipped with a modem, you can configure APN and PIN on this page. In case that the SIM card becomes locked as a result of incorrect PIN, RSU will prompt you to unlock it.

Currently used LTE modules are:

- TOBY-L210 for EU deployments
- TOBY-L201 for US deployments

4.3.1.4. VPN tunnel

RSU supports being connected to two different VPN networks at the same time (for example: CMS and controller). RSU accepts common OpenVPN configuration files. The main configuration file has to be named openvpn.conf.

RSU will also accepts a zip file containing the configuration, certificates and private key. This zip file may have following structure:

- ca.crt - certificate authority certificate
- client.crt - client certificate signed by certificate authority
- client.key - client public key
- ta.key - TLS authorization key
- openvpn.conf - openvpn configuration file (this name is mandatory and must be in lower case)

The configuration for OpenVPN can be provided by:

- Yunex engineering department - in case we are providing you with a VPN solution.
- Your VPN service provider - in case you are using 3rd party company for that.
- Yourselves - in case that you are maintaining your own VPN server.

Only TUN networks are supported.

> If more than one OpenVPN client is to be used, make sure to include `nobind` directive to prevent OpenVPN clients from competing over one port (alternatively you can specify desired port with `lport` directive). See the OpenVPN documentation for more details.

Example openvpn.conf file:

```
client
remote VPN_HOSTNAME.domain.com 70000
dev tun
proto udp

# RSU will automatically change the paths to match
# ones in the RSU file system
ca /var/etc/openvpn/tun0/ca.crt
cert /var/etc/openvpn/tun0/client.crt
key /var/etc/openvpn/tun0/client.key

nobind
persist-key
persist-tun
compress
resolv-retry infinite
keepalive 10 120

verb 3
```

```
mute 5

# Security settings
remote-cert-tls server
cipher AES-256-GCM
auth SHA512
tls-cipher "TLS-DHE-RSA-WITH-AES-256-GCM-SHA384"
tls-auth /var/etc/openvpn/tun0/ta.key 1
```

RSU will ignore options that could be used to undermine its own security, for example the `route-up` option is ignored.

4.3.1.5. WiFi

In this page the WiFi settings can be configured. The WiFi in the RSU is always connected to a bridge and therefore has active DHCP server for WiFi.

User can configure SSID, password (RSU always uses WPA2-PSK) and a channel.

4.3.1.6. Bluetooth

Bluetooth settings allows you to configure pairing key and allows to toggle the discoverability mode of the RSU. Bluetooth is connected to a bridge mode.

4.3.1.7. Firewall

On Firewall page the base firewall ruleset can be configured. This will determine the basic rules for accessing the web UI, XFER and SSH. Other interfaces are opened by the applications and are displayed in the “Dynamic firewall rules” section. You can inspect the complete firewall ruleset with the “Show complete firewall ruleset” button.

> RSU uses nftables as its firewall and advanced user can provide its own basic configuration. Use the “Default” firewall as a base, but make sure know what you are doing.

SSH interface can be activated for a short time on this page.

> SSH server is configured to disconnect you after 15 minutes of inactivity from client side. If this is undesirable, `ServerAliveInterval 30` can be added to the client SSH configuration.

4.3.2. Positioning - GPS

On this page you can configure the RSU position. Various statistics are available in the status part of the page.

In **Auto** mode the RSU gets its location from the GPS chip. That can cause RSU to move slowly around due to accuracy of the GPS chip. **Auto** mode also allows user to choose between **Automotive** and **Stationary** GPS model for corresponding use cases.

In **Fixed** mode you can configure a fixed position for the RSU. You can also use the real GPS to “freeze” the RSU position via the “Fetch from GPS” button.

> Even in fixed mode the RSU needs a valid GPS signal to synchronize its clock. Clear access from the GPS to the sky has to be ensured.

4.3.3. CMS connection

RSU supports various protocol for Central Management System connection.

4.3.3.1. OCIT-C

On the OCIT-C screen you can configure the RSU to connect to the CMS server using the OCIT-C protocol.

The CMS server can then:

- instruct RSU to send out DENM and IVIM messages
- receive short and long term traffic statistics from configured zones via the Zone aggregation functionality
- receive DENM messages messages via the DENM forwarding
- receive RSU detailed status
- update RSU

Which zones shall be used for traffic statistics can be configured in zones settings in the application section of the Web UI.

> The CMS address should be only hostname of the CMS.

> The common settings is: Username is Admin, Password is left empty, and the IP should be the one of the Docker host. The answer can be obtained from your CMS administrators.

4.3.3.1.1. Compatibility notes:

- CMS 8.0 - RSU 1.2.1 - 1.4.x
- CMS 8.1 - RSU 1.3.2 - 2.0.x
- CMS 8.3 - 2.0.x

4.3.3.2. XFER

The XFER interface settings consist of IP authorization settings. Authentication for XFER is done via the client certificates as XFER is based on secured web sockets.

> For example to allow access to RSU from 192.168.0.1 only, create a rule for `192.168.0.1` with mask `255.255.255.255`. To allow access from the whole 192.168.0.1/24 subnet, create a rule for `192.168.0.1` with mask `255.255.255.0`.

More about XFER protocol can be found in *ESCoS Roadside Unit - ITS XFER Gateway Interface Specification* document.

4.3.3.3. SNMP

SNMP page contains general settings for SNMP protocol. Users, their passwords and rights can be configured here. More about XFER protocol can be found in *ESCoS Roadside Unit - SNMP Interface* document.

4.3.4. WAVE

4.3.4.1. General settings

On the General settings page you can configure various general DSRC settings.

PSID drop list allows you to add a list of PSIDs and all received messages with those PSIDs will be dropped during early stage of processing. PSID drop list values shall be in a comma-separated p-encoded hex format.

4.3.4.2. Security

On the Security page you can inspect the current state of the enrollment with the SCMS.

Explanation of the Statistics status:

- connect: number of attempts for communication with PKI
- fail: number of failed attempts
- connect: number of successful attempts

Message Statistics details:

- Sign success - number of successful sent signed messages
- Sign failed - number of failed attempts for sending signed messages
- Verify success - number of successful received and verified signed messages
- Verify failed - number of received messages where verification failed (inspect monitor)

4.3.4.3. Channels

On the Channels page you can see which channels are active on the RSU and see the MAC addresses for those channels.

4.3.5. LTE-V2X

On this page the user can monitor C-V2X PC5 status, view C-V2X device name and firmware version and edit `v2x.xml` configuration file.

The page is only visible if the RSU is equipped with the LTE-V2X module.

> Changing `v2x.xml` is not recommended. Powercycle is recommended after changing the `v2x.xml`.

4.4. Application

In this section of the web UI you can configure application specific settings and use cases.

4.4.1. Zones configuration

Zones in the RSU are generic tool to be used for various other use cases (for example traffic aggregation, traffic prioritization, …).

RSU supports at maximum 64 zones to be configured.

Three shapes of zones are supported:

- Circle
  - Specified with point, radius and direction of traffic it accepts
- Rectangle
  - Specified with two points, width and direction of traffic it accepts
- Cone
  - Specified with points, bearing, aperture, minimum distance, maximum distance and direction of traffic it accepts

> Minimal meaningful zone size can vary with environment around RSU that can affect OBU GPS accuracy. Always configure zones big enough with regards to expected GPS imperfections.

Zone is identified by its name. Using a good name will help to later assign zones in specific use case configuration task.

4.4.2. Message sender

In the message sender you can inspect messages that are being broadcasted from the RSU using the “store and repeat” mechanism. This is used for example by OCIT-C or **snd** command in XFER interface.

> RSU can be sending also messages that are not present in the message sender. For example SPAT messages are being in “immediate forwarding” mode.

Message sender web UI can be also used for sending handcrafted messages during for testing and validation purposes. New custom message can be added to message sender and can be also edited using the editor that is part of the UI.

> TIP: You can use the “Validate” button to check for validity of the messages and “UPER | XER” button can be used to convert between XER and UPER formats.

Message override section can RSU force RSU to use its own real values for the message instead of the data from the message (for example time and position).

> Loopback will send cause the message to be sent out over the radio, but also will be routed through RSU stack as it would be received from different sender. This can be used for simulating traffic and verifying the RSU function.

In case that the RSU is equipped with the C-V2X radio module, the target radio stack (DSRC / C-V2X) can be specified by adding key `"ll":NUMBER` to the DOT3 meta json in. Instead of NUMBER use:

- 1 - message will be sent via DSRC only
- 2 - message will be sent via C-V2X only
- 3 - message will be sent via both - DSRC and C-V2X (this is used if not specified otherwise)

Example DOT3 header: `{"ll":3,"chan":"CCH","datarate":6000,"priority":3,"psid":"20","security":{"cert":true`

4.4.3. Other applications

Other application are dependent on the licenses and application image being present on the RSU. They are described in separate documents.

4.5. Maintenance

Maintenance section contains various tools and system overview.

4.5.1. System overview

On this page you can inspect the versions of FW components installed on the RSU.

The most significant is the **Firmware** version.

With **Mode** you can verify that the RSU is in the **WAVE** mode.

RSU can be updated on this page by either drag&drop the file to a designated area or clicking at the area that will open a file picker dialog. RSU accepts both “.img” and legacy “.hex” images.

With this dialog RSU can be updated with:

- Bootloader image
- Core firmware image
- Application image
- Initial Provisioning - configuration image that resets the RSU into factory state.
- Delta Provisioning - configuration image that can change only parts of configuration while keeping other intact.
- LTE-V2X module firmware update

On RSU2X hardware you can also trigger configuration reset here.

4.5.2. System logs

This page serves for configuring and maintaining the logs on the RSU.

The **Export logs** functionality will provide with an archive with logs and parts of the configuration that is helpful with investigation when irregular behavior is detected on the RSU.

> When containing Yunex help desk, always try to provide the exported logs with your request.

Also all the logs can be deleted from the RSU on this page.

4.5.3. Ping

Allows you to test whether RSU can reach certain IP/hostname with ping command.

4.5.4. Route

Allows you to run `ip route get` command for a FQDN and inspect which route and interface RSU will use when sending packets to that FQDN.

4.5.5. Capture

Allows to record pcaps (tcpdump) of the C2X communication for later analysis in Wireshark. Recording will continue until either configured time limit is reached, no space is left on the device or recording was manually stopped from the Web UI.

> Pcaps may contain personal information and shall be handled accordingly.

5. Certificates & secure communication

To ensure security and confidentiality several security credentials are necessary to connect with the RSU.

This chapter lists all these credentials and provides the procedures, how they can be changed.

Date	Type	Description
VPN	TLS X.509	The RSU provides OpenVPN. Especially connections via LTE should only be established via a VPN tunnel. Therefore a suitable OpenVPN configuration has to be uploaded to the RSU
XFER	TLS X.509	The XFER interface runs over a TLS connection, which requires both client and server side authentication. Thus the client has to have a suitable TLS client certificate installed Service. XFER runs on port 3600.
GUI	TLS X.509	The Service GUI runs over TLS connection, which per default doesn’t require a client side certificate on port 443. For a higher level of security it is recommended to use client side authentication via certificates as well.
WAVE	IEEE 1609.2	The 1609 certificates for the WAVE communication are deployed via the SCMS. Predefined certificates can be uploaded to the RSU via XFER, OCIT or provisioning

6. Secure Configuration and Hardening

In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.

In other words, hardening includes all configurations and settings with the goal of:

- Reducing the opportunities to exploit vulnerabilities in software Minimizing potential methods of attack,
- Limiting the tools available for a successful attack,
- Minimizing the available rights following a successful attack,
- Increasing the probability of detecting a successful attack,

Hardening is intended to make it harder for cyber attackers to breach security barriers and increase the resilience of the device to withstand attacks.

The following hardening measures are highly recommended and should strictly be followed:

Category	**Measure**
Attack Surface Reduction	Disable unused physical interfaces such as WiFi, Bluetooth, LTE, RS232. Only enable if really necessary
Attack surface Reduction	Disable unused logical interfaces such as XFER, OCIT-C
Identity & Access Management	Change default password for WebGUI “admin”
Identity & Access Management	Passwords shall be generated and stored with a password manager like KeePass Passwords shall have a *quality* of at least: 60 bits for *normal* users, 90 bit for administrative users and wireless connections (such as WLAN)
Identity & Access Management	Always tunnel through connections to a back office through a VPN
Identity & Access Management	Use project specific firewall configuration, which only allows necessary ports and protocols
Identity & Access Management	Only enable necessary permissions for XFER clients

7. Specifications

7.1. RSU1 specifications

Description	Value
Output power (802.11p)	-10 to +23 dBm (ETSI Mask C)
Receiver Sensitivity (802.11p)	-97 dBm
Frequency Band (802.11p)	5.9 GHz
Security	HSM for signing of ITS-G5 messages and secure storage of private keys
GNSS	GPS/GLONASS/Galileo/BeiDou 2.0 m CEP position accuracy
Operating System	Linux
CPU	Dual-Core ARM-Cortex A9 @800MHz
Memory	1 GB RAM
Operating Temperature	-40°C to +74°C
Storage Temperature	-40°C to +85°C
IP rating	IP67
Power Supply	PoE+ (802.3at)
Power Consumption	Typ. 12W
Mounting	Mounting kit for wall or pole mounting
Dimensions	270 x 308 x 80 mm
Weight	4.1 kg (with default antenna set)

7.1.1. Connectivity

- 2 x 802.11p 5.9GHz
- 2 x 10/100 MBit Ethernet
- 1 x RS232
- 1 x 802.11 a/b/g/n WLAN
- 1 x Bluetooth 4.0
- 1 x LTE

7.2. RSU2X specifications

Refer to the RSU2X datasheet.

7.3. V2x Standards Conformance:

- IEEE 1609.2/3/4 - 2016
- USDOT 4.1
- SAE J2735, MAR 2016

Contact us

Managing Board

Markus Schlitt, Jan Villwock

Yunex GmbH

Otto-Hanh-Ring 6
81739 Munich
Tel. +49 89 636-00
Yunex.traffic.mobility@siemens.com

www.yunextraffic.com