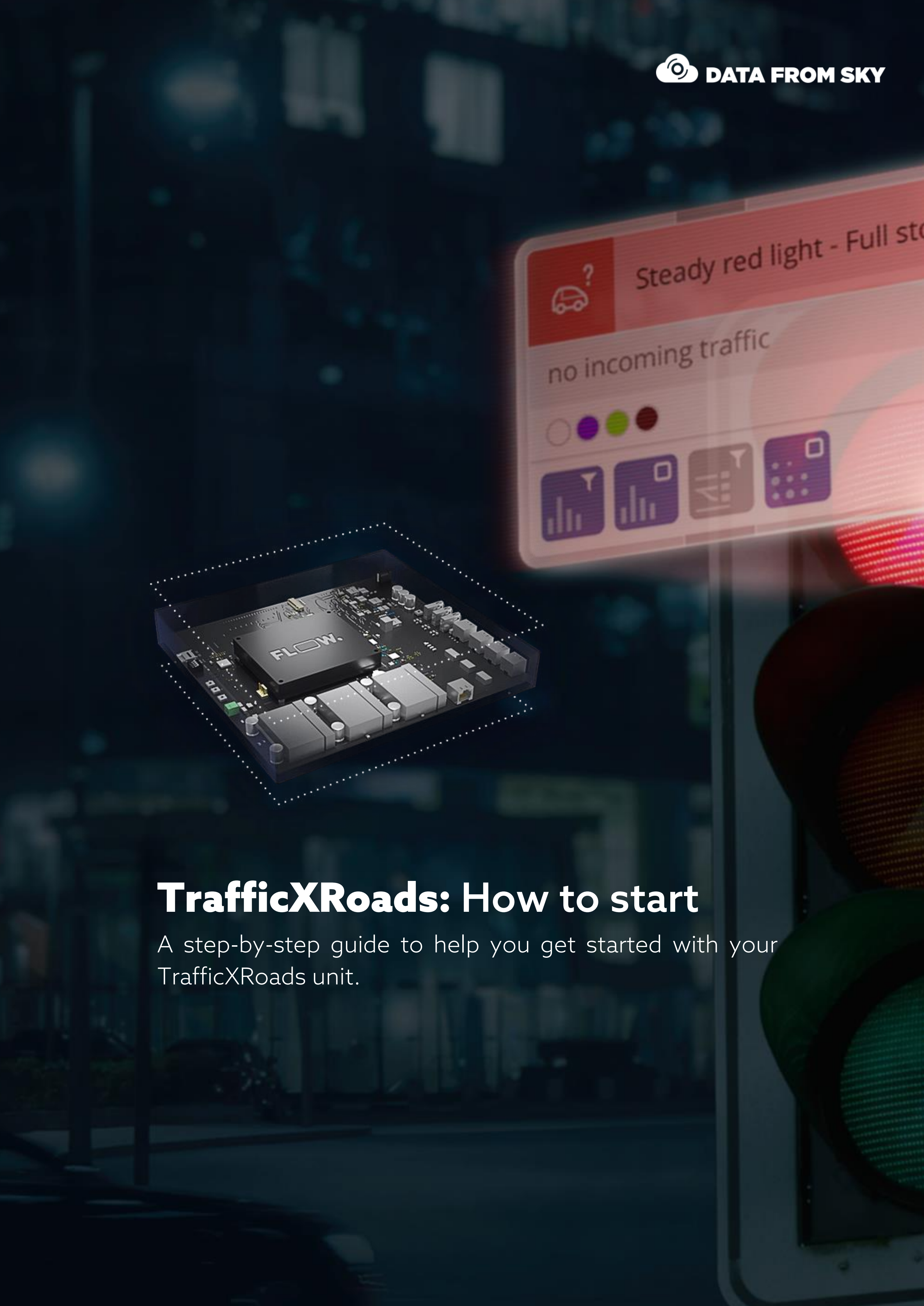
DATA FROM SKY



TrafficXRoads: How to start

A step-by-step guide to help you get started with your TrafficXRoads unit.

TrafficXRoads: How to start

A step by step guide to help you get started with your smart camera.

Thank you for purchasing the TrafficXRoads and joining the FLOW family of next-gen traffic analytic intelligence! You have purchased the most powerful and versatile traffic AI available – it is waiting in the box to be unleashed by your creativity.

We wish you an exciting journey towards a smoother and safer traffic of tomorrow. Let the traffic FLOW.

On behalf of the whole DataFromSky team

David Herman, CEO

Contents

Contents 2
Introduction 3
Quick start 4
Front panel...5
Rear panel 6
Carrier Board 7
Mounting.. 8
System web interface and network settings 10
FLOW – connect and define traffic analytics...14
Detection of traffic events 18
Reducing latency..31
More about FLOW framework...35
Conclusion 37
Technical specification 38

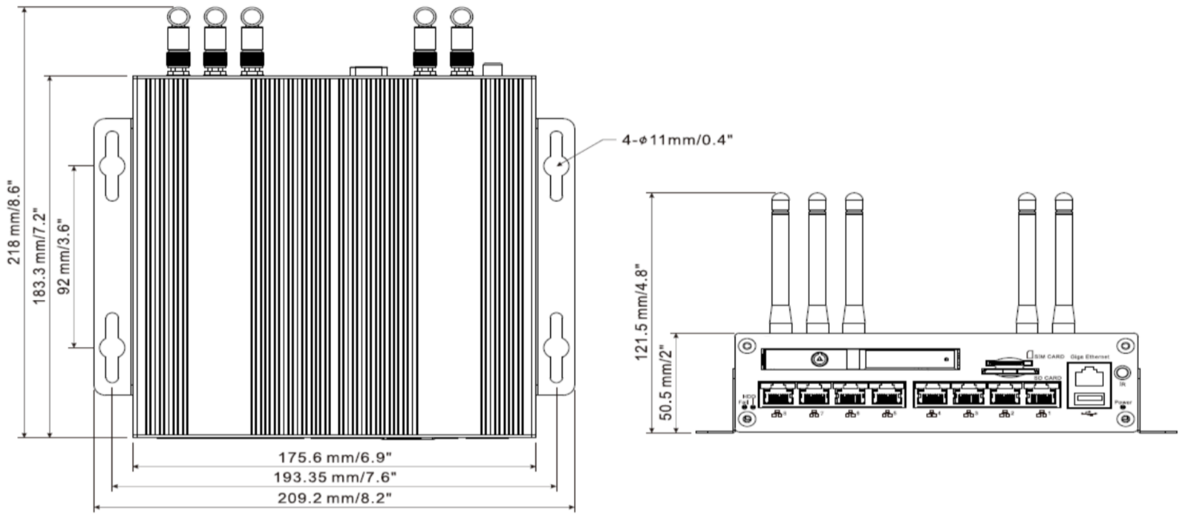
Document version: 20221103

Introduction

TrafficXRoads unit is a video analytics embedded computer designed for real-time detection tasks for dynamic control of traffic light signalling and the collection of traffic data from IP cameras. It has an industrial NVIDIA processor, the Jetson NX that runs the AI-based detection and tracking algorithm which turns any video stream into high quality trajectory data about each road user. The system is powerful enough to analyse data from up to 6 connected cameras in real-time with an operating range of more than 80 meters. The highly optimized and fully configurable trajectory processing engine is able to evaluate dozens of detection tasks in each camera view in parallel.

Product applications:

- Traffic monitoring and control
- Traffic data collection
- Parking management
- Security



Quick start

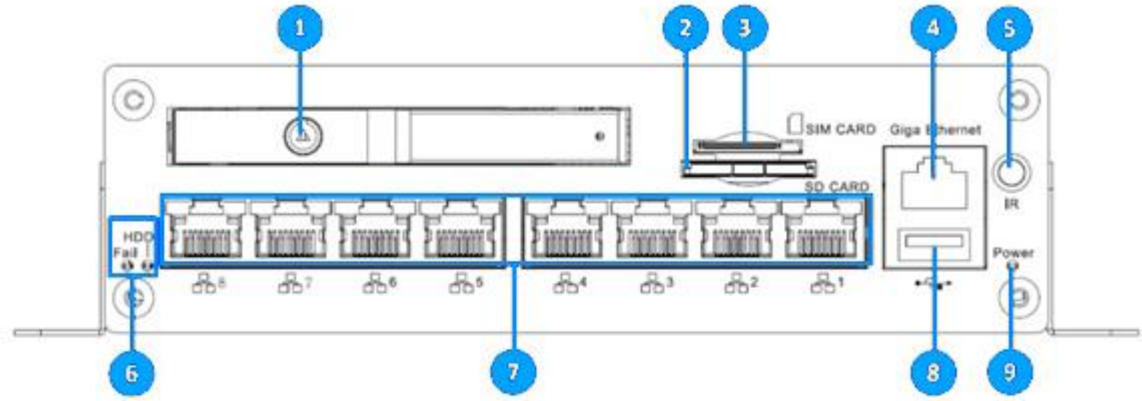
For start you need to connect:

- 12- 24V DC power source
    - minimum 65W (100W recommended)
    - red and yellow +
    - black -
- Modem / your computer (LAN/WAN)
- IP Camera (PoE Ports)

On your computer:

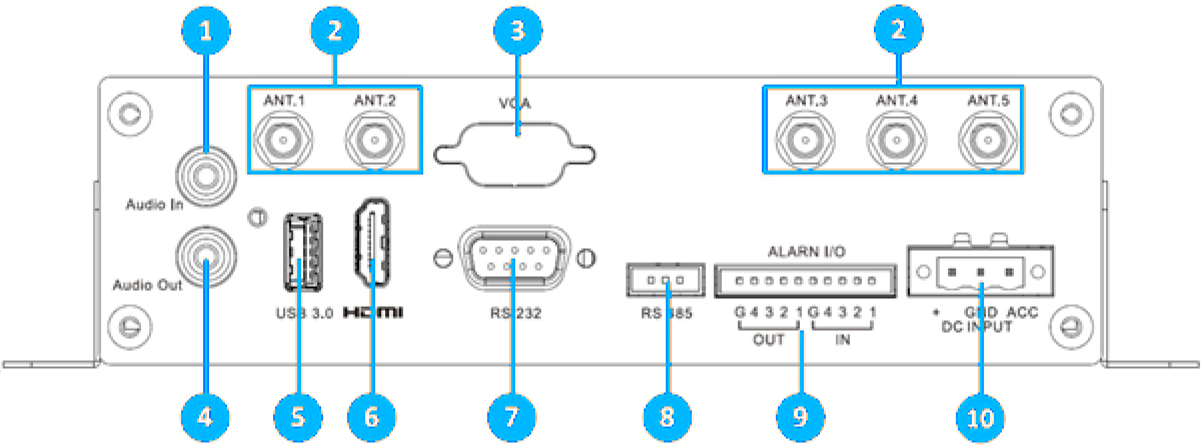
- Find IP of your TrafficXRoad
    - **Device default IP is 192.168.50.10**
    - In case of DHCP server you can search IP via MAC address that is on the top side of device
- Login to web-admin console on the device on https:\\deviceIP:8000 (https://192.168.50.10:8000) and configure as needed
  Default login is "admin" and password is "admin01"
- Start your FLOW and click on *Traffic survey or FLOW device live stream tile* on the launch screen
- Connect via IP address
    - Default login is "admin" and password is "admin"
- Add cameras, interfaces and configure the analytics

Front panel



No.	Name	Description
1	**SSD Key Lock**	Lock and unlock the SSD tray (see 2.3 SSD Installation).
2	**SD Card Slot**	Insert a SD card to the card slot.
3	**SIM Card Slot**	Insert a SIM card to the card slot.
4	**LAN/WAN**	One 10/100/1000 Base-Tx Ethernet ports for connecting to the network
5	**IR**	This function is currently reserved.
6	**LED Indicator**	HDD: HDD LED indicator. Fail: System Fail LED indicator.
7	**PoE Ports**	PoE ports (10/100 MbE, total 75W) for connecting to the IP cameras or other PoE devices.
8	**USB2.0 USB2.0 port.**	USB2.0 port.
9	**Power Indicator**	Power LED indicator.

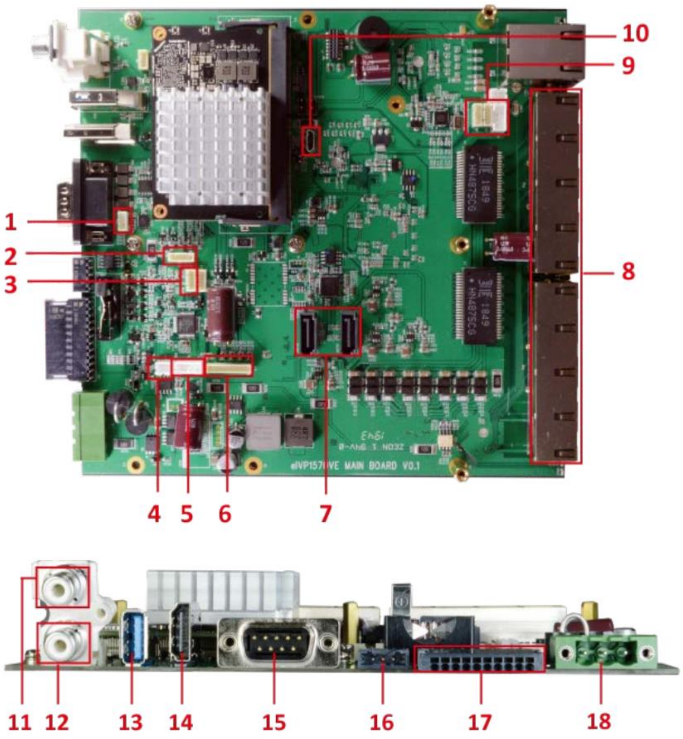
Rear panel



No.	Name	Description
1	**Audio Input**	Connects to audio input devices, such as microphones. Note that the microphones with a (built-in) amplifier and external power supply are required.
2	**Antenna**	Connects the antenna to the AI mobile NVR for 3G / 4G / WiFi / GPS functions
3	**VGA Port**	This port is currently reserved.
4	**Audio Output**	Connects to an audio output device, such as speakers. Note that the speakers with a (built-in) amplifier and external power supply are required.
5	**USB3.0**	USB3.0 port.
6	**HDMI Port**	HDMI display output.
7	**RS-232 Port**	COM port for RS-232.
8	**RS-485 Port**	COM port for RS-485.
9	**Alarm IO**	Provides 4 alarm inputs and 4 alarm outputs.
10	**DC Power Input**	Connecting to the power source

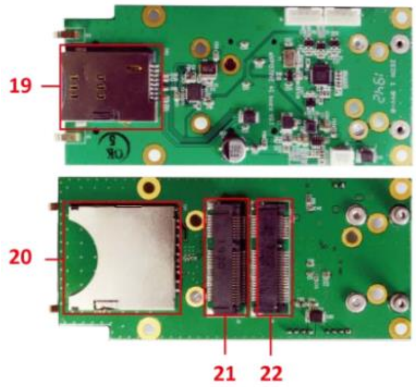
Carrier Board

Main board



Power Board

IO Board



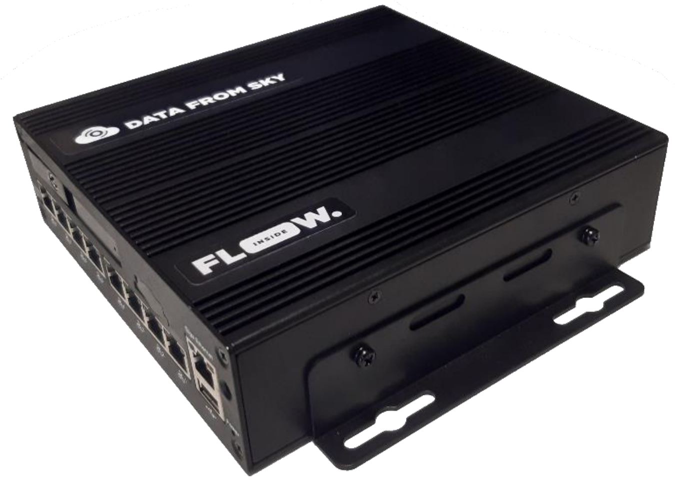
No.	Name	No.	Name
1	Console	12	Audio In
2	VGA	13	USB 3.0
3	HDDD Thermal Sensor	14	HDMI
4	HDD Heater (Reserved)	15	RS232
5	HDD Power	16	RS485
6	Video In / Camera Power	17	Alarm IO (4-input, 4.output)
7	SATA Port x 2	18	Power In
8	10/100 Ethernet PoE Port x 8	19	SIM Card slot
9	USB Port	20	SD Card slot
10	OTG	21	3G, 4G
11	Audio Out	22	GPS

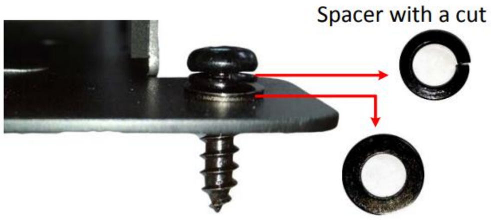
Dimensions (W x D x H)
Main Board: 170 x 179.3 x 35 mm / 6.7" x 7.1" x 1.38"
Power Board: 30.1 x 98 x 25 mm / 1.19" x 3.85" x 0.98"
IO Board: 45 x 98.3 x 18 mm / 1.77" x 3.87" x 0.71"

Mounting

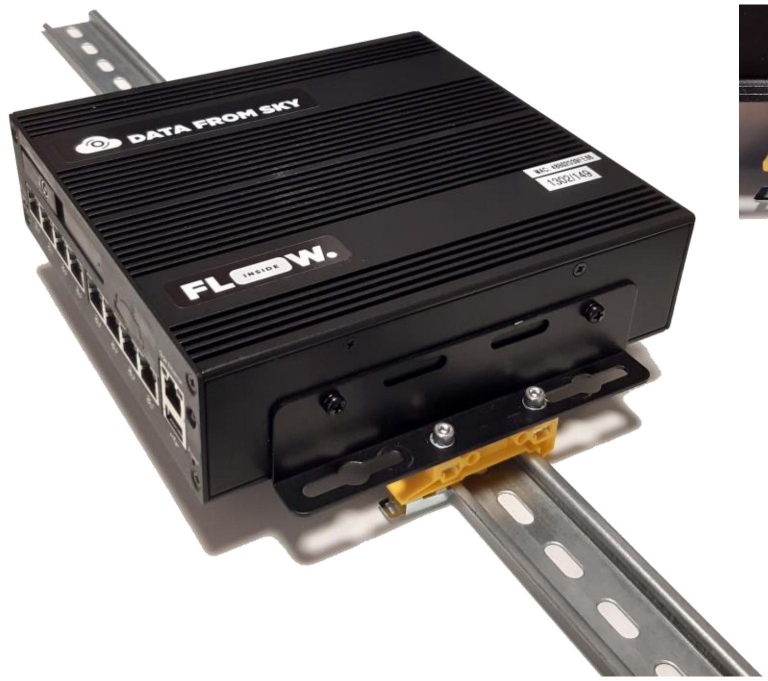
TrafficXRoad is possible to screw it via L – bar or attach on DIN rails.

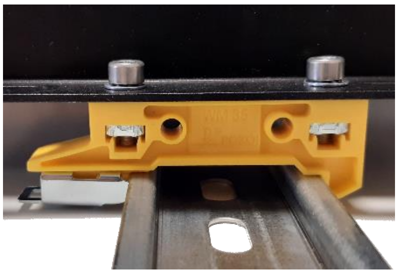
Conection via screw





Conection via DIN rails





Field installation

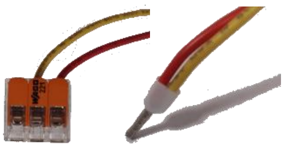
Power source

TrafficXRoads is powered by 12-24 DC power source. Unload device needs minimum 65W and every camera you connect use 5W – 15W extra power. We recommend you 100W power source.

Device is powered by 3 wires:

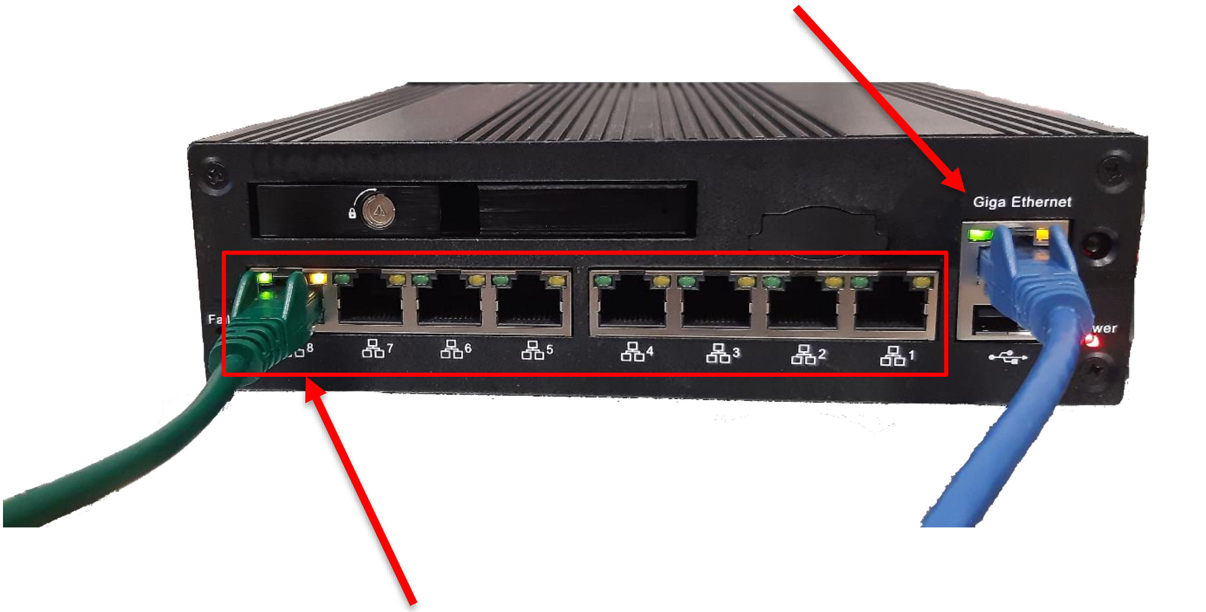
- Red (positive DC pole)
- Black (negative DC pole)
- Yellow (for turning on/off)

⚠ Yellow cable must be connected with red cable. The easiest way to do it is by WAGO clamp or double bootlace ferrule.



Connection

Connect TrafficXRoads to your computer or modem via LAN/WLAN



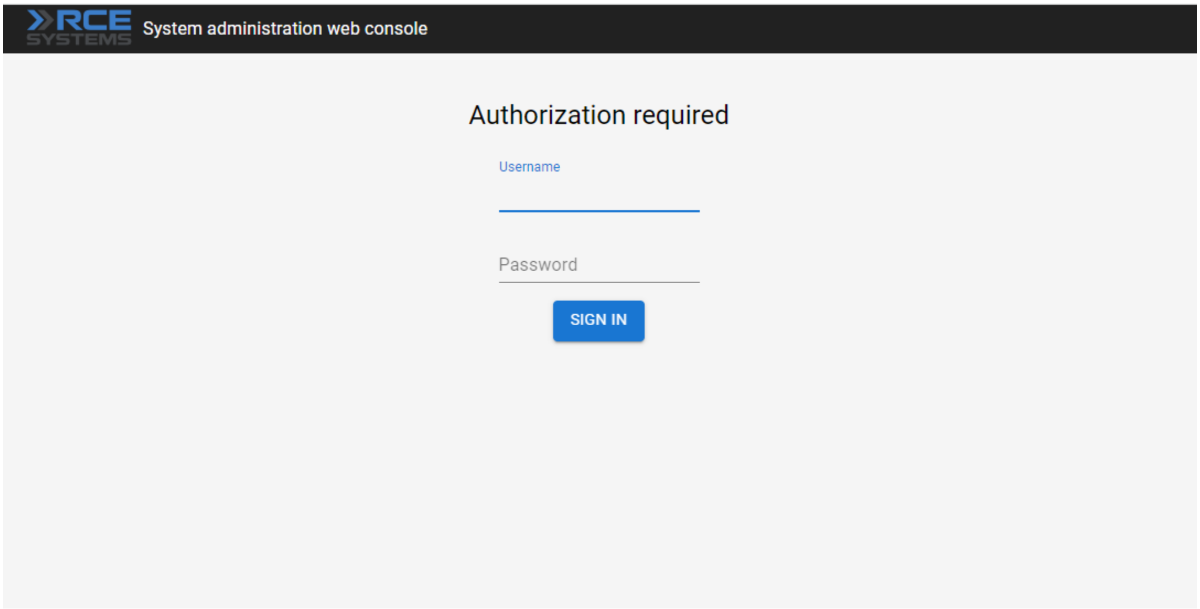
Connect up to 6 IP cameras via PoE ports (1-8). Beware of limiting the maximum power to 75 W.

System web interface and network settings

TrafficXRoads unit can be deployed in different scenarios and with different network setups.

The web administration interface allows you to configure network settings, VPN and do the reboot or factory reset of the unit. By default, the unit has static IP address 192.168.50.10 and the web administration interface can be accessed using the URL: https://192.168.50.10:8000 . To sign in, use the following default login credentials:

- **login: admin**
- **password: admin01**

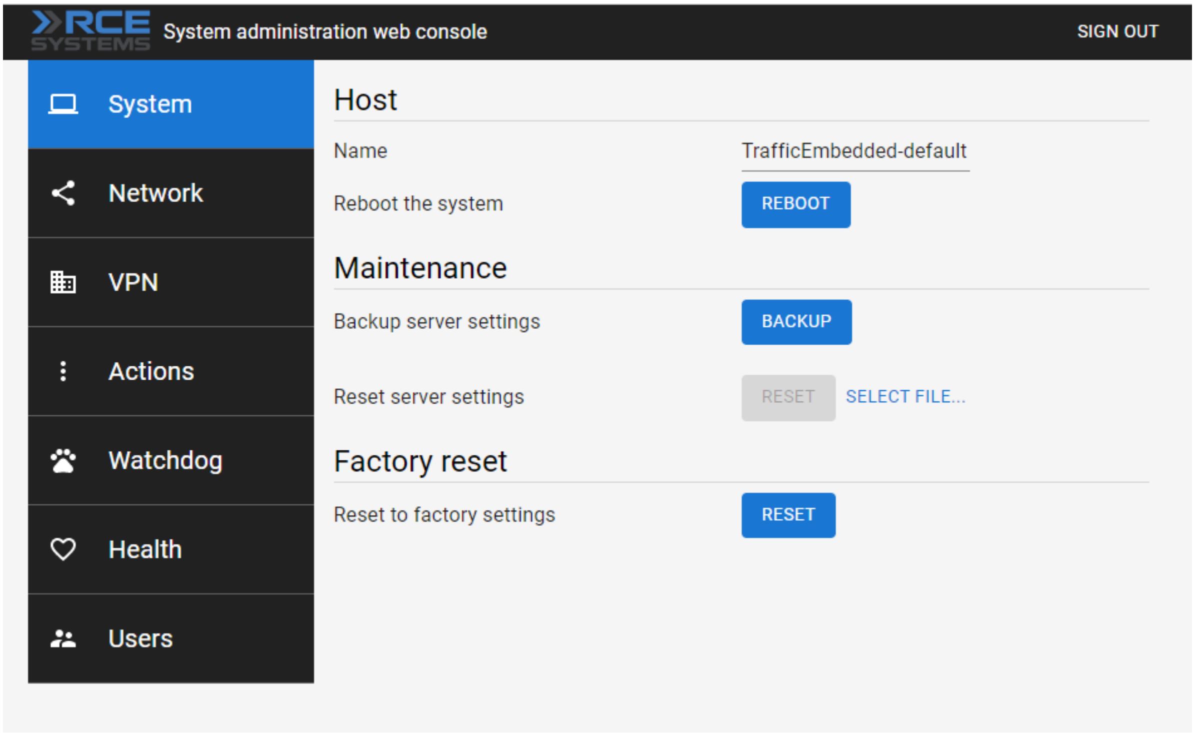


⚠ To be able to access to the web administration interface, your computer must be in the same network. Setup the appropriate IP address and subnet mask at your computer (for example 192.168.50.2/24 i.e. mask is 255.255.255.0).

⚠ All the configurations relating to this video analytic system are done using the FLOW interface, the desktop application FLOW Insights. To connect to the server, you need to know its IP address.

System settings

After a successful login to the web console, the first tab that you see is the *System* tab. On this tab, you can change the name of the unit, do a reboot, backup settings of the web console or restore them if needed. It is possible to do "factory reset" here and restore the web console settings into the default state (including default IP address, names and passwords).



Host

Name: TrafficEmbedded-default

Reboot the system

Maintenance

Backup server settings

Reset server settings

Factory reset

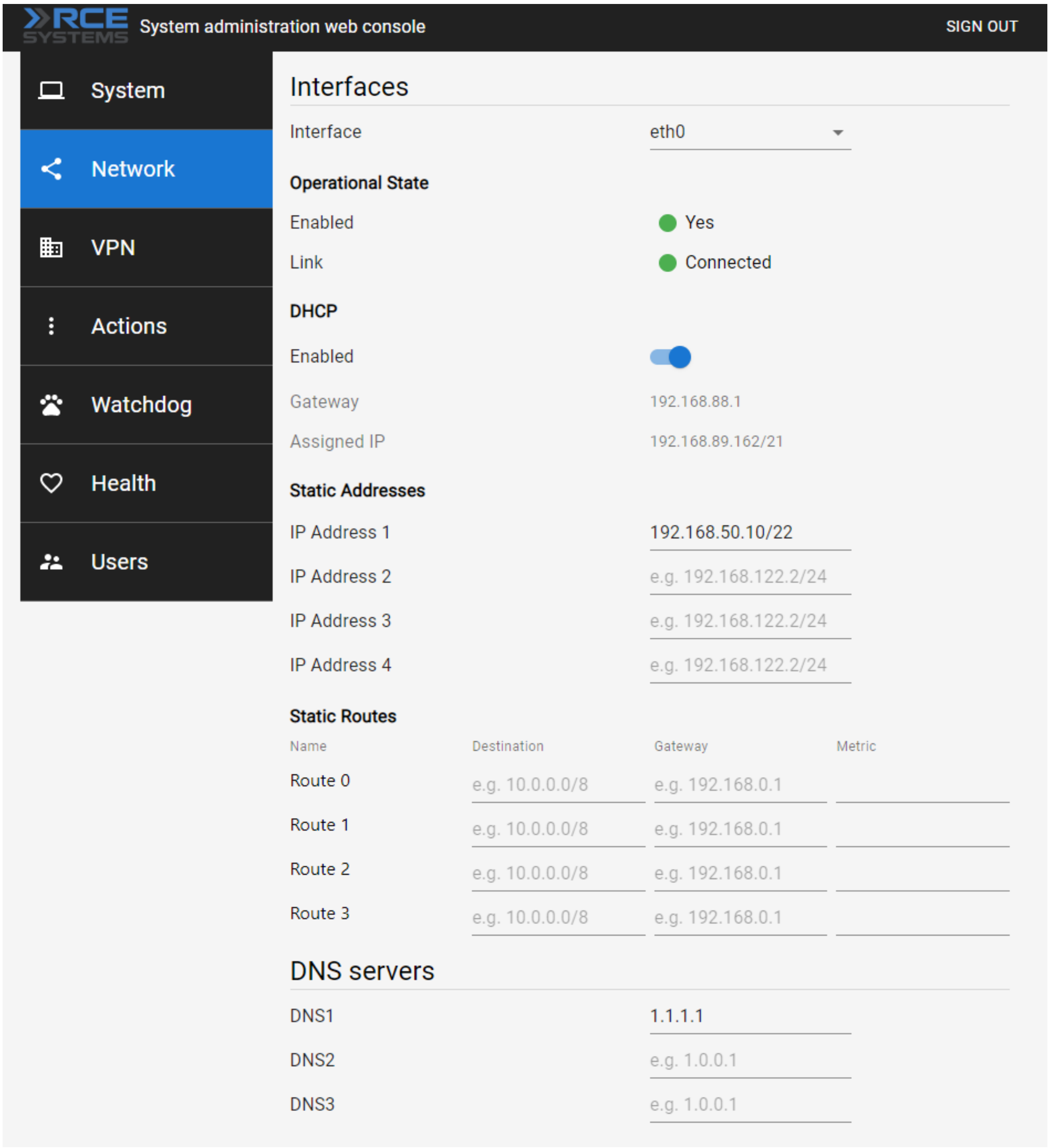
Reset to factory settings

Network settings

The set-up of the Ethernet interfaces is done in the *Network* tab. The unit has two physical Ethernet interfaces but both of them are under the same address (address bonding). In the web interface, the Ethernet interface is under the name *bond0*. In the top part of the tab you can see the chosen interface and its current state – whether the interface is enabled in the system and whether it is connected.

For the Ethernet Interface you can enable/disable the loading of IP address from the DHCP server and set up individual static IP addresses (up to 4) and DNS servers (up to 3).

⚠ We recommend using static IP addresses in real world deployments.


System administration web console
SIGN OUT

Interfaces

Interface: eth0

Operational State

Enabled: ● Yes

Link: ● Connected

DHCP

Enabled: on

Gateway: 192.168.88.1

Assigned IP: 192.168.89.162/21

Static Addresses

IP Address 1: 192.168.50.10/22

IP Address 2: e.g. 192.168.122.2/24

IP Address 3: e.g. 192.168.122.2/24

IP Address 4: e.g. 192.168.122.2/24

Static Routes

Name	Destination	Gateway	Metric
Route 0	e.g. 10.0.0.0/8	e.g. 192.168.0.1	
Route 1	e.g. 10.0.0.0/8	e.g. 192.168.0.1	
Route 2	e.g. 10.0.0.0/8	e.g. 192.168.0.1	
Route 3	e.g. 10.0.0.0/8	e.g. 192.168.0.1	

DNS servers

DNS1: 1.1.1.1

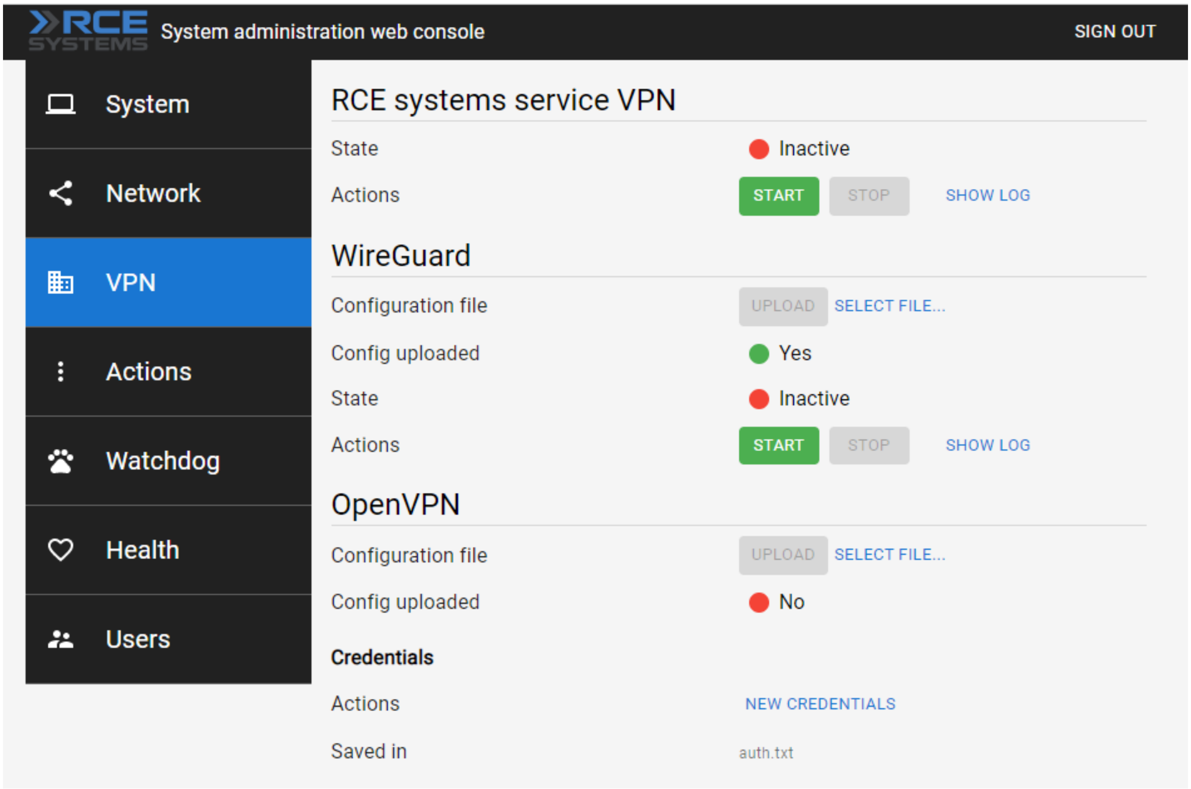
DNS2: e.g. 1.0.0.1

DNS3: e.g. 1.0.0.1

Virtual private networks

The unit has multiple preconfigured VPNs. These include a system service VPN using which the manufacturer can remotely access the unit. This VPN can be deactivated if needed. For the service VPN to work this VPN must be active, the unit must be connected to the internet and port 31228 UDP must be enabled (VPN connection to DataFromSky service VPN on 172.105.65.31).

The unit also has a Wireguad or OpenVPN client VPN network. These VPN networks can be configured by the user as needed. The configuration for both VPN networks is done by uploading a text configuration file according to the requirements of the specific VPN.



RCE systems service VPN

State ● Inactive

Actions START STOP SHOW LOG

WireGuard

Configuration file UPLOAD SELECT FILE...

Config uploaded ● Yes

State ● Inactive

Actions START STOP SHOW LOG

OpenVPN

Configuration file UPLOAD SELECT FILE...

Config uploaded ● No

Credentials

Actions NEW CREDENTIALS

Saved in auth.txt

FLOW – connect and define traffic analytics

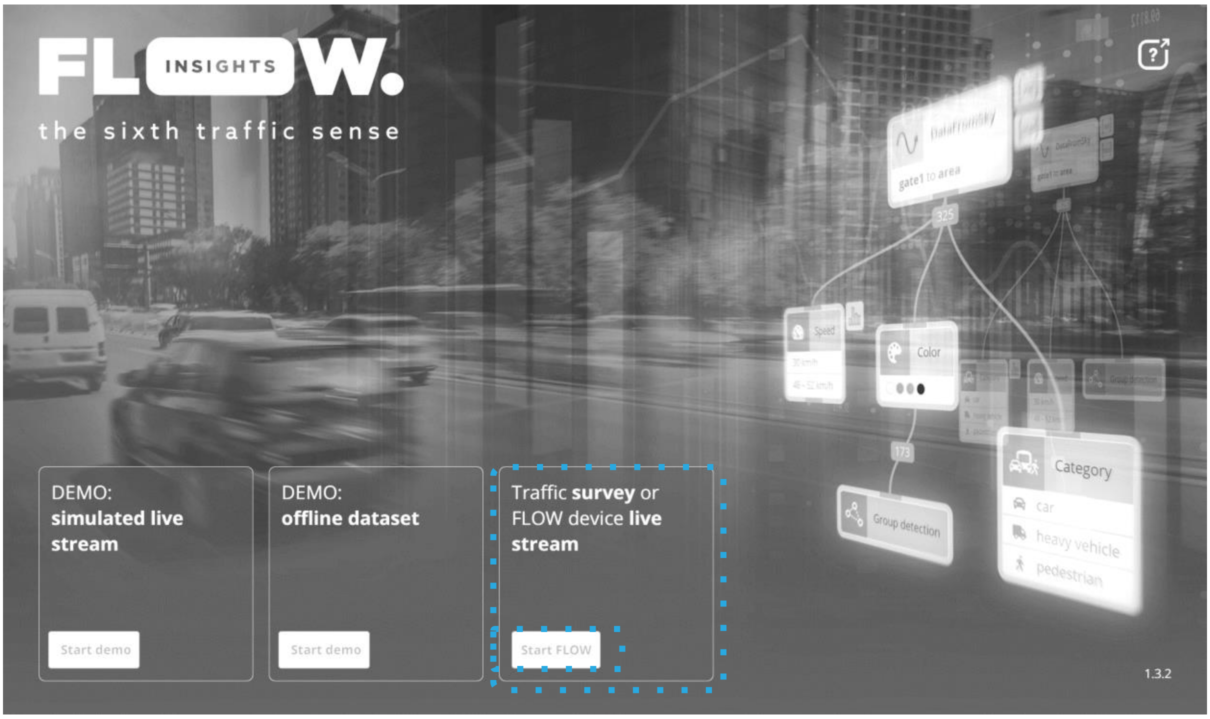
FLOW is an AI-based traffic video-analytical engine that runs on the unit. To configure various traffic tasks on the unit you need the FLOW Insights application which can be downloaded here: https://datafromsky.com/flow-versions/ There you should choose the correct version of FLOW Insights to match the version of the FLOW running on the TrafficXRoads device.

If you have the latest version of FLOW installed on your device, you can get the latest FLOW Insights version here:
http://www.datafromsky.com/download/flow/demokit/FLOW_Demokit.exe

How to connect to the unit with FLOW Insights

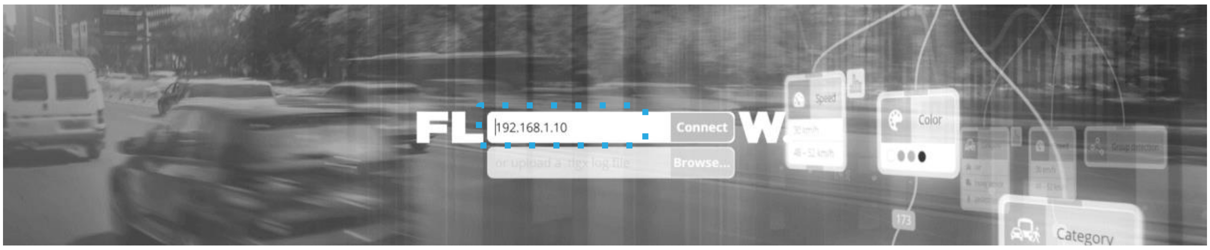
First, download the FLOW Insights desktop application and install it on your computer. It needs to be a 64-bit Windows operating system or Linux system (contact us for the Linux version). The device must be network accessible from your PC and you need to know its IP address (see the Network configuration section).

Launch FLOW Insights on your PC. Click on start FLOW in the third window on the bottom left named "Traffic survey or FLOW device live stream". In the first field, enter the unit´s IP address in the format xx.xx.xx.xx. Leave the second field empty and hit enter.



On the next screen, log in with the following credentials:

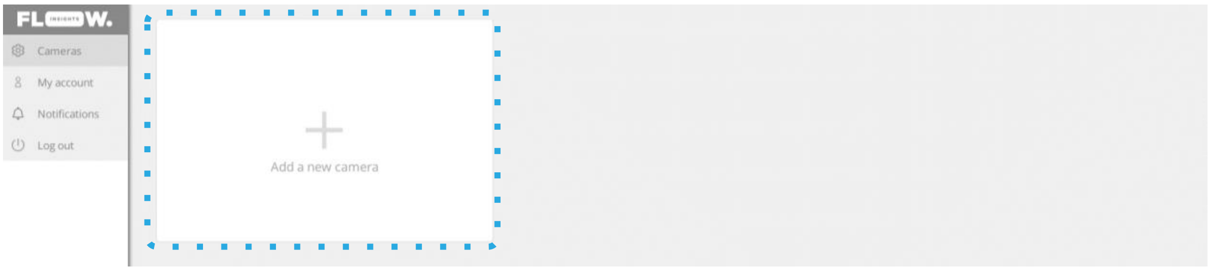
- **Login: admin**
- **Password: admin**



⚠ Note that you should change this password when you log into FLOW insights in the user settings section.

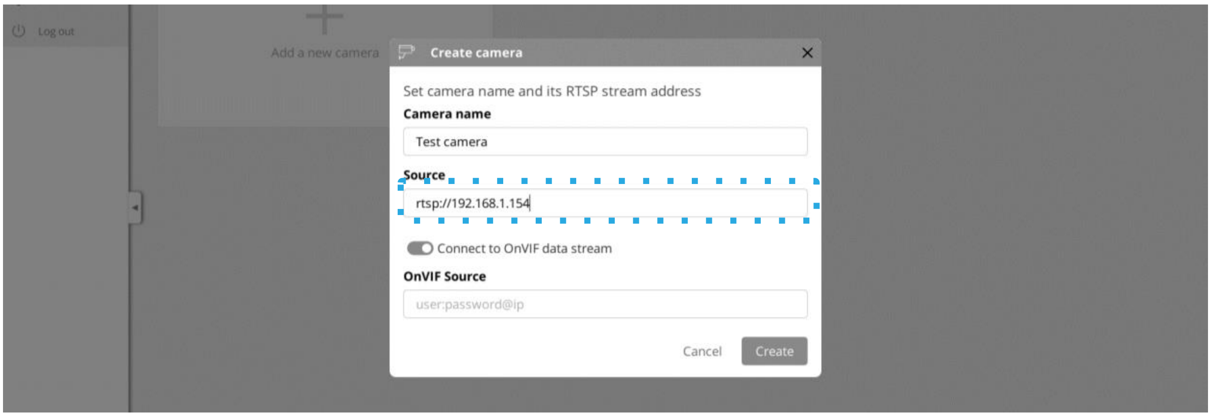
How to add the camera streams / analytics

We are now communicating with the TrafficXRoads unit and you can start configuring it. First, we need to add a source camera stream.



The camera video source stream address and optional OnVIF source address are formatted in the following way:

- Video source: **rtsp://user:password@ip:port/path/file**
- OnVIF source: **user:password@ip**



Set camera name and its RTSP stream address

Camera name: Test camera

Source: rtsp://192.168.1.154

Connect to OnVIF data stream

OnVIF Source: user:password@ip

The required information is camera specific and can be usually found in the camera user manual or at the web interface of the IP camera. The camera must be network accessible from the unit.

After you have filled out the dialog window and you click on the **Create** button the camera stream will be registered. The unit will then keep trying to establish connection with the camera. If the stream is opened, you will see a live preview image in the status panel of the camera and the status will change to **Running**. If the stream does not open, the status panel will signal an error in connection with the camera.

⚠ Unable to establish connection with the camera? Check whether the camera is network accessible from the unit. Also make sure that that the entered RTSP address is correct.

You can connect the other camera streams that you want to analyze with the particular TrafficXRoads unit the same way.

Maximum number of camera streams

The unit is capable to process a certain number of FPS based on the provided/selected video analytics engine.

FLOW distributes the processing power evenly between the analytics. If the sum of FPS from the different camera streams is bigger than the processing power capacity of the processing unit with the particular video analytics engine, then incoming image frames start to get dumped. If this would happen it does not necessarily mean that the traffic statistic would be negatively affected. This means the results would not be affected in case the evaluation FPS on the camera stream would be sufficient in regards to the specific monitored traffic scene. This would also hold true if the time interval between the evaluated image frames would be of such length, that the objects don't move by more than their "size" in the image. In case these conditions would not be met, the tracker might fail in connecting the detections because they would be too far away from the last detected position of the object in the image.

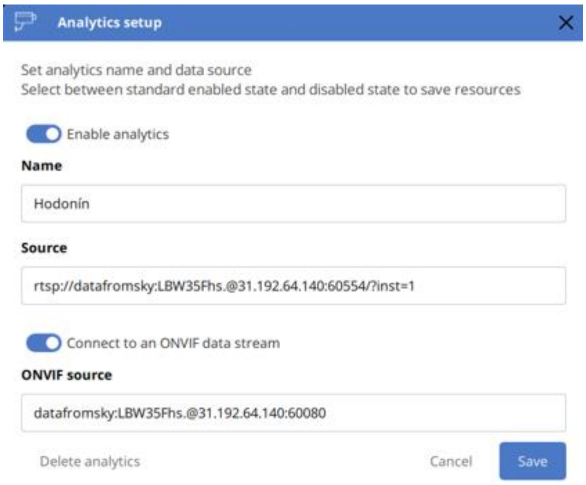
⚠ The maximum number of camera streams can be limited with a license. After reaching this number of streams, the unit will not allow you to add any additional camera streams.

Type of monitored environment and recommended minimum detection FPS

- Pedestrian movements – sidewalk, town square, bus stop (up to 7 km/h): 5 FPS
- Pedestrian and cyclist movements – bicycle path (up to 50 km/h): 10 FPS
- Traffic junction, city traffic (up to 75 km/h): 15 FPS
- Monitoring of district level road - (up to 150 km/h): 20 FPS
- Highway/motorway monitoring - (up to 200 km/h): 25 FPS

PTZ cameras with the ONVIF protocol support

FLOW framework has implemented PTZ camera support for cameras with the ONVIF S protocol. Thanks to this, you can define traffic analytics for the different PTZ camera positions. These analytics are then active only when the camera is in the defined position, otherwise they are inactive. In FLOW you can then create different analytical scenarios tied to the different PTZ camera views/positions from a single PTZ camera.



Analytics setup

Set analytics name and data source
Select between standard enabled state and disabled state to save resources

● Enable analytics

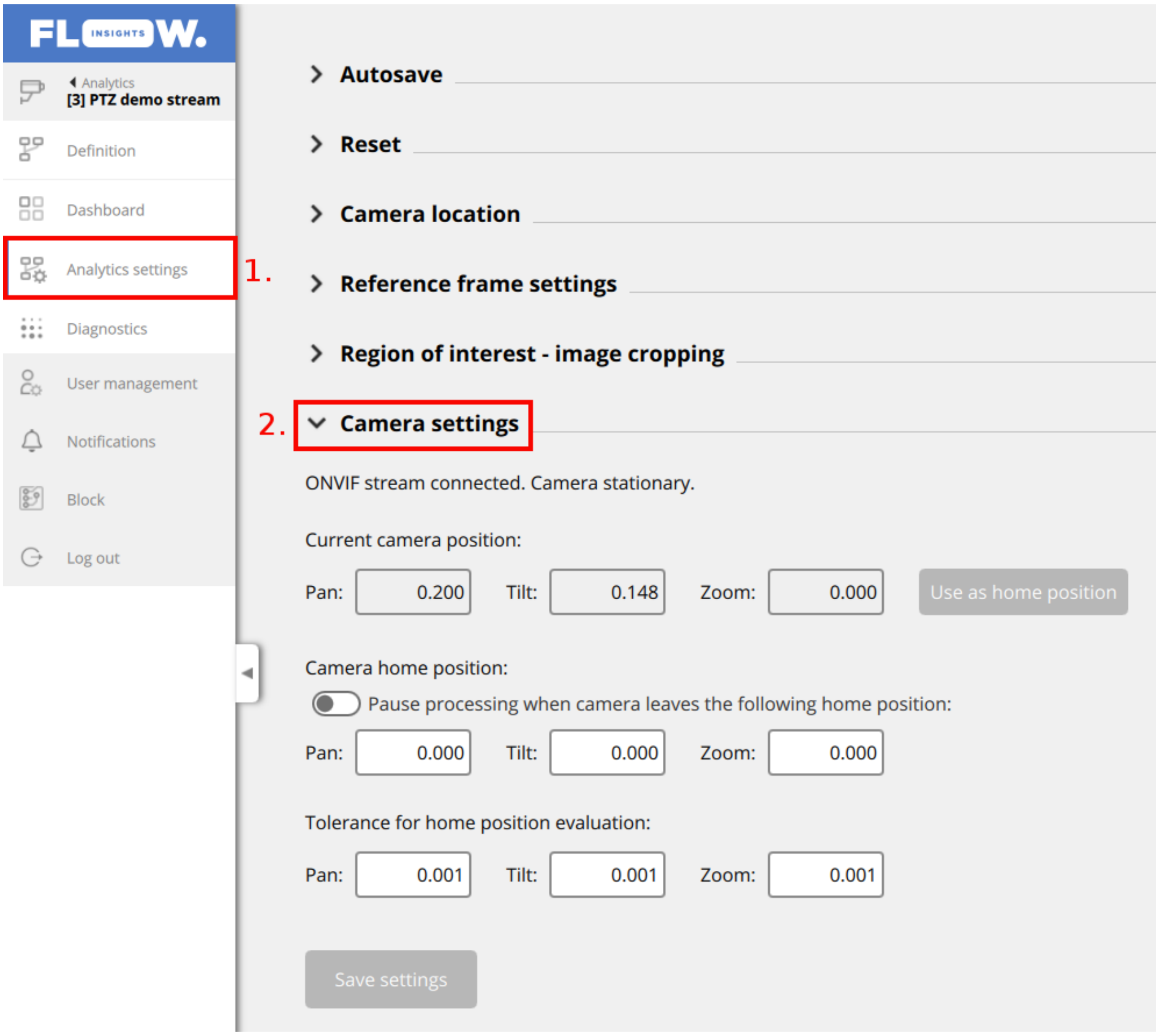
Name: Hodonín

Source: rtsp://datafromsky:LBW35Fhs.@31.192.64.140:60554/?inst=1

● Connect to an ONVIF data stream

ONVIF source: datafromsky:LBW35Fhs.@31.192.64.140:60080

If the PTZ camera has the ONVIF protocol, you can easily define the ONVIF address in the dialog for adding cameras. Next you need to go to the **Analytics settings** and set **Camera home position** including some movement tolerance in the **Camera settings** section. When the camera is in this position, the analytic will be running. In the moment when the camera leaves this position, no more trajectories will be received but the analytical engine will keep running. This means that all the expression, defined time modes etc… will keep being processed.



ONVIF stream connected. Camera stationary.

Current camera position:

Pan: 0.200 Tilt: 0.148 Zoom: 0.000

Camera home position:

○ Pause processing when camera leaves the following home position:

Pan: 0.000 Tilt: 0.000 Zoom: 0.000

Tolerance for home position evaluation:

Pan: 0.001 Tilt: 0.001 Zoom: 0.001

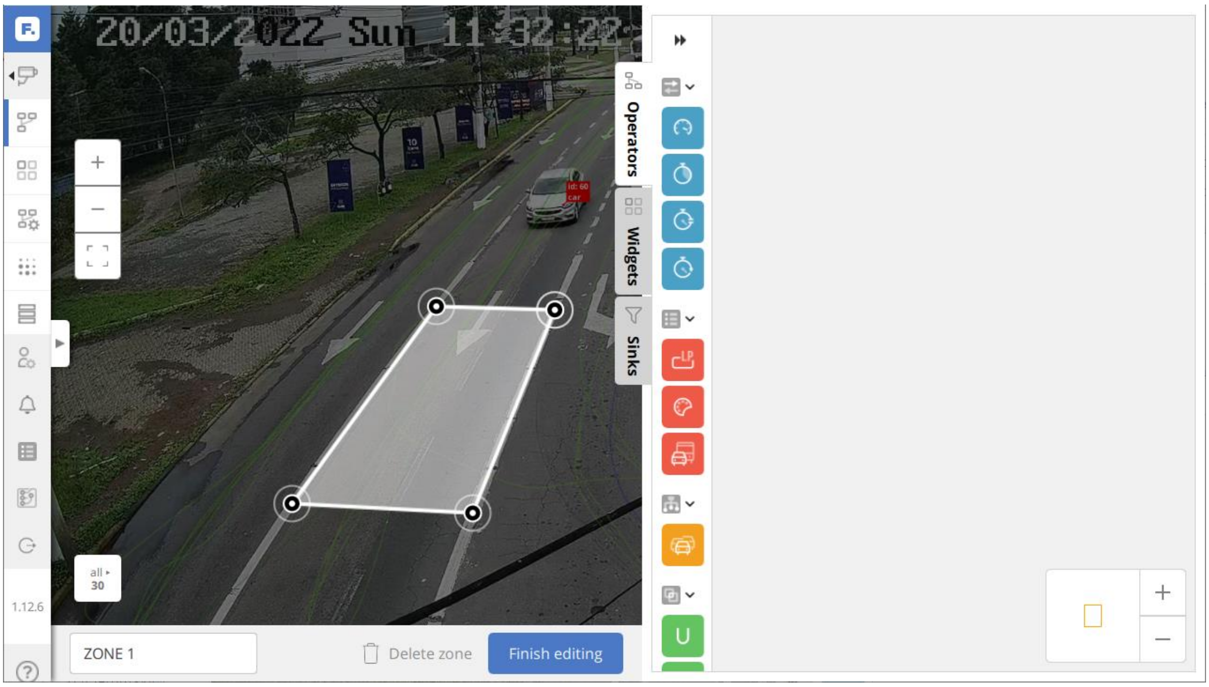
⚠ FLOW does not directly control the cameras but instead acts as a passive receiver of the camera position and zoom information. Based on this information the different analytics get activated to analyze the newly incoming trajectories.

Detection of traffic events

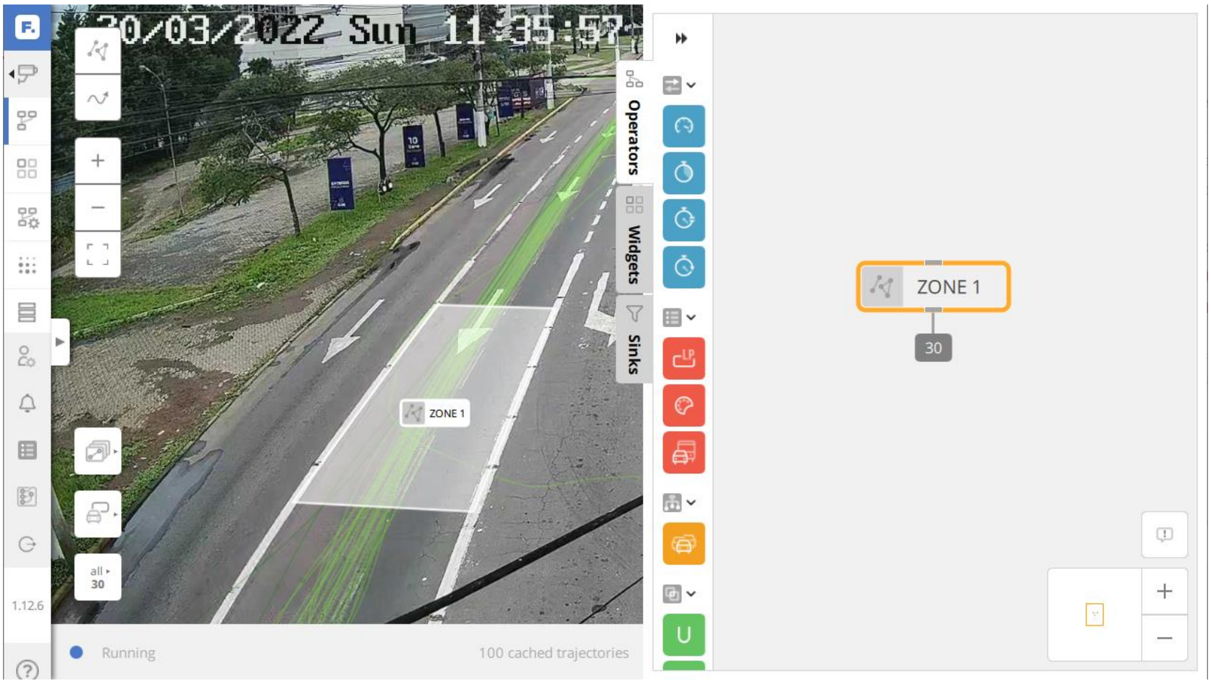
The FLOW framework enables you to define detections of very complex traffic events including interactions between objects. The generic FLOW description can be found here (https://intercom.help/datafromsky/en/collections/2019942-flow-real-time-monitoring), including different tutorials. In this document we will focus only on the selected basic tasks that can be used in detection systems for traffic control. The Definition of detection of traffic events is done in the **Definition** tab.

Basic object presence detection

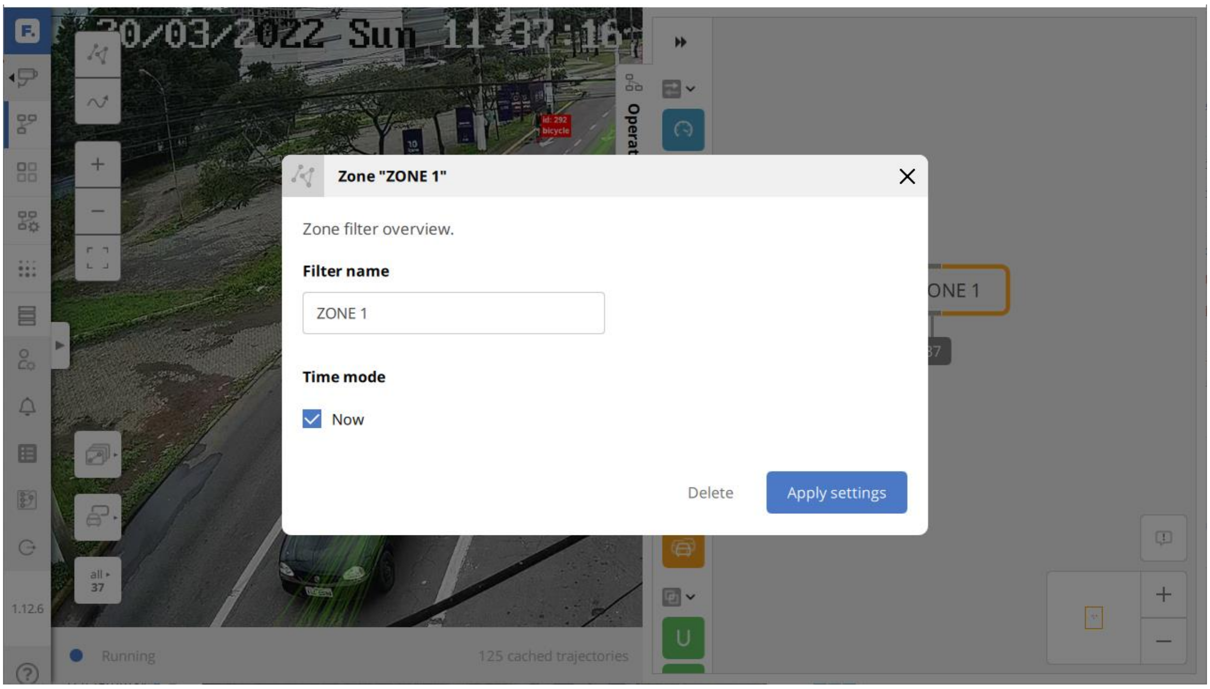
For the detection of object presence in real-time we can use the combination of **Zone** spatial filter in the **NOW** time mode. The **Zone** spatial filter can be combined with the **Category** filter, if you want to react to a presence of a specific object type. The number of detectors is not limited in the system. On the left side, pick the **Create zones/gates** tool and draw a zone in the area where we want to detect the vehicle presence. The system will automatically recognize whether it is a gate or a zone based on the drawn shape.



Next, we move the zone with the **drag and drop** technique into the right side panel, also referred to as workspace, which will instantiate it and the zone will start automatically filtering the trajectories from within the FLOW device cache.



For the zone to react only to the vehicles that are currently located inside the zone, we change it into the NOW mode. We do so by double-clicking the zone in the right panel which will open a dialog window where we can activate the NOW mode.



Zone "ZONE 1"

Zone filter overview.

Filter name

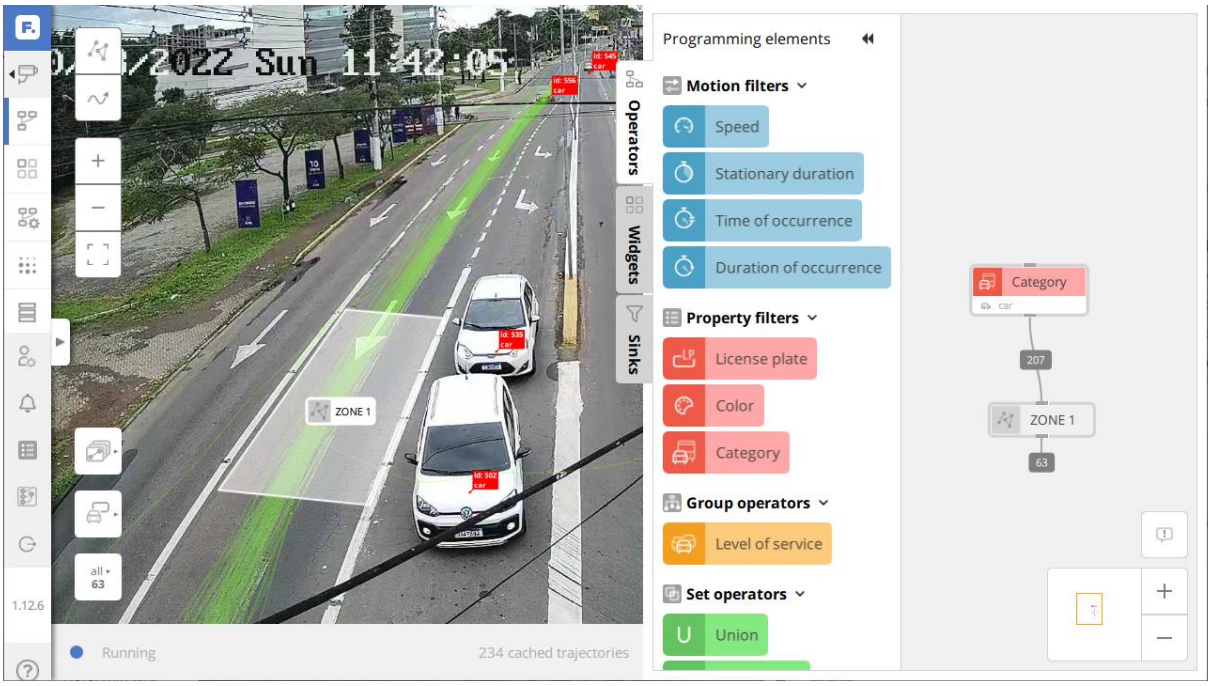
ZONE 1

Time mode

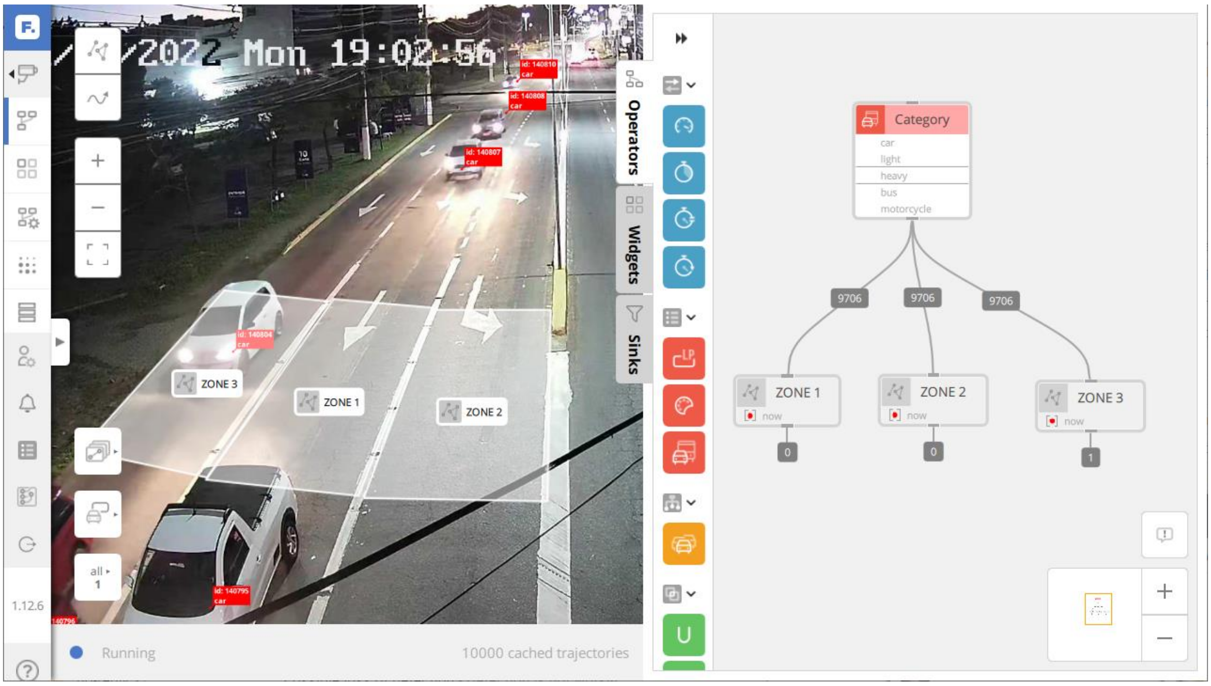
☑ Now

Delete Apply settings

After activating the NOW mode, you will see a number on the output of the zone that represents the current number of vehicles present in the zone. In this configuration the zone reacts to all objects that the system is able to detect.



If you need to set the zone to only detect object of specific categories, we place a category filter before it. This filter is located in the floating panel **Programming elements** in the **Property filters** section. Again, using the drag and drop technique we instantiate the filter and then we connect its output with the zone input. This way we have create a so-called sequence filter. By double-clicking on the **Category filter** we can select what object types we want the filter to allow to pass.



You can create any number of detection zones you like based on the needs of dynamic traffic control. All the zones can be connected to the same category filter.

We publish the data using data sinks or widgets that are available in other parts of the **Programming elements** panel. We use the widgets when we want to see the data on the dashboard or if we want to use them in expressions for controlling relays or an SDLC interface. We use the UDP/REST sinks when the FLOW device is connected to a device that can uses data communication. For traffic control in almost all cases the UDP sinks are used. REST sinks are used for communication with smart city and data platforms.

Detection outputs – communication with traffic controller

The individual detected traffic events can be sent into the traffic controller via different type of interfaces – both data interfaces and physical interfaces (such as relay interface). The TrafficXRoads unit support multiple data interfaces including REST API, WEBHOOKs and UDP. For the data communication between the unit and the controller to work, the controller needs to support the specific data communication interface. Next we will cover interface that are used in traffic most widely – UPD and SDLC as well as the physical relay interface. For all of these interfaces we will continue with our model example from the previous chapter and do so by creating “basic object presence detectors”.

⚠ The data interfaces can be only used for controllers that have implemented the specific interface. Whether or not the data interface is supported should be verified with the traffic controller manufacturer. Alternatively you can contact us at support@datafromsky.com

⚠ The FLOW data interfaces are documented here: https://intercom.help/datafromsky/en/articles/3773368-introduction-to-data-sinks-and-flow-insights-public-api . If you are a traffic controller manufacturer or an integrator and you would like to integrate a some of the data interfaces, don’t hesitate to get in touch at support@datafromsky.com We will gladly help you with the integration.

UDP data interface

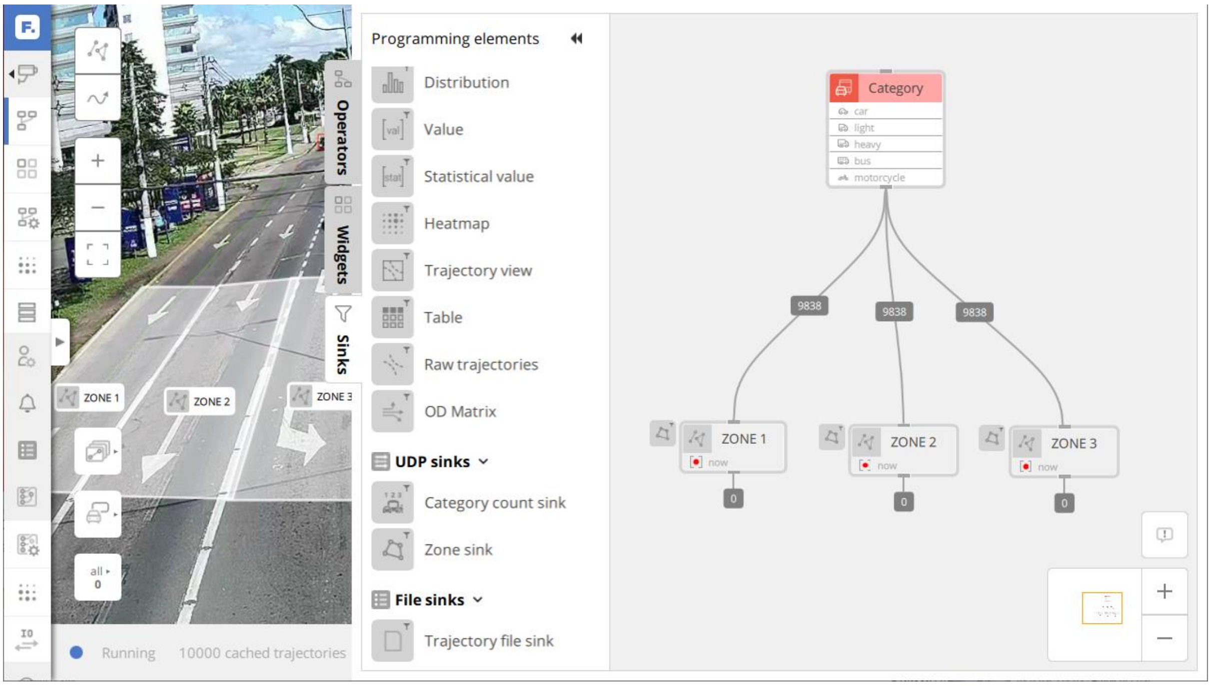
The UDP data interface works based on the subscribe model, where the traffic controller connects to the FLOW device as a client. Once the UDP sink is subscribed the controller will start receiving data from all the defined UDP sinks and analytics.

FLOW supports two types of UDP sinks - ZONE sink and a CATEGORY COUNT sink. ZONE sink sends data about object presence (a list of object IDs) that are on the output of the specific operator. The data are always sent on a subscribe or when the value changes on a specific sink. Data from the CATEGORY COUNT sink are sent only when the controller requests this data.

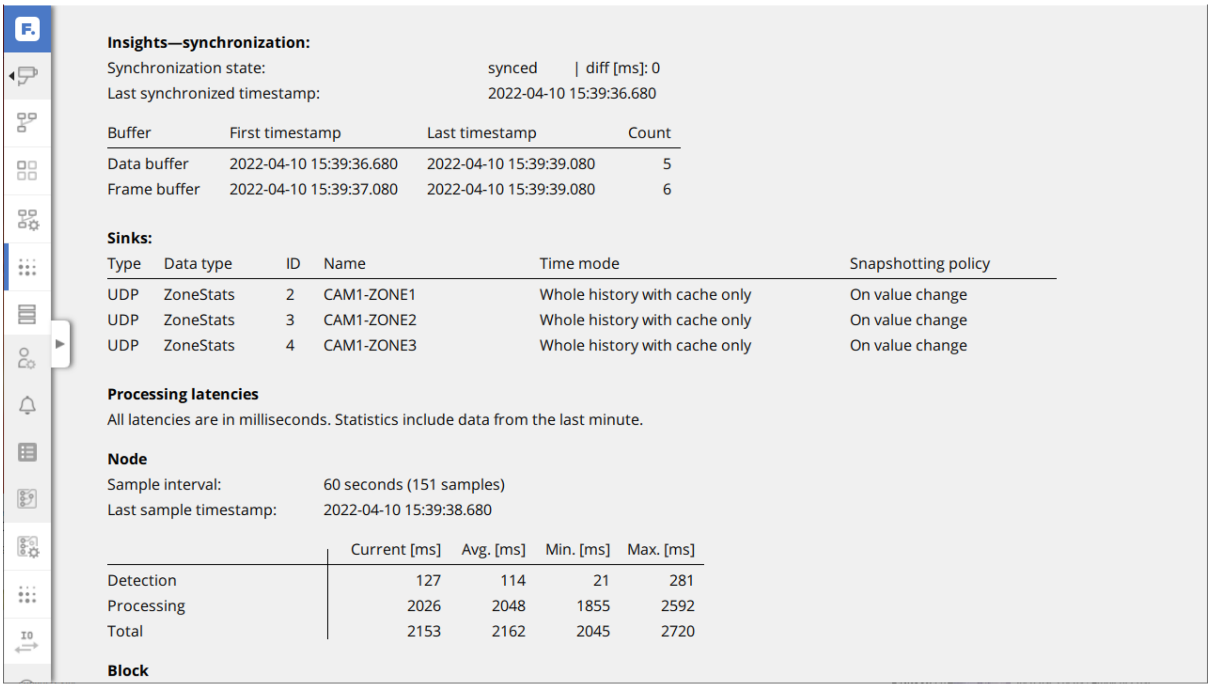
⚠ The "sink name" is used as an ID in payloads for communication with the controller. Therefore, it is necessary that the UDP sinks are unique throughout all the analytics. FLOW does not check whether the sink name is unique.

If you have a controller that has integrated and supports the UDP data communication with FLOW, the publishing of data is very easy. In FLOW we define a traffic detection task that we want using available operators and on the last operator we place the desired UDP sink that we give a unique name. Inside the traffic controller we identify the sink based on its name and we use it as an input signal for traffic control.

Continuing the Object presence example from the previous chapter, we would add UDP ZONE sink with a unique name (in our case we did this systematically CAM[X]-ZONE[Y]) to each of the final ZONE operators in NOW mode. This way we have created 3 detectors of presence in the image CAM1-ZONE1, CAM1-ZONE2 a CAM3-ZONE3, that communicate the information about presence/ absence of vehicle to the traffic controller using UDP.



The list of the created UDP sinks can be found in the analytics and is available on the **Diagnostics** page. The status of the zone is communicated to the controller under the names listed in the **Name** row in the table.



Insights—synchronization:

Synchronization state: synced | diff [ms]: 0

Last synchronized timestamp: 2022-04-10 15:39:36.680

Buffer	First timestamp	Last timestamp	Count
Data buffer	2022-04-10 15:39:36.680	2022-04-10 15:39:39.080	5
Frame buffer	2022-04-10 15:39:37.080	2022-04-10 15:39:39.080	6

Sinks:

Type	Data type	ID	Name	Time mode	Snapshotting policy
UDP	ZoneStats	2	CAM1-ZONE1	Whole history with cache only	On value change
UDP	ZoneStats	3	CAM1-ZONE2	Whole history with cache only	On value change
UDP	ZoneStats	4	CAM1-ZONE3	Whole history with cache only	On value change

Processing latencies

All latencies are in milliseconds. Statistics include data from the last minute.

Node

Sample interval: 60 seconds (151 samples)

Last sample timestamp: 2022-04-10 15:39:38.680

	Current [ms]	Avg. [ms]	Min. [ms]	Max. [ms]
Detection	127	114	21	281
Processing	2026	2048	1855	2592
Total	2153	2162	2045	2720

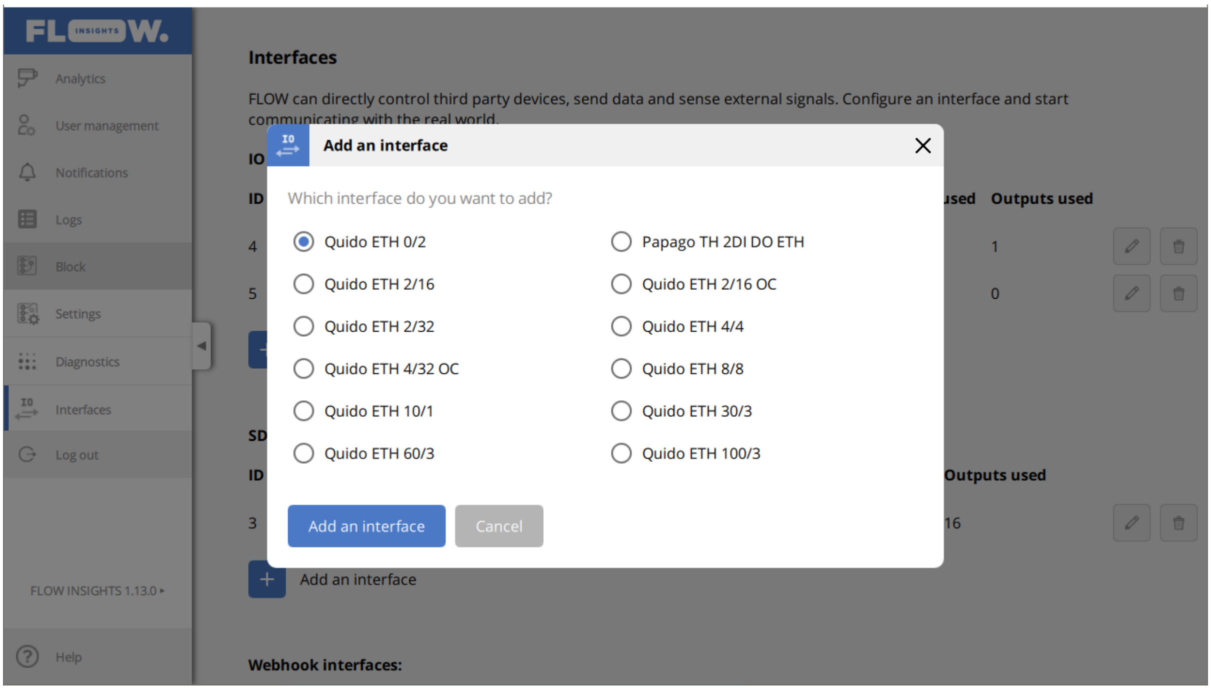
Block

Relay interface

The relay interface is realized using individual I/O module, that is controlled with a connected FLOW device. FLOW device can control multiple I/O module, but a single I/O module can be controlled by only one FLOW device.

⚠ Currently the only supported I/O modules are the „Quido" modules in different variantion in terms of the number of input and output ports.

The registration of I/O module is done in the **Block->Interfaces** tab with the **Add an interface** button in the IO interfaces section. A pop up window will show up with a list of supported I/O modules where you need to select the correct type of I/O module and confirm the choice by clicking on **Add an interface**.



Interfaces

FLOW can directly control third party devices, send data and sense external signals. Configure an interface and start communicating with the real world.

Add an interface

Which interface do you want to add?

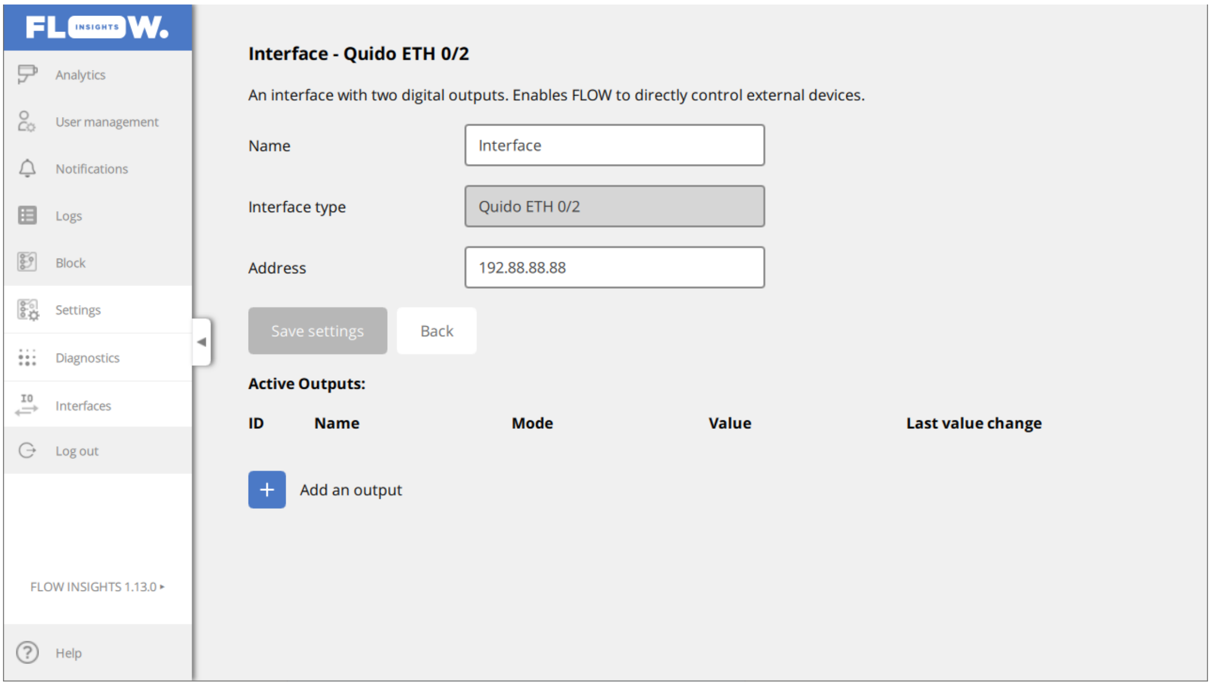
● Quido ETH 0/2	○ Papago TH 2DI DO ETH
○ Quido ETH 2/16	○ Quido ETH 2/16 OC
○ Quido ETH 2/32	○ Quido ETH 4/4
○ Quido ETH 4/32 OC	○ Quido ETH 8/8
○ Quido ETH 10/1	○ Quido ETH 30/3
○ Quido ETH 60/3	○ Quido ETH 100/3

Add an interface | Cancel

Add an interface

Webhook interfaces:

Next it is necessary to configure the I/O module, this means to set its IP address and define the rules for controlling the individual relays. When we click on the pencil icon we will find ourselves in the settings of the specific I/O interface where we can configure IP address of the I/O module and a name. By clicking on the **Save settings** we confirm the configuration and the FLOW device will attempt to communicate with the I/O module. This action will return us to the **Interfaces** section where under the Status field you can tell whether the communication with the I/O module has been established succesfully.



Interface - Quido ETH 0/2

An interface with two digital outputs. Enables FLOW to directly control external devices.

Name: Interface

Interface type: Quido ETH 0/2

Address: 192.88.88.88

Save settings | Back

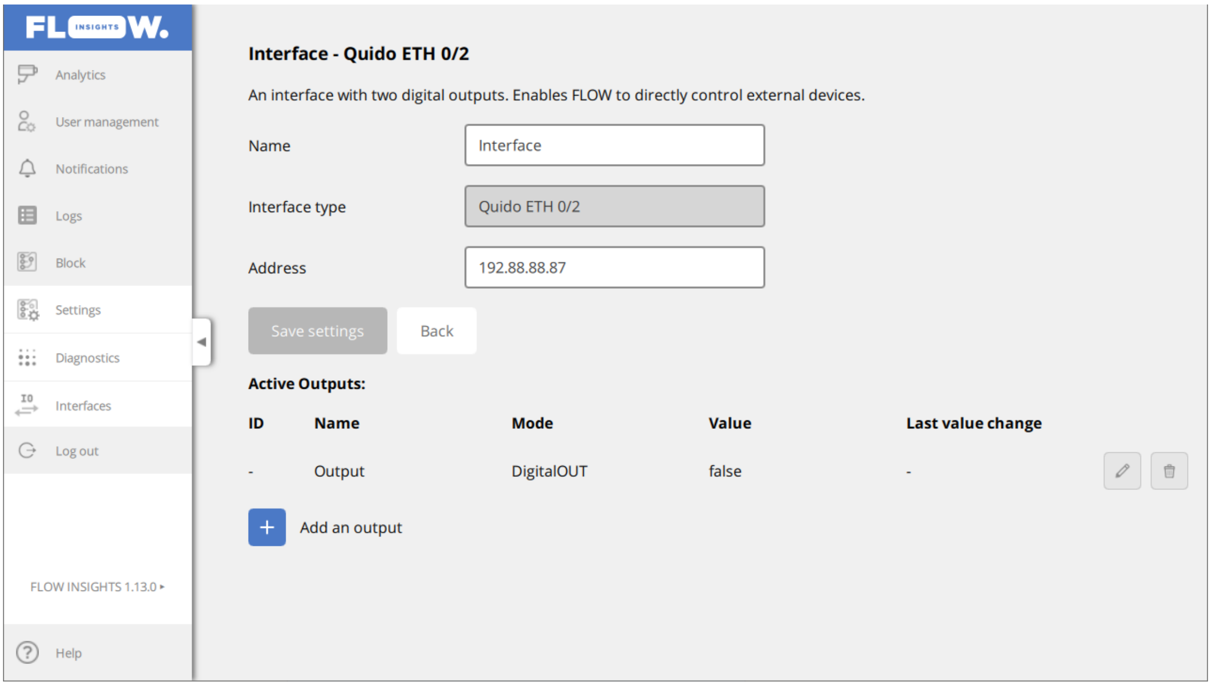
Active Outputs:

ID	Name	Mode	Value	Last value change

+ Add an output

⚠ If you see Offline in the status of the I/O interface, it is necessary whether the I/O module is turned ON, network connected to the FLOW device and whether the entered IP address is correct.

Next it is necessary to configure the rules for the individual output relays. New output relays can be defined in the the I/O moduel settings by clicking on the **Add an output** button. After you click on this button the output will be registered and and can be further configured in detail by clicking on the pencil button.



Interface - Quido ETH 0/2

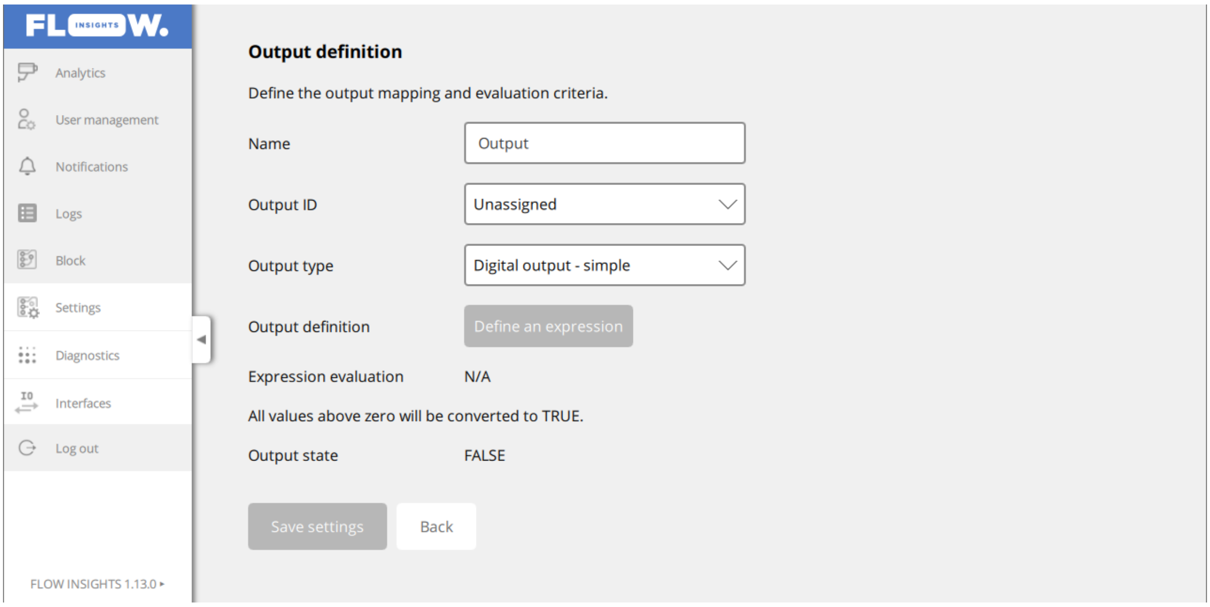
An interface with two digital outputs. Enables FLOW to directly control external devices.

Name	Interface
Interface type	Quido ETH 0/2
Address	192.88.88.87

Active Outputs:

ID	Name	Mode	Value	Last value change
-	Output	DigitalOUT	false	-

By configuring the output we mean the Naming (under Name field), assigning physical relay (Output ID field) and the definition of control rule for ON/OFF (Output definition field).



Output definition

Define the output mapping and evaluation criteria.

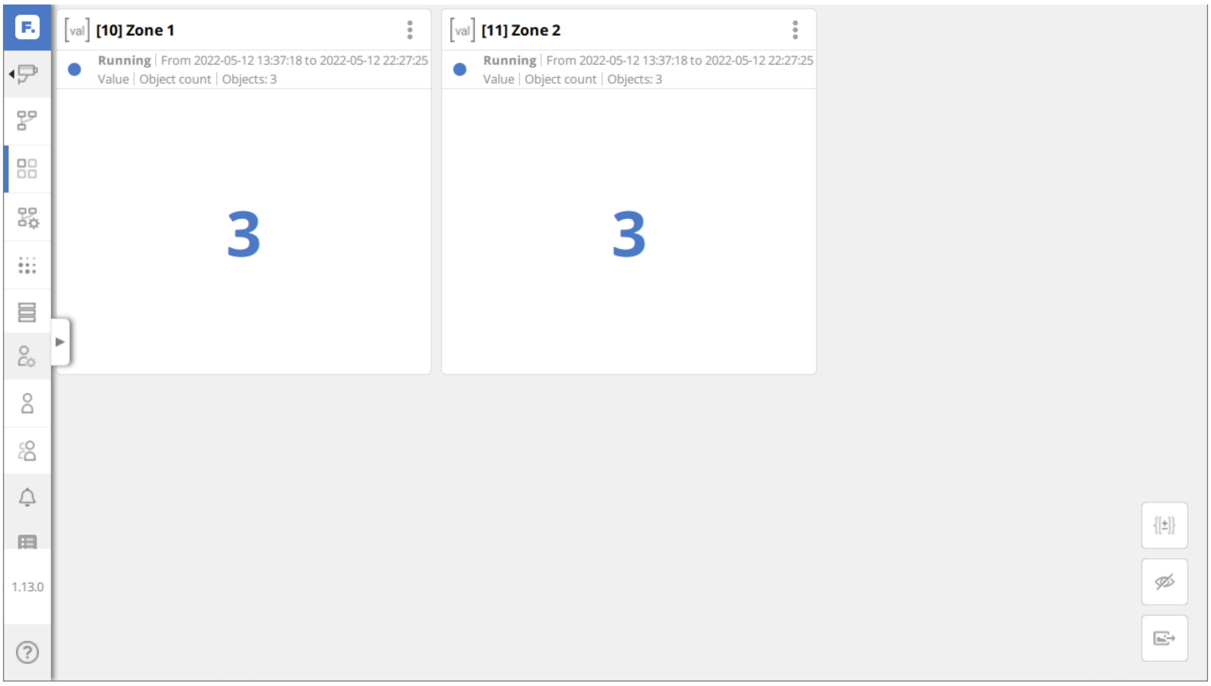
Name	Output
Output ID	Unassigned
Output type	Digital output - simple
Output definition	Define an expression
Expression evaluation	N/A

All values above zero will be converted to TRUE.

Output state	FALSE

Save settings   Back

The rule for turning the relay ON/OFF is defined as an expression where you can refer to different widgets that are in the dashboard. These need to be simple value or statistical value type widgets. If you want the relay to be triggered based on the object presence in a zone you first need to propagate it from the analytics into the Dashboard for example by using Simple value widget and then you will be able to use the widget value as a variable in the expression for controlling the relay. The interface for difining the expression can be accessed by clicking on the **Define an Expression** button next to the Output definition.

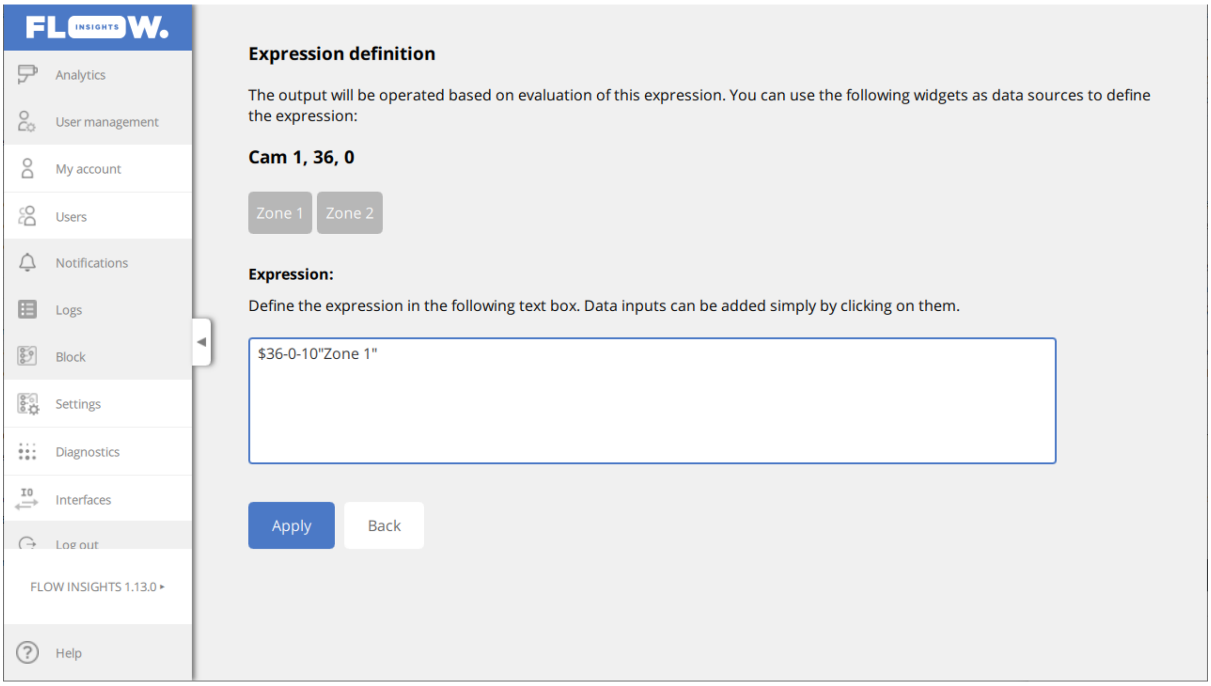


[val] **[10] Zone 1**
Running | From 2022-05-12 13:37:18 to 2022-05-12 22:27:25
Value | Object count | Objects: 3
3

[val] **[11] Zone 2**
Running | From 2022-05-12 13:37:18 to 2022-05-12 22:27:25
Value | Object count | Objects: 3
3

In the expression definition the widgets from individual defined analytics will be atomatically made available for the use. By clicking on the name of the widget you add it into the expression. The expression widget has full Javascript language support, so it is possible to use standart numerical operators, comparison operator and even if-else conditions, functions, etc. If the result of evalution of the is not 0, the relay is turned ON (triggered), if the result is 0 – the relay is turned OFF (untriggered). The evaluation is done always on a value change of any of the widgets that are used as inputs in the expression.

You can check if the relay is working by simply entering 0 or 1 and saving it. Based on the evaluation the relay is then turned ON or OFF.



Expression definition

The output will be operated based on evaluation of this expression. You can use the following widgets as data sources to define the expression:

Cam 1, 36, 0

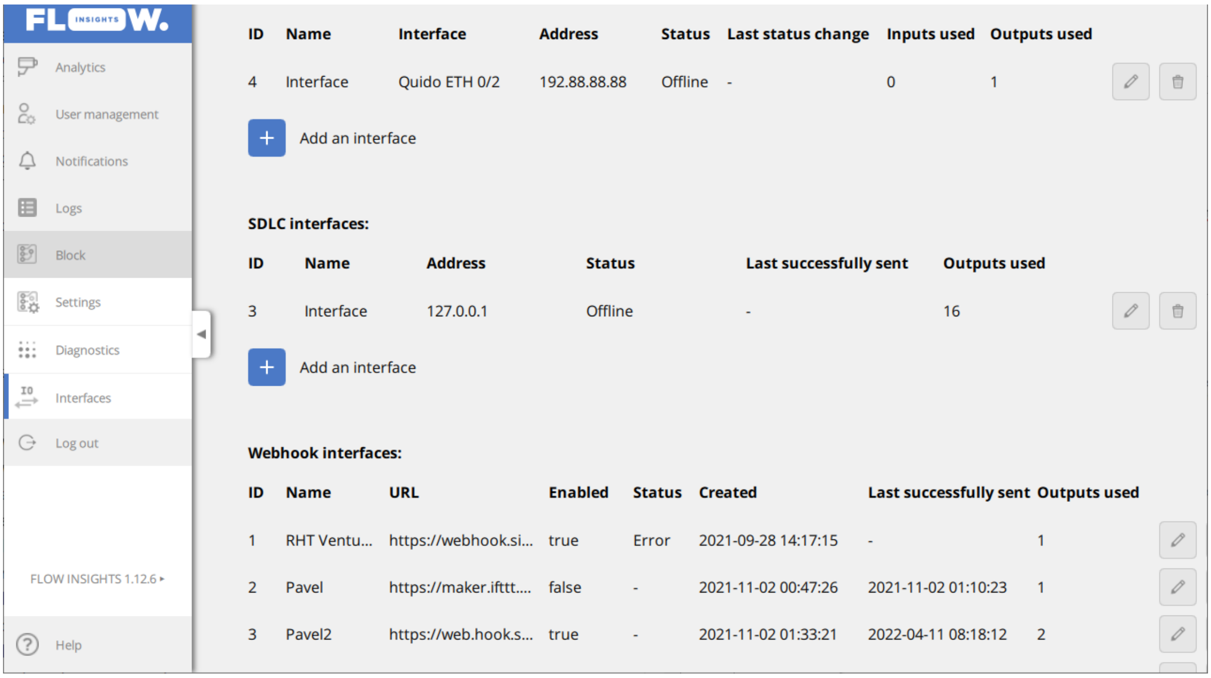
Expression:

Define the expression in the following text box. Data inputs can be added simply by clicking on them.

```
$36-0-10"Zone 1"
```

SDLC data interface

FLOW also supports communication with the controller using the full-duplex Synchronous Data Link Control (SDLC) protocol for short. This is realized using the SDLC convertor. The currently supported convertor is the Luxcom EM-HDLC. In is necessary to register the convertor as an interface in the **Block->Interfaces** tab. It has an SDLC connector and functions as a DR BIU on the CU side - this means it automatically responds to Call data and Diagnostic requests from the CU. The FLOW unit can connect to its Ethernet port. By sending UDP packets in a specific format, it can change the content of the converter's responses on the SDLC bus.



ID	Name	Interface	Address	Status	Last status change	Inputs used	Outputs used
4	Interface	Quido ETH 0/2	192.88.88.88	Offline	-	0	1

+ Add an interface

SDLC interfaces:

ID	Name	Address	Status	Last successfully sent	Outputs used
3	Interface	127.0.0.1	Offline	-	16

+ Add an interface

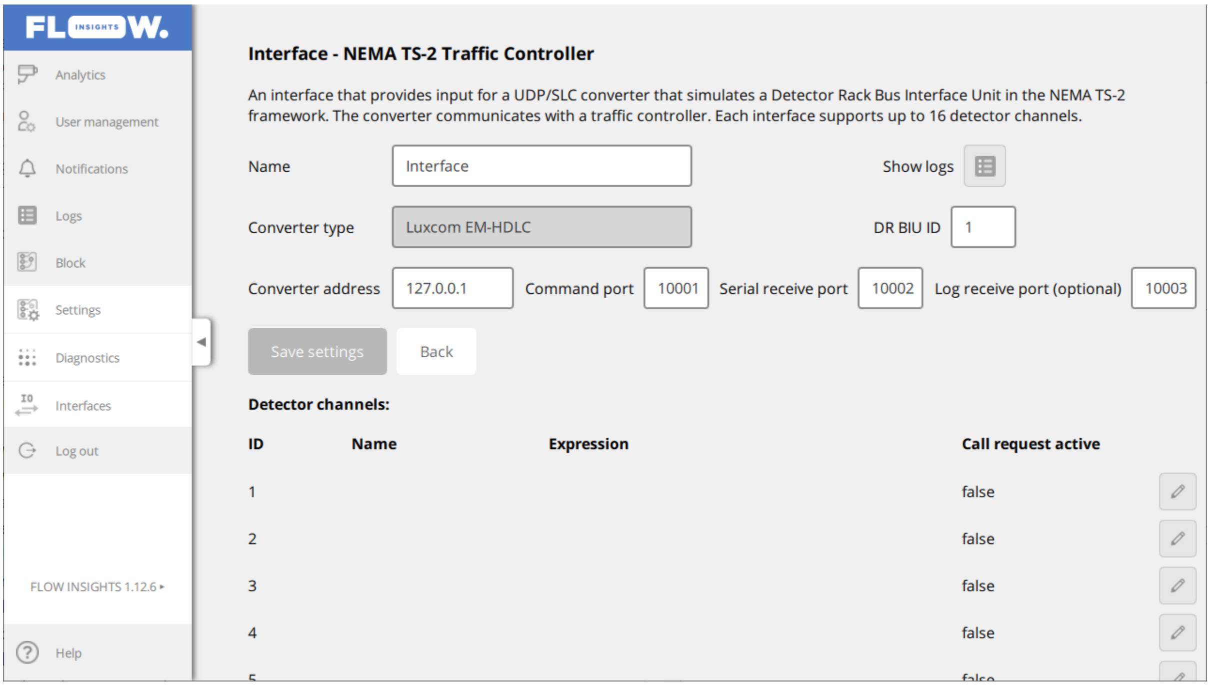
Webhook interfaces:

ID	Name	URL	Enabled	Status	Created	Last successfully sent	Outputs used
1	RHT Ventu...	https://webhook.si...	true	Error	2021-09-28 14:17:15	-	1
2	Pavel	https://maker.ifttt....	false	-	2021-11-02 00:47:26	2021-11-02 01:10:23	1
3	Pavel2	https://web.hook.s...	true	-	2021-11-02 01:33:21	2022-04-11 08:18:12	2

⚠ Please note that the number of added convertors is not limited by the FLOW device. Single FLOW device can communicate with multiple convertors at once.

Next it is necessary to set up the communication with the convertor. The convertor's setup procedure is, to some extent, described in the firmware user manual. Basically you need to set up access to the convertor's web management interface, then set up the corresponding IP addresses and ports:

- **Serial forward IP address** - The IP address of the embedded unit.
- **Serial forward UDP port** - The port where you want the embedded unit to receive SDLC communication.
- **Syslog IP address** - The IP address of the device that system log will be sent to (probably the embedded unit).
- **Syslog port** - The port where the log messages will be sent to.
- **Command IP address** - The IP address of the embedded unit. The convertor will **discard** all messages coming from a different IP address.
- **Command UDP port** - The port where the embedded unit will send commands for the converter and receive responses from.



Interface - NEMA TS-2 Traffic Controller

An interface that provides input for a UDP/SLC converter that simulates a Detector Rack Bus Interface Unit in the NEMA TS-2 framework. The converter communicates with a traffic controller. Each interface supports up to 16 detector channels.

Name: Interface — Show logs

Converter type: Luxcom EM-HDLC — DR BIU ID: 1

Converter address: 127.0.0.1 — Command port: 10001 — Serial receive port: 10002 — Log receive port (optional): 10003

Detector channels:

ID	Name	Expression	Call request active
1			false
2			false
3			false
4			false
5			false

It's recommended to avoid ports in the range 0-1023, as binding network sockets to them may require your application to have administrative or root privileges. By default, the DR BIU ID of the converter is 1. If you want to change it, you need custom firmware update from Luxcom. On the web interface's Status page, you can see statistics about sent and received messages. *Command count* tells you how many valid commands have been received from the embedded unit.

⚠ Correct set up of the network communication can be verified on the **Interfaces** page in the **SDLC interfaces** section, where you should see **Online** under the **Status** field. If not, the FLOW device has not established data connection with the convertor.

After the correct set up of the communication interface with the SDLC unit, the configuration logic is the same as with the **Relay interface**. For the different input channels, you define expressions utilizing the published traffic data from widgets on dashboards of the individual analytics.

Reducing latency

For many traffic control scenarios, it is necessary for the system to have as low latency as possible so the traffic events are communicated to the controller in the shortest time possible. To do this you can do multiple optimizations that we will discuss further. It is important to keep in mind that designing a system to meet low-latency goals will require other tradeoffs.

Reducing latency in a camera

Latency introduced by the camera is caused by image processing and encoding latency. Here are some tips how to reduce the latency in a camera as much as possible:

- **Resolution**: choose a lower resolution if possible. Higher resolutions imply more data do be processed which may lead to higher latency.
- **Enhancements**: rotation, scaling, deinterlacing, noise reduction, and more can also add latency. Reduce the image enhancements as much as possible, but be aware of the effect on image quality, especially in night conditions.
- **Encoding**: H.265 has lower latency than H.264
- **Number of streams:** Limit the number of streams to the number you really need. Each unique combination of video settings will require its own individual encoding process, adding load to the camera processor, causing delay.
- **Frame rate:** Higher frame rate will reduce delays caused by buffers. For a stream with 30 FPS, each frame will take 1/30 of second to capture. The expected latency is **33** ms in buffers.
- **Audio:** Audio causes appreciable amount of latency. Remove the audio.
- **Bitrate:** Reduce the amount of data being generated and transferred. Find the lowest bitrate in which the image quality is still sufficient for automatic processing.

On the camera side the process is largely an exposure, image enhancement, compressing and packing. Roughly speaking, the time it takes to process one frame in the camera is under 50 ms.

Reducing latency in the network

Limit the total data volume being sent through the network. Make sure that your network has a good quality of service, and that all the hops within the network are configure to suite your video demand. Connect the cameras directly to the unit if it is possible.

Reducing processing latency in TrafficXRoads

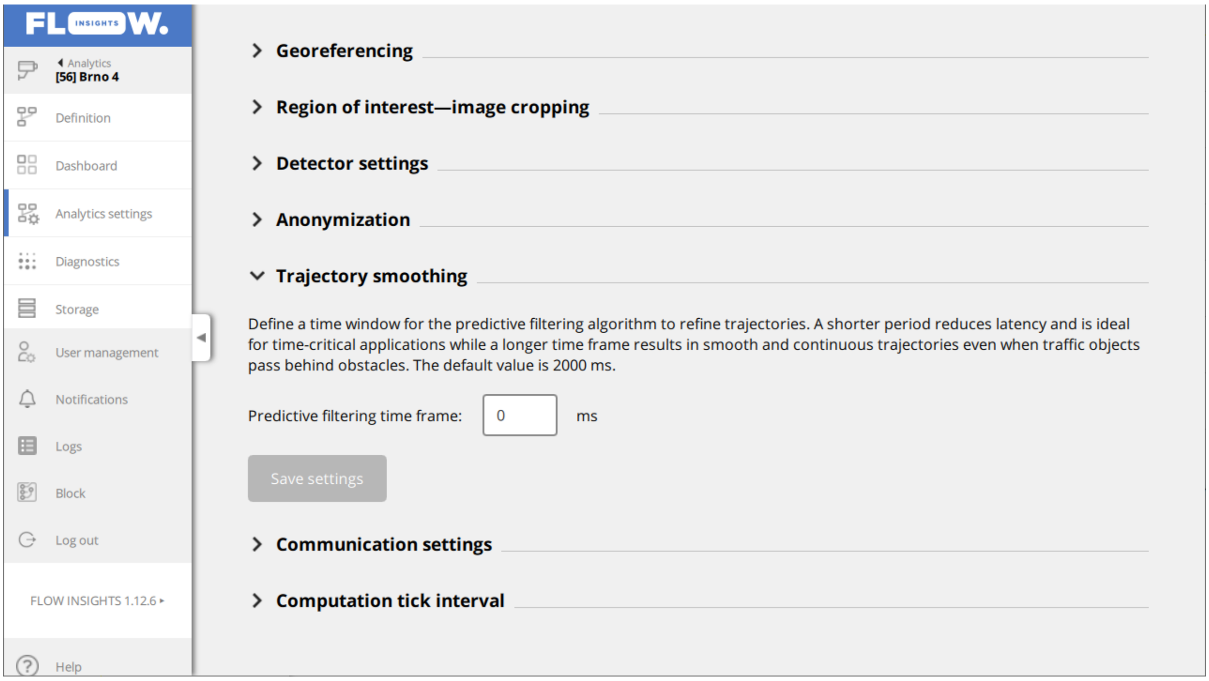
The FLOW framework enables configuration of different settings that lead to significant reductions in processing latency. These include the reduction of smoothing buffer for the tracker and increasing the frequency of trajectory evaluation. Both parameters are under the settings of the analytics and can therefore be defined separately for each one.

Trajectory smoothing parameter

This parameter defines how long is the buffer size for the tracker in milliseconds. The buffer is used to improve the results of tracking. It does that by presenting the state of the system on the tracker output but later (based on the specified milliseconds) but with the utilization of the most recent data. Longer buffer settings of the tracker lead to less trajectories disconnecting in scenes with occlusions. Lower buffer settings lead to faster system response times.

Recommendations:

- 0 ms: For maximum responsiveness for tasks with object presence detection where continuous trajectories are not necessary.
- 200 ms: For systems with 10+ detection FPS where it is important to have both continuous trajectories and fast system response
- 2000 ms: For application where the speed of response is not crucial but continuity of trajectories is – for example for collecting traffic statistics

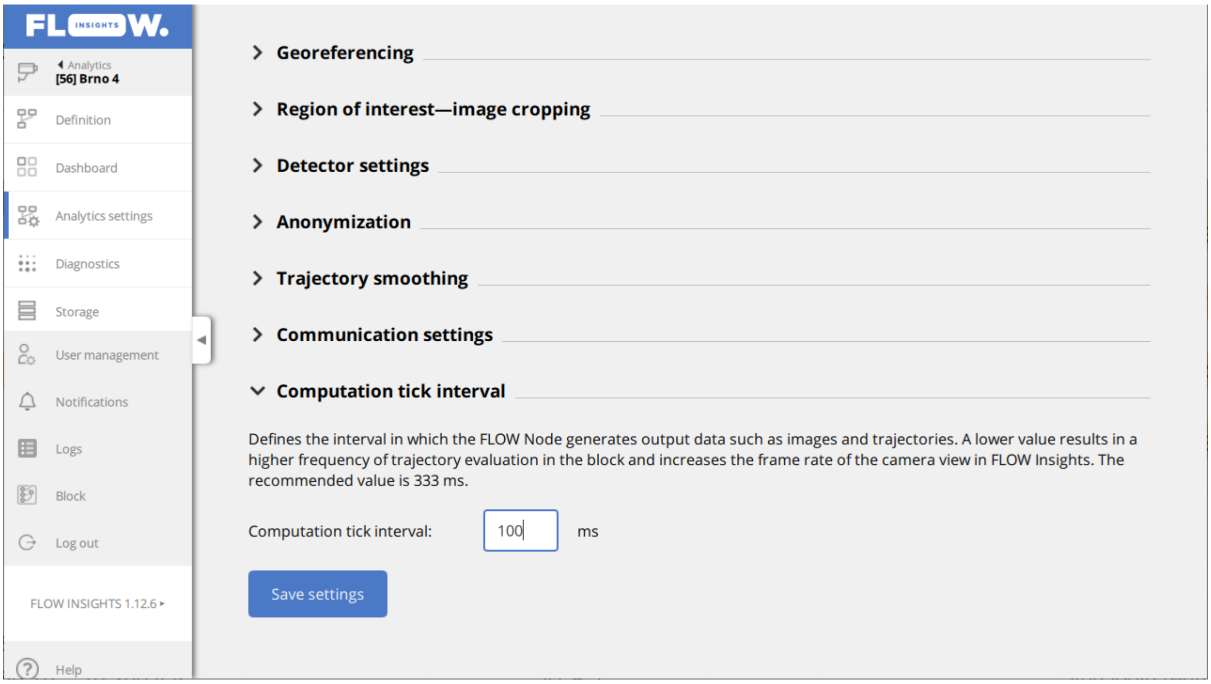


Define a time window for the predictive filtering algorithm to refine trajectories. A shorter period reduces latency and is ideal for time-critical applications while a longer time frame results in smooth and continuous trajectories even when traffic objects pass behind obstacles. The default value is 2000 ms.

Predictive filtering time frame: 0 ms

Computation tick interval parameter

This parameter defines how often the FLOW engine evaluates the trajectories and generates events and results. This step is followed by evaluation of expressions, sending results to I/O modules, WEBHOOKs, UDP protocol and the generation of MJPEG images. High frequency (low tick interval) leads to higher processing load on the FLOW device and reduces reaction time. Lowest possible value is 100 ms. By default, the value is set to 333 ms. For traffic control tasks we recommend 100 ms.



Georeferencing

Region of interest—image cropping

Detector settings

Anonymization

Trajectory smoothing

Communication settings

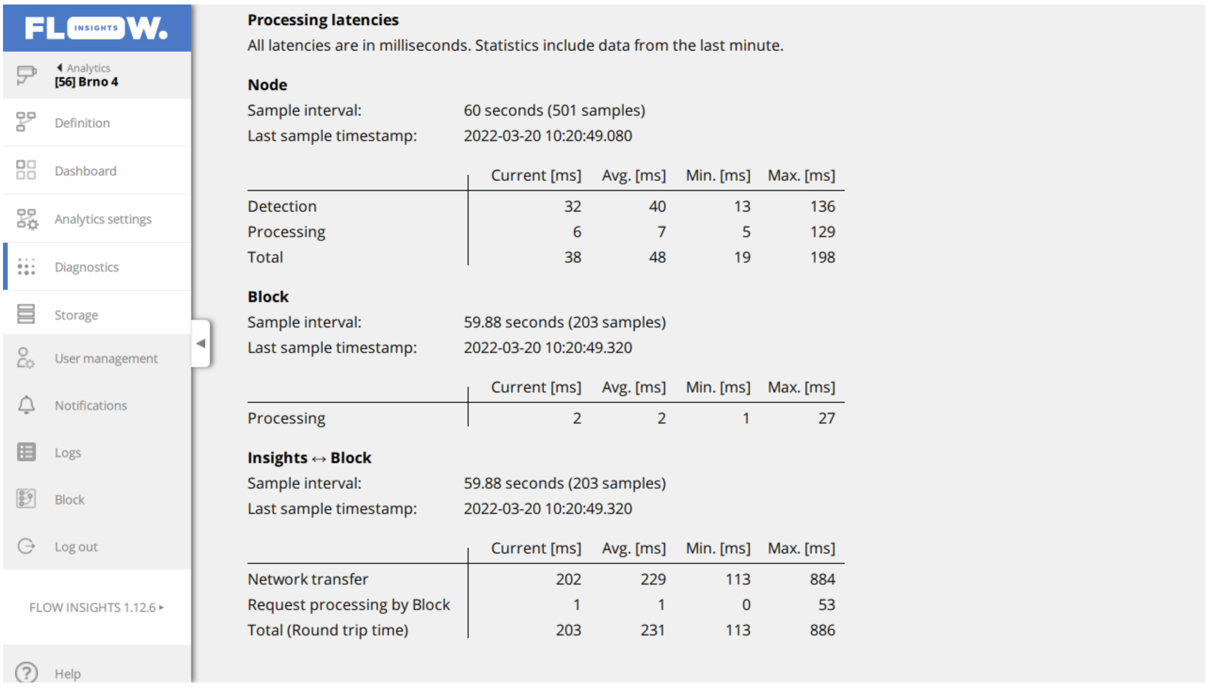
Computation tick interval

Defines the interval in which the FLOW Node generates output data such as images and trajectories. A lower value results in a higher frequency of trajectory evaluation in the block and increases the frame rate of the camera view in FLOW Insights. The recommended value is 333 ms.

Computation tick interval: 100 ms

Processing latency – basic diagnostics

The processing latency of the FLOW device can be checked on the **Diagnostics** page of individual analytics. For traffic control both the latency of the video-analytical part the FLOW NODE (line **Total**) and also the latency of trajectory evaluation FLOW BLOCK (line **Processing**). It concerns only the time it takes to process the image/evaluate the trajectories (including the tracker buffer). The value in the **Insights -> Block** section are not important for the communication with the controller, they only relate to the data transfer into the FLOW Insights configuration application.



Processing latencies

All latencies are in milliseconds. Statistics include data from the last minute.

Node

Sample interval: 60 seconds (501 samples)

Last sample timestamp: 2022-03-20 10:20:49.080

	Current [ms]	Avg. [ms]	Min. [ms]	Max. [ms]
Detection	32	40	13	136
Processing	6	7	5	129
Total	38	48	19	198

Block

Sample interval: 59.88 seconds (203 samples)

Last sample timestamp: 2022-03-20 10:20:49.320

	Current [ms]	Avg. [ms]	Min. [ms]	Max. [ms]
Processing	2	2	1	27

Insights ↔ Block

Sample interval: 59.88 seconds (203 samples)

Last sample timestamp: 2022-03-20 10:20:49.320

	Current [ms]	Avg. [ms]	Min. [ms]	Max. [ms]
Network transfer	202	229	113	884
Request processing by Block	1	1	0	53
Total (Round trip time)	203	231	113	886

⚠ **Node – Detection** time should always be 20% shorter than the minimum detection FPS for the specific scene type. **Node – Processing** also includes the configurable tracker time buffer.

⚠ **Block – Processing** time should always be at least 50% shorter than the set **Computational tick interval**. If that is not the case, the unit is overloaded and is unable to evaluate the data quickly enough. It is necessary to lower the number of analytics or reduce the number of data outputs.

Reducing latency on the outputs

By latency on the output we mean the transfer of the information about a traffic event from FLOW device to the controller. The best communication tool with the lowest latency are the UDP sinks. Next is the SDLC interface utilizing convertors and last, the I/O module (relay interface) namely:

- UDP sinks: < 1 ms
- SDLC including the convertor: ~ 1 ms / based on the convertor
- IO module – relay interface: ~ 11 ms

⚠ For maximum reduction of the latency between the unit and the traffic controller we suggest using UDP interface if the traffic controller is data compatible with the FLOW device.

Conclusion

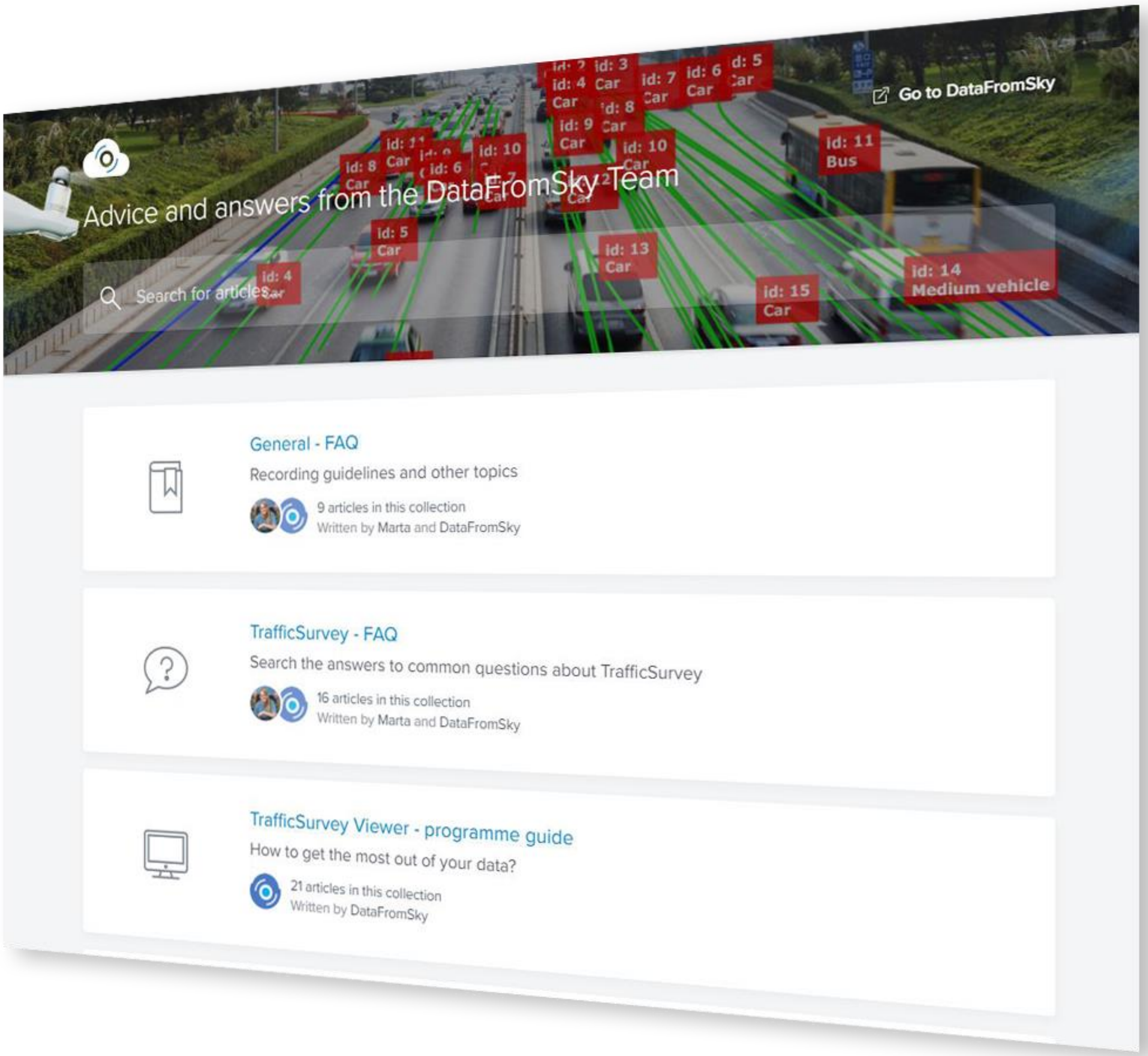
The latency is worsened by both image grabbing, communication between the camera and the unit, in the image analysis and in the communication between the unit and the traffic controller. With good system settings, many of the latencies can be significantly reduced and a very low latency can be achieved (200 – 350 ms), in breakdown:

- Camera: ~ 50 – 150 ms
- Image transfer: < 10 ms (local network)
- TrafficXroads: ~100 ms
- Communication to traffic controller: < 1 ms (UDP, local network)

Lower latencies are achievable with the use of industrial cameras (even as low as 50ms). Get in touch with us if that is something you would like to implement.

More about FLOW framework

FLOW framework is a complex system that supports a variety of hardware devices. FLOW currently runs on TrafficCamera, TrafficEmbedded, TrafficXRoads, TrafficEnterprise and TrafficDrone (mobile processing unit). No matter the hardware requirements or use case you are able to work in the same system. The complete and up-to-date manual about all aspects of FLOW framework is available online at https://intercom.help/datafromsky/en/collections/2019942-flow-and-flow-insights where you can find a plethora of articles about the framework, how it works or how to set up the analytics for a variety of use-cases.



Advice and answers from the DataFromSky Team

General - FAQ

Recording guidelines and other topics

9 articles in this collection
Written by Marta and DataFromSky

TrafficSurvey - FAQ

Search the answers to common questions about TrafficSurvey

16 articles in this collection
Written by Marta and DataFromSky

TrafficSurvey Viewer - programme guide

How to get the most out of your data?

21 articles in this collection
Written by DataFromSky

You can use the search bar on the top to help you find what you are looking for.

Simplified signpost

Basic FLOW principles:
We suggest starting with the FLOW basics article:

- https://intercom.help/datafromsky/en/articles/3773025-the-basics-of-flow-insights

Data filtration - How to use FLOW filters and operators:
We also suggest reading some of the articles about the various types of filters such as the spatial filters article which is the most important one:

- https://intercom.help/datafromsky/en/articles/3656473-spatial-filters-in-flow-insights

Visualization – widgets and dashboards:
To learn everything, you need to know about widgets and data visualization please read this article:

- https://intercom.help/datafromsky/en/articles/3666528-using-widgets-to-view-data-on-the-dashboard-in-flow-insights

Tutorials – how to create:
The best way to learn FLOW is by applying it to a specific use-case making it easily understandable. Choose a specific use-case guide that you like and follow along:

- https://intercom.help/datafromsky/en/collections/2019942-flow-and-flow-insights#use-case-tutorials-how-to-series

Generic:
Some general guidelines that you may find useful on how to capture video can be found here:

- https://intercom.help/datafromsky/en/collections/2232238-general-faq

In case you have not found what you have been looking for please get in touch with us using the live chat or send us email to support@datafromsky.com.

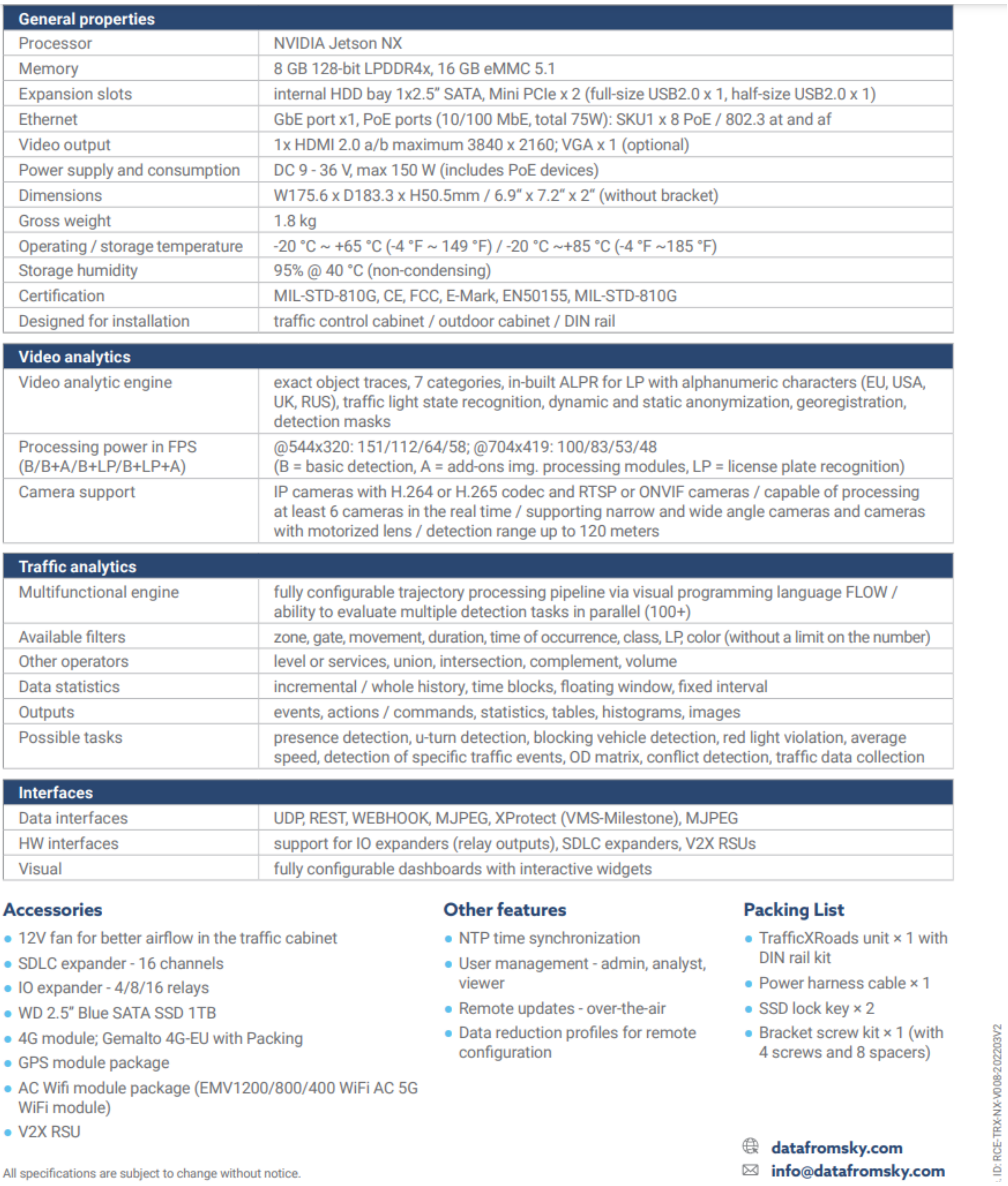
Conclusion

This manual has covered the basic configuration of TrafficXRoads unit. We went over the contents of the TrafficXRoads package, Field installation, Camera framing, Power supply, Network setup, and Quick start guide.

FLOW has regular updates with new functions, performance improvements and bug fixes. Inside FLOW Insights you will be notified when new FLOW version is available, however please do not update FLOW Insights without updating the TrafficXRoads unit first. If you would like to update the version of FLOW on your TrafficXRoads unit please get in touch with us at support@datafromsky.com.

We hope you will enjoy TrafficXRoads unit. If you have any kind of feedback, please reach out to us at info@datafromsky.com.

Technical specification XRoads V008



General properties	
Processor	NVIDIA Jetson NX
Memory	8 GB 128-bit LPDDR4x, 16 GB eMMC 5.1
Expansion slots	internal HDD bay 1x2.5" SATA, Mini PCIe x 2 (full-size USB2.0 x 1, half-size USB2.0 x 1)
Ethernet	GbE port x1, PoE ports (10/100 MbE, total 75W): SKU1 x 8 PoE / 802.3 at and af
Video output	1x HDMI 2.0 a/b maximum 3840 x 2160; VGA x 1 (optional)
Power supply and consumption	DC 9 - 36 V, max 150 W (includes PoE devices)
Dimensions	W175.6 x D183.3 x H50.5mm / 6.9" x 7.2" x 2" (without bracket)
Gross weight	1.8 kg
Operating / storage temperature	-20 °C ~ +65 °C (-4 °F ~ 149 °F) / -20 °C ~+85 °C (-4 °F ~185 °F)
Storage humidity	95% @ 40 °C (non-condensing)
Certification	MIL-STD-810G, CE, FCC, E-Mark, EN50155, MIL-STD-810G
Designed for installation	traffic control cabinet / outdoor cabinet / DIN rail

Video analytics	
Video analytic engine	exact object traces, 7 categories, in-built ALPR for LP with alphanumeric characters (EU, USA, UK, RUS), traffic light state recognition, dynamic and static anonymization, georegistration, detection masks
Processing power in FPS (B/B+A/B+LP/B+LP+A)	@544x320: 151/112/64/58; @704x419: 100/83/53/48 (B = basic detection, A = add-ons img. processing modules, LP = license plate recognition)
Camera support	IP cameras with H.264 or H.265 codec and RTSP or ONVIF cameras / capable of processing at least 6 cameras in the real time / supporting narrow and wide angle cameras and cameras with motorized lens / detection range up to 120 meters

Traffic analytics	
Multifunctional engine	fully configurable trajectory processing pipeline via visual programming language FLOW / ability to evaluate multiple detection tasks in parallel (100+)
Available filters	zone, gate, movement, duration, time of occurrence, class, LP, color (without a limit on the number)
Other operators	level or services, union, intersection, complement, volume
Data statistics	incremental / whole history, time blocks, floating window, fixed interval
Outputs	events, actions / commands, statistics, tables, histograms, images
Possible tasks	presence detection, u-turn detection, blocking vehicle detection, red light violation, average speed, detection of specific traffic events, OD matrix, conflict detection, traffic data collection

Interfaces	
Data interfaces	UDP, REST, WEBHOOK, MJPEG, XProtect (VMS-Milestone), MJPEG
HW interfaces	support for IO expanders (relay outputs), SDLC expanders, V2X RSUs
Visual	fully configurable dashboards with interactive widgets

Accessories

- 12V fan for better airflow in the traffic cabinet
- SDLC expander - 16 channels
- IO expander - 4/8/16 relays
- WD 2.5" Blue SATA SSD 1TB
- 4G module; Gemalto 4G-EU with Packing
- GPS module package
- AC Wifi module package (EMV1200/800/400 WiFi AC 5G WiFi module)
- V2X RSU

Other features

- NTP time synchronization
- User management - admin, analyst, viewer
- Remote updates - over-the-air
- Data reduction profiles for remote configuration

Packing List

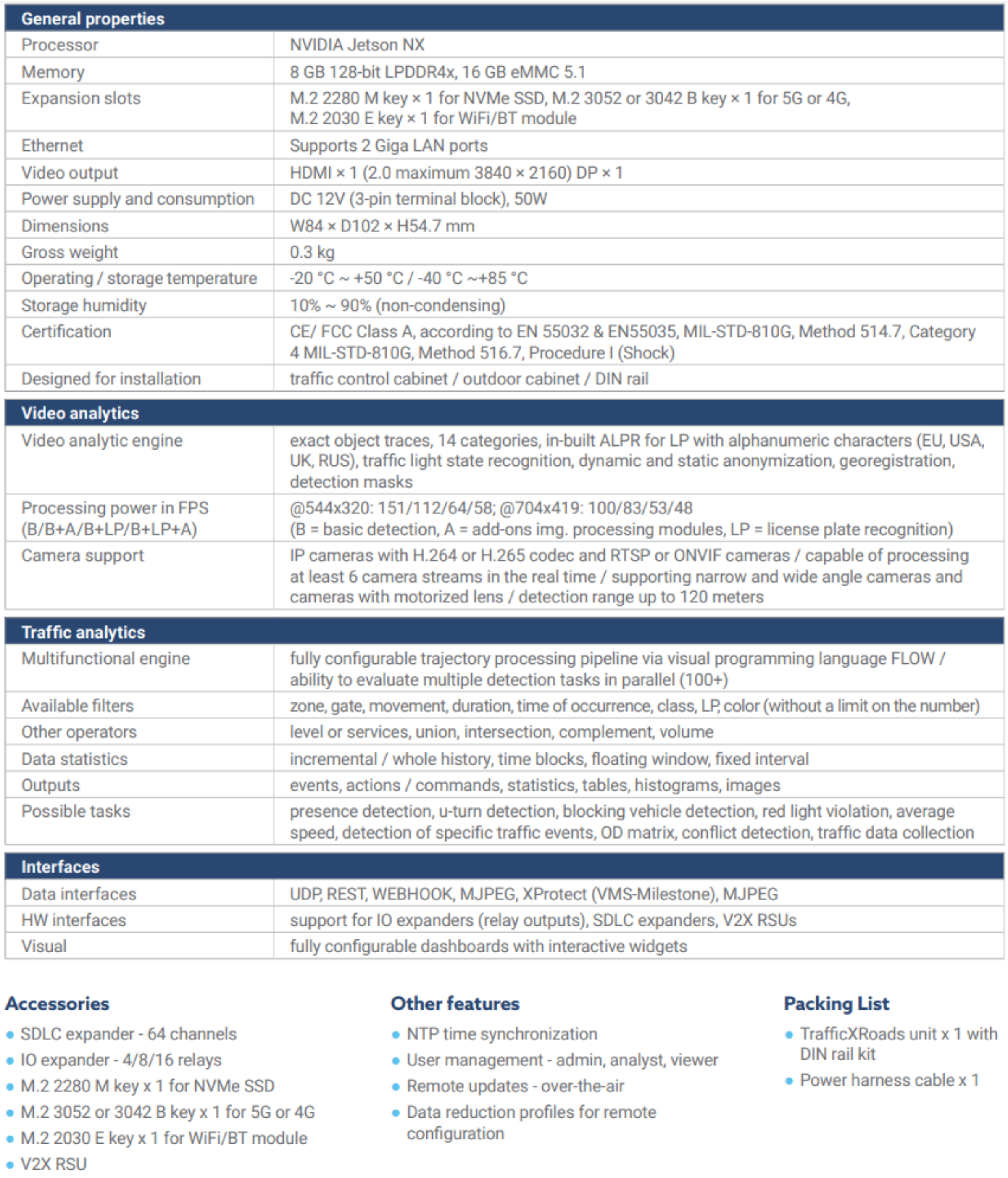
- TrafficXRoads unit × 1 with DIN rail kit
- Power harness cable × 1
- SSD lock key × 2
- Bracket screw kit × 1 (with 4 screws and 8 spacers)

All specifications are subject to change without notice.

🌐 dataframsky.com
✉ info@dataframsky.com

ID: RCE-TRX-NX-V008-202203V2

Technical specification XRoads B000



General properties	
Processor	NVIDIA Jetson NX
Memory	8 GB 128-bit LPDDR4x, 16 GB eMMC 5.1
Expansion slots	M.2 2280 M key × 1 for NVMe SSD, M.2 3052 or 3042 B key × 1 for 5G or 4G, M.2 2030 E key × 1 for WiFi/BT module
Ethernet	Supports 2 Giga LAN ports
Video output	HDMI × 1 (2.0 maximum 3840 × 2160) DP × 1
Power supply and consumption	DC 12V (3-pin terminal block), 50W
Dimensions	W84 × D102 × H54.7 mm
Gross weight	0.3 kg
Operating / storage temperature	-20 °C ~ +50 °C / -40 °C ~+85 °C
Storage humidity	10% ~ 90% (non-condensing)
Certification	CE/ FCC Class A, according to EN 55032 & EN55035, MIL-STD-810G, Method 514.7, Category 4 MIL-STD-810G, Method 516.7, Procedure I (Shock)
Designed for installation	traffic control cabinet / outdoor cabinet / DIN rail
Video analytics	
Video analytic engine	exact object traces, 14 categories, in-built ALPR for LP with alphanumeric characters (EU, USA, UK, RUS), traffic light state recognition, dynamic and static anonymization, georegistration, detection masks
Processing power in FPS (B/B+A/B+LP/B+LP+A)	@544x320: 151/112/64/58; @704x419: 100/83/53/48 (B = basic detection, A = add-ons img. processing modules, LP = license plate recognition)
Camera support	IP cameras with H.264 or H.265 codec and RTSP or ONVIF cameras / capable of processing at least 6 camera streams in the real time / supporting narrow and wide angle cameras and cameras with motorized lens / detection range up to 120 meters
Traffic analytics	
Multifunctional engine	fully configurable trajectory processing pipeline via visual programming language FLOW / ability to evaluate multiple detection tasks in parallel (100+)
Available filters	zone, gate, movement, duration, time of occurrence, class, LP, color (without a limit on the number)
Other operators	level or services, union, intersection, complement, volume
Data statistics	incremental / whole history, time blocks, floating window, fixed interval
Outputs	events, actions / commands, statistics, tables, histograms, images
Possible tasks	presence detection, u-turn detection, blocking vehicle detection, red light violation, average speed, detection of specific traffic events, OD matrix, conflict detection, traffic data collection
Interfaces	
Data interfaces	UDP, REST, WEBHOOK, MJPEG, XProtect (VMS-Milestone), MJPEG
HW interfaces	support for IO expanders (relay outputs), SDLC expanders, V2X RSUs
Visual	fully configurable dashboards with interactive widgets

Accessories

- SDLC expander - 64 channels
- IO expander - 4/8/16 relays
- M.2 2280 M key x 1 for NVMe SSD
- M.2 3052 or 3042 B key x 1 for 5G or 4G
- M.2 2030 E key x 1 for WiFi/BT module
- V2X RSU

Other features

- NTP time synchronization
- User management - admin, analyst, viewer
- Remote updates - over-the-air
- Data reduction profiles for remote configuration

Packing List

- TrafficXRoads unit x 1 with DIN rail kit
- Power harness cable x 1