SAIMOS® VIDEO ANALYTICS

TECHNICAL GUIDELINE

Version 3.5

03.05.2021

ONG-IT GmbH • Stiftgasse 27 • 1070 Vienna • Austria • Reg. No. FN 353657i • VAT No. ATU66022314
Phone: +43 (1) 997 13 69 • Fax: +43 (1) 997 13 69 - 555 • office@saimos.eu • www.saimos.eu

Legal Information and Notices

The material and information contained on this document is for general information purposes only. You should not rely upon the material or information on the document as a basis for making any business, legal or any other decisions. Whilst we endeavour to keep the information up to date and correct, ONG-IT makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the document or the information, products, services or related graphics contained on this document for any purpose. Any reliance you place on such material is therefore strictly at your own risk. In no circumstances, shall ONG-IT be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of or inability to use, this document or any of the material contained in it. ONG-IT will not be liable for any false, inaccurate, inappropriate or incomplete information presented on this document.

DISCLAIMER

There might be national restrictions by law in using some or all of quoted items. It is the sole responsibility to check for such potential restrictions by the reseller or end-customer. Video Analytics- and/or Video Recording solutions must be only used within end-customer's premises and must not be used on public places. The operation of Video Analytics- and/or Video Recording solutions by the end-customer must be in accordance with local laws and policies. In no circumstances, shall ONG-IT be liable for the usage of products and/or solutions purchased and/or installed by ONG-IT.

REVISION

Rev.	Date	Description	Prepared	Checked	Approved
3.5	03.05.2021	Update section 1.2	-	KE	KE
3.4	01.12.2020	Update section 1	-	KE	KE
3.3	19.10.2020	Added LiDAR in section 2.1	-	JK	JK
3.2	30.06.2020	Corrected LPR requirements	-	JK	JK
3.1	11.05.2020	Update SAIMOS® Face Analytics	-	KE	KE
2	11.05.2020	Update SAIMOS® Scrambler, SAIMOS® Face Analytics	-	KE	KE
1	23.04.2020	Update LPR countries	-	KE	KE
0	10.04.2020	Issued to Public	-	KE	KE

TABLE OF CONTENTS

1 GENERAL

SAIMOS® Video Analytics is a CPU/VPU based solution and doesn't require any GPU. By that, it's possible to operate SAIMOS® VA on physical servers as well as in virtual environments including cloud.

Our SAIMOS® platform has Intel's OpenVINO integrated, which allows us to integrate additional neural networks for inference. By that our custom development capabilities are becoming quite time- and cost efficient, while our standard portfolio continues increasing.

Due to our Server/Node architecture, technically, we do not have any limits in the number of cameras connected to SAIMOS®.

1.1 UPDATE PLANS & SUBSCRIPTIONS

We're providing software updates up to 3 times a year (similar to Milestone). Such updates might include software fixes, software enhancements, additional functionalities, performance improvements, etc. The costs for a software update plan are 20% of the MSRP per annum. The first 12-months of software update are included with the purchase of perpetual licenses (except CORE licenses).

An alternative to perpetual licenses are our subscription licenses, which are priced on a monthly basis, while a min. of 6 months per license/channel must be purchased. Our Subscription plan is a typical SaaS approach, which means that licenses are rented (update plans are included in the subscription model).

1.2 HARDWARE REQUIREMENTS

Our SAIMOS® Video Analytics suite does have the below listed minimum hardware requirements. Please consider the below guideline for the minimum dimensioning of the required hardware in client's respective project. Please check CPU benchmarks on https://www.cpubenchmark.net/.

In general, SAIMOS® Video requires **Intel CPUs** meeting the below minimum specifications:

- AVX2 or higher
- minimum Single Thread Rating of 2.000 (www.cpubenchmark.net)
- approx. 500 – 600 passmarks per channel for **Perimeter, Count (2D & 3D) & Object**
- SAIMOS® Face Analytics, requires 4 cores per channel
- SAIMOS® LPR requires 2 cores per channel

The operating system of the servers should be 64 bits while the following OS are supported:

- Ubuntu 18.04 & 20.04
- Windows Server (min. 2016)
- Windows 10 Professional / Enterprise (not recommended due to Windows Update issues)

The video analytics server(s) can be either physical or also virtual machines are supported.

Please note, that the suggested server sizing is considering SAIMOS® Video Analytics only.

1.3 FAILOVER AND REDUNDANCY

For SAIMOS failover and redundancy, it is recommended to use full virtualization of the setup with an Active / Passive failover strategy using technologies like VMware, vSphere, Fault Tolerance or similar (https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.avail.doc/GUID-7525F8DD-9B8F-4089-B020-BAA4AC6509D2.html) for the server.

Using this strategy does not require additional SAIMOS licensing fees.

For a processing node redundancy strategy it is also possible to setup a N:1 or N:N system with automatic channel migration on node failure. Live channel migration can be realized via RESTful interface commands.

For SAIMOS database backend redundancy, it is recommended to run the SAIMOS C3 database in a redundant PostgreSQL cluster.

2 TECHNOLOGY

Within the next sections, we're providing an overview regarding our SAIMOS® Video Analytics solutions.

2.1 SAIMOS® VIDEO ANALYTICS

SAIMOS® Video Analytics brings the power of our Video Analytics Framework into Milestone XProtect® in a seamless integrated way. It provides different algorithms for several use cases like perimeter security, people counting and left/removed object detection, face analytics, LPR, etc. and is optimised for CPU usage. By that, our CAPEX and OPEX is more efficient compared with professional GPU solutions.

The combination of SAIMOS® Video Analytics and Milestone XProtect® enables users to benefit from field proven analytics functionality provided by SAIMOS® while using the full capabilities of Milestone XProtect® for a comprehensive solution experience.

Configurations are made directly within the Milestone XProtect® Management Client.

SAIMOS® Video Analytics Products	
Perimeter	Person and object detection for indoor and outdoor use. Protects assets against unwanted intrusion with a flexible rule system for loitering, maximum speed and direction detection.
2D Counting	Person and object counting system for indoor and outdoor use Counts persons or objects and delivers insightful statistics and heatmaps as well as live occupancy data.
3D counting	Person counting by utilising 3D sensors, which results in higher accuracies compared to 2D counting.
Object	Left/removed object detection for indoor usage. Secures indoor areas against theft or left objects in low frequented areas like emergency exits, server rooms or pathways.
Scrambler	Real-time dynamic blurring of moving objects.
Face Analytics	Face Detection and -recognition, including blacklist and whitelist functionality. Can used indoors and outdoors as well as live and in forensics mode. Real-time alarm notifications.
LPR	License Plate Recognition for free-flow traffic as well as parking scenarios. Black- and whitelisting is supported and alarms could also trigger external I/O devices.
LiDAR	SAIMOS® does also integrate LiDAR sensors into its analytics engine and by that also into Milestone XProtect®. By that, we do support People Counting, Occupancy, Proximity Detection, Perimeter Protection, Cross-Camera Tracking and PTZ Object Tracking.

Milestone Integration Features	
Configuration within Milestone XProtect® Management Client	Manage all SAIMOS® analytic channels from within the Milestone XProtect® Management client. The embedded SAIMOS® Server view can be used for further configuration of the SAIMOS® components.
Automatic Event and Alarm creation	SAIMOS® VA channels with alarm capability will automatically generate Alarm definitions. The Alarm definitions can be adapted to the user's preferences using the standard Milestone Alarm definition interface. Alarms including metadata can be viewed within the Milestone XProtect® Smart Client Alarm view or in a custom view with Alarm List and Alarm preview.

Quick Overview:

2.2 SAIMOS® PERIMETER

The below list provides general description of the SAIMOS® Perimeter functionality:

- Person and object detection for indoor and outdoor use
- Protects assets against unwanted intrusion with a flexible rule system for loitering, maximum speed and direction detection.
- Offers a flexible rule system allowing for multiple possibilities to implement efficient area monitoring
- Is fully integrated into Milestone VMS via Plug In and can be configured directly within the Milestone VMS Management Client.
- The scene calibration and rule definition allow for an initial configuration in just a few minutes

General Overview:

- Person and object detection for indoor and outdoor use
- Perimeter Protection / Intrusion Detection
- Minimal false alarm rates by machine learning (AI)
- Flexible rule and zone system
- Configurable in a few steps

Below are some use-case examples:

- **Area Security:**
  - Securing outdoor areas by combining several rule sets
  - Detection of loitering and running persons for critical areas
  - Ensures that access to critical areas is not violated during certain hours

- **Perimeter Security:**
  - Protects the perimeter from unwanted intruders
  - Send alerts to a control room in case of an alarm
  - Definition of rules with direction restriction
  - Definition of pre-alarms for early detection of intruders

- **Indoor Security**
  - Creating complex scenarios for indoor systems
  - Connect Third Party alarms such as access control and fire safety
  - Control of the on/off state of channels with building security systems

Algorithms & Functions:

- Intrusion detection
- Loitering
- Direction detection
- Maximum allowed speed

Configuration

- Automatic camera detection / two individually configurable alarm zones
- Easy scene calibration based on body sizes directly in the live video view
- Intelligent system for minimized false alarm rates
- Optimized for 24/7 real-time operation

Technical Requirements:

- Minimal pixel density: 12 pixel / meter
- Windows / Linux | RAM: min. 4 GB | HDD: min. 5 GB | CPU: Intel/AMD/ARMv8

Performance:

Given a standard setup for perimeter protection with low to medium scene complexity, a F1 score in the range of 0.75 to 0.90 can be expected for standard IP camera setups as well as thermal camera setups. Whereas the F1 score is calculated as follows:

$$F_\beta = \frac{(1+\beta^2)\cdot \text{true positive}}{(1+\beta^2)\cdot \text{true positive} + \beta^2 \cdot \text{false negative} + \text{false positive}}$$

2.2.1 CAMERA SETUP

A standard camera setup for perimeter protection shall meet at least the following criteria:

- A camera setup for perimeter is defined as standard if either a standard IP camera with low light detection capability or a thermal camera with at least VGA resolution and a thermal resolution of <= 50 mK is used for the setup.
- The camera lens shall have at least 5mm focal length.
- It has to be mounted at a height between 3.5 – 5 m with a relative mounting angle to the ground of 10 – 20°.
- The target resolution of an object subject to detection shall be at least 12 px/m.
- Objects subject to detection must have a clear contrast relative to the scene background (at least 10% of pixel value difference for all possible intensity values).
- Additionally, the perimeter scene has to be free of obstacles within the detection zone and all possible disturbances that can influence the scene, like animals and plants or high grass, must to be minimized.

If the above requirements are exactly followed an accuracy of far beyond 85% can be achieved. However, changes in external conditions (such as lighting, weather, etc.) can negatively impact the overall scoring and accuracy of the analytics and increase the false alarm rate. In general, it should be understood that a maximum of 2 false alarm rates per camera per week can occur for a standard perimeter protection set-up.

2.3 SAIMOS® 2D COUNTING & HEATMAPPING

Within SAIMOS® C3 CORE, **Counting & Heatmapping** is a 2D functionality that comes within this license level. The below list provides general description of this functionality:

- 2D Person and object counting system for indoor and outdoor use.
- Counts persons or objects and delivers insightful statistics and heatmaps as well as live occupancy data.
- SAIMOS® Count is based on reliable and robust object counting and contains extensive statistical analysis, visualization and reports.
- Easily configurable real-time analysis in a modern design.
- Fully integrated into Milestone XProtect via Plug In and can be configured directly within the Milestone XProtect Management Client.
- Flexible Dashboard

Below are some use-case examples:

- **Shop Optimization:**
  - Customer flow analysis: Where and when do how many people move?
  - Optimization of product assortments
  - The right number of employees at the right time

- **Center Management:**
  - Detailed analysis of visitor frequency
  - Quantification of the number of visitors in the shops
  - Frequency-dependent facility management

- **Event Management Analysis of the area capacity:**
  - Occupancy monitoring

Algorithms & Functions:

- **Frequency analysis:**
  - Counts persons or objects entering or leaving an area
  - Each channel can contain any number of counting zones
  - Full flexibility through elegant area system
  - Modern and flexible statistics with a wide range of filter options

- **Occupancy analysis:**
  - Combines one or more counting areas into one occupancy monitor
  - Sends alerts for customizable occupancy scenarios
  - Provides occupancy statistics for analysis and planning

- **Heatmapping:**
  - Shows which areas are more or less frequented
  - Adjustable visualization and differing colour schemes
  - Can be filtered by time range

- **Dashboard:**
  - Summary of all evaluation modules in a customizable overview

- **Reports:**
  - Automatically email reports to any number of recipients or save them to a physical data source

Data Interfaces:

- RESTful / Modbus IP

Technical Requirements:

- Minimal pixel density: 12 pixel / meter
- Windows / Linux | RAM: min. 4 GB | HDD: min. 5 GB | CPU: Intel/AMD/ARMv8

2.3.1 CAMERA SETUP

Given an optimal counting setup, counting accuracies of far beyond 80% can be expected from the system. Nevertheless, we do have installations with +95% accuracy. An optimal counting setup is defined as follows:

For an optimal 2D counting setup, a camera has to be mounted on top of the respective counting area with its lens having a relative angle of 90° to the floor (top down). The resulting target resolution of an object to be counted has to be at least 12 px/m where the respective object has to have a clear contrast compared to the scene background (at least 10% of pixel value difference for all possible intensity values).

The lens of the camera has to have a focal length of at least 3mm and has to cover the whole counting area for all object heights subject to counting. Objects subject to counting have to be clearly visible while entering and exiting the respective counting area. The targeted scene must not allow for crowding of objects and has to guarantee a minimal occluded object flow throughout the scene where the possibility of object merges has to be minimized.

2.4 SAIMOS® OBJECT

The below list provides general description of the SAIMOS® Object functionality:

- Left/removed object detection Secures indoor areas to identify theft or left objects in low frequented areas like emergency exits, server rooms or corridors.
- SAIMOS® Object detects left or removed objects in indoor scenarios.
- Customized configuration of target object sizes and detection parameters supports optimal adaption as per individual application scenarios.
- SAIMOS® Object is used to monitor emergency exits, escape routes, service corridors, server rooms and similar environments.
- Surveillance of critical areas in shops, museums or airports are additional areas of application.
- Fully integrated into Milestone VMS via Plug-In and can be configured directly within the Milestone VMS Management Client.

General Overview:

- Left/removed object detection for indoors
  Detection for left or removed objects for indoor usage
- For low frequented regions that should stay free of obstacles
- Adjustable object-size & timely detection
- Works also for observation periods > 5 min

Below are some use-case examples:

- **Critical Infrastructure:**
  - Securing critical infrastructure against
  - Blocking of pathways
  - Blocking of entries or emergency exits
  - Loitering
  - Left/removed objects
- **Theft detection / Secure your inventory:**
  - Detect object removal from desks or walls, etc.

Algorithms & Functions:

- Detects left or removed objects
- Variable object size
- Configurable alert timeout
- Optimized for indoor scenarios with stable light conditions

Configuration:

- Easy scene calibration based on object sizes directly in the live video view
- Optimized for 24/7 real-time operation

Technical Requirements:

- Minimal pixel density: 12 pixel / meter
- Windows / Linux | RAM: min. 4 GB | HDD: min. 5 GB | CPU: Intel/AMD/ARMv8

Performance:

Given an optimal setup to detect left or removed objects, a F1 score for left/removed object detection of 0.6 or higher can be expected. Where the F1 score is calculated as follows:

$$F_\beta = \frac{(1+\beta^2)\cdot \text{true positive}}{(1+\beta^2)\cdot \text{true positive} + \beta^2 \cdot \text{false negative} + \text{false positive}}$$

2.4.1 CAMERA SETUP

An optimal setup for left/removed object detection shall meet at least the following criteria:

- For a 2D left/removed object detection the camera has to be mounted in a position that the target object is fully visible within the resulting scene and does not cover more than 40 % of the full scene view.
- The resolution of a target object has to be at least 30 x 30 px where the respective object has to have a clear contrast compared to the scene background (at least 10% of pixel value difference for all possible intensity values).
- The lens of the camera has to have a focal length of at least 3mm. The observed scene must not allow for crowding of objects and has to guarantee a minimal occluded object flow throughout the scene.
- A scene for left/removed object detection must to be indoors with constant light conditions throughout the scene and detection period.
- There must be no external light influences.
- The detection scene has to have a minimal frequency in respect of people / crowding.

If the above requirements are exactly followed an accuracy of far beyond 85% can be achieved. However, changes in external conditions (such as lighting, weather, etc.) can negatively impact the overall scoring and accuracy of the analytics and increase the false alarm rate. In general, it should be understood that a maximum of 2 false alarm rates per camera per week can occur for a standard perimeter protection set-up.

2.5 SAIMOS® FACE ANALYTICS

The below list provides general description of the SAIMOS® Face Analytics functionality:

- Face Detection and Recognition utilizing AI
- Face Reports (count, time, etc.)
- Grouping & sorting of equal faces
- Live and Forensics mode
- Blacklist/Whitelist
- Reporting for time efficient evaluation
- Alarm notifications via pop-up window

General Overview:

- Dedicated cameras with respective positions for face recognition should be used to reach a good detection- and recognition performance
- Dedicated setup planning is recommended
- Dedicated camera streams from the cameras are recommended
- MJPEG HTTP for maximum image quality
    - Live Setup with forensic analytics possibility
- Real-time Detection:
    - Instant feature calculation
    - Instant Blacklist matching (1:N)
    - Additional factor for Access (1:1, special project requirements)
- Comprehensive face logging
    - Face including overview image
    - Labeling for Black/Whitelists
    - Commenting for auditing and reporting
- Person database
    - Comment on a person
    - Manage images of a person

Below are some use-case examples:

- **No Mask Detection:**
    - Detect people not wearing face masks
- **Blacklisting:**
    - Receive alarms on unwanted persons (e.g. shoplifters, etc.)
- **Whitelisting**:
    - VIP recognition for improved customer experience
    - Receive images from non-registered persons entering your premises
- **Access Control:**
    - Complement access control systems with face recognition
- **Observations (for authorities only):**
    - Time-efficient analysis of collected video evidence during observations

Algorithms & Functions:

- Detection (FuSt) → Deep Learning – FDDB +85% on ROC
- Recognition (Fully End-to-End Cascaded CNN for Facial Landmark Detection)
- 97% mean accuracy based on Image-Restricted LFW (please refer to http://vis-www.cs.umass.edu/lfw/)
- Parameter to adjust the level of similarity in face recognition
- Several algorithms available for face detection to support different scenarios
- Optimized for CPU usage

Configuration:

- Easy scene calibration based on object sizes directly in the live video view
- Optimized for 24/7 real-time operation

Technical Requirements:

- Minimal pixel density: 150 pixel / meter
- Windows / Linux | RAM: min. 4 GB | HDD: min. 5 GB | CPU: Intel, 4 cores per channel

Storage Requirements:

- Approx. 500 KB per detected face
- For example, 500 persons per day will require a storage of approx. 200GB per annum

2.5.1 CAMERA SETUP

An optimal setup for Face Analytics shall meet at least the following criteria:

- Camera position is important for the setup performance
  - As frontal as possible
  - Max. deviation angle of +/- 15° horizontally and vertically
- Concentrated on the faces not the overall scene
- minimum 350 px/m (min. 100 px/face) for good recognition results
- Lighting conditions should be stable with as little shadow effects as possible
- Contrast should be optimal (day and night)

If the above requirements are followed an accuracy of far beyond 80% can be achieved. However, changes in external conditions (such as lighting, weather, etc.) can negatively impact the overall scoring and accuracy of the analytics and increase the false alarm rate. In general, it should be understood that false alarm rates heavily depend on the camera positions, environmental conditions, people wearing sunglasses, non-frontal faces, etc.

2.5.2 NOTES FOR THE NO MASK DETECTION USE CASE

Using SAIMOS Face Analytics for no mask detection requires only the face detection algorithm for detecting faces that have a very high detection probability. There is no face recognition for re-identification used.

This means that the camera setup needs to be to the optimum as best possible (see 2.5.1 above) in order to have the detector best tuned towards a no-mask detection, which itself is an inversion of not detecting a complete face. Bad or non-optimal setups will inevitably lead towards a higher false detection rate as the used detector is quite sensitive for also detection partial faces.

Using only the detection mode of SAIMOS Face analytics does not include recognition algorithms. Only lower re-identification methods are utilised for successfully tracking the same face throughout the scene, which does not result in the storage of a feature-vector, which could be used for re-identification of individuals. These tracking re-identification methods do not store detection features permanently on a hard disk but are used within the temporary RAM for a configurable number of seconds. The usage of these methods is to reduce the amount of detections as well as to distinguish one face from the other within the same frame of a stream and do not identify individuals or persons.

2.6 SAIMOS® LPR

The below list provides general description of the SAIMOS® LPR functionality:

- Automated License Plate Recognition (ANPR / LPR)
- License plate Search & Reports (count, time, etc.)
- Live- and Forensics mode
- Blacklist/Whitelist
- Alarm notifications via pop-up window
- I/O connectivity toward barriers and other equipment
- Parking as well as free flow traffic

General Overview:

- Dedicated cameras with respective positions for LPR should be used to reach a good detection- and recognition performance
- Dedicated setup planning is recommended
- Dedicated camera streams from the cameras are recommended
- MJPEG HTTP for maximum image quality
- Real-time Detection
- Comprehensive logging of license plates
    - License plate including overview image
    - Labeling for Black/Whitelists
    - Commenting for auditing and reporting

Below are some use-case examples:

- **Car Park:**
    - Automatically open the barrier on registered license plates
    - Automated ticketing and invoicing system
    - Could be combined with Face Recognition
- **Petrol Station:**
    - Log vehicles retention time for business intelligence and performance evaluation
    - Get knowledge about your loyal returning customers
    - Reduce petrol theft
- **Hotel Parking**:
    - VIP recognition for improved customer experience
    - Support valet parking services
    - Comply with local regulations
- **Truck loading bays:**
    - Automatically open the barrier for registered license plates
    - Log vehicles retention time for business intelligence and performance evaluation
- **Smart City:**
    - Control traffic
    - Apply city taxes based on a pay-by-usage model

Algorithms & Functions:

- Nearly world-wide license plate coverage
- Deep-learning based algorithm
- Parameter to adjust the usage for free-flow traffic or parking
- Optimized for CPU usage

Configuration:

- Easy scene calibration based on object sizes directly in the live video view
- Optimized for 24/7 real-time operation

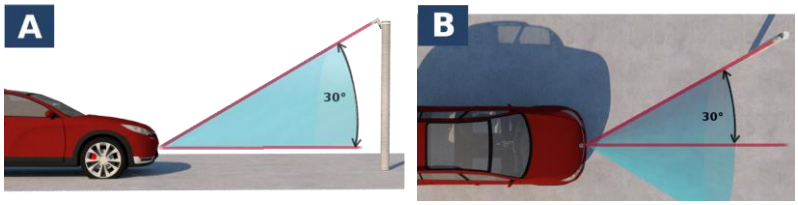
Technical Requirements:

- Absolute minimal character height: 8 pixels
- Recommended minimal character height: 12 pixels
- Windows / Linux | RAM: min. 4 GB | HDD: min. 5 GB | CPU: Intel, 4 cores per channel

2.6.1 CAMERA SETUP

An optimal setup for LPR for access control applications (car parking) using a camera with an 8mm lens shall meet at least the following criteria:

- The working distance of a camera with an 8mm lens ranges from 2-8 m (12mm lens ranges from 4-16 m)
- It is recommended to switch the camera to high resolution mode if its needs to read at distances above 4 m
- The camera should be mounted and stabilized on a place which is least 2 meters away from the closest position where the License Plate is expected. Closer distances can work, but the reading accuracy may be less in those situations.
- Camera position is important for the setup performance
    - The viewing angle from the camera to the license plate should not exceed 30° in any direction
    - The field of view of the camera is 30° horizontally, and 20° vertically



    - The camera should be mounted at least 2 meters from the expected closest position of a license plate
    - License plate rotations shall not exceed 20° clockwise or counter clockwise

Under all conditions, images should be sharp, with minimal motion blur, and of proper exposure. The license plates should not at all be overexposed - if you have to make a choice, it's better to have slightly darker images than too bright ones.

Achieving a reasonable image quality is sometimes not trivial, and a careful consideration of an installation must include:

- Illumination conditions at the location
- Required sensor resolution
- Gain and shutter settings

As a general recommendation, the following exposure (shutter) times are advised:

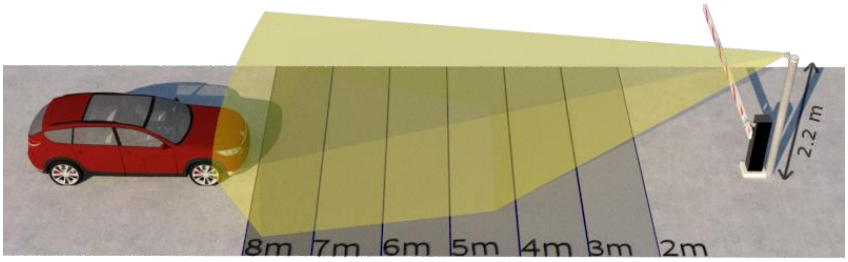
- on highways, for **high speed** vehicles - a shutter time of 0.1-3 ms is recommended
- in urban areas, for **medium speed** vehicles - a shutter time of 0.1-3 ms is recommended
- in parking situations, for **slow vehicles** - a shutter time of 1-20 ms is recommended

Taking control of the camera imaging sensor is most important when it comes to obtaining a good image quality day and night and under all possible illumination conditions.

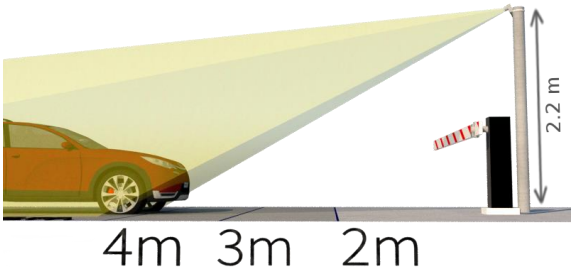
A camera in an outdoor environment or close to that (e.g. the exit of a parking garage) is subject to harsh illumination from the sun which might create reflections, or from headlights of cars which may beam directly into the camera mounted at the gate.

For best reading results, it's recommended to mount the camera on a minimum height of ca. 80cm. This avoids the disturbance of the vehicle headlights shining directly into the camera, which otherwise might reduce the image quality when the vehicle is very close to the camera.

Alternatively, it's possible to mount the camera on a hight of approx. 2,20m but this may limit the useful range within which license plates can be read.



From this height and perspective, the camera recognizes vehicles resp. their plates, which are more than 4 meters away from its position. Tilting the camera further down would make the viewing angle to the plates too steep (more than 30°), and as a consequence decrease the reading performance.



2.6.2 SUPPORTED COUNTRIES

Following default European classifiers are available (other classifiers can be created on demand):

- Europe Standard: Austria, Belgium, Bulgaria, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom
- Europe Full (all countries except of Russia)
- Europe Full incl. Russia (slower)
- Europe Central West: Austria, Belgium, Czech Republic, France, Germany, Hungary, Italy, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Switzerland, United Kingdom
- Europe North: Denmark, Finland, Norway, Sweden
- Europe North East: Belarus, Estonia, Latvia, Lithuania, Russia, Ukraine
- Europe South East: Bulgaria, Croatia, Greece, Montenegro, Serbia, Turkey

Europe

- Austria
- Belarus
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Moldova
- Monaco
- Montenegro
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Russia
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Ukraine
- United Kingdom

North America

- Canada (incl. state recognition)
- Mexico
- USA (all states, incl. state recognition)

South America

- Brazil
- Colombia
- Peru

Oceania

- Australia (incl. state recognition)
- New Zealand

Africa

- Egypt
- Kenya
- Morocco
- South Africa

Middle East

- Bahrain
- Israel
- Jordan
- Kuwait
- Oman
- Qatar
- Saudi Arabia
- Turkey
- United Arab Emirates (incl. state recognition)

Asia

- Armenia
- Azerbaijan
- Brunei
- China
- Georgia
- Hong Kong
- India
- Indonesia
- Kazakhstan
- Kyrgyzstan
- Malaysia
- Philippines
- Singapore
- Taiwan
- Thailand (incl. province recognition)
- Uzbekistan

2.7 SAIMOS® SCRAMBLER

SAIMOS® Scrambler is a privacy functionality, which provided dynamic real-time blurring. The below list provides general description of this functionality:

- Reliably scrambles moving and/or static areas within video streams for privacy protection in monitored areas.
- User-friendly configuration for simple setup - with polygonal shapes directly in the live video view - enable basic configuration within a few minutes.
- Supports seamless integration with Milestone XProtect and Siveillance VMS video management system.

General workflow of blurring:

Below are some use-case examples:

- **Surveillance of Public Areas**
  - Dynamic and static blurring for public places
    - Company areas with public access
  - Permanently and/or dynamically blurring of critical public areas
  - SAIMOS® Scrambler can be coupled with external alerts via TCP interface to disable
  - Scrambling when a critical event occurs

- **Surveillance of exclusive areas**
  - Disguise surveillance data in high-security environments or exclusive areas to protect the privacy of the individuals being monitored
  - Permanent and/or dynamic scrambling of private areas
  - Disabling of the scrambling via the TCP interface when alarm keys are pressed, or certain events occur

Algorithms & Functions:

- Scrambling of static areas
- Scrambling of dynamic areas based on motion detection
- Configurable scrambling size
- Flexible definition of static scrambling areas and areas of interest with polygons
- TCP interface for activating/deactivating scrambling if required
- Streaming of the encrypted stream via RTSP to VMS systems

Configuration

- Automatic camera detection
- Unlimited number of individually configurable scrambling zones

- Easy calibration
- Optimized for 24/7 real-time use
- User-friendly, browser-based user interface with appealing design

Stream Integration

- RTSP (H.264, MJPEG, MPEG4 | TCP / UDP) HTTP/HTTPS (MJPEG, H.264, MPEG4)

2.7.1 INTEGRATION WITH MILESTONE XPROTECT®

There are 3 different approaches to integrate SAIMOS® Scrambler with Milestone XProtect®:

1. **Protocol Integration**
   Input (SAIMOS): Milestone (Protocol Integration)
   Output: Milestone Universal Driver (1, 16, 64)
   a. An existing camera stream directly from Milestone is used as input for SAIMOS Scrambler. The output is then re-integrated as a virtual camera via the Universal Driver.
   b. The original stream is secured by advanced rights management of Milestone and only certain users can access the original stream.
   c. This is the option with the lowest latency due to the direct interfacing with Milestone XProtect
   d. Control of the scrambling (on/off) is possible via TCP commands (optional).

2. **Dual-Stream RTSP /HTTP**
   Input (SAIMOS + Milestone): Camera (RTSP, HTTP)
   Output: Milestone Universal Driver (1, 16, 64)
   a. In this variant the SAIMOS Scrambler retrieves the stream directly from the camera. Mostly the retrieved stream has a lower resolution (e. g. VGA). Additionally, the original high-resolution stream is recorded by Milestone. The output of the SAIMOS Scrambler is added to the Milestone system via the Universal Driver.
   b. The original stream is secured by advanced rights management of Milestone and only certain users can access the original stream.
   c. This variant can introduce latencies between the high-resolution stream and the scrambled stream as both are completely independent streams used by two different applications.
   d. Control of the scrambling (on/off) is possible via TCP commands (optional).
   e. This is the option with the lowest requirements regarding performance for the SAIMOS Scrambler and the Milestone XProtect Recording Server.

3. **Single-Stream RTSP / HTTP**
   Input (C3): Camera (RTSP, HTTP)
   Output: Milestone Universal Driver (1, 16, 64)
   a. In this variant the SAIMOS Scrambler retrieves the stream directly from the camera. Mostly the retrieved stream has a lower resolution (e. g. VGA). The output of the SAIMOS Scrambler is added to the Milestone system via the Universal Driver.
   b. There is no original stream without scrambling.
   c. Control of the scrambling (on/off) is possible via TCP commands (optional). Normally, if an alarm is triggered the scrambling is removed from the stream to ensure recording of the un-scrambled stream.
   d. This option has a high risk that information is lost in case of an emergency.

2.7.2 PERFORMANCE

Due to various stream resolutions and methods of integration, it is not possible to predict the performance of the SAIMOS Scrambler to 100 %. It depends on multiple factors like the size of the scrambling, the complexity of the scene and the chosen resolution (also input to output). The most performance of the application is consumed by the encoder. These are the general performance values:

- approx. 800 Passmark with 360p→360p (1 Mbit),
  - 8x8 scrambling with 15 FPS, 25 % static scrambling
  - approx. 30 – 80 MB RAM per channel
- approx. 2100 Passmark with 720p → 720p (3 Mbit),
  - 16x16 scrambling with 15 FPS, 25 % static scrambling
  - approx. 250 MB RAM per channel

For these performance values we assume a process with at least 4 real cores having a Single Thread Rating (by Passmark) of at least 2000 (mostly processors between 2.9 and 4 GHz). For dynamic blurring, we recommend to use a stream with low resolution as the most important details will be scrambled anyways.

A scrambling of streams with more than 720p is not recommended by SAIMOS.

The application is sandboxed and every channel runs as independent process on the OS. This means virtualization as well as multi socket system are perfectly possible and have no impact on performance of the SAIMOS Scrambler.

3 CONTACT DETAILS

Below are our contact details:

ONG-IT GmbH
Stiftgasse 27
1070 Vienna
Austria

Tel.: +43 1 997 13 69
Fax: +43 1 997 13 69 – 555
eMail: contact@saimos.eu
www: www.saimos.eu