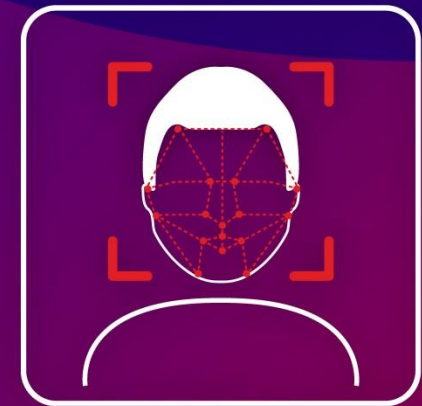




Facial Recognition 2.0

New Focus on Face Recognition
TRASSIR video analytics module for facial
recognition



The TRASSIR brand was created to bring high-tech CCTV systems to the market. The brand combines professional video processing equipment (cameras, servers, analytics modules) and neural network-based software. TRASSIR analytics modules are used for monitoring and providing access to the premises, monitoring the perimeter, delimiting dangerous areas, and monitoring the wearing of protective clothing.

The equipment's primary function is to ensure customer safety while enhancing the business's efficiency. The TRASSIR brand has developed and patented ground-breaking technologies, such as: IP video servers, the most powerful video recorders and NVRs, flagship proprietary IP cameras.

20 years
of experience in video surveillance

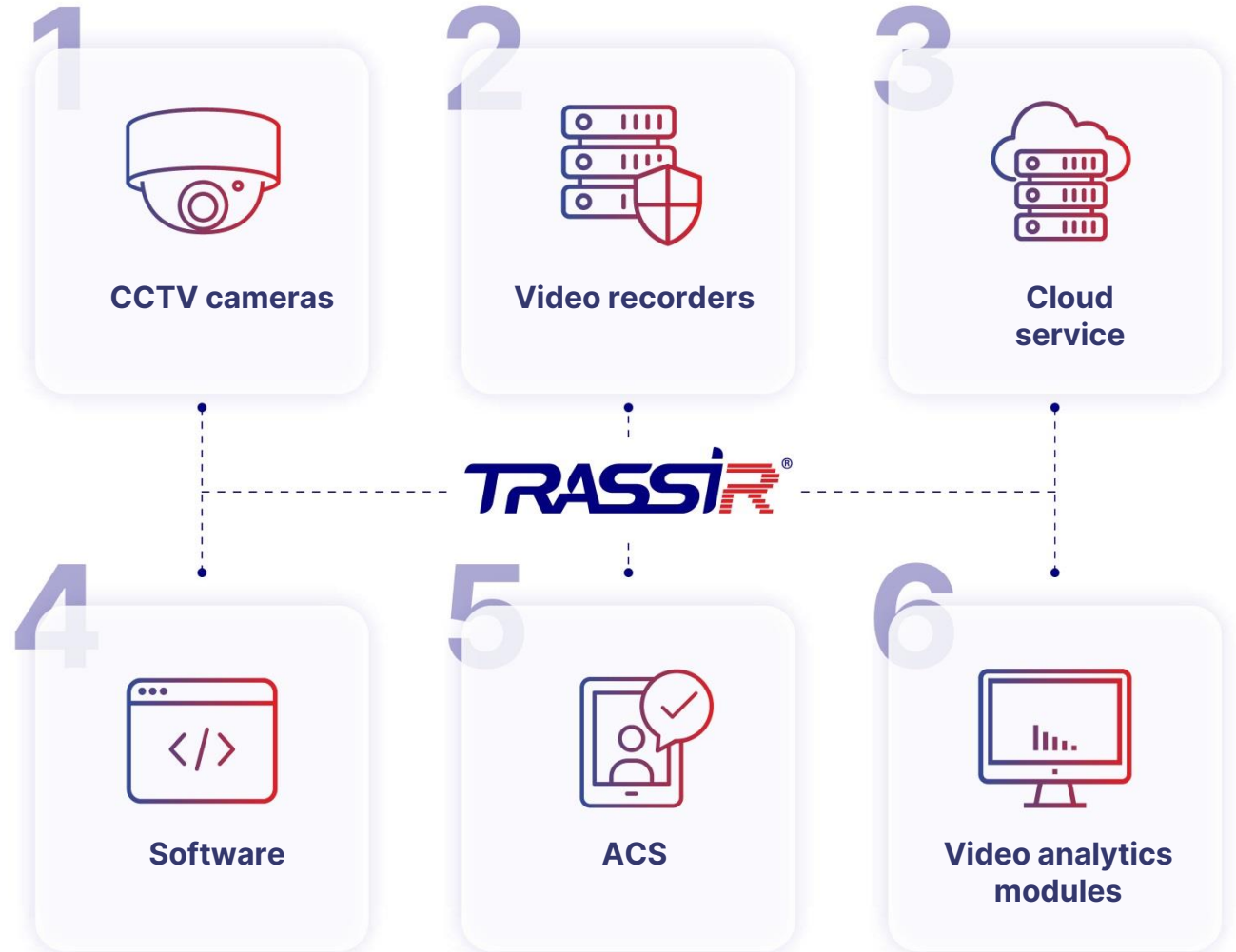
5000+
loyal customers worldwide

800+
qualified staff

35
countries
with TRASSIR solutions integrated



**TRASSIR ecosystem
for effective
security monitoring**



TRASSIR Face Recognition 2.0 – a new and improved version of the Face Recognition smart video analytics module for facial recognition and people search based on a pre-configured database.

Highly efficient and reliable, provides accurate recognition in a variety of scenarios.

Face recognition



Facial Recognition 2.0

The operating principle of the module is to create a database of faces and check each detected face in real-time to see if it matches anyone in the database.

- Face detection quality – 99.8%

- Works as both part of a single server and as a component of a multi-server system with a single face database

- Includes the option to copy and synchronise the face database

- Allows database imports with photos for recognition and search



Face Recognition 2.0 Module Features

CAPACITY TO RECOGNISE THE USE OF FRAMED PHOTOS, DETERMINATION OF 'LIVE' FACE MIMICKING

Operates using passive detection technology, which is suitable for access control: it can distinguish a live person from a photo being used for deceptive purposes.

The neural network analyses frames and captures changes in the face compared to a static image.



ADVANTAGES:

- ✓ Facial interaction is not required for detection by the system
- ✓ The module is compatible with any existing equipment
- ✓ Requires fewer resources than previous versions

SEARCHING FOR PEOPLE BASED ON CERTAIN APPEARANCE ATTRIBUTES

Enables facial attributes to be obtained for advanced analytics and to search for people based on specific parameters (race, age, sex, hair colour, beard, moustache, glasses, headwear, protective mask, etc).

The face database can be accessed from a local or remote TRASSIR server with the option to copy, import and synchronise the face database.

CREATING A DATABASE OF UNIQUE PERSONS

The database of unique persons stores reference photos for making comparisons. All appearances of the person recognised in the video are viewed in the face log.

How filtering happens

Searching for an intruder using attribute filters is lightning fast. The route of movement can be traced and used to help identify potential accomplices. Filter features: sex, age, race, facial hair, headwear, glasses, emotions, hair colour, mask.

1

How the database of unique persons is created

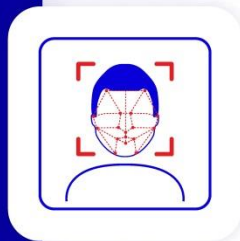
The appearance of the same face in a video frame is automatically entered into 'Person', like a folder on a computer. 'Person' speeds up and simplifies the search of the large video archive and in real-time video streams from CCTV cameras.

2

USING A CENTRAL FACE DATABASE

Multi-server system support

Face Recognition 2.0 supports a multi-server system: it successfully operates as both part of a single server and in a multi-server system with a single Face Database, thereby saving server resources.



Database synchronisation

Enables the face database to be copied and synchronised, which is crucial for efficient operation with an unstable communication channel.

COUNTING UNIQUE VISITORS

The visitor analytics function is integrated with the TRASSIR Face Recognition 2.0 module with the TRASSIR Face Analytics module – a face recognition and analytics module.

Counting unique visitors

TRASSIR Face Recognition 2.0 recognises unique visitors and allows you to set up face counters on connected cameras. Accurately determines the number of people in the frame.

Advantages:

The visitor counting function is to monitor queues and waiting areas, as well as public gatherings; it also prevents suspicious unauthorised gatherings.

Visitor analytics

TRASSIR Face Analytics analyses data and collects statistics on sex, age, and number of unique and returning visitors. Improves the quality of service and offers the goods and services you actually need.

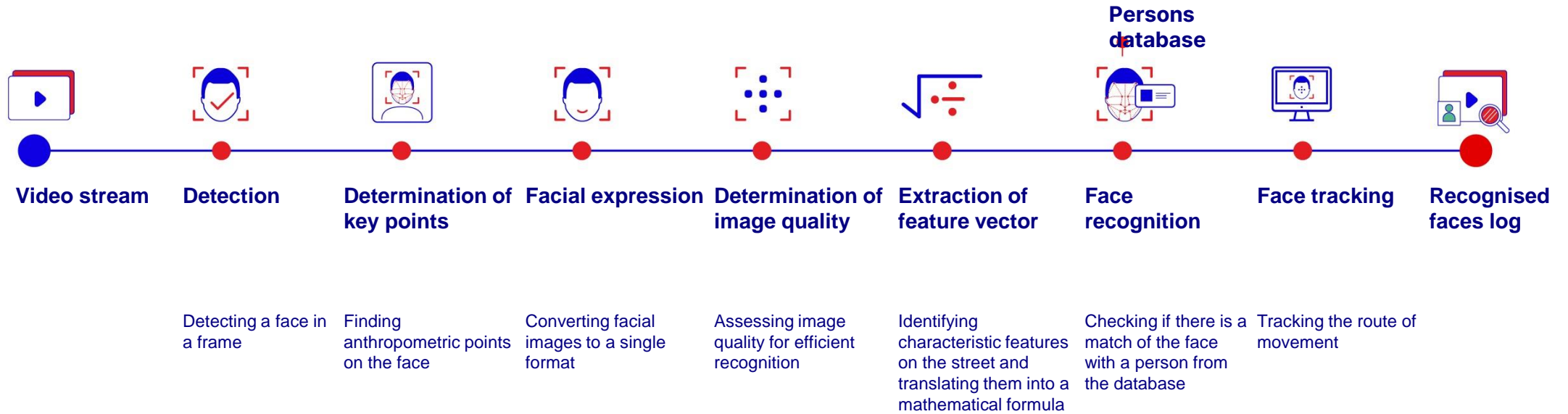
Advantages:

Collection and analysis of accurate quantitative data about visitors at facilities and events improves security and event organisation.



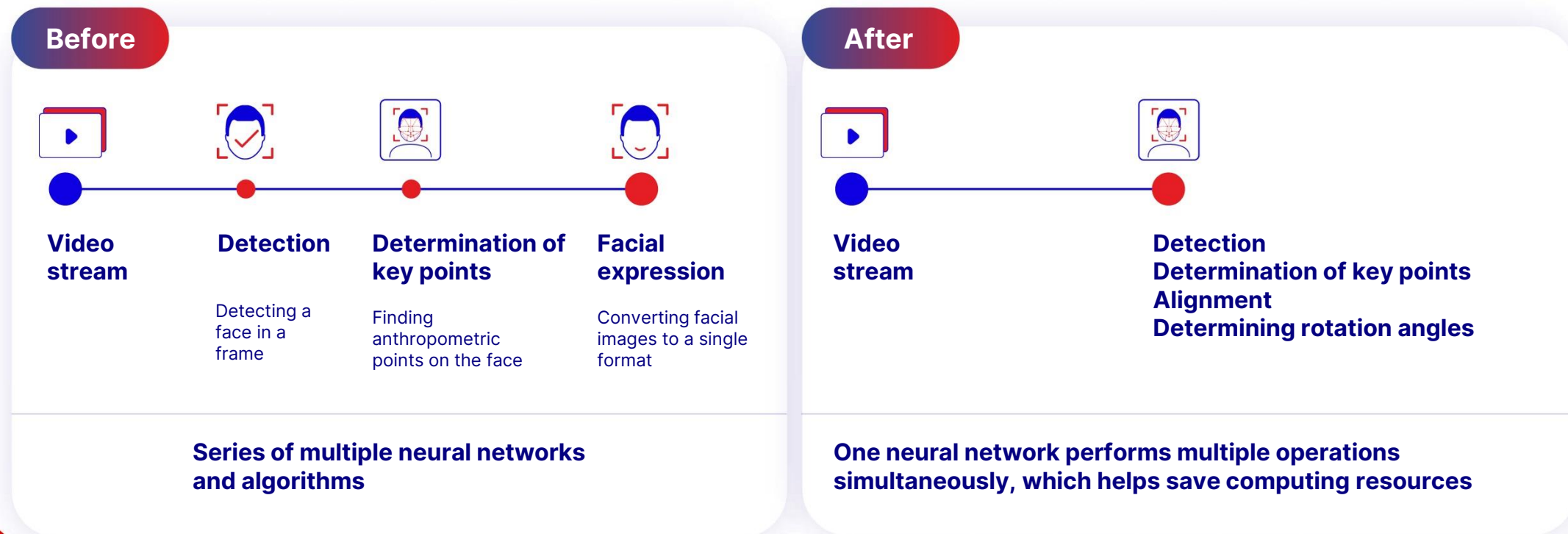
Face Recognition 2.0 Module Features

HOW DOES FACE RECOGNITION WORK?



UPDATED FEATURE: UNIQUE ARCHITECTURE

We developed a unique architecture that allows multiple stages of face recognition to be performed simultaneously.



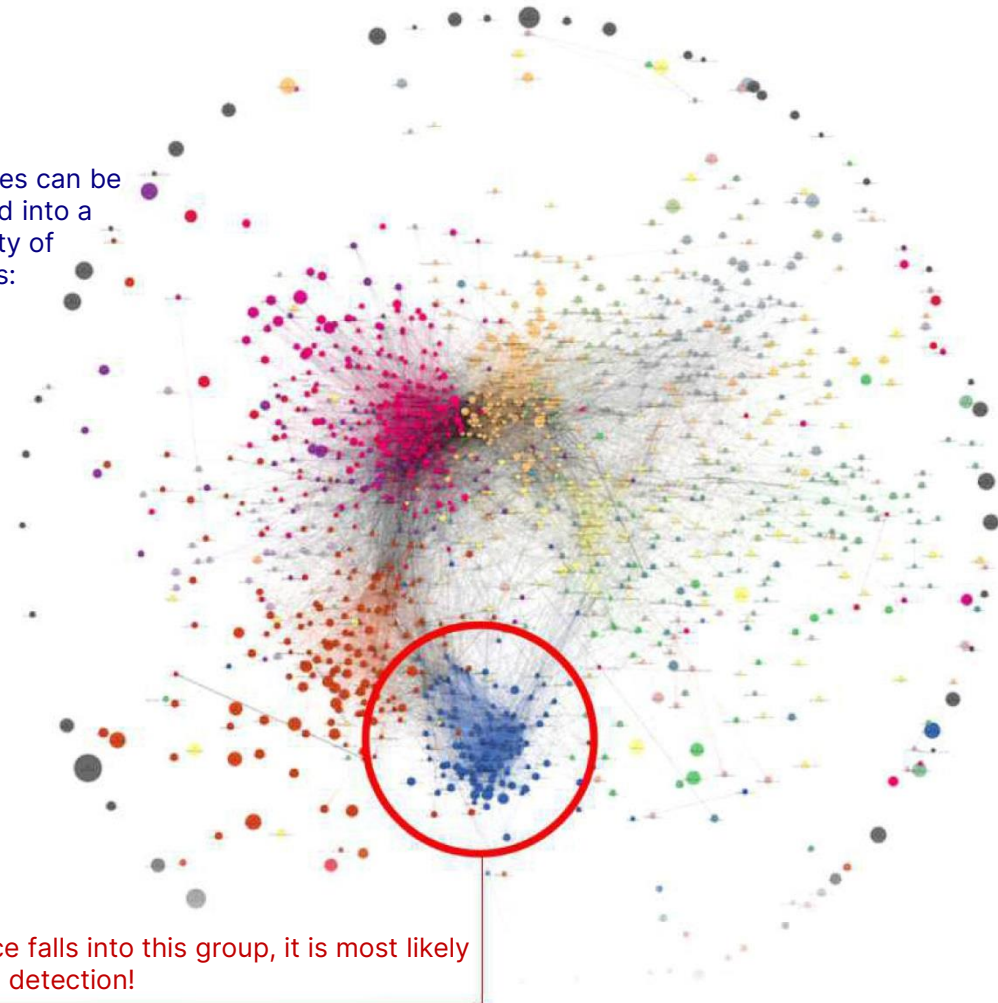
UPDATED FEATURE: FALSE DETECTION FILTERING TECHNOLOGY

We implemented a new false detection filtering technology based on clustering.

Operating principle

- **Faces are distributed into clusters by similarity**
The neural network conditionally distributes faces into 400,000 clusters grouped by similarity and determines which cluster it belongs to
- **A 'garbage cluster' is formed**
The 'garbage' cluster includes low-quality facial images and images of objects that are not faces
- **False detection is identified and discarded**
After highlighting facial features, the face is checked if it falls in the 'garbage cluster'. If it falls into this cluster, it is most likely a false detection and is discarded

All faces can be divided into a plurality of groups:



UPDATED FEATURES: HIGH-PRECISION FACE TRACKING MECHANISM

We introduced a new face tracking mechanism.

Before: optical tracking

- Low efficiency when faces overlap with each other
- Low efficiency with a bad angle

Now: feature vector-based tracking

- If a face disappeared from the frame and then reappeared, a new tracker matched it with a previously detected track and compared unique facial features



COMPARING INDICATORS

Face detection quality:

- Old version 88%
- New version 99.8%

Quality of recognition:

- At difficult angles, the new version has 20% better recognition

Number of false face recognitions:

- Old version 11%
- New version ~0%

Number of false detections:

- The number of false face detections (arms, legs, bags etc) drops to 0



**Ready-made business
and security solutions
with Face Recognition 2.0**



BANKING SECTOR

→ Detecting forged documents

If it is suspected that a client has presented a falsified contract to another person for the purposes of withdrawal, the manager can compare a photo of the genuine owner of the agreement from the CPM database with the potential fraudster. Takes action if fraud is confirmed.

→ Detecting bank card theft

A client forgot their card in the ATM, the next client pulled it out before the ATM could withhold it and made purchases. The incident was investigated: the face of the thief was recognised and blacklisted.

→ Preventing transactions with someone else's bank card

The system recognises the face of the person making transactions with a card at an ATM and compares it with the photo of the genuine card owner from the CPM. If there is a discrepancy, the manager contacts the real owner or blocks the card.

→ Preventing unauthorised access to data

An access control system with dual authorisation based on biometric features will help prevent intruders from entering the bank office and leaking information. Thus, the use of a stolen pass or someone else's pass in collusion with its owner is avoided. The thief's face is recognised and blacklisted.

RETAIL

→ Tackling theft

Upon detecting theft, the thief's face is recognised and placed on a single 'black list'. If the thief returns, they are either barred from entering or their actions are carefully monitored.

→ Tackling employee fraud

Facial recognition detects employee attendance, detects 'phantom workers' employed so that someone else can receive their salary, and prevents fraud committed by using other another employee's pass to register working hours.



INDUSTRY

→ Preventing theft, vandalism, terrorism

Security personnel at large companies cannot physically remember the faces of every employee and hired worker. Therefore, it is possible for unauthorized persons to enter the site using a fake pass. An access control system integrated with face recognition modules identifies authorized persons and does not let intruders through.

→ Maintaining privacy

An access control system with identifier- and face-based authorisation, uses a face recognition module to prevent unauthorised access as a result of stolen identifiers or their transfer to third parties.

→ Monitoring visits to the company

An access control system is deceived by presenting an identifier and a large photograph of its owner at the checkpoint rather than the actual person's face to simulate the person's arrival at the workplace, concealing absenteeism. Face 'aliveness' recognition technology will detect such fraud.



BUSINESS CENTRES AND OFFICES

→ Monitoring employee performance

The access control system is integrated with the face recognition module to determine the employee's arrival and departure time, actual working hours, time spent in the break room, and movement between rooms, and automatically generates an action report.



RESTAURANTS AND HOTELS

→ Brand promotion on the internet, advertising effectiveness assessment

Face Recognition 2.0 recognises unique and returning visitors, performs demographic analytics, and calculates conversion. The analytics performed improve the effectiveness of targeted advertising, after which Face Recognition 2.0 calculates the influx of new unique visitors.

→ Monitoring employee performance

Security personnel at large restaurants cannot remember the faces of every employee and therefore cannot recognise the person violating workplace rules. Face Recognition 2.0 recognises violators and automatically generates reports on hours worked and time spent away from the workplace, which form the basis for sanctions or disciplinary action.



TRASSIR®

Recommendations Camera and Recorder Selection



SELECTING A CAMERA



For the detector to function correctly, the distance between pupils in the resulting image must be at least 60px.

The average distance between pupils in an adult is 64mm. Therefore, the pixel density in the capture area should be $60/64 \sim 0.938\text{px/mm} = 938\text{px/m}$.



The required camera resolution depends on the width of the field of view:

- ✓ With an object distance of 5 metres and a field width view of 2 metres, the required resolution is 2MP

- ✓ With a width of 3 metres – 5MP

- ✓ With a width of 4 metres – 8MP

TRASSIR CAMERAS FOR FACE RECOGNITION 2.0 MODULE

COMPANY ACCESS CONTROL SYSTEM



TR-D2D2 v2

- ➔ 2MP resolution
- ➔ Matrix 1/2.9, sensitivity 0.003lx
- ➔ Indoor casing

SHOP ENTRANCE



TR-D4151IR1

- ➔ 5MP resolution
- ➔ Matrix 1/2.8, sensitivity 0.003lx
- ➔ Neat casing that does not attract attention

CAFE/RESTAURANT ENTRANCE



TR-D8181IR3 v2

- ➔ 8MP resolution
- ➔ Matrix 1/2.7, sensitivity 0.005lx
- ➔ Casing suitable for both indoor and outdoor use

TRASSIR RECORDERS FOR FACE RECOGNITION 2.0 MODULE



NeuroStation Compact RE

Low-cost network recorder for IP cameras running TRASSIR OS (Linux) with video analytics support

Up to 10 available channels for the Face Recognition 2.0 module



NeuroStation

Best network recorder option when it comes to value for money and video analytics support

Up to 26 available channels for the Face Recognition 2.0 module



UltraStation - I

Resilient high-capacity video servers with reliable data storage up to 465.66TB

Up to 13 available channels for the Face Recognition 2.0 module



trassir.com



welcome@trassir.com

