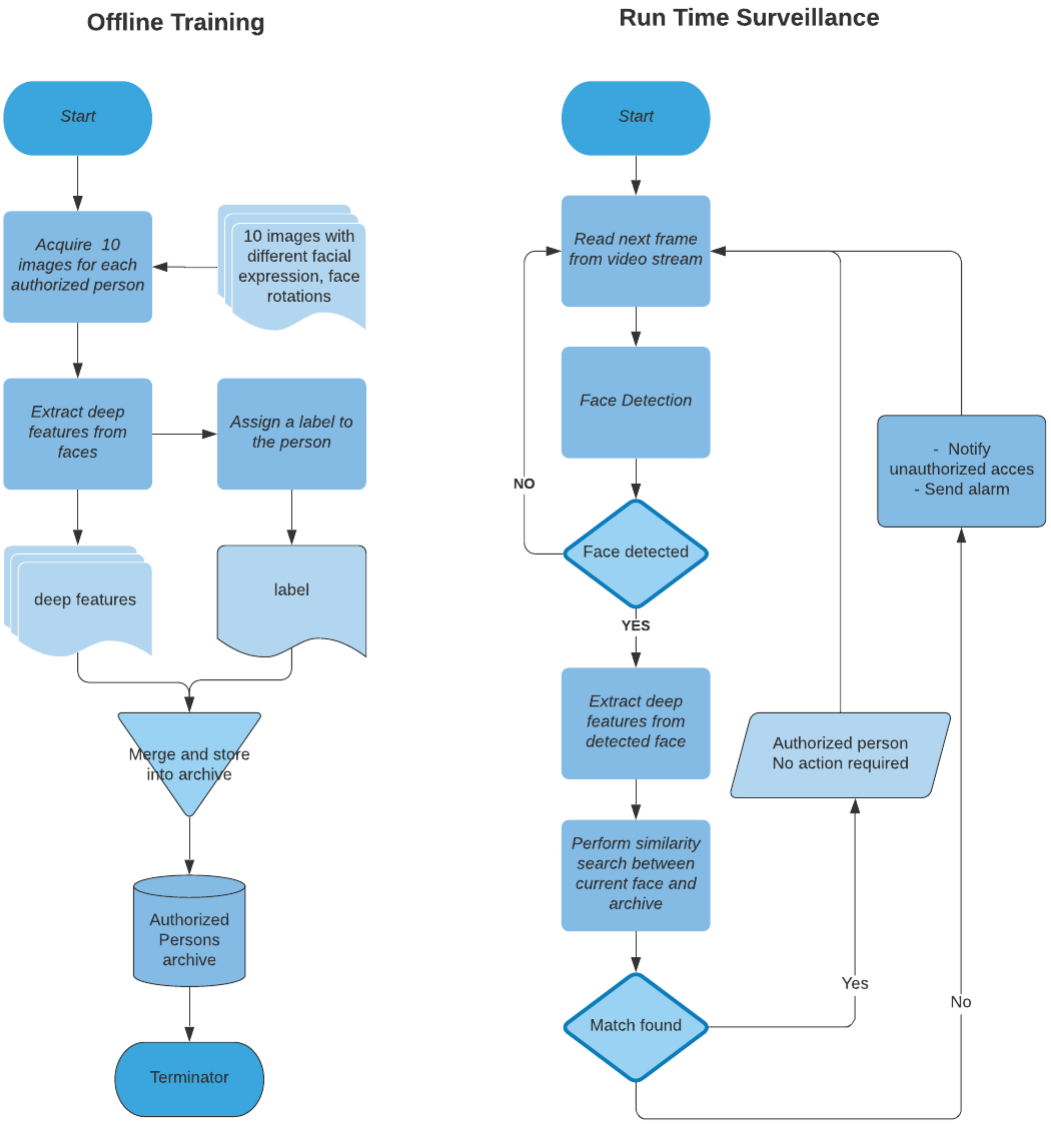
WG2: Flowchart for Intrusion Detection software

In the following, we present a flowchart prepared for describing the intrusion detection software that we implemented last year for the COST Action.

It is composed of two different phases: offline training and run-time surveillance.

In the offline training, the persons authorized to enter the monitored environment are added to the system. To do this, we acquire 10 images of the face of each authorized person, that possibly capture different facial expressions, different head rotations, and poses. From these images, we extract some visual information by using a deep neural network (we call this *deep features*) and we assign a label to that person. We then bound the label to the deep features extracted and we store them into the authorized persons archive. This archive is then deployed into the system to be used at run time.

At run time, each frame of the analyzed video stream is processed as follows. First, a face detection algorithm is executed; if no face is detected, the process ends and the next frame is processed. If at least a face is detected, the deep feature from each face is extracted by using the same deep neural network used in the training phase. With each deep feature extracted, a similarity search is performed with the authorized persons archive; if a match is found, it means that the person was authorized to enter and no further action is required. If no match is found, that person was not authorized to enter, so a notification of unauthorized access is raised and an alarm is sent to the security supervisor.



Dr Claudio Vairo, CNR, Italy, on behalf of WG2, 2020