DT0222: Software Architecture
a.y. 2017-2018
https://app.schoology.com/course/1179370010/

Henry Muccini
University of L'Aquila, Italy

Project:
Masaccio – Monitoring for urbAn SAfety with the IoT

System Specification Document

The Masaccio system has the objective to monitor people and things in closed and open spaces for maximizing people safety. Masaccio can be deployed in a single room, in an entire building, or even in a city. Therefore, its architecture has to be as scalable as possible.

The Masaccio architecture consists of three main macro-components:

1. A monitoring sw/hw sub-system, taking care of collecting, storing, organizing, and analysing big amount of sensored data coming from the environment;
2. A dashboard that illustrates the current safety situation in the monitored area;
3. An actuating sub-system taking care of implementing human assisted automatic actions in case of emergencies.

The monitoring sub-system may contain tens of buildings and city areas where sensors are placed in order to collect row data (e.g., city evacuation, crime monitoring, outdoor and indoor evacuation). You can think of any sensor kind that may be used (in isolation or in combination with others) to maximize people safety. The basic kind of sensors you can think of are: people counters, cameras, BT beacons, temperature and humidity sensors, earthquake sensors, RFID/NFC sensors and readers, environmental sensors, and so on (e.g., mobile phones, smart floor, social media).

The dashboard sub-system, instead, has the main objective of showing the current state of the buildings/areas/city on a configurable dashboard. The dashboard shall highlight the critical situations so to inform the civil protection personnel.

Main Constraints

The system shall be able to handle up to 2.000 sensors, deployed in different areas of the city. Sensors may sense data within different time ranges (from a few seconds to a few minutes). They communicate their data in average every 180 seconds, with an estimated data traffic of 40.000 messages per hour. The system must be resilient to failures, and shall be operative even in case of disasters (with an eventual degraded mode) by guaranteeing that no critical messages are lost and are delivered in at most five seconds. Fault tolerance is a concern as well.

Some Potential Services

This is a list of a few services that may be realized inside our project. Feel free to add new services.

Access Control service: Different users (with different rights) are enabled to access to offices, laboratories, parking spaces etc. The basic service consists in checking the users' rights, track entry/exit time, and deny or allow access (e.g., preventing access to high-risk areas close to an hazard). The access can be also conditional to some conditions, such as load, temperature, available sits. Different stakeholders with different roles may receive different treatments.

Evacuation service: the city can be equipped with fire and other security sensors. When one (or more) of those sensors are activated, information from cameras, and sensors are collected to locate people in the building and to guide them towards the best exit. Once people are located, they are reported on a map owned by the security people. In this way, they know areas that are more populated, with respect to the diagnosed security problem. They can then be directed to different emergency exits, so to avoid the

overload of only a subset of those exits. Smart emergency exit devices (e.g., people counters or cameras linked to emergency exit intelligent signs) inform the users on the load of the specific exit.

First responders communication service: the system shall include a platform that enables "first responders" (like operators, fireman service, emergency, police) to interact and exchange information even in case of emergency.

Smart Information service: Our system collects a big amount of data, that while computed, provides situational aware information about the monitored area. Some of this information can be made available to the population, so to increase their awareness on the surrounding.

Basic Services:

Feel free to add missing requirements or improve the list below.

- Read data: this use case enables to read the data from the card, from RFIDs, turnstile and more;
- User rights check: the system checks if the user has the right to access a certain space;
- Run-time Access control: while the user may have the right to access a space, run-time data is checked to see if she can really access the space;
- Check-in, Check-out: when the user accesses a space, its presence is registered to a DB;
- Statistics: to compute statistics out of the system usage;
- Data Analytics services;
- Actuators.

Basic Actors:

- User;
- Civil protection operator;
- Security manager;
- Sensor network Administrator;
- System Administrator;
- Etc.

Basic Hw components:

- Situational Awareness Sensors: people counters, cameras, beacons, counters, etc.;
- Environmental Sensors: temperature, humidity, pressure, rain, etc.
- Readers: RFID, NFC, card readers;
- Displays: Kiosk, tablets, interactive displays;