

**: Project VISOR :**

**Life View and actionable Intelligence On safety and secuRity**

**during Smart Events**

Jheronimus Academy of Data Science

Initiation Document

**On a normal day there are about 262 megabytes of data traffic per square kilometer. On a festival day that traffic rises to 33,000 megabytes / km2 .[[1]](#footnote-1)**

Our public life de facto largely takes place in the public spaces.

Open spaces are usually in the open air; however, these can also be part of municipal institutions and other (semi-)government buildings. Public spaces are not only limited to physical places, but also relate to the "mental and social" spaces[[2]](#footnote-2). This implies that public spaces should allow citizens to be themselves without unsolicited interference from others. An important feature of the public spaces is that they are usually multifunctional, and as such are used for summer / winter events, including music festivals, public holidays, markets, and so on.

Every year an abundance of large and small events (>1000) take place in such public spaces in the Netherlands. It is not uncommon for dangerous situations to occur at these events, sometimes resulting in fatal incidents.

Safety and security play a crucial role in public spaces given the massive influx of people, as well as, terrorist threats, noise, crime, riots, harassment, pollution, environmental crimes, fires, undesirable social behavior, looting, public drunkenness, dehydration, drug incidents, bacterial infections, and a multitude of other dangers that affect the quality of life.

# Rationale

Public order and safety in public areas is generally guaranteed by an integrated approach of organizers, municipalities, law enforcement officers (including private security services), fire brigades and emergency medical services, including first aid. A wide range of instruments is used by these chain partners[[3]](#footnote-3), including drawing up scenarios, crowd management, risk analyzes for foreseen and unforeseen threats, event permits, briefing, and investigation.

Although such approaches do have a positive impact on supervision and enforcement in public areas, it can be concluded at the same time that much can still be improved.

The smarter collection and use of data, interpretation from the operation, as well as the more sophisticated collaboration based on data and interpretation, seems potentially a decisive weapon in the fight against disorder and insecurity in public spaces. With the VISOR project prototypes and experimentation we aimed at developing effective baselines and advanced assistive technology to support the aforementioned fight and ancillary activities connected to it.

# Current State Of Art

Several studies[[4]](#footnote-4),[[5]](#footnote-5) have shown that better exploitation of open- and closed data on can be of decisive importance in monitoring security at major festivals and events. Live dangers can be detected through live monitoring of shared messages. Calamities around violence, drug and alcohol use can for examples be battled in this way.

Other studies have focused on using GPS data for better crowd control. In [[6]](#footnote-6), the research results are presented to a cloud-based platform that uses GPS data for crowd management and has been deployed in 14 events in England, Switzerland and the Netherlands, including the coronation of King Willem-Alexander. In recent research [[7]](#footnote-7),[[8]](#footnote-8), attention is also paid to the privacy considerations of such technology.

Another important technological development is the use of augmented aka mixed reality (AR / MR), through "smart" glasses such as the Google Glass, the HoloLens, Vuzix and Oculus Rift in the live identification of objects, animals and people.

Augmented reality is already being used to gather real-time intelligence during raids, training, surveillance, and patrols as reported by the FBI[[9]](#footnote-9). For example, two experiments with augmented reality are presented in which the Dutch police use them for forensic research in, among other things, a simulated XTC laboratory[[10]](#footnote-10).

In such data-driven, AR-centric initiatives, privacy and data security generally play a decisive role. In the meantime, not only international research has been carried out - see for example[[11]](#footnote-11) - but also in practice experience has been gained, for example in the de-escalate experiments that have been conducted in the busiest and most lively night-life area of the municipality of Eindhoven- stratums eind [[12]](#footnote-12).

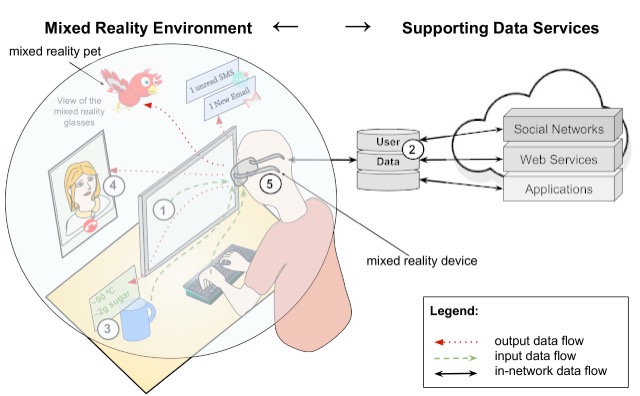


Figure A mix-reality environment

Figure 1 illustrates a mixed reality environment with supporting data services (APIs) and five security points:

(1) input security - in this case for the user who, through his smart glasses, has access to emails and calendar data of any user,

(2) data protection of data originating from various sources including social media and external systems,

(3) output security - output generated by AR can be manipulated by malicious users,

(4) user interaction security - at the moment that the AR user in AR interacts with other AR users; and finally,

(5) Device security - the physical security of an AR device (typically smart glasses or smart phone).

The above signifies the fact that currently ufficiently mature technology is available to better map security and order in public spaces through (Big) data, and proactively respond to security risks and resulting, undesirable effects.

***What is lacking to date, however, is a repeatable, structured, objective, transparent, thorough and validated scientific research in which the above technology is integrated and applied in a "proof-of-concept", where its effects are measured and systematically evaluated in different real-world, semi-controlled experiments.***

# Objectives of VISOR

The overarching objective of VISOR is to increase order and safety in public spaces in general, and smart events more in particular, by exploiting the capabilities that data science technologies hold to the max.

The **VISOR** project aims to develop a multifunctional toolbox that enables the stakeholders(s) involved in organizing an event, festival, market, parade, exhibition or other event in a public space to (1) before, (2) during an event , and (3) afterwards, to gather intelligence from data and learn (knowledge) best practices (see Figure 2). The key stakeholders that may reap the benefits of VISOR include: municipalities, security companies, legal enforcement agencies, and, event organizers.



Figure The Three Main Phases of VISOR

We will now explain the envisioned conceptual operation of the three main phases of VISOR in some more detail (see Figure-3):

**Phase 1: Prepare & Profiling**

Prior to an event, VISOR enables to:

1. Apply privacy-by-design to ensure compliance of collected and consulted data with AVG laws and regulations;
2. Identify, extract, collect ("crawling"), transform ("wrangling"), and storing social media data about an event. For example, data from Facebook, Instagram and Googlemaps;
3. Distill a data profile from this integrated data. This profile can be, for example, a person or group profile, but can also be a profile sketch of objects (stages, streets, tents, etc.), or other geo-location specific properties including routes, event areas and the such;

**Phase 2: Run and Monitor**

During an event, **VISOR** tools offer:

1. "Live" social media messages; and, combine these messages with live images "on-the-ground" which are collected by security officers with smart glasses;
2. Next analyze these live messages and video content and correlate them with the profiles obtained from Phase 1 with the aim of identifying possible yet to be determined safety risks and accompanying intelligence to this end eventually,
3. Communicate to a central "command center" / "war-room" / "post", eg by visualizing them.

**Phase 3: Learning & Sharing**

Finally, **VISOR** functionality offers to "play back" an event and accelerate "flush" to learn from situations that could have been better, and to share it with third parties.

In addition, and perhaps more importantly, VISOR will include a detailed report and analysis of the effectiveness of VISOR during the event in terms of socio-economic-legal-ethical and organizational aspects. These aspects will be studied from the perspective of all stakeholders involved.

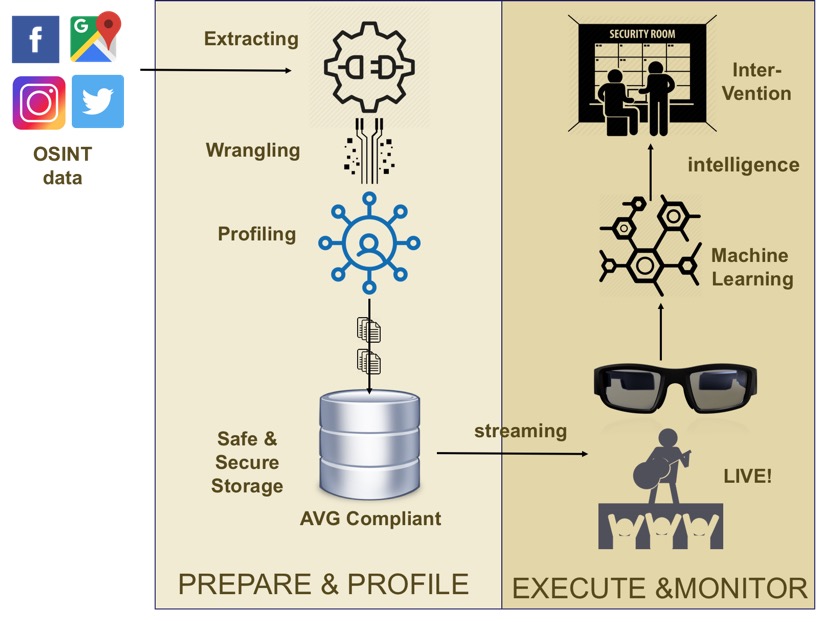


Figure Conceptual Architecture of VISOR

In the **VISOR** project, the above challenges will be addressed through a short-cycle, experiment-driven approach. The experiments are characterized by a do-measure-learning cycle, in which is "done" (hypothesis is established), "measured" (hypothesis is tested by means of scientific quantifiable measurements), and learned (new knowledge is built up).

We envision two main experiments with the VISOR equipment. First and foremost, the VISOR baseline architecture will be tested, and training data for its algorithms will be collected, during PaasPop. During three following days, up to 6 experiments will be run, along 3 scenarios.

In the second experiment, VISOR will be further improved and consolidated.

# PaasPop: Locus of the Experiments

PaasPop traditionally kicks of the festival season in the Netherlands. It is organized each year in the municipality of Meierijstad (Schijndel) as a three-day event during the Easter weekend. In 2019, Paaspop will be organized in on April 19th, 20th and 21th.

Typically, there are 15 stages with more than 175 bands, including a wide range of musical and theater genres.



Next to its broad music offerings, Paaspop also boasts many other activities including a barber shop, hot tubs, a camping shop, a coffee lounge, a retro seventies-eighties roller-skate track, an old school Arcade hall and a actual cinema.

Mutli-day tickets holders typically reside at the luxurious camping site of the festival. The camping site boasts not only spots for their own tents, but also, festival caravans, huts and glamping like festival tents such as Wigwags.

# Experiments at Paaspop

During Paaspop we will run three experiments to iteratively test and further improve the VISOR toolset. These experiments will run for a 2-4 hours a festival day; after each experiment the results are evaluated and factored into the VISOR toolset.

# PaasPop Event Experimentation: Principles and Assumptions

We have defined 3 guiding principles underpinning the Paaspop experiments:

1. The experiments revolve around safety and security in general within the Paaspop festival terrain, and will as such *not* be directed towards detection of criminal activities and persons;
2. The experiments will be designed in such a way that the privacy of festival goers is persevered;
3. The experiments will not interfere with the normal security and safety operations.

In addition to these principles, the experiments will take place in the following setting:

1. Software and hardware:
   1. A local hardware infrastructure will be put in place comprising:
      1. Three Screens/Monitors
      2. 20 TB WD My Book Duo 20TB
      3. 3 VUZIX glasses
      4. 3 Android smart phones
   2. Software will be deployed on:
      1. VUZIX glasses during Paaspop
      2. SurfSara cluster for training of the ML model.
2. Unit: the experiments will be prepared, overseen and evaluated from the VISOR Control Room which sits in a container at the festival terrain. The unit will provide three working places, a meeting table and storage.
3. Student volunteers. VISOR will rely on 6 student volunteers to conduct the experiments.
4. ….

# PaasPop Event Datasets

Data sources that will be exploited during the VISOR Paaspop experiment include:

* Upfront data:
  + Ticket sales info
  + Camping rental info
  + Facebook/social media info
  + GoogleMaps
  + Training material from the web (e.g.,
* Streaming data:
  + Drones footage
  + Fixed camera’s (CCTV)
  + Video “on the ground” (smart glasses/phone)

# PaasPop Event Experimentation Scenarios

The Paaspop scenarios have been designed based on various discusisons with the key stakeholders, viz. the security company and Paaspop, in conjunction with the Meierij stad municipality and the regional police. In addition, the scenarios have been discussed with the key system and software architects, and legal experts.

In order to have maximum value from the experiments, and learn from them to the fullest extend possible, we have decided to vary them in terms of mere size, impact and sensitivity to failure. Consequently, the envisioned scenarios will vary in terms of risk, where risk entails a function of probability of failure/issues and impact from low to high .

We have the following four main scenario’s:

1. **MR Messaging (low probability/low impact)**. Messages will be sent from the control tower to the VUZIX glasses- they will be project for example potential warnings, request to check areas, etc. The probabilioty that a risks occurs that will jeopardize scenario-0 is very low; from a technical perspective this scenario is not that challenging.
2. **Object and person identification (low probability/high impact)**. Exploiting VUZIX smart glasses and/or mobile telephone objects and people will be identified and marked in mixed reality settings. To safeguard privacy, only student volunteers and/or security staff will be identified. For this purpose, they will allow to provide pictures of their face. Theoretically speaking, this experiment could be setup as a adversarial scenario where the drone person/object and the smart glass variant will compete.
3. **Moshpit Identification and Prediction** **(low probability/high impact).** This scenario will mainly be conducted in tents exploiting video footage from CCTVs and the smart glasses/smart phones. The training of the model can be achieved with existing data (photos and videos), viz., ….
4. **Pickpocketing** (**low probability/high impact)**. This scenario aims at detecting suspicious behavior of criminals amongst the Paaspop public, and predicting pickpocketing. One of the risks of failure lies in the fact that to date very little pickpocketing footage is available, making the training of the ML models an exceedingly challenging task.

# PaasPop Experimentation: VISOR Prototype Architecture

We have carefully designed the PAASPOP VISOR architecture in configurable manner starting from a baseline architecture and incrementally building up in complexity and computational power. The baseline architecture is graphically shown in Figure-4.

The baseline architecture assumes a on/off training layer implying that VISOR machine learning algorithms will be pre-trained before the Paaspop event. In particular, the VISOR algorithms will be trained before Paaspop in order to make predictions or decisions without being explicitly programmed to perform a particular task, e.g., identification of potential pickpockets. We will rely on TensorFlow for easy prototyping and fast debugging, exploiting eager execution. TensorFlow can run on multiple [CPUs](https://en.wikipedia.org/wiki/Central_processing_unit) and [GPUs](https://en.wikipedia.org/wiki/GPU) (with optional [CUDA](https://en.wikipedia.org/wiki/CUDA) and [SYCL](https://en.wikipedia.org/wiki/SYCL) extensions for [general-purpose computing on graphics processing units](https://en.wikipedia.org/wiki/General-purpose_computing_on_graphics_processing_units)).[[11]](https://en.wikipedia.org/wiki/TensorFlow#cite_note-Metz-Nov10-11) TensorFlow is available on 64-bit [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS), [Windows](https://en.wikipedia.org/wiki/Windows), and mobile computing platforms including [Android](https://en.wikipedia.org/wiki/Android_(operating_system)) and [iOS](https://en.wikipedia.org/wiki/IOS). We will deploy TensorFlow on the SurSara Lisa cluster to allow high-performance computing of images and video.

The resulting trained model is taken into production during Paaspop (e.g., through RESTUL APIs) and uploaded and then deployed on in the Android operating backbone of the VUZIX smart glasses. External streaming data from the security video camera’s (“CCTVs”) and/or drones can be accessed and analyzed through their respective APIs.



Figure VISOR Paaspop baseline architecture

The second architecture that may be tested during Paaspop – the “Twin Track” Architecture – extends the baseline architecture with durable data storage and a specific architecture track dedicated to factor in large-scale and flexible cloud computing technology. In particular, this architecture allows to store video images captures from drones and/or CCTVs on a local physical data repository infrastructure as well as optionally creating a specific datalake over safe and secure cloud storage. This architecture enables to further improve future versions of the VISOR ML models exploiting all data collected during Paaspop.

1. <http://www.smartbiz.nl/article/150586/big-data-en-het-festivalseizoen-hoe-meer-data-hoe-beter-het-festival/> [↑](#footnote-ref-1)
2. <http://turfschipper.nl/onzichtbareor.pdf> [↑](#footnote-ref-2)
3. [http://www.eventsafetyinstitute.nl/wp-content/uploads/2014/12/politie\_en\_ evenementen\_definitief\_ schoon\_ blu-2.pdf](http://www.eventsafetyinstitute.nl/wp-content/uploads/2014/12/politie_en_%20evenementen_definitief_%20schoon_%20blu-2.pdf) [↑](#footnote-ref-3)
4. [https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/13896/3/Understanding%20 Generation%20Y %20and%20 Their%20Use%20of%20Social%20Media\_A%20Review%20and%20Research%20Agenda.pdf](https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/13896/3/Understanding%20%20Generation%20Y%20%20and%20%20Their%20Use%20of%20Social%20Media_A%20Review%20and%20Research%20Agenda.pdf) [↑](#footnote-ref-4)
5. [https://www.researchgate.net/publication/287206488\_A\_Crowd\_Monitoring\_Framework\_using\_Emotion\_Analysis\_of\_Social \_Media\_ for\_Emergency\_](https://www.researchgate.net/publication/287206488_A_Crowd_Monitoring_Framework_using_Emotion_Analysis_of_Social%20_Media_%20for_Emergency_)Management\_in\_Mass\_Gatherings [↑](#footnote-ref-5)
6. <https://jisajournal.springeropen.com/articles/10.1186/s13174-015-0040-6> [↑](#footnote-ref-6)
7. <https://www.portokalidis.net/files/techu_mobisys17.pdf> [↑](#footnote-ref-7)
8. <https://dl.acm.org/citation.cfm?id=3081345> [↑](#footnote-ref-8)
9. <https://www.fbi.gov/file-repository/stats-services-publications-police-augmented-reality-technology-pdf/view> [↑](#footnote-ref-9)
10. <http://delivery.acm.org/10.1145/2960000/2957302/p267-datcu.pdf?ip=131.155.239.210&id=2957302&acc=ACTIVE%20SERVICE&key=0C390721DC3021FF%2EECCBF8AC29DF345E%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1543921964_bb23871df4c780802595187b3e3efaf8> [↑](#footnote-ref-10)
11. <https://cacm.acm.org/magazines/2014/4/173222-security-and-privacy-for-augmented-reality-systems/abstract> [↑](#footnote-ref-11)
12. <https://www.geonovum.nl/uploads/documents/6-Werken%20met%20Sensoren,%20gewoon%20doen.pdf> [↑](#footnote-ref-12)