Title:	Document Version:
D3.4 LETSCROWD ESM implementation guidelines for crowd protection Version 1	1.0

Project Number:	Project Acronym:	Project Title:
H2020-740466	LETSCROWD	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M12 (April 2018)	M12 (April 2018)	R-PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other.

**Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission).

Responsible:	Organisation:	Contributing WP:
Carlo Dambra	PROPRS	WP3

Authors (organisation):

C. Dambra, A. Gralewski (PROPRS), C. Graf (RAILSEC), Y. Alon (RAILSEC), H. Nitsch, S. Allertseder (BayFHVR), A.G. Silva (ESYS), C. Peres (ADM), J. A. Alonso Velasco (ERT), I. Jacobs, G. Smet (LPV), V. Da Silva Reis, P. Esteves Grilo (PSP), P. Townsend (CROWD), M. Bolognesi, G. Garzo (INTERNO)

Abstract:

This document represents a progress report on WP3 risk assessment, including identified vulnerabilities, threats and hazards, the related likelihoods and consequences and possible approaches to implement a methodology for static and dynamic risk assessment in mass gatherings. It will be the basis for deliverable D3.4.

Keywords:

Mass gathering, static risk assessment, risk assessment, dynamic risk assessment, crowd management, weak signal

Revision History

Revision	Date	Description	Author (Organisation)
V0.01	10.04.2018	First version	C. Dambra, A. Gralewski (PROPRS), C. Graf, Y. Alon (RAILSEC), P. Townsend (CROWD)
V0.02	12.04.2018	First full draft	C. Dambra, A. Gralewski (PROPRS)
V0.03	24.04.2018	Includes feedback from LEAs plus other contribution from PROPRS	C. Dambra, A. Gralewski (PROPRS), J.A. Alonso (ERT), M. Bolognesi, G. Garzo (INTERNO), I. Jacobs (LPV), C. Peres (ADM)
V0.04	26.04.2018	Final draft for internal review	C. Dambra, A. Gralewski (PROPRS)
V1.00	30.04.2018	Final version to be submitted to EC	C. Dambra, A. Gralewski (PROPRS)

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement № 740466.

More information available at https://letscrowd.eu

Copyright Statement

Executive Summary

The report presents the Dynamic Risk Assessment (DRA) approach to public event gatherings which adhere as much as possible to ESM principles. The approach follows a static and dynamic risk assessment presented in the previous report D3.2 and includes the feedback received from LEAs.

The main methodology is based on a qualitative approach utilising Boston Square and should be augmented by,

- Crowd simulation modelling,
- Specific mitigation processes.

It should follow the current processes used in e.g. fire and/or football risk events. The majority of the risk of interest to LETSCROWD are associated with low probability but with high impact category and involves weak signals when data collection is considered.

An approach based on the analysis and processing of weak signals is considered additionally, for low probability but with high impact event (e.g. terrorism and similar activities). In relation to weak signals these should be collected prior and during the actual event. The present DRA approach proposed is based upon collecting sensor data from human and electronics devices to identify precursors and possible threats and attacks.

The weak signal received from the sensors should have an identifier and carry attributes associated with time signature, location and significance (Credibility and Reliability),

A measure of significance is suggested which is function of Credibility, Reliability and Time distance and when normalised varies from 0 (not significance not trustable) and 1 (absolutely trustable). Possibility of combining significance for two events is also provided to allow to evaluate signals coming from different sources. Examples of logic trees leading to an attack mode is also given.

Finally, a possible system for helping decision makers in making decisions during DRA is presented. The proposed system has always the man-in-the-loop and is based on a variety of sensors providing data via datalogger to time dependent GIS, knowledge base, in support of the decision maker. It is acknowledged that development of knowledge base to allow weak signals to be combined and level of risk allocated is very important and should be developed.

Index

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

This document represents the first version of the overall dynamic risk assessment methodology to effectively produce policies and deploy technologies following the ESM principles.

1.2 SCOPE OF THE DOCUMENT

The scope of this document is:

- To define a possible approach to Dynamic Risk Assessment (DRA) taking into account the findings of Deliverable D3.2 and further feedback from LEAs.
- To define an architecture for the DRA and the corresponding information flow.

1.3 STRUCTURE OF THE DOCUMENT

The document is structured as follows:

- Section 2 offers an introduction to the problem of Dynamic Risk Assessment (DRA) and to the main issues to be faced during mass gatherings events.
- Section 3 summarises the findings from Deliverable D3.2 covering:
  - The implementation of a practical approach.
  - A detailed, but not exhaustive, list of threats, attack modes, types of available sensors and possible precursors of attack modes related to mass gathering events.
- Section 4 starts to define the proposed approach for the DRA, dealing with Weak Signals, Suspicious Events and Patterns and defining possible criteria to detect, classify and rank them according to risk criteria keeping always the man-in-the-loop.
- Then, Section 5 describes the proposed DRA system architecture and the related information flow.
- Finally, Section 6 proposes the way forward for the necessary refinements to be considered for the 2nd version of the DRA methodology and draws some intermediate conclusions.

1.4 DEFINITIONS

Table 1 proposes a list of definitions that will be used across the entire document to clarify the meaning of the main concept introduced by the proposed approach.

Table 1 - Definitions

Term	Definition
Dynamic Risk Assessment (DRA)	The Dynamic Risk Assessment is defined by the Health Protection Agency (HPA)[1] in UK as the "*continuous assessment of risk in the rapidly changing circumstances of an operational incident, in order to implement the control measures necessary to ensure an acceptable level of safety*". In LETSCROWD the **Dynamic Risk Assessment** definition can be modified as follows: "*The continuous assessment of risk in the rapidly changing circumstances of mass*

[1] http://www.istr.org.uk/docs/dymamicriskassessment.pdf

	gathering events, in order to implement the control measures necessary to ensure an acceptable level of safety and/or security".
Hazard	Something that is dangerous and likely to cause damage
Mass Gathering	A Mass Gathering event can be defined (World Health Organisation (WHO), 2008) as: "*more than a specified number of persons (which may be as few as 1000 persons although much of the available literature describes gatherings exceeding 25000 persons) at a specific location for a specific purpose (a social function, large public event or sports competition) for a defined period of time. In the context of this document, an organised or unplanned event can be classified as a mass gathering if the number of people attending is sufficient to strain the planning and response resources of the community, state or nation hosting the event*".
Security	Security is defined in the Cambridge Dictionary (Cambridge University Press, s.d.) as "*Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries*"
Situational Awareness	According to (Endsley, 1995) "*Situational awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and a projection of their status in the near future*".
Threat	An expression of intention to inflict evil, injury, or damage.
Weak Signal	A weak signal can be defined (Schoemaker & Day, 2009) as "*A seemingly random or disconnected piece of information that at first appears to be background noise but can be recognized as part of a significant pattern by viewing it through a different frame or connecting it with other pieces of information*".

2 DRA APPROACH

The methods for Static and Dynamic Risk Assessment (SRA and DRA respectively) described in D3.2 are the cornerstones regarding risk assessment approaches. For the purpose of LETSCROWD the preferred approach is qualitative assessment using Boston Square, and this should be augmented by:

- Crowd simulation modelling
- Developed mitigation processes

The Dynamic Risk Assessment (DRA) starting point is the Static Risk Assessment (SRA), in order to understand the potential risks associated with the specific event, or for the general risk to the public. It is clear that public musical festival risks will be different to football match events, organised demonstration or any general public event risks. In the present climate, the added dimension of terrorism makes the assessment much more complex.

The DRA approach to, e.g., fire risk events is quite well understood and rehearsed. The events start with detection, fire starts up, residents and passers-by call the police and fire brigade. The services are dispatched, residents are evacuated, the evacuation distance is then determined by the fire strength and potential for escalation e.g. what materials are stored on a site. Similarly opposing fans are normally escorted to and from the stadium. For both of these scenarios a procedure for dealing with such events should already exists.

As described by the UK College of Policing (UK College of Policing, 2014), "*Analysis forms part of the intelligence cycle. Together with research, it is a method of processing material in order to support and assist decision making. The intelligence cycle is a cyclical and sequential process that allows information to be developed into intelligence*".

Here a possible approach to mass gathering event analysis to dynamically assess risks based on weak signals is additionally considered, whether they lead to terrorist activities or any other risks. The approach should follow the current processes used for risk events e.g. fire, opposing fan clashes, i.e. identify from weak signals what is at risk with the aim to identify which services to be alerted to deal with the threat.

Two situations should be distinguished (see Figure 1)

1. Information that is collected in the Pre-Event phase.
2. Information collected during the Event Execution phase.

Information collected before the event can

- Indicate the possible attack mode, and possible targets.
- How to possibly deal with some of the received weak signals.
- Suggest measures than can be taken to mitigate such attack by monitoring the specific situations prior to and during the public event and to respond accordingly.

The information collected during the event is more complicated to interpret, assess and assign counter measures.

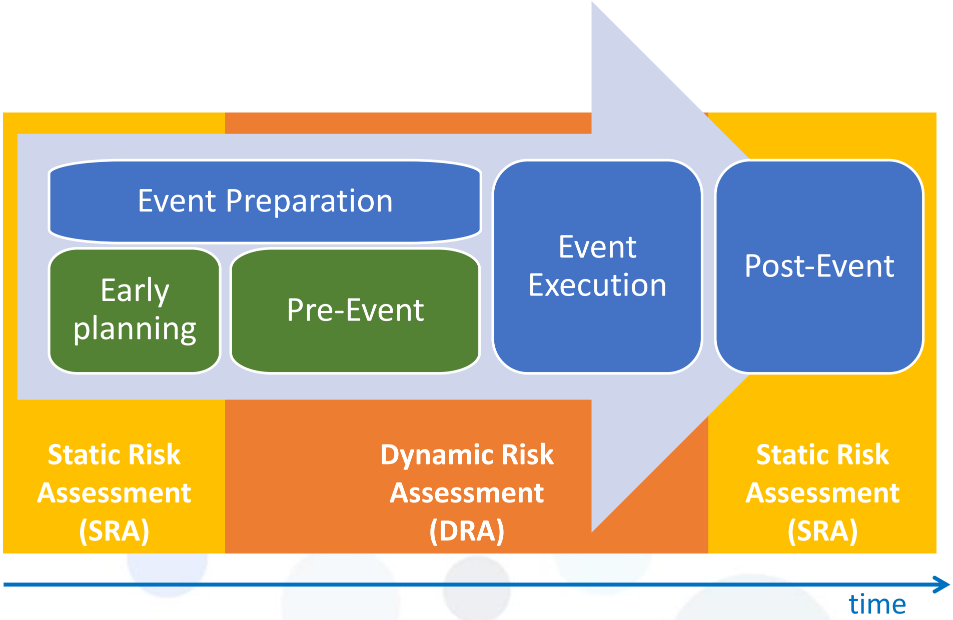

Event Preparation
Early planning
Pre-Event
Event Execution
Post-Event
Static Risk Assessment (SRA)
Dynamic Risk Assessment (DRA)
Static Risk Assessment (SRA)
time

Figure 1 - The Static & Dynamic Risk Assessment stages

The time factor to act is an important parameter to evaluate, since this can determine the development of potential consequences: unattended package could be some forgotten luggage or could be full of explosives and could be detonated by a timer or remotely. However, it is clear that if processes exist to follow the person who left the package, there is a possibility to characterise the risk by knowledge, under what circumstances the package has been left and by behaviour of the person who left it.

Considering all the risks and circumstances which lead to it, the data to be collected is vast and requires some system to assist the monitoring, recording and in helping the decision maker to make a decision.

3 MAIN FINDINGS FROM DELIVERABLE D3.2

In this section an excerpt of Deliverable D3.2 is reported, to help the reader to understand the current approach. In particular:

1. The suggested way forward.
2. The identified sensors, an example of the possible threat precursors to be identified by the weak signals, the possible attack modes and, finally, the possible threats to the crowd.

3.1 IMPLEMENTATION OF A PRACTICAL APPROACH

From the analysis of the problem in Deliverable D3.2 and previous sections it is possible to draw the following conclusion that will be the basis for the implementation of a practical approach:

- The main threats of interest for LETSCROWD are those linked to terrorism including lone wolves and domestic extremisms, since the risks associated to clashes between different groups are already well known by LEAs and much more predictable in terms of dynamic behaviour.
- Given the above assumption, most of the risks to be considered are falling within the Low Probability High Impact category, thus making difficult to collect data on likelihoods and consequences.
- The Static Risk Assessment phase of the involved LEAs appears to be well structured according to standard principles of risk assessment and therefore it can be simply improved by introducing:
    - Crowd modelling to better assess consequences on participants;
    - Data analytics to improve the extraction of knowledge from databases of past events.
- The difficulty in collecting statistical evidence on the most critical threats makes the qualitative approaches more appropriate for the LETSCROWD Dynamic Risk Assessment, taking also into account the need to have the “man in the loop”.
- The most promising approach appears to be a situational awareness tool integrating:
    - Real-time GIS able to manage heterogeneous alerts.
    - A standardised protocol to handle risk-related geo- and time-referenced alerts.
    - A semi-automatic procedure to
        - Manage the alerts and evaluate how they dynamically contribute to the risk(s) for which they can be considered precursors.
        - To display the most significant alerts to the operator to allow him to dynamically modify the levels of the different considered risks accordingly;
        - Identify and show to the operator the most appropriate procedures to handle the new levels of risk.

3.2 SENSORS, PRECURSORS, ATTACK MODES AND THREATS

The sensors can be those listed in Table 2 (provided as example and not exhaustive, it can be extended according to LEAs needs):

Table 2 - Possible sensor’s types

Sensor ID	Sensor type	Description
S01	Cyber Threat Intelligence (CTI)	Detection of cyber-attack that can directly or indirectly compromise the security of the event, e.g. Distributed Denial of Service (DDoS) to the

Sensor ID	Sensor type	Description
		network supporting CCTV system.
S02	Human-Centred Computer Vision (HCCV)	Any camera-related system (fixed, mobile or drone-mounted) with the attached processing (including, e.g., face recognition, number plate recognition, motion detection, people tracking, 3D crowd fluxes based on stereo cameras, etc.).
S03	Semantic Intelligence (SI)	Detection of conversation on Open Sources or Social Networks that could represent a precursor of a threat.
S04	Human as Sensor (HS)	It can be a member of the public, a policeman, a member of the staff, etc. each one obviously with its own credibility.
S05	Physical Sensor (PS)	Thermal sensors, explosive sensors, metal detectors, etc.

Each Weak Signal is related to - alone or in combination with other WSs - one or more **Precursors** (see examples in Table 3) of possible **Attack Modes** (Table 4) corresponding to possible **Threats** (Table 5). These tables were already reported in Deliverable D3.2 and have been updated using partners' experience and available reports (Association of Chief Police Officers of England and Wales and Northern Ireland (ACPO), 2009).

Although the list of Precursors in Table 3 quite complete, it is important to always bear in mind that threats can be so, by a conjunction of details that can subjectively be interpreted as such when they are assessed within a given context, place, time, attitude and situation. Determining a generic and fixed list of threats' precursors limits other possible threats, so it is necessary to take into account other possible situations that together with others and under the human eye, may become a new threat. This aspect is therefore explicitly taken into account in the DRA methodology described in Section 4 when dealing with Suspicious Events and Patterns that can be generated either by automatic rules or by the man-in-the-loop identifying and correlating specific weak signals.

The Threat information is mainly used to set-up the event scenario (e.g. to a priori select the sources of information on which to crawl information knowing the expected threat) than to assess risk levels: when dealing with dynamic risk assessment is key to anticipate Attack Modes and the reason for the attack is less important.

Table 3 - Possible threat's precursors

Precursor ID	Precursor description
P01	Filming, taking notes or photographs, or watching for extended periods, focusing on security cameras, hallways, fire exits, access and egress routes
P02	People behaving strangely
P03	People bringing unusual packages into event
P04	People found in off limits areas, particularly near plant or server rooms or places of concealment
P05	Vehicles parked in suspicious circumstances (e.g. vehicle parked near the venue, with one or more people remaining in the vehicle, for longer than would be considered usual)
P06	Anomalous vehicle

Precursor ID	Precursor description
P08	Suspicious social network activities (e.g. chat on social media that could be related to a possible attack to the crowd)
P09	Splitting into groups (signalling multiple points of attack)
P10	Identical luggage carried by several persons
P11	Abandoned object
P12	Cyber-attack to critical infrastructures
P13	Traceable signs of radicalisation on social media
P14	Group of people with similar symbols (clothing, flags, etc.)
P15	Mobilisation via social media
P16	Vehicle entering a pedestrian area
P17	Vehicle stolen
P18	Person collapsing
P19	People fighting
P20	High conjunction
P21	Crowd restricted movements
P22	Individual wearing clothing not suitable with the conditions of the location, time and weather
P23	Individual whose luggage is not compatible with his appearance
P24	Individual carrying a baggage that is disproportionately heavy to its dimension
P25	Individual showing nervousness or fear in front of police
P26	Individual showing interest for security, procedural and/or organisational aspects
P27	Two or more persons secretly keeping in touch
P28	Flying drone (or any other UAV)
P29	Pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures (bomb threats, leaving hoax devices or packages)
P30	The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s)
P31	Delivery vehicles arriving at the event at the wrong time or outside of normal hours.
P32	Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment
P33	Attempts to disguise identity - motorcycle helmets, hoodies, etc. or multiple sets of clothing to change appearance
P34	Extended wait in line for tickets or admission (can be a precursor for crowd control problems)

Table 4 - Possible Attack Modes

Attack Mode ID	Attack Mode description

AM01	(Squad of) Suicide bomber(s)
AM02	Vehicle used as weapon (vehicle ramming)
AM03	VBIED Vehicle-Born Improvised Explosive Device
AM04	Bomb/IED (e.g. in an abandoned object)
AM05	CBRN attack
AM06	Cold steel (e.g. stabbing)
AM07	Hijacking of social networks
AM08	Shooting
AM09	Combined attack (two or more attacks simultaneously launched against the event)
AM10	Riot
AM11	Fire
AM12	Drone-based attack
AM13	Hostages

Table 5 - Possible Threats to the crowd

Threat ID	Threat description
T01	Terrorism
T02	Domestic extremism
T03	Lone wolf
T04	Clashes between different groups

4 PROPOSED APPROACH

4.1 WEAK SIGNAL (WS)

The Dynamic Risk Assessment (DRA) system bases its reasoning on the receipt of **Weak Signal** (WS), the minimum quantum of information managed by the DRA, i.e. the detection of each sensor involved.

Each Weak Signal WS generated by a sensor is sent to the control room for further processing. The message shall contain the following minimal information:

- A unique **ID**
- Absolute time **t** in which it has been generated.
- Geolocation (x, y) - if available.
- The signature of the detection, i.e. all the **features** related to what it has been detected by the sensor using a pre-defined semantic (e.g. using keywords).
- The **Reliability** (**R**) of the of the detection, e.g. a speeding car is detected with 95% reliability (where the expressed uncertainty could be generated by the difficulty in measuring the speed or by a tree shadowing the car).
- A snapshot of what has detected to help the operator to confirm, discard (false alarm) or amend the detection of the sensor.

Each Weak Signal has a **Significance** (**S**) value assigned to it that is a combination of the **Credibility** (**C**) of the Sensor m (assigned a priori by LEAs experts) in detecting the considered precursor, the **Reliability** (**R**) of the detection and the **Time Distance** (TD) from the event (a speeding car can be considered differently if it is happening 3 days before the event or during the event).

The Significance of the considered Weak Signal detected at time t by the Sensor m ranges in the [0 , 1] interval and is computed as follows:

$$S(ID) = \frac{\alpha\, C(m) * \beta\, R(ID) * \gamma\, TD(t)}{Normalising\ Factor} \in [0,1]$$

where

- C and R are typically integer between 1 and 5 (where 1 is very low and 5 is very high);
- TD is a value in [0, 1] depending if it is close or far from event (the closer the WS to the event execution the greater the TD value);
- the Normalising Factor keep S(ID) in [0, 1];
- α, β and γ are correcting factors to tune the role of each factor in the product.

As stated above, Significance assumes values in the [0, 1] interval, where 0 means **no significance** and 1 **maximum significance**.

4.2 SUSPICIOUS EVENTS AND PATTERNS

When a WS is received it is necessary to process it to evaluate if it can become, alone or in a group, of interest for the event. To this end two more structures are introduced:

- **Suspicious Event** (**SE**), build by a single WS that has sufficient significance to become an SE
- **Suspicious Pattern** (**SP**), two or more WS can create a SP if they have sufficient significance and are linked together according to one of the criteria described below (see Section 4.2.2).

4.2.1 Suspicious Event

A WS can become a **Suspicious Event** (**SE**) per se according to its Significance and/or other conditions set in the system (e.g. the Sensor that has generated it, the specific detection that requires attention independently from the reliability of the detection, etc.). In this case, the Significance of the SE becomes the Significance of the WS:

$$S(SE) = S(ID)$$

Intelligence Alerts (**IA**), i.e. those signals coming from the intelligence services, can be considered a special Suspicious Event with maximum Significance S(IA) = 1.

4.2.2 Suspicious Pattern

A WS alone could be insignificant, but when put in combination with other WS could become important. Therefore, the WS could be grouped into a **Suspicious Pattern** (**SP**). To build a Suspicious Pattern at least 2 (two) WS are necessary.

The Suspicious Pattern can be generated:

1. Before the event takes place, using the LEAs' knowledge stored in the Knowledge Base (see Section 5.1 for more details of its role in the architecture) that defines the rules for building the patterns. The Knowledge Base is specific to each LEA and mechanisms to share it according to existing EU/international protocols could be considered.
2. Dynamically, during event preparation and execution, using an automatic grouping of WS using logic similar to those currently used, for example, at some airport security checks: 3 or more credible WS (precursors) "**simultaneously**" (i.e. within a short period of time) coming from different sources of information can be considered as SP. The minimum number of credible WS can be adapted to the specific local conditions.
3. Dynamically, using **data analytics** that works on all received WS and generates suspicious pattern. there are more and more increasing concerns for intelligent systems to automatically discover unexpected behaviours or anomaly events from weak signals. Recently, researchers started to publish deep learning techniques to automatically learn high-level representations, and then avoid the requirement of domain experts in designing features (Vu, 2017) (Xu, Ricci, Yan, Song, & Sebe, 2015) (Hasan, Choi, Neumann, Roy-Chowdhury, & Davis, 2016).

Therefore, Suspicious Patterns can be of 6 types:

- **Group** (**GSP**): a set of WS (or SE or SP) without time and geographic constraints. The attention of the operator is raised when at least a subset of WS (or SE or SP) belonging to the pattern is received with a reasonable degree of significance. An example of a Group is the SP6 "Suspicious Vehicle" shown in Figure

2 with 4 WS attached to it representing the same truck detected by different sensors (details in Figure 3). It is sufficient to have received the WS independently of the time sequence in which they are detected to raise the attention of the operator.

- **Sequence** (**SSP**): a set of WS (or SE or SP) that need to be received in the correct sequence. An example of a Sequence is the Abandoned Object Pattern. It has 3 WS:
  1. Individual with a bag
  2. Bag left unattended (from a steward)
  3. Individual leaving the scene for a given time (e.g. 10 minutes).

  It is necessary to detect the 3 precursors in the correct order to raise the attention of the operator. Another possible example is the following:
  1. Three individuals, e.g. wearing the same hat and carrying the same backpacks, arrive in the scene
  2. One of them approaches a steward trying to gather information regarding the security systems and procedures.
  3. The 3 are separating to 3 different parts of the venue and disappear from the cameras
  4. Backpack left unattended (from police).
- **Area** (**ASP**): a set of WS (or SE or SP) confined in the same area received in a pre-defined time interval. In this case the constrain is on being all within the same area
- **Simultaneous Group** (**SGSP**): the grouping is generated using the strategy of "**simultaneous events**" described above.
- **Data Analytics** (**DASP**): the grouping is generated using **data analytics** approaches as described above.
- **Operators Group** (**OSP**): the grouping is generated by the operator that groups 2 or more WS according to his/her experience.

Also SPs can have a Significance value associated to them that is computed using the Significance values of all the elements of the tree connected to it.

A possible approach to combine Significance values for an SP with 2 WSs contributing to it with significance S_1 and S_2 respectively, is derived from Certainty Factors (Lucas, 2001) theory using the following formula (taking into account that

$$S(S_1\ and\ S_2) = S_1 + (1 - S_1) * S_2$$

Having more than 2 WS contributing to the same SP, it is possible to iteratively apply the proposed formula as follows (in case of 3 WSs with Significance S_1, S_2 and S_3, respectively):

$$S_{1\ and\ 2} = S(S_1\ and\ S_2) = S_1 + (1 - S_1) * S_2$$

$$S_{1\ and\ 2\ and\ 3} = S(S_{1\ and\ 2}\ and\ S_3) = S_{1\ and\ 2} + (1 - S_{1\ and\ 2}) * S_3$$

As it is specified above, the idea is to build, whenever possible using the LEAs expert knowledge a tree of possible events (Weak Signals, Suspicious Events, Suspicious Patterns) happening at the venue on which reasoning on risk.

An example of a possible tree with WSs, SEs and SPs is given in Figure 2 while a detail of Suspicious Pattern SP6 with 4 WSs (each one with its own significance value) is provided in Figure 3.

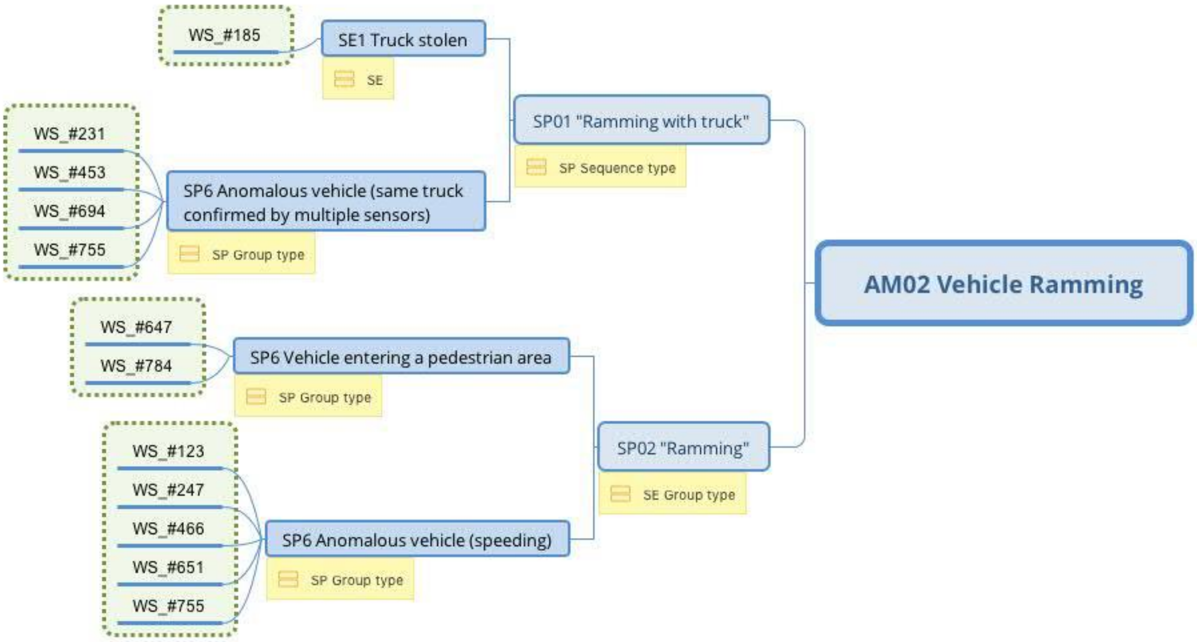


Figure 2 - Example of tree with SE, SP and AM

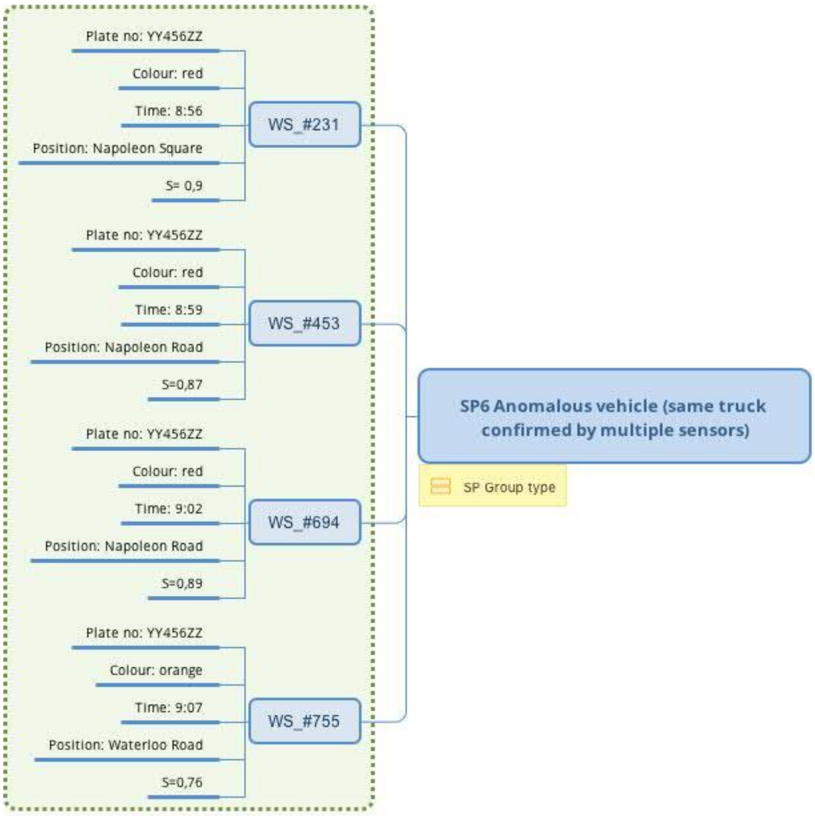


Figure 3 - Detail of the SP6 Suspicious Pattern

The Significance value of the Suspicious Pattern SP6 in Figure 3 is $S_{SP6} = 0,9996568$

4.2.3 Critical elements

Suspicious Events and Patterns, when triggered by WS, can be then classified as:

- **Non-Critical**, i.e. elements that do not constitute an immediate threat to the crowd.
- **Critical**, i.e. elements that constitute an immediate threat to the crowd.

Critical Suspicious Events and Patterns shall be brought immediately to the attention of the operator that should take the necessary mitigation actions.

4.2.4 Risk Level

Using the above methodology, the **Risk Level** can be computed using escalation approaches. A possible approach could be:

- IF Time Distance from the event is Far AND no Critical SE or SP are triggered, THEN the Risk Level is Very Low
- IF Time Distance from the event is Far AND some Non-Critical SE or SP are triggered, THEN the Risk Level is Low
- IF Time Distance from the event is Far AND at least one Critical SE or SP is triggered AND Crowd Density is Low, THEN the Risk Level is Medium
- IF Time Distance from the event is Close AND at least one Critical SE or SP is triggered AND Crowd Density is Low, THEN the Risk Level is High
- IF Time Distance from the event is Close AND at least one Critical SE or SP is triggered AND Crowd Density is High, THEN the Risk Level is Very High

The proposed Risk Level could be referred to either the whole event or the specific attack modes.

Clearly, exact IF-THEN rules, thresholds and quantities need to be defined by LEAs according to their protocols, rules, experience including also socio-political and environmental conditions.

5 THE DRA ARCHITECTURE AND INFORMATION FLOW

5.1 DRA ARCHITECTURE

The Dynamic Risk Assessment system is based on the following main modules (see Figure 4):

- A **Data-Logger** (DL) that collects and stores all what has been detected by the available sensors.
- A **Knowledge Base** (KB) that contains the LEAs expert knowledge on how to process the detected WSs and stores the classification of all received events and the decisions taken, thus acting also as a **Juridical Recorder** (JR).
- A time-dependent **Geographical Information System** (GIS) with an underlying database that stores all the processed information.
- An KB Decision Support Engine that applies the rules stored in the KB and reason on WS, SE and SP.
- An operator's workstation, that shows to the operator a **dashboard** with all elements to take decisions, including for example
    - The tree with received Weak Signals, activated Suspicious Patterns and - if the available knowledge allows - corresponding Attack Modes and Threats to provide a proxy to the probability of an event.
    - The critical events (SE, SP), with the proposed mitigation actions.
    - The intelligence alerts (IA).
    - A **GIS map** with all received information (WS, SE, SP) displayed accordingly to their geo-location (if available).
    - A **timeline** with all received information (WS, SE, SP) displayed according to the receipt time to allow the operator to identify possible sequence of threatening events. The timeline allows to display a chronology of events. As suggested by the UK College of Policing (UK College of Policing, 2014) chronology of events can be "*based around themes which can include people, vehicles, groups, addresses, telephones and general non-specific types of events (e.g., suspicious sightings). These 'theme lines' run in parallel and can be used in evaluation and analysis to understand what and who were where at any point in time, and any gaps or discrepancies in accounts*".
    - The **crowd density** as measured by the sensors to be used as a proxy of the possible consequences to the crowd (the higher the crowd density, the worse the possible consequences).
    - The different **Levels of Risk** associated to Attack Modes or to Threats.

The Juridical Recorder, that stores all events (WS, SE, SPs, decisions of the operator, etc.) occurred during mass gatherings with the exact timing, can be consulted post event to evaluate what happened, the decision taken in the correct sequence and evaluate also responsibilities.

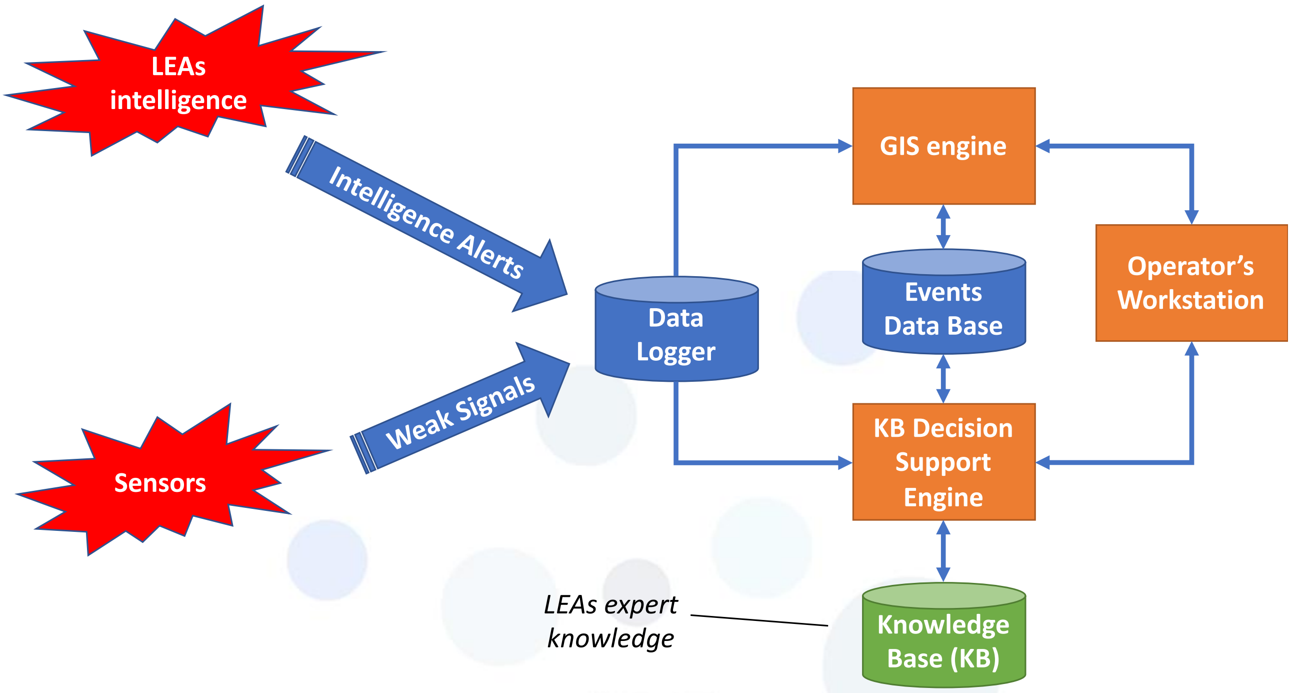


Figure 4 - The DRA system

5.2 A DATA MODEL AND FORMAT FOR WEAK SIGNALS

5.2.1 Possible data model

The need to standardise the reporting of suspicious activities has pushed the United States of America to launch the Nationwide **Suspicious Activity Reporting** (SAR) Initiative (NSI)[2], a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analysing, and sharing SAR information.

NSI initiative has developed a model to organise the reporting of suspicious activities: the Information Sharing Environment (ISE) for Suspicious Activity Reporting (SAR) Functional Standard (FS) that provides XML schemas and UML model (Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), 2015).

The ISE-SAR FS includes

- A collection of artefacts that support ISE-SAR information exchanges.
- A Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element.
- The schemas, each one consisting of a document, extension, and constraint schema.

The UML diagram shown in Figure 5 represents the Exchange Model artefact required in the information exchange development methodology.

[2] https://nsi.ncirc.gov

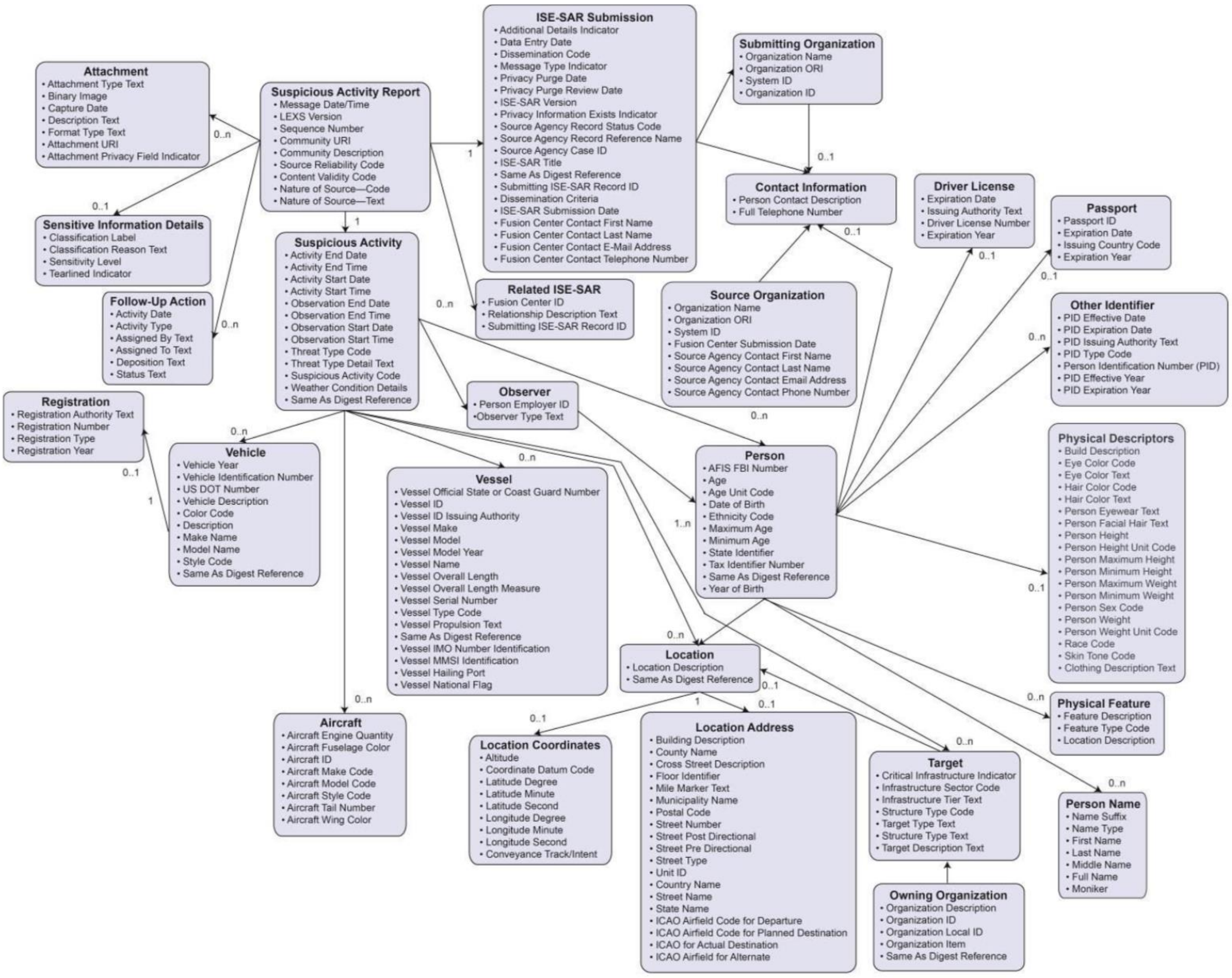


Figure 5 - UML diagram of the ISE-SAR FS

5.2.2 Data format

The Weak Signals are transmitted from the generating sensor to the Data Logger using a message according to Common Alerting Protocol (CAP) standard (Schoemaker & Day, 2009) developed by the OASIS Consortium[3], modified according to the LETSCROWD needs.

The CAP protocol provides an open, non-proprietary digital message format for all types of alerts and notifications offering the following capabilities:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial 9 representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;

[3] https://www.oasis-open.org

- Compatible with digital signature capability; and,
- Facility for digital images and audio.

A CAP alert message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> and/or <resource> segments where:

- The <alert> segment provides basic information about the current message.
- The <info> segment describes an anticipated or actual event in terms of its urgency, severity and certainty.
- The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears in the form of a digital asset such as an image or audio file.
- The <area> segment describes a geographic area to which the <info> segment in which it appears applies.

5.3 DRA INFORMATION FLOW

The DRA system could manage the received information as follows:

- Every sensor that detect something generates a Weak Signal (i.e. a set of information formatted according to what is described in Section 4.1). Similarly, also Intelligence Alerts are formatted accordingly.
- Weak Signal and Intelligence Alerts are transmitted to the Data Logger, and then to both the KB system and the GIS.
- The KB Decision Support Engine classifies the received information according to the approach described in Section 4.
- The classified information is displayed on the dashboard to the operator (e.g. an increased level of risk).
- The operator then can act on it or ignore it.
- If operator/decision maker acts on the information, the KB system helps him/her with displaying possible options to adopt. The decision maker can take one of these options or use his/her own judgement to deal with the risk.

In any case, the original information is stored for further analysis for post-event analysis.

The philosophy behind such a system is that the decision maker is in full control at all times of the processes which are taking place. The KB and GIS are here only to help with data traffic, display the information and helping in the decision-making process by providing mitigation options and any required information.

5.4 POSSIBLE ACTIONS IN CASE OF CRITICAL SUSPICIOUS EVENTS OR PATTERNS

The actions to be implemented in case of Suspicious Events or Patterns are strongly dependent on the LEAs policies, standards, habits, experience and socio-political and environmental conditions.

To provide an example of possible actions, the suggestions given by the UK Government, National Counter Terrorism Office to event organisers for Suspicious Items (UK National Counter Terrorism Security Office, 2017) are reported in Table 6.

Table 6 - Guidance for Staff in case of Suspicious Items

When dealing with suspicious items apply the 4 C's protocol:

CONFIRM whether or not the item exhibits recognisably suspicious characteristics

The HOT protocol may be used to inform your judgement:

Is it HIDDEN?

- Has the item been deliberately concealed or is it obviously hidden from view?

OBVIOUSLY suspicious?

- Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
- Do you think the item poses an immediate threat to life?

TYPICAL Is the item typical of what you would expect to find in this location?

- Most lost property is found in locations where people congregate. Ask if anyone has left the item. If the item is assessed to be unattended rather than suspicious, examine further before applying lost property procedures.

However, if H-O-T leads you to believe the item is suspicious, apply the 4Cs

CLEAR the immediate area

- Do not touch it
- Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out
- Keep yourself and other people out of line of sight of the item. It is a broad rule, but generally if you cannot see the item then you are better protected from it
- Think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights
- Cordon off the area

COMMUNICATE - Call 999

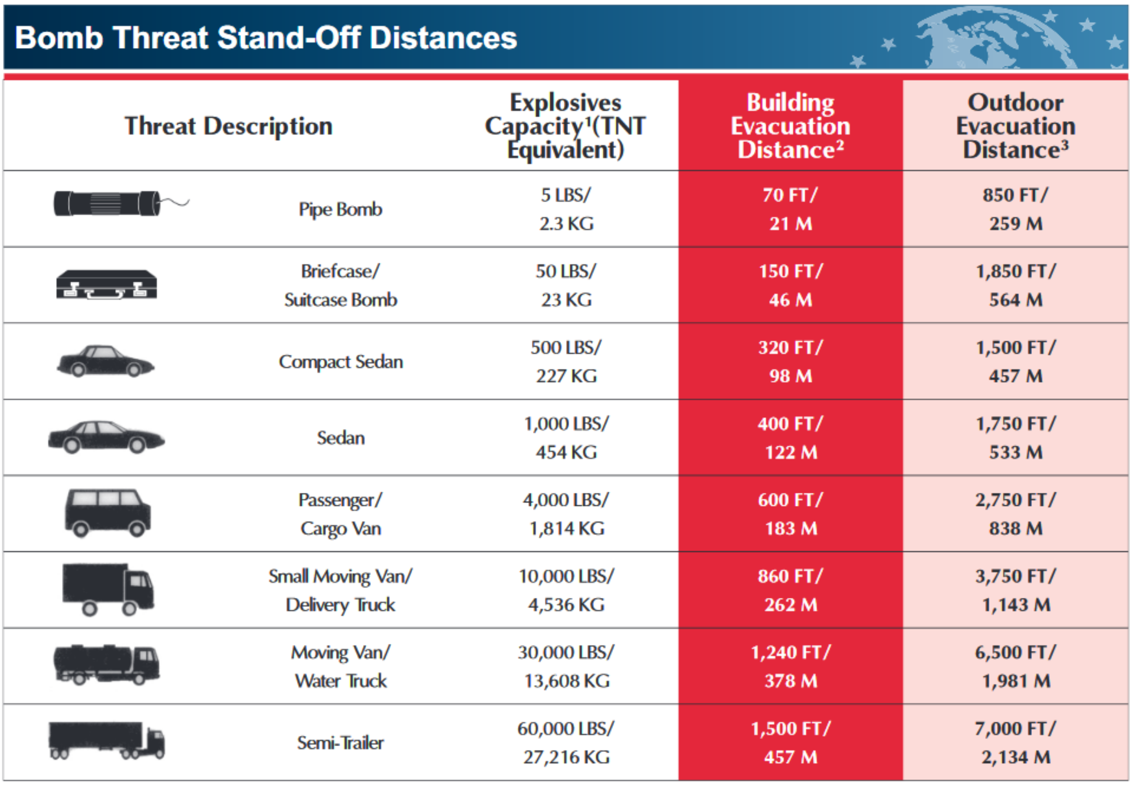
- Inform your control room and/or supervisor
- Do not use radios within 15 metres

CONTROL access to the cordoned area

- Members of the public should not be able to approach the area until it is deemed safe
- Try and keep eyewitnesses on hand so they can tell police what they saw

Another possible action with the support of GIS, is to define the area to be evacuated in case of a bomb threat and the time necessary to evacuate the area. With the GIS support, information on the effects of each explosive type (see e.g. the information provided by the Office of the Director of National Intelligence[4] in Figure 6), and a crowd evacuation model.

[4] https://www.dni.gov/files/NCTC/documents/features_documents/2006_calendar_bomb_stand_chart.pdf



Bomb Threat Stand-Off Distances

Threat Description	Explosives Capacity[1](TNT Equivalent)	Building Evacuation Distance[2]	Outdoor Evacuation Distance[3]
Pipe Bomb	5 LBS/ 2.3 KG	70 FT/ 21 M	850 FT/ 259 M
Briefcase/ Suitcase Bomb	50 LBS/ 23 KG	150 FT/ 46 M	1,850 FT/ 564 M
Compact Sedan	500 LBS/ 227 KG	320 FT/ 98 M	1,500 FT/ 457 M
Sedan	1,000 LBS/ 454 KG	400 FT/ 122 M	1,750 FT/ 533 M
Passenger/ Cargo Van	4,000 LBS/ 1,814 KG	600 FT/ 183 M	2,750 FT/ 838 M
Small Moving Van/ Delivery Truck	10,000 LBS/ 4,536 KG	860 FT/ 262 M	3,750 FT/ 1,143 M
Moving Van/ Water Truck	30,000 LBS/ 13,608 KG	1,240 FT/ 378 M	6,500 FT/ 1,981 M
Semi-Trailer	60,000 LBS/ 27,216 KG	1,500 FT/ 457 M	7,000 FT/ 2,134 M

Figure 6 - Explosive evacuation distance

According to the Outdoor Evacuation Distance in Figure 6, all personnel within a circle with the radius specified by the explosive's type "*should seek shelter immediately inside a building away from windows and exterior walls. Avoid having anyone outside—including those evacuating—in this area*".

6 WAY FORWARD AND CONCLUSIONS

6.1 WAY FORWARD

The proposed methodology needs to be validated into the field as soon as the demonstrations foreseen in WP6 will be set-up and running, according to each LEA competency and local, regional or national authorities.

To anticipate some of the possible outcomes, the proposed DRA approach will be validated through visits to the control rooms of some of the LEAs involved in DRA demonstrations.

The visit to LEAs will allow to:

- Better understand the sequence of currently available weak signals and their confidence level into the currently available sensors and automated tools (if available).
- Discuss the formation of Suspicious Events and Patterns and the thresholds to be introduced for the evaluation of Significance of the received information.
- Start the tuning of the DRA.

6.2 CONCLUSIONS

The following conclusions can be derived:

- A general method of DRA for crowd management is presented.
- Specifically, a method is presented, to deal with incoming of weak signal information.
- A knowledge base should be developed to allow weak signals to be combined and level of risk to be allocated to an event with full control of the process by the man-in-the-loop.
- A possible system has been suggested to help the decision makers in taking decisions during DRA event. This would utilise: sensors, a datalogger, time dependent GIS and knowledge base.
- It is necessary to validate and tune the whole approach during the demonstration phases planned in WP6.

7 REFERENCES AND ACRONYMS

7.1 REFERENCES

Association of Chief Police Officers of England and Wales and Northern Ireland (ACPO). (2009). *Counter Terrorism Protective Security Advice for Major Events.* The National Counter Terrorism Security Office (NaCTSO).

Cambridge University Press. (n.d.). Retrieved from Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/security

Endsley, M. (1995). Towards a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), pp. 32-64.

Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS). (2015). *Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Functional Standard.*

Hasan, M., Choi, J., Neumann, J., Roy-Chowdhury, A. K., & Davis, L. S. (2016). Learning temporal regularity in video sequences. Las Vegas: 29th IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

Lucas, P. J. (2001). Certainty-factor-like structures in Bayesian belief networs. *Knowledge-Based Systems, 14*.

OASIS Consortium. (2010). *Common Alerting Protocol Version 1.2.*

Schoemaker, P. J., & Day, G. S. (2009). How to Make Sense of Weak Signals. *MIT Sloan Management Review, 50*(3).

UK College of Policing. (2014, December 4). *Intelligence management - Research and analysis*. Retrieved from https://www.app.college.police.uk/app-content/intelligence-management/analysis/

UK National Counter Terrorism Security Office. (2017, March 24). *Guidance - Recognising the terrorist threat*. Retrieved from GOV.UK: https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat#suspicious-items---guidance-for-staff

Vu, H. (2017). Deep Abnormality Detection in Video Data. Melbourne: Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17).

World Health Organisation (WHO). (2008). *Communicable disease alert and response for mass gatherings: key considerations.*

Xu, D., Ricci, E., Yan, Y., Song, J., & Sebe, N. (2015). Learning deep representations of appearance and motion for anomalous event detection. BMVC.

7.2 ACRONYMS

Acronym	Definition
C	Credibility
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-Circuit Television
CTI	Cyber Threats Intelligence
DASP	Data Analytics Suspicious Pattern
DL	Data Logger
DRA	Dynamic Risk Assessment
GIS	Geographic Information System
GSP	Group Suspicious Pattern
HCCV	Human-Centred Computer Vision
HS	Human as Sensor
IA	Intelligence Alert
IED	Improvised Explosive Device
JR	Juridical Recorder
KB	Knowledge Base
LEA	Law Enforcement Agency
PS	Physical Sensor
R	Reliability
S	Significance
SE	Suspicious Event
SI	Semantic Intelligence
SGSP	Simultaneous Group Suspicious Pattern
SP	Suspicious Pattern
SSP	Sequence Suspicious Pattern
SRA	Static Risk Assessment
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
VBIED	Vehicle-Born Improvised Explosive Device
WS	Weak Signals