Situation Assessment for a Centralised Intelligence Fusion Framework for Emergency Services

Dafni Stampouli
Innovation Works
EADS UK
Newport, Wales, UK
Dafni.Stampouli@eads.com

Daniel Vincen
Innovation Works
EADS UK
Newport, Wales, UK
Daniel.Vincen@eads.com

Gavin Powell
Innovation Works
EADS UK
Newport, Wales, UK
Gavin.Powell@eads.com

Abstract – There is an identified need for systems to combine information from hard (electronic) and soft (human) sensors. In this paper we report an ongoing development of a centralised framework to provide data and information fusion for interoperability of emergency services. Issues relating to situation and threat assessment are discussed and fusion processes are suggested. Examples of how these processes can be applied to several police scenarios are given. Uncertainty grading of source is also examined and initial implementation attempts are presented.

Keywords: Information fusion, human and non-human sensors, command and control, emergency situation assessment.

1 Introduction and Motivation

There is an increased need for the development of a centralised framework providing the next generation of computer-based Control and Command, Communications and Information Sharing, and Assistance of Intelligence Staff functions enabling interoperability between different emergency services. Such system can also be applicable to both military forces and civil authorities in conventional tasks, and in time of emergency and war. A centralised intelligence fusion framework is currently being developed to address the needs for information sharing, situation assessment and decision support. This is aimed at UK civilian authorities such as Police, Fire and Rescue, and Ambulance Services. The term centralised refers to the efforts for centralised control of emergency support, by a central authority such as the centralized government. It does not refer to the system architecture which will be primarily distributed. There is extensive research for combining data from traditional sensors (hard data) and a number of fusion systems are currently available [1, 2]. However, little work is available on combining human and non-human sensors. Soft data, as opposed to hard data, refers to data extracted from non-electronic sensors, such as intelligence reports, and open source material available on the internet. Furthermore, in terms of the dominant JDL model for data fusion [3], especially in levels 2 and 3 of data fusion – situation and threat assessment – there is a lack of a standardised theoretical framework and an implementation approach to support these higher levels. In this paper we discuss current developments towards addressing and automating these processes within a centralised fusion framework initially developed with UK emergency services, which could be additionally adopted in other countries.

The term intelligence fusion is used to make the process distinct from data fusion which is lower level of fusion and usually refers to fusion and tracking of electronic sensor data, or pixel-level fusion, while the information fusion also referred to as feature level fusion.

This paper is organised in six sections, section 2 discusses issues such as the generation of knowledge and common problems with soft and hard data fusion. Section 3 reviews the processes of situation assessment and threat assessment. Section 4 evaluates the grading of uncertainty and how it can be incorporated into the credibility of the sources and the information acquired. Section 5 discusses the system engineering and describes in detail the involved processes, drawing examples from UK police scenarios. The paper closes with some concluding remarks in Section 6.

2 From Data to Intelligence

According to Waltz [4], data is the individual measurements or observations that form the lowest level of abstraction of knowledge. Human reports, sensor recordings, and evidence that are considered to be relevant are used to refer to elements of data. Information on the other hand is defined by Waltz as organised sets of data, and it refers to data that is sorted, classified, and linked together to allow further search and analysis. Once information is searched, analysed, understood and explained it becomes knowledge. Knowledge encapsulates the understanding of the static and dynamic relationships of the data, the modelling the structure and past and future behaviour of the entities involved. The knowledge management field has adopted two distinct categories of knowledge as object: the explicit knowledge which is
tangible, it can be captured, codified, stored, repeated and taught. It is the basis for logical reasoning and it enables reasoning process to be automated. On the other hand, tacit knowledge is intangible, it is contained in human experience, and it is undocumented. It is also often context rich and subjective [4]. Waltz also defines a level above knowledge: human wisdom which is a unique human cognitive capability to apply knowledge to achieve an objective. Intelligence is therefore defined as a special selection of knowledge required to accomplish a mission. It is intelligence that reveals implications and critical threats and opportunities to jeopardize mission accomplishment. It is therefore our aim, within the fusion community, to move from the explicit representation of the environment (data, and information) towards the mixed tacit and explicit knowledge which will initiate informed action. Behavioural models and simulated environments can represent complex and dynamic situations and compare them with observed situations. At the same time, data mining technologies will be able to discover knowledge in unstructured data both at the content and context level, leading to a development of a combined tacit and explicit knowledge process framework, which will be easily substituted, modified and reused.

Intelligence within effective crime analysis and crime prevention is a key tool helping tackle underlying emergency services problems from neighbourhood policing, to the investigation of serious and organised crime and terrorism. Within the required Centralised Intelligence Framework, the aim is to effectively and efficiently collect, analyse and disseminate information or material which has been identified to be of intelligence value and will enable better situation awareness and decision-making in terms of priorities and tactical options.

Emergency services, and in particular policing operations, benefit from the utilisation of humans in order to collect, report and make sense of information. The primary advantage of using human sensors is their ability to notice and report on relationships and inferences which are not provided by traditional sensors, which only measure features and attributes of certain entities. There are however several issues with employment of human sensors as reported by Hall et.al. [5]. Initially there is a need to quantify the reliability and uncertainty of human data, and incorporate this into the fusion model, then there is the issue of how to task human as sources of information and even how to extract information and knowledge from them. In this paper we report on how these issues are addressed and incorporated in the development of a Centralised Intelligence Fusion Framework for Emergency Services.

3 Situation and Threat Assessment

Situation Awareness, according to Endsley’s definition [6], is “the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.” Endsley [6, p. 36] argues that “it is important to distinguish the term situation awareness, as a state of knowledge, from the processes used to achieve that state. These processes, which may vary widely among individuals and contexts, will be referred to as situation assessment or the process of achieving, acquiring, or maintaining situation awareness.” Thus, in brief, situation awareness can be defined as “a state of knowledge,” and situation assessment as “the processes” used to achieve that state. It is important to note that situation awareness is not only affected by the processes used to derive it, but also pinpoints the direction of future actions and affects the resulting output. For example, according to current state of awareness one can determine the areas to focus attention next and how to interpret the information perceived [7].

Bosse, Roy and Wark [8] define situation assessment as a “qualitative evaluation of the situation that has to do with the notions of judgement, appraisal, and relevance”. In both military and civilian applications, there are two relevant components of situation assessment, namely Impact and Threat Assessment. Impact assessment is defined as “the force of impression of one thing on another; an impelling or compelling effect. There is a notion of influence: one thing influencing the other. In that sense, impact assessment estimates the effects on situations of planned or estimated actions by the participants including interactions between action plans of multiple players.” They also define threat assessment as “an expression of intention to inflict evil, injury, or damage. The focus of threat analysis is to assess the likelihood of truly hostile actions and if they were to occur, to project possible outcomes…”

Salerno [9, 18] on the other hand, defines situation assessment as being solely concerned with estimating the current state of the world environment and impact or threat assessment as the process of projecting the current situation into the future and predicting future states. This distinction is favoured by the authors and is followed throughout this study. Development efforts are directed towards providing this complete model of situation and threat assessment, it is however a process that is attempted one step at a time. Therefore the work presented here is focusing in the understanding of the current situation, in terms of constituent entities and relationships among them and identifying its impact and threat. Furthermore it explains suggested processes to achieve this, while briefly discussing the projection of the current situation into the future, determining whether detrimental events are likely to occur or not and their potential impacts or threats.

Situation is defined as a view or collection of activities that the system is aware of at any instance in time. An activity is something that is done as an action or movement and it is composed of entities related to one or more events. The activity can be used as a hypothesis for the fusion process in order to examine and assess a situation and work towards situation awareness. An entity is defined as a distinct object that has an individual physical or non-physical existence, while an event is something that takes place, an occurrence at an arbitrary place and time. Prior knowledge can be taken into account and that is defined as
relationships or associations that can be learnt through knowledge discovery techniques and validated by an operator or provided directly into the system by a reliable source.

There are several issues about situation and threat assessment which need to be addressed by these higher level fusion processes [10]. There is often difficulty in ontologically defining relevant evidence, as these are often diverse and might interfere in unexpected ways. The supporting evidence building up a situation might be spread spatially or temporally, and it is often difficult to associate them. Furthermore, there is incomplete development of models portraying individual or group intent, event planning and execution. At the same time, when designing the automation of the situation assessment system, one must realise that it is not aiming towards awareness of an actual state but a representation of one. The performance of the situation assessment system depends on the fidelity of that representation [10]. There is no easy or single answer to such issues but the developers working towards a higher level fusion engine need to be aware of such constrains and actively seek ways to overcome them in any given application.

4 Uncertainty Grading

Situation and Threat Assessment processes need to be able to represent and deal with uncertainty both in the source data received and in the models used to interpret such data in terms of relationships, knowledge representation and situation recognition, (also referred to as Ontological Uncertainty) [10]. This is particularly important when fusing data from a wide range of sources including HUMINT (HUMan INTelligence), COMINT (COMmunications INTelligence) and open source data. Reasoning about the quality of that information is required to express the competence of such sources, their ability to observe what was reported, their reliability, the need for corroboration of the information and the restrictions on handling or disseminating what was reported. When dealing with ontological uncertainty, there are two distinct issues that need to be codified and represented; namely the fidelity of the model (whether the model represents faithfully well understood processes) and the precision of the model (whether the semantics of the model are clearly defined). Probabilistic methods are used to apply such types of uncertainty. Belief networks such as Bayesian Networks are used to reason about relationships among entities and deal with the structure of situations incorporating uncertainty. Ontologies are also used to describe concepts in a domain, by explicitly specifying ‘the objects, concepts and other entities that are assumed to exist in some area of interest and the relationships that hold among them’ [11].

There has been development of probabilistic ontologies to address the issue of semantic consistency and mapping. Costa et al. [12] developed a framework providing means to model uncertainty in ontologies. Probabilistic Ontologies provide explicit knowledge about an application, such as the entities that exist in the domain, the properties of those entities and how they are related, the processes and events that happen within those entities, and the uncertainties or missing information about those forms of knowledge. Probabilistic Ontologies are used to help explicitly describe knowledge about a domain and the uncertainty associated with that knowledge in a principled, structured and sharable way and in a format that can be processed using a computer [12]. PR-OWL is an extension to Web Ontology Language (OWL) which allows support of uncertainty and is based on Multi-Entity Bayesian Networks, a first order Bayesian logic that unifies the Bayesian probability theory with the first order logic [13].

Wright and Laskey [14] identified that the fusion of multiple sources requires the appropriate weighting of information to quantify the quality of the source of information. They suggested a credibility model that characterises the quality based on the source of the information and in the circumstances under which the information was collected. The suggested model includes multiple attributes to characterise the source credibility and competence. This paper adopts the above mentioned model and suggests an enhancement of the attributes used in order to fit with the National Intelligence Model (NIM) produced on behalf of the Association of Chief Police Officers in the UK [15]. The NIM model is used to provide guidance on characterising the information based on the nature of the information, the way it was obtained, or the circumstances of the person providing the information, which indicates whether the information should be treated in confidence or in a sensitive manner. The suggested 5x5x5 standard [15] is the National Information/Intelligence Report form which allows the Police Service and other agencies to record, evaluate and disseminate information. It is used at the point of audit and ensures consistency between forces, thus enabling them to share intelligence more easily. This study has incorporated the suggested model to grade each piece of information according to the attributes in Table 1.

<table>
<thead>
<tr>
<th>Reliability of Sources</th>
<th>Always Reliable</th>
<th>Mostly Reliable</th>
<th>Sometimes Reliable</th>
<th>Unreliable</th>
<th>Untested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin and Corroboration of Information</td>
<td>Known to be true</td>
<td>Information originated by source, no corroboration</td>
<td>Information originated by 3rd party and corroborated</td>
<td>Cannot be corroborated</td>
<td>Suspected False</td>
</tr>
<tr>
<td>Handling Codes</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Competence of Sources</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity of Source</td>
<td>True</td>
<td>False</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Uncertainty attributes

Reliability is referring to the authenticity and trustworthiness of the source. Origin and Corroboration of Information are denoting the provenance of the information and whether corroboration was possible. Handling codes are designed to provide an initial risk assessment allowing
those involved in the dissemination of intelligence to record their decisions on the suitability of sharing the intelligence. The details of the coding can be found in the original source [15]. Handling code is required to accompany the information but has no direct effect on the propagation of the beliefs associated with the information themselves. Competence refers to the person’s capability to observe well and understand what they observed, while the Opportunity shows whether the source was available at that point to obtain the reported information. For example a CCTV camera is always reliable, and the information it provides is known to be true, but depending on the weather conditions, the distance from the event under observation and on the resolution of the images it might have low competence at the recording of a vehicles number even if the opportunity was there. Similarly a member of the public might be an untested source in terms of reliability, but might report the event with competence if they were present at the event and the opportunity existed.

Figure 1 shows an example of information collection in the attempt to identify the number plate of a get away vehicle in a bank robbery. If there are two sources of information the uncertainty attributes discussed above are assigned for each source.

Bayesian decision theory is a fundamental theory used to represent the decision problem in probabilistic terms using plausibilities, combining prior knowledge with observations, and refining the degrees of plausibility as evidence occurs. Bayesian reasoning became extensively popular with the introduction of Bayesian networks, a probabilistic graphical representation of knowledge in an uncertain field, used for representing and combining large numbers of uncertain hypotheses.

In the example below, a get away vehicle needs to be identified by the police. The evidence from the CCTV is not adequate to confidently identify the number plate of the car. Even though the reliability and origin of the source is very high, the competence is low. On the other hand, the uncertainties relating to a statement of a member of the public are different. The reliability of the source is not tested, as the specific person did not give evidence in the past, the information was not corroborated, but there is high competence which increases the confidence of the statement. This model is also able to deal with partial information. So if competence of source is unknown, the probabilities can rely only on the prior knowledge relating to this attribute.

![Figure 1. Example of a Bayesian Network used for grading and analysing the uncertainty of information.](image-url)

Laskey and her associates [12, 13, 14] suggest a multi-entity Bayesian network (MEBN) which provides a synthesis of classical logic and Bayesian probability theory. MEBN encodes domain knowledge as parameterized argument structures called MEBN Fragments (MFrags). An MFragment is a modular component representing a small, individual, and conceptually meaningful part of the total argument structure supporting or denying a given
hypothesis. MFrags can then be combined to build models relating complex configurations of many features. They can be repeatedly used to represent multiple related entities of a given type, and can be re-used across multiple scenarios.

The authors are currently working towards building MEBN fragments to represent domain knowledge and create multiple scenarios used within Emergency Services.

5 System Engineering for Data Fusion

The operational architecture, which describes the operational elements, the processes, the information and work flow required to accomplish the fusion for situation and threat assessment functions, is given in Figure 2. This section describes in detail these processes and the information exchange between the different operational elements. And it justifies the design rational for such a system to satisfy the requirements of a fusion framework for emergency services. Some examples are drawn from possible Police scenarios to enrich and contextualise the explanation of the model.

Figure 2. Generic data fusion model for situation and threat assessment.

Figure 2 illustrates the data fusion model for situation and threat assessment, independent of fusion level. The diagram presents the processes and issues involved in data fusion process within a framework used for Emergency Services. The listed functions are planning, data collection, data association, situation assessment and threat assessment.

According to levels of fusion, as portrayed by Salerno’s Model of Higher Level Fusion [9, 18], these functions aim to identify the existing entities, their size and their attributes, and their kinematic information (level 1 fusion). Then they intend to perform behaviour analysis and create activity models, investigate the intent, and identify the potential impacts (level 2 fusion). Furthermore, projecting the current situation in the future they attempt to identify and analyse potential situations and impacts of those (level 3 fusion). More detail about each one of them is described in detail below.

5.1 Planning

At the start of the process is the definition of knowledge that is required to make operational decisions [4, 17]. This will depend on the application and the event to be handled and will be represented in terms of knowledge models. The data collection plan is defined by the data requirements and specifies the elements of data needed, as well as the sources that can provide the data that would lead to that knowledge. The decision makers as part of the human interface can have a direct input into the collection plan and the entities involved to help deal with unexpected and diverse evidence collection as discussed earlier. The diagram shown in Figure 3, presents the operation architecture for the planning and data collection processes.

5.2 Data Collection

Collection of raw data includes both openly available and closed sources accessed by humans or via technical means. In a typical police scenario, sensor data can include audio and video from surveillance cameras or in the near future from portable sensor devices carried by the officers attending the event. Additionally information may be input from the Automatic Number Plate Recognition system (ANPR) that police uses, or where available, image data obtained by police aerial platforms (UAVs, aeroplanes, helicopters) surveilling an area of interest. Human sensors may include police reports obtained during investigation, or observation, reports from the public (both victims and witnesses), as well as individual informers. Valuable input is also provided by national databases and liaison with other civilian agencies, organisations and authorities such as Children and Violent Adults, (CAVA) and the Violent and Sex Offenders register (VISOR), as well as open source material available in the web.

The collected data often needs to be associated, processed, aligned, indexed, organised, reformatted, spatio-temporal and semantic registration, and source characterisation. Hard sensor data is processed via image and signal processing techniques, such as feature extraction.
and pattern recognition methods. Human report information need to be processed via knowledge elicitation techniques to generate meta-data denoting participating entities, activities and relationships into well-defined semantic terms and vector or scalar variables. At the same time, open and closed source data is collected via software methods and search engines and data mined into useful information. Furthermore, generation of new objects of interest and continuous monitoring of the collection plan might lead to refinement and update of the input tasking process.

5.2.1 Source Characterisation

Among the most vital steps prior to the data association process is the characterisation of the input sources and the data generated by them. The error characteristics of each data either in forms of biases or other forms need to be accounted. A possible error might be either technical (audio capture or transcription error, or image recognition error in the ANPR system), or human errors and biases (false evidence provided during interrogation). Modelling or accounting for these errors and the possibilities for corroboration of data from multiple sources is essential and is something the authors are currently working on.

5.3 Data Association

Data association is a fundamental problem in multi-target and multi-sensor fusion. Traditional data association relates to associating sensor tracks to targets. In this case human reports and sensor information need to be ontologically associated and related in time and space and organised into individual target entities. It is common that electronic sensor data will have disparate formats, geometries, resolutions, extracted features, time references, and requires transformation of measurements and extracted information into a common spatial and temporal reference. Similarly contextual information needs to be extracted from the hard sensor data in order to be linked at a semantic level with soft sensor data [5]. We are currently working on meta-data generation for soft data by identifying and documenting associated data elements or attributes (name, type), data formats or structures (fields) and properties (location, ownership, associated context, quality and condition). The aim of the data association process is to identify the entities that are involved, the attributes that are required for each entity, to discover relations and relationships between entities and collect the elements required for the situation assessment process.

This is linked directly towards the knowledge base creation, which is the process of explicitly representing knowledge. This includes knowledge about the world (targeted in the specific application), characteristics about knowledge specific to the domain, and general procedural knowledge about reasoning [4]. Cohen et. al. [16], in DARPA, the Rapid Knowledge Formation project worked towards providing rapid knowledge capture, representation, and reasoning targeting the intelligence analyst process. We are working towards the development of tools to create knowledge bases specific to the intelligence required by the police, fire and ambulance services.

The diagram shown in Figure 4 presents the operation architecture for assessing the current and future situation, taking into account modelled uncertainties and risks.

![Figure 4. Current and future state estimation operational architecture.](image)

5.4 Situation Assessment – Current State Estimation

The first step for situation assessment process in an emergency services command and control system is to obtain a complete and concise understanding of the current situation. This can be separated into two distinct processes according to the situation at hand. Situation awareness derived from an analysis of an event, and possible threat awareness derived form a synthesis of specific evidence. Situation Awareness derived from Intelligence Analysis where an event or major incident has taken place and the system identifies the succession of causes and the entities (people/vehicles/places) involved, trying to determine the sequence of events and the evidence required to support the resulting hypotheses. The primary aim of the situation assessment process is to provide a better understanding of the situation, and a clear presentation of what objects are involved, how they are related, what events took place, how the situation evolves over time etc.

The diagram shown in Figure 5, presents the processes required to understand current state of situation, in the case of an event, and inform the human command and control interface.
Figure 5. Situation Assessment – Analysis - Process

The process starts with an event briefing, this leads to identification of the state variables and the entities evidently involved. Then the collection plan is devised and the data collection starts. This might identify further entities involved which will lead to the collection plan being revisited. Additional input from the Human Interface can assist or direct the collection of data. Data collection is informed with the uncertainties modelled, as part of the source grading process. Then the data combination and reasoning starts, incorporating the uncertainty relating to the fidelity of the model (whether the processes are represented faithfully and are well understood) and the precision of the model (whether the semantics of the model are clearly defined). The hypothesis generation and testing puts the situation scenarios under test and displays the results to the user to provide situation awareness and aid the decision making process.

Currently we are working in coordination with agent-based intelligence towards the production of inductive (learning and generalization) and deductive (decision and detection) reasoning processes knowledge bases. These models are goal directed and focus on agent awareness of purpose, values, and beliefs. Furthermore, they are specific to task type and provide reusable combination of model elements. Situational understanding and accumulated knowledge enables dynamic modelling to forecast current situations and depending on the defined organisational goals, provide a thorough evaluation of optional courses of actions in order to assist the decision making process.

5.5 Threat Assessment

The process of threat assessment includes similar elements to the situation assessment but refers to projected situations. The aim is to assess potential future situation and determine the likelihood and the cost associated with the specific events. This involves knowledge models of risks or costs to be integrated into the threat assessment process. The threat assessment includes threat event prediction, an explicit representation of indication and warnings, and a trigger to detect and characterise the threat and an assessment to analyse the potential event. Note that the identification of a threat is different to the calculation of the impact of a situation. The impact, in general, can refer to the influence or effect of the actual or potential situation to the environment or objects of interests. Appropriate measures need to be defined both for impact and threat assessment to rank the criticality and urgency of the situation at hand. This is something that will be addressed in future works and will be discussed in future publications.

Figure 6. Situation Threat Assessment – Synthesis - Process

The diagram shown in Figure 6, presents the processes required to recognise potential future situations or threat, based on readings of observable data. This process starts with observable data. This is different to raw data since it entails some information that is intended to activate the trigger function. An example of observable data is the output from the ANPR system, given that a vehicle’s registration number does not match the vehicle’s model and make description, therefore the vehicle is likely to be stolen. Such information will activate the trigger which is informed by a pool of trigger models identifying potential events. Examples of such models will include identifying and locating, using CCTV cameras, a convicted criminal outside their probation area, or locating a convicted paedophile within the confines of a school. The next process starts generating situation alternatives. For example the probation violation might be due to the person wishing to visit a relative in that area. This will be one alternative that will be hypothesized and tested. Other alternatives might include the likelihood to plan carrying out a similar criminal activity as those previously convicted. This will generate new observable variables and will initiate a new collection plan to identify similar crimes, performed in the area, since the person last reported to their probation office. Furthermore it will look into associates of the person and if they were also seen in that area to check the potential of collaboration into similar criminal activity. Data collection is again informed with the uncertainties modelled, as part of the source grading process. Afterwards the data combination and reasoning starts, incorporating the uncertainty relating to the knowledge models. Each scenario will be generated with the use of knowledge models and hypothesis tested and displayed to the user.

Decision making is informed by threat assessment, but still regarded as an outcome of mental processes (cognitive process) and relies solely on the human operators. The human is leading the selection of a course of action among several alternatives generated and tested by the system. The
output of the decision making process can be an action or an opinion of choice.

6 Conclusions
A centralised framework for data fusion and decision support in civilian services is discussed in order to provide more effective analysis of the vast amounts of information collected, a more comprehensive situation awareness model, and a better decision support system to the human command and control operators. Issues relating to situation and threat assessment have been discussed and the processes suggested to implement them were presented. Uncertainty grading of source and incoming information is also discussed and possible implementation attempts are given. Future work is focusing on fusion of information extracted from intelligence reports, generating knowledge models to represent events and preferred actions, and investigating technologies that could be used to develop the proposed framework. It is important to emphasize that the purpose of such development is not to eliminate the human commanders but to deliver to them meaningful and timely information which will reduce the workload and enhance the process of human judgement. The implementation and architectural considerations of such a system are discussed in [19].

References