Towards Sensor Modular Autonomy for Persistent Land Intelligence Surveillance and Reconnaissance (ISR)

Paul A Thomas[a], Gillian Marshall[b], David Faulkner[b], Philip Kent[b], Scott Page[c], Simon Islip[c], James Oldfield[c], Toby P. Breckon[d], Mikolaj E. Kundegorski[d], David J. Clark[e], and Tim Styles[f]
[a](pathomas@dstl.gov.uk) DSTL, Porton Down, Salisbury, UK; [b]QinetiQ Ltd, Malvern, UK; [c]Cubica Technology Ltd, Woking, UK; [d]Durham University, Durham, UK; [e]Create Technologies Ltd, Cockermouth, UK; [f]AptCore Ltd, Bristol, UK.

ABSTRACT

Currently, most land Intelligence, Surveillance and Reconnaissance (ISR) assets (e.g. EO/IR cameras) are simply data collectors. Understanding, decision making and sensor control are performed by the human operators, involving high cognitive load. Any automation in the system has traditionally involved bespoke design of centralised systems that are highly specific for the assets/targets/environment under consideration, resulting in complex, non-flexible systems that exhibit poor interoperability.

We address a concept of Autonomous Sensor Modules (ASMs) for land ISR, where these modules have the ability to make low-level decisions on their own in order to fulfil a higher-level objective, and plug in, with the minimum of pre-configuration, to a High Level Decision Making Module (HLDMM) through a middleware integration layer. The dual requisites of autonomy and interoperability create challenges around information fusion and asset management in an autonomous hierarchical system, which are addressed in this work.

This paper presents the results of a demonstration system, known as Sensing for Asset Protection with Integrated Electronic Networked Technology (SAPIENT), which was shown in realistic base protection scenarios with live sensors and targets. The SAPIENT system performed sensor cueing, intelligent fusion, sensor tasking, target hand-off and compensation for compromised sensors, without human control, and enabled rapid integration of ISR assets at the time of system deployment, rather than at design-time.

Potential benefits include rapid interoperability for coalition operations, situation understanding with low operator cognitive burden and autonomous sensor management in heterogenous sensor systems.

Keywords: Asset protection, intruder detection, sensor autonomy, sensor fusion, modular sensors, sensor management, autonomous decision making.

1. INTRODUCTION

In the context of both defence and security environments there is a need to protect high value land-based assets, such as military bases, civil dockyards and power stations, from asymmetric threats, typically human incursions into the area. A key enabler to protection is detection, but this imposes a high operator burden. Typically detection involves streaming raw, or lightly processed real-time data from a suite of sensors to screens which are constantly monitored by human operators. An example of this is a CCTV system monitored by humans as illustrated in Figure 1.

In such detection scenarios, operators are known to experience vigilance decrement over time[1]. Vigilance decrement typically occurs after 20 to 30 minutes of continuous work (varying with the level of concentration required) and results in less likely or slower suspicious event detection[2]. Vigilance decrement is exacerbated by such factors as low operator to screen ratio[3] - more cameras being introduced to the system for 'better' security coverage, information overload[3] - operators exposed to multiple different sources of information (e.g. radio call groups, telephone, e-mail, and cameras) and difficult to interpret data (e.g. radar plots rather than imagery).

Therefore, increasing the autonomy of detection systems is desired in order to reduce operator fatigue with a resulting increase in performance for detection and recognition of threats.

Figure 1: West Midlands Police CCTV control room [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0), via Wikimedia Commons].

Many current security systems adopt a bespoke design approach in order to solve complex system integration issues, including but not limited to autonomous detection. Such systems require a bespoke network to connect the sensors to the operator, bespoke processing and/or detection algorithms tuned to the performance characteristics of the sensors and bespoke warning rules tuned to the specific threat in the scenarios. This highly specific design approach lacks versatility in that there is limited scope for sensor redeployment, algorithm substitution or reconfiguration of the system for a different scenario. Additionally, in bespoke systems, failure of any one subsystem introduces significant vulnerabilities to the system as a whole.

Therefore, a desire exists, particularly for military security systems, for a modular open architecture. By introducing a modular architecture it is expected that the system as a whole will be more flexible and more resilient to individual failures, with lower procurement and ongoing costs.

The dual motivations of autonomy and modularity can be challenging to reconcile, since more sophisticated processing algorithms often rely on closer coupling with the sensor, whereas modularity is predicated on abstraction of the interface and “swappability” of the modules. Our work attempts to address such motivations by adopting a system architecture which deliberately enforces sensor modular autonomy (Section 2), developing autonomous sensor modules to fit this architecture (Section 3), exploring the higher level sensor fusion and sensor management issues emerging from this (Section 4) and integrating all components to form a working demonstration (Section 5). The results from the demonstration are presented in Section 6 with conclusions and further work in Section 7.

2. SYSTEM ARCHITECTURE

2.1 SAPIENT Concept

Sensing for Asset Protection with Integrated Electronic Networked Technology (SAPIENT) is an architectural concept which deliberately imposes sensor modular autonomy in order to explore the issues raised in Section 1. SAPIENT defines two types of module in the system: Autonomous Sensor Modules (ASMs) and a High-Level Decision Making Module (HLDMM). This architecture is illustrated in Figure 2.

ASMs are capable of sensing the environment, processing their raw data and performing target detection for preconfigured target profiles. Under the SAPIENT concept ASMs are also capable of autonomously making decisions on their own sensor parameters (e.g. field of view, angle of view, focus, etc. for passive EO sensors, or transmit power, beam direction, etc. for active sensors), in order to improve detection / threat discrimination. ASMs are self-contained units requiring only interfaces for data connectivity and power to operate. Inside the ASMs are such components as sensor head, data processing and autonomous decision making (see Figure 2). All internal communications between the sensor, data processing and autonomous decision making functionality are not visible to the rest of the system. ASMs process their raw sensor data into information (e.g. target descriptions and location estimation) suitable for near-real time transmission to the HLDMM.

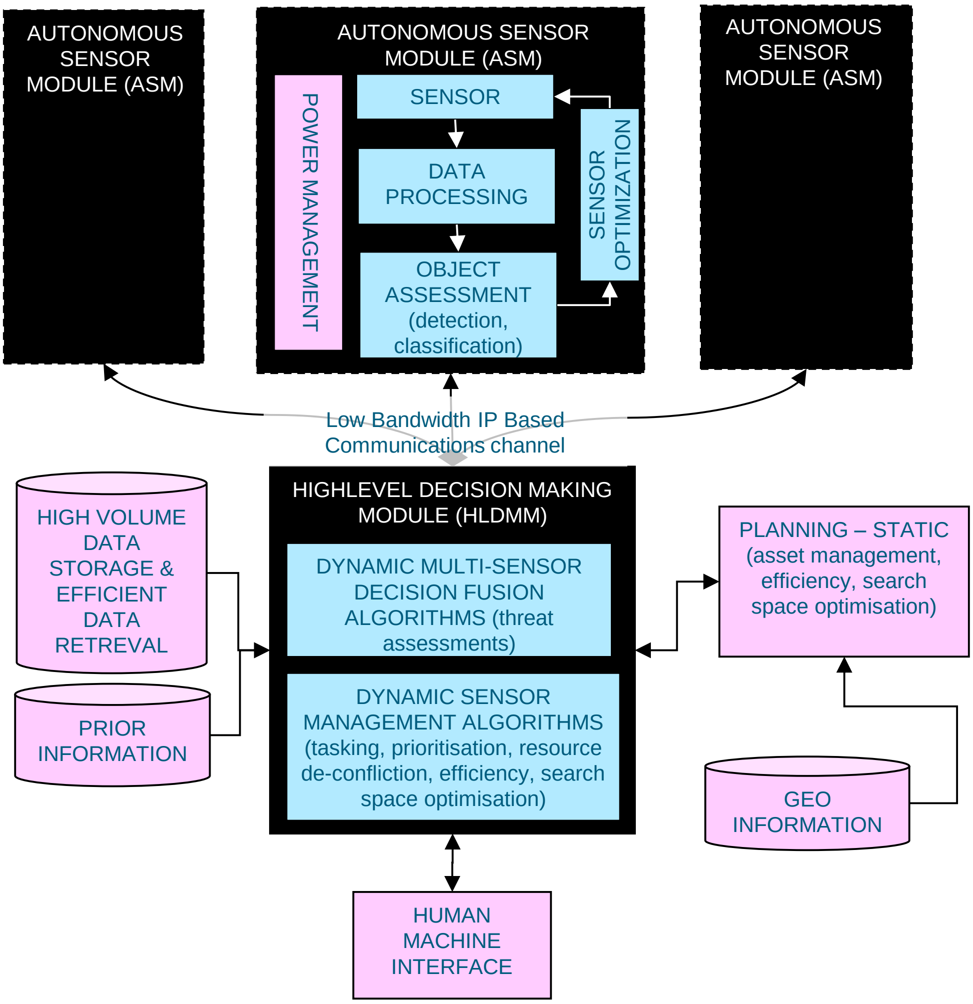

AUTONOMOUS SENSOR MODULE (ASM)
AUTONOMOUS SENSOR MODULE (ASM)
POWER MANAGEMENT
SENSOR
DATA PROCESSING
OBJECT ASSESSMENT (detection, classification)
SENSOR OPTIMIZATION
AUTONOMOUS SENSOR MODULE (ASM)
Low Bandwidth IP Based Communications channel
HIGH VOLUME DATA STORAGE & EFFICIENT DATA RETREVAL
PRIOR INFORMATION
HIGHLEVEL DECISION MAKING MODULE (HLDMM)
DYNAMIC MULTI-SENSOR DECISION FUSION ALGORITHMS (threat assessments)
DYNAMIC SENSOR MANAGEMENT ALGORITHMS (tasking, prioritisation, resource de-confliction, efficiency, search space optimisation)
PLANNING – STATIC (asset management, efficiency, search space optimisation)
GEO INFORMATION
HUMAN MACHINE INTERFACE

Figure 2: SAPIENT Architecture showing modules as black boxes, with their internal functionality shown in blue boxes. Peripheral services, essential to any implementation but not part of this research work are shown in pink.

The HLDMM provides overall management of the autonomous sensors modules, including providing tasking, prioritisation, resource de-confliction, efficiency and search space optimisation. The HLDMM is also responsible for fusion of the output from the ASMs in order to assess the threat conditions and the recommended course of action.

As a result each type of component (ASM or HLDMM) exercises decision making[*] and autonomy[†] at its own level. The ASM's decision making is the processing chain between raw sensor data and object assessments, and the autonomy is the optimization of sensor parameters discussed above; whereas the HLDMM decision making is in its decision fusion algorithms and its autonomy is the sensor management functionality.

[*] Decision making refers to the processing chain leading up to object assessment or situation assessment (Levels 1 or 2 in the JDL fusion model[4]). Although 'decisions' are also made in the process of sensor management.

[†] There are many definitions of 'Autonomy' in current use. For the purposes of this paper we choose to distinguish between systems that act according to a pre-defined 'script' or program, which we define as 'Automatic', and those that optimise a metric or free parameter in order to determine their action, which we define as 'Autonomous'. This definition aligns closely with those in other strategy documents[5,6].

Therefore, task allocations from the HLDMM are ‘high-level’ in that they include a degree of freedom within which the ASMs can exercise their autonomy. Typically high level tasks from the HLDMM would thus describe an area to monitor and/or targets to look for, rather than low level instructions regarding angle of view, focus, zoom level, etc. ASMs would dynamically optimise their low level parameters to complete these tasks, depending on contextual information.

The SAPIENT concept specifies that each ASM contains one and only one sensor type, to ensure that fusion only occurs in the HLDMM. Also, data pushed from the ASM should only be the low bandwidth output from the object assessment function (see 5.2), not raw data. As a slight moderation to this, the HLDMM is permitted to request raw data (e.g. thumbnail imagery) for specific detection events to present to the user for verification purposes, but the ASM would not routinely stream this data out.

2.2 Research Architecture

In order to develop solutions to the issues emerging from this concept, we developed a system protocol that deliberately enforces sensor modular autonomy. This provides a research architecture, rather than a prototype for an operational system, but it allows experimentation and demonstration of the concept in live scenarios with real sensors.

The SAPIENT research architecture is based around a central database, which each ASM populates with declarations and detections (this is low bandwidth messages rather that streaming raw data). A data agent manages the data-flow into the database. This allows the data agent to monitor and if necessary limit data bandwidth. The ASMs communicate with the data agent using messages as described in Section 5.2. The HLDMM queries the database, and performs higher-level fusion and reasoning based on the data therein. The HLDMM tasks the ASMs via the HLDMM data agent. This passes the task on to appropriate ASM via the data agent. Separately, the HLDMM populates another database table via the HLDMM data agent with data describing fused tracks and alerts. This data forms the basis of an overall situational awareness output to a human operator. More details on this architecture are given in Section 5.1.

The communications architecture of SAPIENT was chosen to be simple, light-weight and easy to integrate with, to minimise the risk of integration with multiple module suppliers on a variety of sensor platforms. It was envisaged from an early stage in the design that there might be a requirement to migrate SAPIENT communications to another network technology. Therefore, we ensured that the precise nature of the messaging protocol was not critical to the concept, allowing its implementation on other common messaging protocols such as Publish-Subscribe, Request-Response or Direct Connection.

3. AUTONOMOUS SENSOR MODULES

The aspiration of this work was to proceed to a physical demonstration using example instances of ASMs and an HLDMM. So we developed a suite of example ASMs with complementary features for detection of human intruders into a protected area. Of course, the concept described above is not dependent on any particular instances of ASMs so a SAPIENT compatible system could be built from an entirely different set, if more suited to the application.

3.1 Thermal imager

The thermal imager ASM (developed by Durham University) enables autonomous detection, tracking and behaviour classification of human targets based on passive long-range infra-red imagery (8-12µm). Targets are reported in real-time with geo-referenced co-ordinate positions (GPS position), associated short-term motion history (via tracking) and a probabilistic assessment (confidence) of both target type (as human) and current behaviour classification (as belonging to one of a discrete set of behaviour labels).

This primary sensing functionality (thermal imaging) additionally facilitates the detection of targets in low-light conditions, smoke, fog and in addition targets using camouflage within a low-EM signature (stealth) of a passive sensing device.

The ASM provides the HLDMM with rich target information encompassing {probabilistic target detection/classification, target geo-location, tracked trajectory, probabilistic behaviour classification}. The ASM is aware of its spatial coverage and reports “gaps in coverage” (obscuration) to the HLDMM. The ASM has its own GPS and compass capability for automatic self-localization at time of deployment.

Furthermore the ASM is capable of accepting the required taskings from the HLDMM in respect of:

- restricting the spatial region of target reporting;
- adjusting target reporting/update frequency;
- restricting reported targets by classification of type or behaviour;
- restricting reported targets by probabilistic assessment of type or behaviour;
- reporting low confidence targets (below detection/classification thresholds) within a specified sub-region of the ASM sensing footprint.

The ASM is additionally capable of reporting its current "sensor integrity" whereby any tampering with the sensor unit (or discovery of the unit within covert deployment) will be autonomously detected.

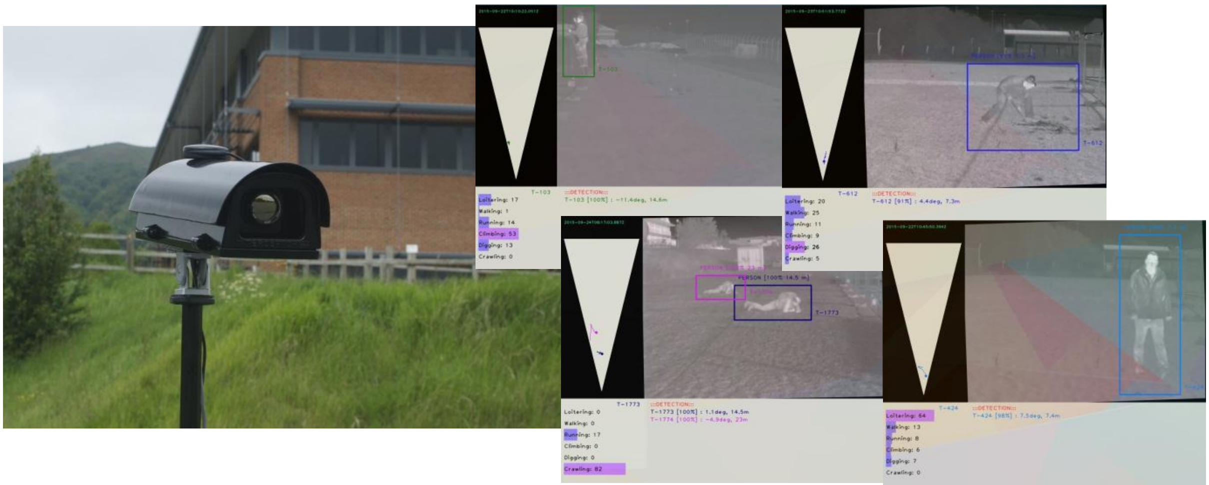


Figure 3: Durham University developed ASM (photograph left) based on a Thermoteknix MIRICLE 307K thermal camera. The screenshots on the right hand side show behaviour classifications as follows (clockwise from top left): Climbing, Digging, Loitering, Crawling. Each screenshot comprises the thermal image (top right pane) with detection box overlay, the geolocation and tracking window (top left pane) and the classification histogram (bottom pane).

A detailed description of the target classification work has been previously published[7,8], but in brief this ASM employs probabilistic detection/classification, passive geo-location via a technique that is independent of variations in target posture (i.e. behaviour) and within the statistical error bounds for pedestrian height posture, and Support Vector Machine (SVM) regression based pedestrian posture estimation operating on Histogram of Orientated Gradient (HOG) feature descriptors. Furthermore, tracked target trajectories are estimated, and probabilistic behaviour classification from the set of {Loitering, Crawling, Walking, Running, Throwing, Climbing} is performed.

This primary sensing functionality (thermal imaging) additionally facilitates the detection of targets in low-light conditions, smoke, fog and in addition targets using camouflage within a low-EM signature (stealth) of a passive sensing device.

The output of the ASM to the HLDMM (via the SAPIENT middleware) is {probabilistic detection/classification, passive geo-location, tracked target trajectory, probabilistic behaviour classification}.

3.2 Radar

The Radar ASM uses 24 GHz radar to determine the range, Doppler speed and direction of objects within the Field Of View (FOV). The measurement data is processed to score the object against the supported classes of {vehicle and pedestrian}. Vehicles are scored against classes of {two wheel and four wheel} and sizes of {heavy, medium and light}, and pedestrians are scored against the activities of {loitering, crawling, walking and running}.

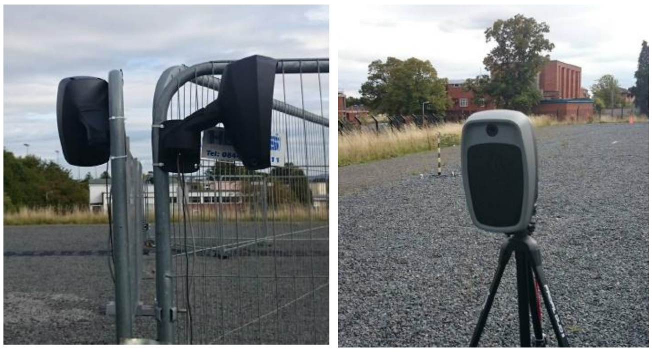


Figure 4: AptCore Ltd developed Radar ASMs in their enclosures.

Four radar ASM demonstrator units were constructed as part of the development. These were designed for unattended operation in all weather conditions and light levels, with a size and power consumption representative of a production unit. The AptCore ACR radar processor algorithms were used in an FPGA to minimise the size and power requirements of the ASM, with one of the units running on battery power.

The Radar ASM receives one or more tasks from the HLDMM that define an area to cover and one or more classes of object to report. Detected objects are tracked internally, and when sufficient confidence in the track is reached (typically within one second), a detection report is transmitted over the network if the track matches a task area and class.

The ASM is capable of measuring the range and Doppler speed of multiple objects. The system will classify objects as vehicles or pedestrians within a FOV of 80°. The radar is able to resolve the direction of multiple objects at each range, with good accuracy.

The radar front end has an adjustable transmit power level and is capable of focussing the transmitted beam in any direction (within the FOV). These features are used autonomously to increase the range and reliability of detections. The transmit power level is limited for license free operation, with the added benefits of reduced size and power consumption, and the prevention of any radiation hazard.

3.3 Scanning Laser Rangefinder

The concept behind the SLATE (Scanning Laser Automatic Threat Extraction) ASM is to produce a sensor module that provides a complementary view of the world to the camera-based systems that are usually used for wide area surveillance. SLATE uses a Scanning Laser Rangefinder that provides precise (<1cm) positions, sizes, shapes and velocities of objects within the field-of-view (FoV).

SLATE is based around the Hokuyo UTM30LX and UST20LX Scanning Laser Rangefinders (SLRs), providing shape, tracking and description to enable intelligent object recognition. The intelligence built into the SLATE system escalates high-level information to a controlling system or user, dealing internally with the sensor data and providing improved false alarm rates and mode switching. SLATE makes use of a SLR to generate either a two-dimensional cross section or three-dimensional model of the world around it. Moving objects are automatically separated from the background then tracked and classified, enabling precise shapes, sizes and velocities to be measured. Tracking people using SLATE is very accurate, with the limiting factor due to the determination of the target's centre. Boundaries and regions can also be set to trigger messages. SLATE can also operate in a second mode enabling the detection of static objects within the field of view. This mode can be used to identify new stationary objects in a crowded environment of moving objects.

The UTM30LX has a quoted reliable 30m range with a 270 degree field of view, although it can see up to 60m. This model gives the greatest coverage of a potential deployment area. The UST20LX has a shorter range (20m), but is smaller and lighter, while maintaining all the other properties.

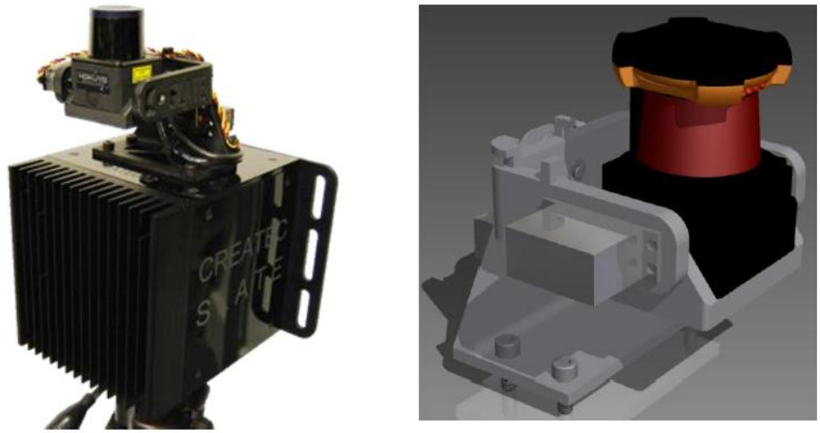


Figure 5: (Left) the prototype SLATE ASM developed by Create Technologies Ltd, and (right) a view of the ASM gimbal that enables positioning of the scanning laser rangefinder.

To level the laser scanner to the ground and to perform 3D scanning the sensor must be capable of moving through two axes. To achieve this, two Hitec HT-7940TH servos are used with a 3D printed frame. The servos are controlled via a Pololu Maestro 6-Channel servo controller. To provide GPS, Compass and Accelerometers for the demonstration an Ardupilot 2.6 Mega is used, which provides a useful array of packaged sensors that are easy to integrate into a system. The GPS and Compass provide the ability for the ASM to locate itself within the world during initialization. The accelerometers are used to provide a tamper alarm.

A single SLATE ASM comprises of a SLR and an on-board processing unit. These units have the ability to directly connect to the wider SAPIENT system. SLRs have several features which make them highly suited to the SAPIENT application. They are active sensors, largely immune to camouflage and able to operate at night and in poor visual conditions. SLATE’s ability to locate targets precisely allows subtle boundary-crossing judgements, e.g. which side of a chain-link fence is a target. SLATE’s ability to track targets in 2D throughout its FoV enables information such as running and walking that can indicate intent and reduce false alarm rates.

By escalating only high-level information to the HLDMM the difficulties in interpreting the sensor data are removed from the HLDMM and constrained to the ASM where the expertise in understanding the data lies. The sensor will provide a precise 3D FoV to the HLDMM ensuring that gaps in coverage are clearly identified.

In its primary mode the ASM provides the following functions: discriminate between vehicular and human activity; generate an alarm when a human is observed to cross a boundary, loiter by a fence or run in certain areas; provide a live track of humans tagged with their activity-history; generate an advisory notice when the environment changes the FoV so that the HDLMM can re-task other sensors.

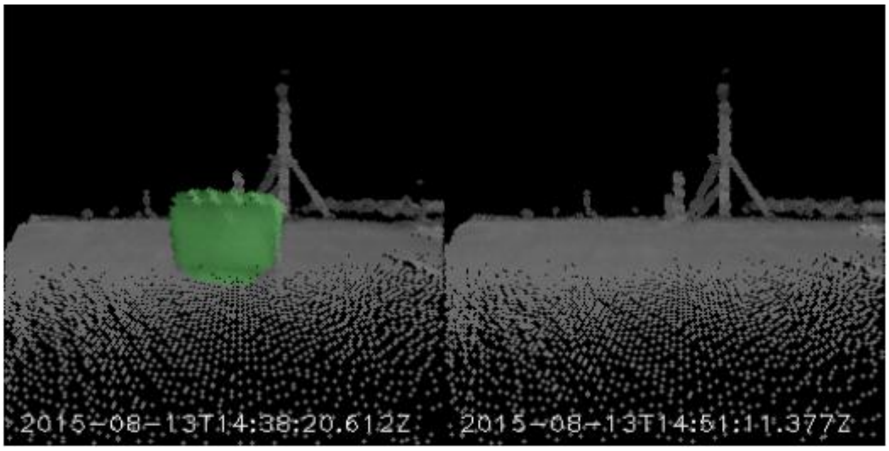


Figure 6: In the 3D scan mode the SLATE ASM will identify changes in the environment. This is suitable for detecting dropped objects that could potentially be Improvised Explosive Devices

SLATE’s second mode of operation ‘nods’ the ASM to produce a 3D point cloud of the FoV. Ground-plane information is extracted to enable the system to track targets across non-flat ground. 3D data can also be used to detect emplacement of packages or fence cutting cued by observation of suspicious behaviour.

3.4 EO Pan, Tilt, Zoom (PTZ) camera

Most existing security installations include CCTV for visual observation. In many cases Pan-Tilt-Zoom (PTZ) cameras are used to provide both wide area coverage and, in the event of interesting activity, zoomed-in high resolution views for recognition and identification purposes.

Intruder detection systems often provide an approximate location of an event but may have limited ability to determine the event type or provide identification. The inclusion of PTZ cameras within SAPIENT provides a capability for verification of activities. This is achieved through the use of geometric calibration such that the camera can be automatically slewed to look at an area of the scene where activity has been detected by another sensor. The zoom of the camera is also automatically optimized to provide appropriate field-of-view to observe typical human and vehicular activity.

This capability requires a PTZ camera that can be directed to an absolute orientation in pan and tilt and a specified zoom range. For the purposes of SAPIENT, we used a Bosch MIC 400 series camera (commonly found in outdoor PTZ applications). The relationship between abstract zoom settings used by the camera and physical field-of-view is modelled in software to enable appropriate automatic selection of zoom.

The inclusion of a camera enables the use of visual analytic techniques for automatic detection of threats. Many analytic techniques only work well with fixed field-of-view cameras by looking for variations from a background scene model. With a PTZ camera the situation is much more dynamic due to camera movement. For SAPIENT, pedestrian detection techniques[9] originally developed for Automatic Driver Assistance Systems have been used and optimised. These are able to immediately detect humans within the camera field-of-view without requiring background scene modelling.

It is possible to infer the approximate ground location and size of detected objects within the scene given known camera orientation and field-of-view. Further assessment of the detected object size against anthropometric models is used to reduce false alarms.

The system can provide an automatic person tracking function, which builds on the human detection analytics. With “follow mode” engaged, the PTZ camera will automatically adjust pan, tilt and zoom settings to keep a detected human central in the field of view. The zoom is dynamically controlled to keep the human at reasonable size in the image to maximize the likelihood of subsequent detections.

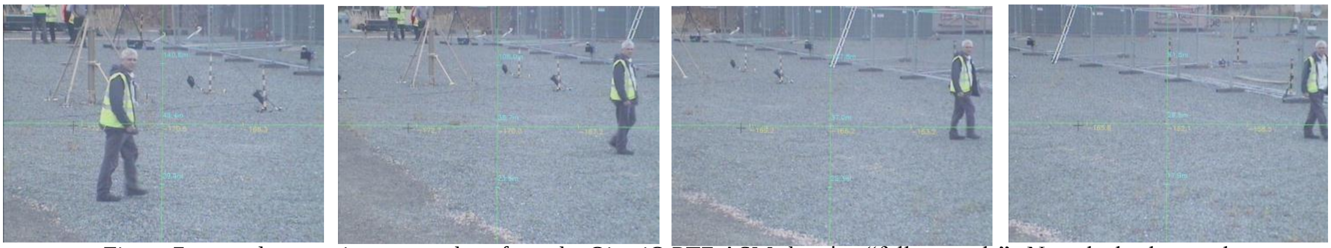


Figure 7: several successive screen shots from the QinetiQ PTZ ASM showing “follow mode”. Note the background features which indicate how the ASM has autonomously changed its field of view to keep the target in the frame.

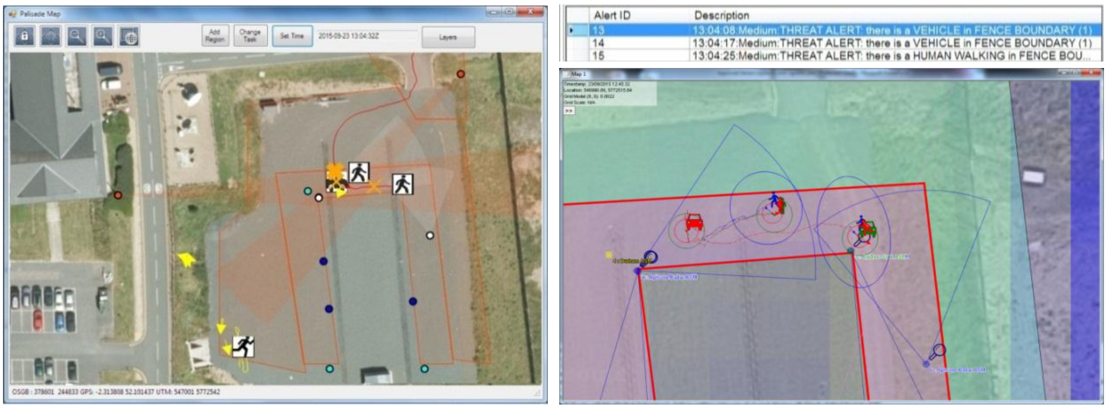
4. HIGH-LEVEL DECISION MAKING MODULE

The SAPIENT HLDMM provides the overall Situational Awareness, Threat Assessment, and Sensor Management functionality for the SAPIENT system. It is responsible for processing the ASM reports, performing data fusion and reasoning on those reports, outputting target, threat and other situational awareness data to the operator via the SAPIENT GUI, calculating optimum use of the ASM resources and issuing ASM tasking messages. Based on an open architecture, the HLDMM module supports a range of ASMs of varying technologies allowing dynamic ‘plug and play’ during operation.

The core HLDMM data fusion algorithm includes multi-sensor, multi-target data association and tracking, target type classification and fusion, target behaviour classification and fusion. The resulting classifications and target tracks are used to prioritise targets and evaluate the level of threat presented to the asset based on the operational context that is defined by the operator/installer, thus making the system adaptive to different scenarios. Operational context is defined through the definition of different zones of interest, and target threats of interest. When threats are detected the HLDMM raises "Alarms" for inspection by the operator.

The HLDMM Sensor Management function computes ASM control taskings to improve Situational Awareness based on a number of measures. Taskings include controlling areas of interest, cross-cueing, hand-off, and image capture for threatening targets. A further feature of the HLDMM is its ability to provide "Warnings" to the operator when the level of uncertainty about potential threats is high, for example because of coverage gaps. This provides a new level of operator guidance and system capability.

The design of the HLDMM results in improved system performance over standard systems in terms of probability of (threat) detection, false alarm rates, coverage awareness, and reduced operator workload. By taking into account the specific operational context, the system will only alert the operator to relevant threats, minimising the amount of information the operator has to process. The HLDMM embodies a number of advanced features that allow it to optimise the probability of threat detection, minimise false alarm rates and adapt to different ASMs.



Alert ID	Description
13	13:04:08:Medium:THREAT ALERT: there is a VEHICLE in FENCE BOUNDARY (1)
14	13:04:17:Medium:THREAT ALERT: there is a VEHICLE in FENCE BOUNDARY (1)
15	13:04:25:Medium:THREAT ALERT: there is a HUMAN WALKING in FENCE BOU...

Figure 8: (Left) the output from the Cubica Technologies Ltd HLDMM as displayed on the user GUI, showing identified vehicle and pedestrians in the scene (icons indicate walking and running activities identified) and the resulting taskings issued to the PTZ ASMs (red cones); (top right) the alert outputs associated with the scene; (bottom right) "under the hood" of the HLDMM showing input declarations from the ASMs (blue and green icons and location ellipses) and fused results (red icons) which are sent to the user GUI.

4.1 Decision Fusion

The HLDMM reads ASM registration data in order to understand the baseline capability and performance of each ASM. ASM reports are fused at multiple levels in order to generate a central store of target tracks and associated meta-data, such as classifications (e.g. Human / Vehicle) and behaviour (e.g. Walking / Loitering / Climbing). The ASM Data Fusion process is tightly integrated with the ASM Trust Model which maintains a model of the real-world performance of each ASM in terms of detection, false alarm, and classification performance.

The HLDMM supports ASMs with varying geolocation and classification capabilities, including ASMs that only provide detections (or tracks) and ASMs that only classify a sub-set of the classes or behaviours of objects in the SAPIENT taxonomy. Furthermore, the HLDMM can support both probabilistic and non-probabilistic classification data.

The target track and associated meta-data is stored for higher level processing and for (potential) transmission to the SAPIENT display.

4.2 Flexible Context Driven Processing

Perhaps the most important feature of the HLDMM is its ability to evaluate Threat in a context-driven manner. This capability is critically important in reducing operator burden and making effective and efficient use of the available ASM suite.

The HLDMM allows the operator or installer to define the key areas of interest in a prioritised manner, the Threats of interest, and the surveillance objectives. This can either be completed as a one-off event at installation, or the priorities, areas and objectives can be varied live at any time in order to adjust to changes in context.

For example, the operator may define two areas; one around the boundary of the core asset to be protected, and a second (possibly lower priority) area located elsewhere (for example a storage area / power cabinet / comms tower). They may specify that they are only interested in human threats in these areas. This sets the context for the HLDMM and allows it to minimise operator burden by only raising relevant alerts and avoiding false alerts.

An advanced operator can influence the ASM task planning function by rapidly building a context-driven planning strategy based on a range of high level tasks including Threat Search, Threat Localisation, Threat Identification and Threat Scanning. This simple yet highly flexible configuration capability facilitates easy redeployment and ensures that all of the ASM resources are efficiently used. In the absence of operator input at installation time, the HLDMM will automatically invoke a standard configuration to protect a given boundary area, allowing for ultra-rapid setup.

Finally, the HLDMM can be configured with prior knowledge of target presence (i.e. where targets can appear and disappear in the scene, and even how they might typically move). This additional information is used by the HLDMM to consider briefly "looking away" from some areas in order to trade-off other objectives or areas.

4.3 Real-Time Threat Evaluation

Once the HLDMM is aware of the operator context, it evaluates the current Threat condition in real-time using a probabilistic framework.

The HLDMM reasons over the outputs of the Data Fusion process and raises an Alert when it is sufficiently confident that a relevant event is occurring based on the operator's context. Human readable Alert messages are formed for transmission to the SAPIENT display along with supporting meta-data such as associated tracks, threat imagery, confidence, and time of threat.

Alerts are dynamically prioritised based on the operator's context definition. This ensures that the operator's attention is drawn only to the most relevant pertinent data even when multiple events are occurring simultaneously. The user is presented with an ordered list of Alerts as shown below.

4.4 Optimisation of ASM Taskings

The HLDMM embodies a dynamic ASM Tasking / Sensor Management capability. Based on the current operational context, the HLDMM evaluates a very large number of possible ASM tasking combinations that could be invoked. Each of these combinations is evaluated in terms of its expected impact on the knowledge about the current threat conditions.

Crucially, this means that if the operator has specified that they are only interested in one target type in a certain area, the HLDMM will select ASM tasks that are most likely to improve the system's understanding accordingly. The HLDMM will prioritise tasks according to their relative benefit in terms of Threat Search, Threat Localisation, Threat Identification and Threat Scanning, according to the current planning strategy. For example, ASMs may be tasked to gather imagery of a known threat in preference to searching for new threats.

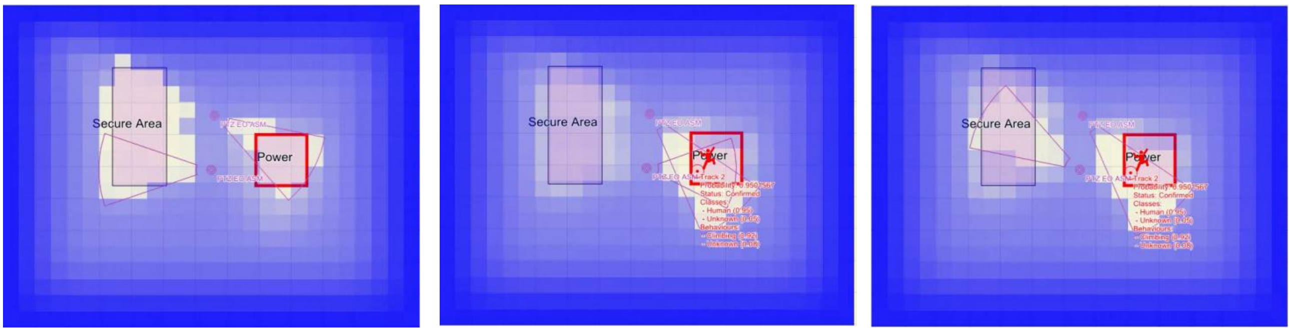


Figure 9: Example "under-resourced" scenario with primary "secure area" zone and secondary "power cabinet" zone, two PTZ sensors (red cones) with potential threat detected in secondary zone (Left); As the threat is confirmed the left hand PTZ is tasked to support image capture of the threat (knowing that) in the meantime the probability of undetected threat increases in the primary zone (middle); as this probability increases the left hand PTZ is retasked to the primary secure area zone

Multiple regions, threat types, and objectives can be supported simultaneously, allowing the operator to set demanding surveillance goals. A hybrid stochastic search – brute force optimization algorithm is utilised to provide both scalability and high performance optimisation.

Figure 9 demonstrates an example “under-resourced” scenario where there are insufficient ASMs to cover both areas of interest (ASM failures and/or degradations may produce similar conditions).

In this case the HLDMM has tasked one of the ASMs to search for new potential Threats in the ‘Secure Area’, and a different ASM to search for new Threats in ‘Power’ building (Figure 9, left) – note that this tasking is not explicity prescribed but is a result of an information theoretic optimisation process given the user context. However, when a threat appears in the Power building (Figure 9, middle) the HLDMM calculates the risk associated with tasking the left hand ASM away from the Secure Area to support localisation and image gathering of the threat and both resources are tasked to make observations. After some time this results in an increasing uncertainty over potential threats in the Secure Area. Therefore, as time progresses tasks are occasionally issued to instruct one of the ASMs to “look away” from the Power building (Figure 8, right) to gain information about the Secure Area whilst the threat is surveilled. In arriving at this tasking, the HLDMM has taken into account the likelihood of targets arriving in the unobserved area whilst the ASMs are “looking away” versus the current level of uncertainty over the observed target, and will only allow this to occur if the resulting uncertainty is lower and the strategy is consistent with the contextual planning strategy. This novel planning approach dramatically increases the benefit of ASM tasking by freeing up otherwise constrained ASM resources.

5. SYSTEM INTEGRATION

We designed an open architecture, Interface Control Document, GUI and middleware for the SAPIENT concept. The architecture has been deliberately designed to be extendable in the future, and includes provision for mobile sensors (including UGVs, UAVs and dismounted soldiers). It can also be made interoperable with emerging Base Protection Standards.

5.1 Architecture

The SAPIENT architecture passes concise, high-level threat information between a number of ASMs and an operator GUI. ASMs pass threat information to the HLDMM which performs fusion and threat detection. This passes high-level threat and alert information to an operator GUI for further action as required. A common interface is defined between the modules. By supporting this interface, any suitable sensor can be made ‘plug-and-play’ into SAPIENT.

The SAPIENT middleware provides the glue for the system. It handles all the communication between the different system modules and stores the SAPIENT information in an Open Source database for immediate use or after-action review. For simplicity, each module has a single communication channel via the SAPIENT middleware. The middleware has been designed to be simple to use and deploy and includes intuitive system health monitoring.

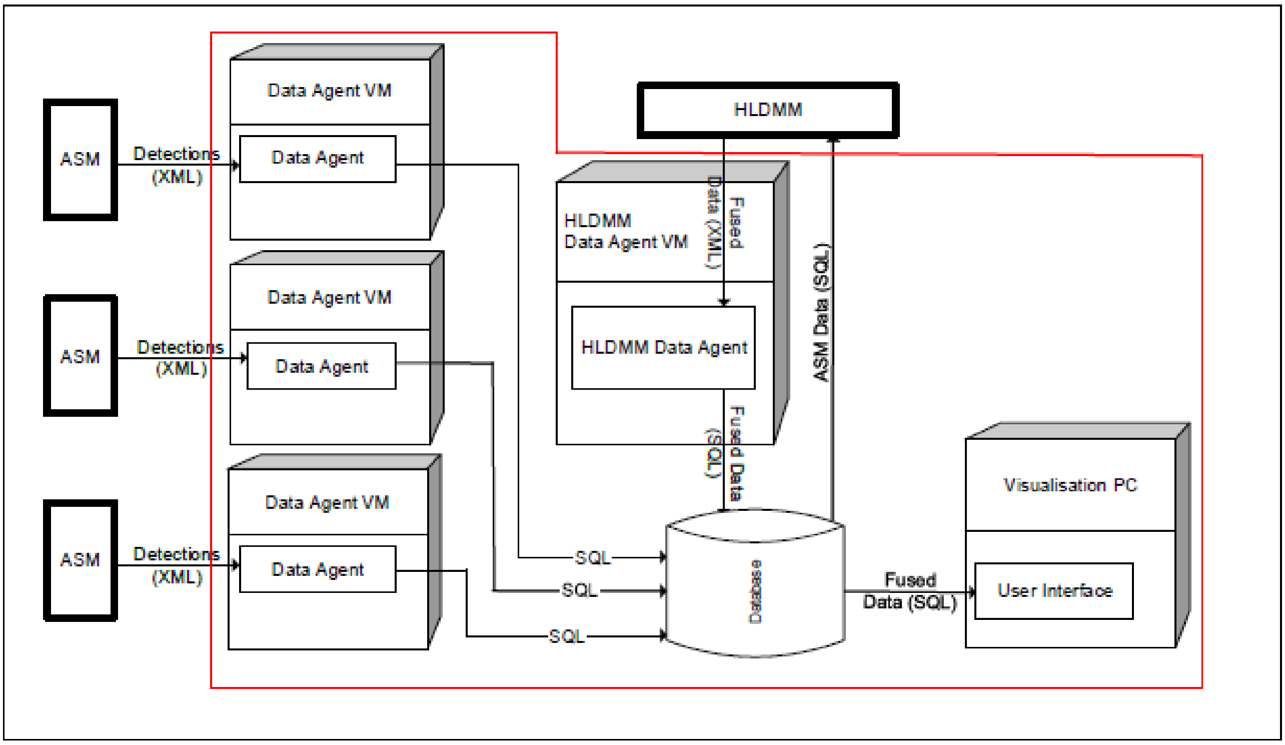


Figure 10: The SAPIENT architecture illustrating data flow from ASMs via the SAPIENT middleware to the HLDMM and GUI.

5.2 Interface Control Specification

We defined the interface between the different sensor and decision making modules and the SAPIENT middleware with the principles of simplicity, flexibility and extendibility in mind, to enable rapid integration, deployment and future adaption. The interface defines a small number of concise but extendable XML messages that may be sent between modules. These are concise enough to allow rapid integration of simpler sensors whilst being flexible enough to support a wide variety of fixed and mobile surveillance sensors. They also support target type and behaviour classification information to allow the system to automatically discriminate between threat types. E.g. Human Digging, Climbing, Car Loitering, etc. The messaging is independent of the communication medium. In this way the SAPIENT messaging can be made inter-operable with emerging base-protection standards.

A draft form of the Interface Control Specification will be made publically available at https://www.gov.uk/sapient/.

5.3 Graphical User Interface

The SAPIENT GUI is built on QinetiQ’s Palisade platform that has been in service for several years as a simple, intuitive user experience for monitoring the physical security of sites. A map view using geo-referenced aerial imagery is overlaid with the location of detected activity on site whether that is deemed threatening or benign. Threats are highlighted to the operator with any accompanying information such as an image snapshot to give them “eyes-on” the target.

6. DEMONSTRATION AND RESULTS

The final part of this work involved a proof of concept demonstration incorporating live ASMs, live targets and a live HLDMM. We wanted to fully exercise the system in a realistic generic intruder detection environment with challenging conditions. The two purposes of this demonstration were to demonstrate, to a variety of stakeholders (both from military and civil security domains), that the concept is feasible, and also to experience and solve systems issues. The demonstration was not a rigorous experimental trial designed to fully test performance, but a more qualitative assessment of systems and integration issues.

6.1 Vignette Design

We carefully designed three vignettes to demonstrate the full range of capabilities of the SAPIENT system, including the local autonomy of the ASM modules and the system-level autonomy provided by the HLDMM. The vignettes were also designed to build in complexity from one vignette to the next, thus allowing the stakeholders to develop a fuller understanding of the system capabilities. In particular, the vignettes were designed to demonstrate:

- Baseline (non-threat) events:
- Vehicles and people in non-threat zones;
- Suppression of nuisance alarms;
- Active sensor management – for example PTZ sensors cued by HLDMM to step-stare, looking for threats.
- Hostile Scenarios:
- Vehicle and pedestrian targets entering threat zones:
  - Tracks fused from multiple sensors;
  - Multiple targets detected, tracked, and prioritised;
  - Behaviours classified;
  - Alerts raised, with associated snapshot.
- Key Autonomous Behaviours:
  - Sensors detecting and reporting location of pedestrians, moving vehicles and dropped objects;
  - PTZ and radar tasked to cover regions of interest, to search for threats, confirm & localise detections, and PTZ tasked to gather imagery of threats;
  - PTZ "follow" – autonomously following a pedestrian of interest;
  - Laser autonomously switching mode to take 3D scan of a dropped object;
  - Sensor modules alerting the system to occlusions and tampering;
  - Alerts displayed on an end user GUI
    - Accompanied by a snapshot and text description.

6.2 Sensor Laydown

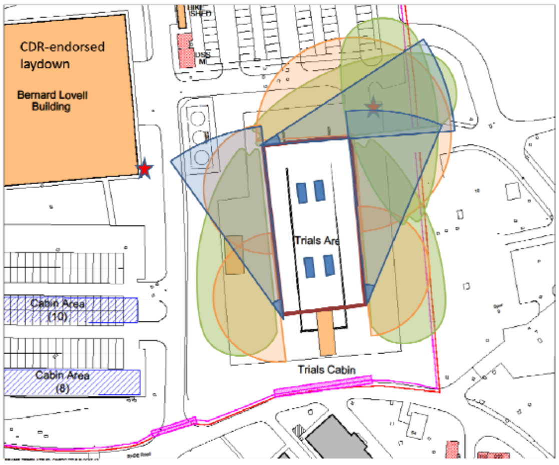


Figure 11: The sensor laydown implemented for the SAPIENT demonstration. Showing two PTZ ASMs (Red Stars), three Thermal Imager ASMs (blue cones), four radars with steerable beams (green lobes), one 30m laser scanner and three 20m laser scanners (orange segments). Also shown is the Herras fencing (solid brown line) surrounding an inner protected area containing four shipping containers (dark blue rectangles).

Figure 11 shows the demonstration layout. The sensor coverage was deliberately designed with multiple overlapping fields of view from heterogeneous sensors, with the majority of the sensors arranged to protect the area immediately outside the Herras fencing. It is accepted that this arrangement, with such a high degree of overlap, is unlikely to be implemented in a real scenario, however it was very useful in a research context to explore the issues around track-level fusion from multiple different sensor modalities. Shipping containers were used in the area to be protected which had the effect of providing obscurations for the two PTZ cameras, such that neither one is able to see the whole of the area of interest.

6.3 Vignettes

<u>Vignette 1 – Basic capability</u>

In this initial vignette, the basic capability of the SAPIENT system was demonstrated, including:

- Multiple benign events (vehicles and pedestrians in non-alert zones);
- A simple attack of a person entering an alert zone adjacent to the fence, and performing a suspicious activity.

<u>Vignette 2 – ASM Autonomy</u>

In this vignette, the intelligent autonomy of the ASMs was demonstrated, including:

- · PTZ follow;
- · Laser switching mode to take a 3D scan;
- · Radar beam-steering.

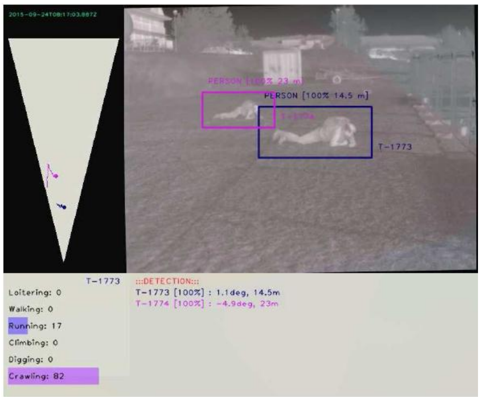
<u>Vignette 3 – HLDMM Autonomy</u>

The final vignette was designed to demonstrate the system’s capability in dealing with a complex attack which occurred simultaneously on both sides of the protected area. Existing systems, which typically rely heavily on an operator monitoring a bank of monitors, struggle in these circumstances – if the operator’s attention is taken up with monitoring and responding to a diversionary attack in one location, he is more likely to miss a second attack occurring concurrently. Additionally, this vignette was designed to show the HLDMM’s sensor management function, particularly under challenging circumstances when multiple sensors were disabled and hence coverage was lost down one side of the protected area.

6.4 Results

The SAPIENT Demonstration Day was designed to show off the capabilities of the SAPIENT system, and to provoke discussion amongst the attendees about future possible exploitation routes. It was not intended to be a metricated trial or experiment, and no performance metrics were sought or gathered. Broad results have been captured and documented below, and represent development opportunities for future iterations of the system. Note: individual detection performance for the ASMs and fusion/sensor management performance of the HLDMM will be published in forthcoming papers.

6.4.1 Thermal imager



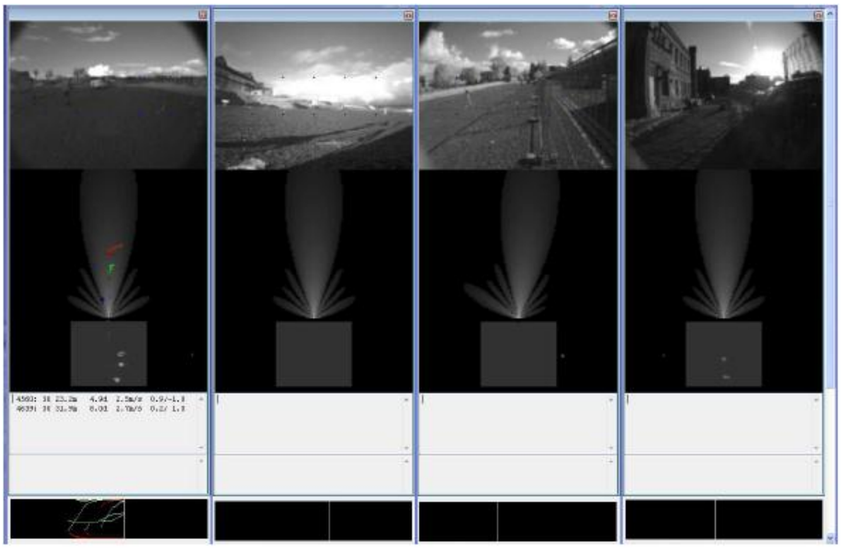
```
T-1773
Loitering: 0
Walking: 0
Running: 17
Climbing: 0
Digging: 0
Crawling: 82
```

```
:::DETECTION:::
T-1773 [100%] : 1.1deg, 14.5m
T-1774 [100%] : -4.9deg, 23m
```

Figure 12: Thermal imager ASM engineering GUI showing two crawling intruders from Vignette 3.

Figure 12 shows the engineering interface to one of the thermal imagers at the point where two attackers are crawling in towards the fence. The right hand pane shows the video stream from the TI camera, with the location of the two detected people outlined, giving their distance and the classifier's confidence in their being human (in this case, 100% for both). The cone on the left shows the tracks associated with the two detections, colour-coded to match the boxes superimposed on the video stream. Below that is the output of the behavioural classifier for the closer target (Target number 1773 is the person outlined in navy blue) showing that the system is confident the person is crawling.

6.4.2 Radar



```
4580: 38 23.2m   4.9d  2.5m/s  0.9/-1.0
4639: 38 31.9m   8.0d  2.7m/s  0.2/ 1.0
```

Figure 13: Radar ASM engineering GUI showing: a black and white video image of the scene; a "radar cone" display showing the radar beam, and detected plots & tracks, a range-Doppler map (objects further up the map being further away, objects moving towards the radar appear to the left of centre and objects moving away from the radar appear to the right), a list of current tracks and a plot of the classification over a moving time window

Figure 13 shows the radar engineering GUI at a point in time towards the end of Vignette 3. Nothing is happening in the fields of view of three of the sensors, but activity is occurring that is being monitored by the first sensor. This can be seen in the left-hand panel, where the vehicle and pedestrians have been detected and are being tracked as they leave the trials area. They are the red (vehicle) and green (pedestrian) tracks in the radar cone, with the latest detections giving range, bearing, velocity and classification in the text box below. The classification figures show the pedestrian scores 0.9 as a pedestrian and -1.0 as a vehicle, while the vehicle scores 0.2 as a pedestrian and 1.0 as a vehicle. The classification is plotted over time at the bottom of the panel, where the detection, vehicle and pedestrian confidences are plotted in white, red and green respectively. There is one high scoring red line for the vehicle, one high scoring green line for the pedestrian at 23 metres, and a third set of lines for the pedestrian a few metres away, who is just entering the radar field of view.

6.4.3 Scanning Laser Rangefinder

Figure 14 shows a snapshot of Vignette 3 from the perspective of the laser scanners. The image is displayed as an "eagle-eye view" of a 3-D point-cloud. In this view of the scene, the entrance to the trials site is in the middle of the right hand edge, and is covered by the right-most sensor labelled "slate1_laser". In the snapshot above, two people are walking/loitering in the lower half of the image, one next to the sensor in the bottom middle of the image, and the second person to the right of that. Two crawling people have also been detected as humans in the top middle of the image. A parked-up van has been detected at the other corner and is identified with high confidence as a 4-wheeled vehicle. The lighter-grey detections in the top of the image have been classified by the laser ASM as noise or non-significant and have been suppressed at source, i.e. they have not been passed up to the HLDMM or the operator GUI.

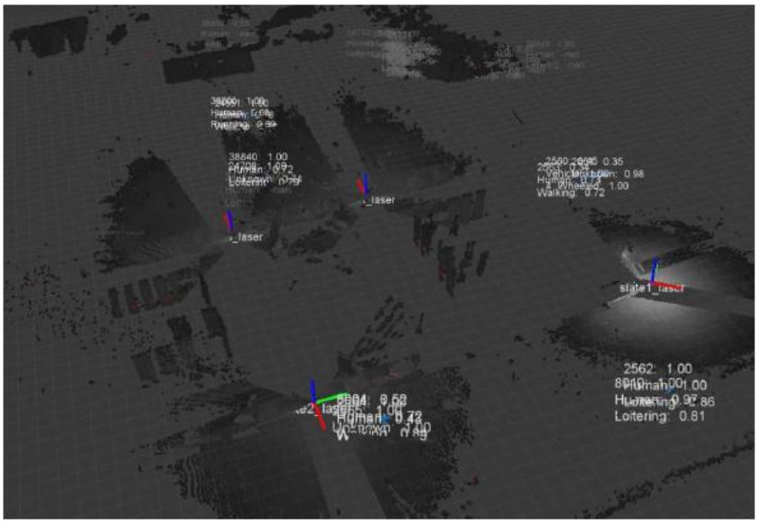


Figure 14: Scanning Laser Rangefinder ASM engineering GUI with the four sensor locations shown by primary-coloured axes. White text denotes detections of people and vehicles, with the text string providing information on classification (human/vehicle) and activity (walking/loitering)

6.4.4 EO Pan, Tilt, Zoom (PTZ) camera

Unfortunately, no screenshots were taken from the PTZ ASM on the day of the demonstration, and the original video was not recorded so it is not possible to recreate the outcome.

6.4.5 High Level Decision Making Module

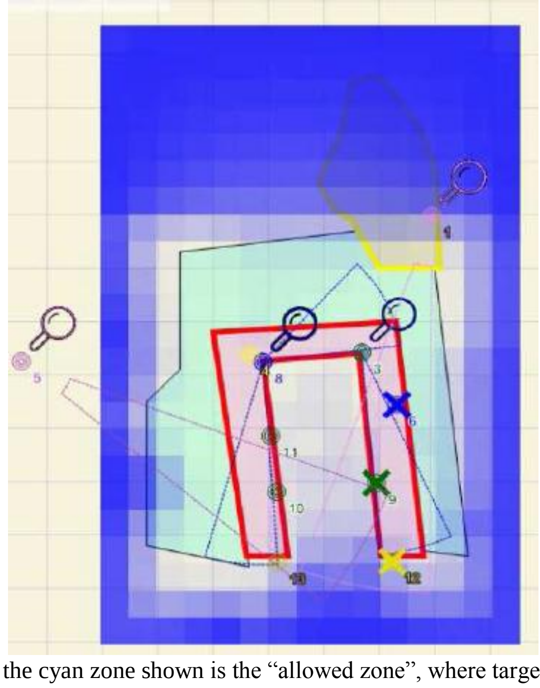


Figure 15: HLDMM GUI: the cyan zone shown is the “allowed zone”, where targets do not generate an alert. There is a high-priority “alert zone” shown in pink with red border which protects the immediate vicinity of the fence, and a lower priority “alert zone” in yellow covering the entrance to the Trials Area. The blue background fading to white is a representation of the HLDMM’s “Threat Domain Model” – a probabilistic model of potential target presence. The darker the blue, the less information the HLDMM has about the region

The final act of a complex vignette is shown in Figure 15 above, At this point in the action, all the protagonists have left the scene, having first disabled/tampered with a radar (blue cross), laser (green cross) and thermal imager (yellow cross).

All three ASMs have reported that they have been tampered with, so the HLDMM is aware that the entire right hand side of the fence-line has been left unprotected. In response, the HLDMM has tasked the PTZ top right to cover lower the right area (pink arc), whilst the Radar top left is tasked to cover immediate area in front next to the fence-line (blue arc).

Note: although it can't be seen in this static snapshot, the field of view of the PTZ and Radar return to cover the entrance to the Trials area (yellow zone) intermittently in accordance with the HLDMM's planning strategy and domain model, taking a "calculated risk" that nothing significant will occur in the unprotected area whilst they are scanning elsewhere.

7. CONCLUSIONS AND FUTURE WORK

This work showed that it is feasible to set up a security system with the concept of delegated responsibility for detection, classification and (in some cases) tracking, to Autonomous Sensor Modules.

These ASMs produce threat declarations rather than raw data. This enables local decision making, tailored specifically to the sensor, to be employed. Similarly the sensor is able to autonomously optimise its sensing parameters to make better threat declarations.

The threat declarations are handled by a middleware layer and accessed by a high-level decision making module. Despite the lack of access to the raw data, the HLDMM is able to fuse heterogeneous sensor declarations and make inference about the threat state in the scenario. Lack of access to raw data is a challenge for fusion systems but this sub-optimal fusion scenario appeared to have acceptable accuracy and presents significant operational advantages (i.e.. low bandwidth communications, flexible system configuration, and lower system cost).

The HLDMM is able to reason over and optimise the set of taskings it issues to the ASMs, despite the degree of autonomy the ASMs have in the way they execute the tasks. In effect this mirrors the issues in Management Studies regarding the balance of authority, responsibility and accountability when delegating tasks from human managers to subordinates.

Interestingly, under this concept the sensors can get away with generating more false alarms, since the HLDMM is able to supress these to some extent. For example, in other systems, designers generally apply a confidence threshold of 50% before reporting detections, but in SAPIENT some of the ASMs start reporting at 20% (with a reported confidence level) which enables the HLDMM to have a more sensitive view of the scenario while supressing alarms that are not consistent with reports from other ASMs.

This concept could have application in multiple scenarios where reduction in operator burden in the detection process is of benefit. Of course, some targets by their very nature are only discernible by human analysis. In this situation the system will still have benefit in cueing the operator on to a potential target, but raw data or snapshots of imagery will need to be transmitted. However, importantly this transmission will occur as a "pull" from the HLDMM rather than a stream of data "pushed" continuously from the sensor.

Overall the system performed very well in the demonstration. Showing strong fusion and sensor management performance and demonstrating a concept which has significant bandwidth, flexibility and cost advantages.

It is important to note that the demonstration scenario did not attempt to reproduce any particular operational application. Quantitative performance will be strongly linked to the metrics that are important in whatever application is chosen. For example there will be a closely coupled trade-off between Probability of detection (P(d)), False alarm rate (FAR) and timeliness of declaration for any specific scenario with specific targets. In future work, assessment of the performance of SAPIENT for specific applications will be evaluated against the required values for these metrics. Also the draft ICD (publically available at https://www.gov.uk/sapient/) will be reviewed for its applicability in other domains.

8. ACKNOWLEDGEMENTS

This work was supported by Innovate UK and the UK Ministry of Defence (Reference DSTL/CP94441).

REFERENCES

[1] "Human factors in CCTV control rooms: a best practice guide," Centre for the Protection of National Infrastructure (CPNI), January 2014, <https://www.cpni.gov.uk/documents/publications/2014/2014001-human_factors_cctv_control_rooms.pdf>.

[2] Nuechterlein, K. H., Parasuraman, R., Jiang, Q., "Visual sustained attention: image degradation produces rapid sensitivity decrement over time," Science, 220, 327-9 (1983).

[3] Keval, H., and M. A. Sasse., "Man or gorilla? Performance issues with CCTV technology in security control rooms." Proc. 16th World Congress on Ergonomics Conference, International Ergonomics Association, 10-14 (2006).

[4] Blasch, E. and Plano, S., "JDL Level 5 fusion model: user refinement issues and applications in group tracking," Proc. SPIE 4729, Aerosense, 270–279 (2002).

[5] "Automation in Military Operations", POST Note 0511, Houses of Parliament, Parliamentary Office of Science and Technology (October 2015).

[6] NIST Special Publication 1011-II-1.0, Autonomy Levels For Unmanned Systems (ALFUS) Framework Volume II: Framework Models, Version 1.0, Contributed by the Ad Hoc ALFUS Working Group Participants, Hui-Min Huang, Elena Messina, James Albus, Ph.D., December 2007

[7] Kundegorski, M. E., and Breckon, T. P., "A Photogrammetric Approach for Real-time 3D Localization and Tracking of Pedestrians in Monocular Infrared Imagery," Proc. SPIE Optics and Photonics for Counterterrorism, Crime Fighting and Defence, SPIE, 9253, 01, 1-16 (2014).

[8] Kundegorski, M. E., and Breckon, T. P., "Posture Estimation for Improved Photogrammetric Localization of Pedestrians in Monocular Infrared Imagery," Proc. SPIE Optics and Photonics for Counterterrorism, Crime Fighting and Defence, 9652, XI, 1-12 (2015).

[9] Dalal, N., Triggs, B., "Histograms of oriented gradients for human detection," Proc. 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005), 1, 886-893 (2005).