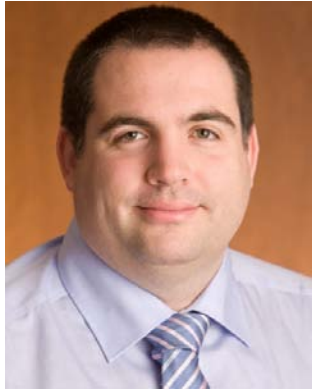


## ***iDIVA - enabling risk-based targeting of security measures***

*Following the SDSR's statement that "we must win the battle for information, as well as the battle on the ground", it is clear that a major challenge faced by security forces and counter-terrorism agencies is accessing, and making timely use of, relevant information.*



By Mark Fulbrook

Our airports are crowded with passengers inconvenienced by ever more stringent security processes, while airport and security personnel are under increased pressure to maintain passenger throughput. Although security checks are necessary, they are not always targeted at the greatest threats. The challenge is to identify potentially suspicious individuals for the security resources to focus on, while providing a smooth transit through the airport for trusted individuals.

There are numerous sources of data and intelligence that can be used to build up a picture of an individual, from the moment an airline ticket is booked through to when a passenger enters an airport and presents themselves at a security comb. Currently, however, this information is not exploited. As Marijn Ornstein, Manager of Security Policy at Schiphol Group has said, "If you look at all the recent terrorist incidents, the bombs were detected because of human intelligence not because of screening ... If even a fraction of what is spent on screening was invested in the intelligence services we would take a real step toward making air travel safer and more pleasant."<sup>1</sup>

**iDIVA (intelligence Data Integration, Visualisation & Analysis)** is a fast and effective tool for integrating disparate data sources, from multiple information owners, to provide actionable intelligence and shared situational awareness. By exploiting all available information and intelligence assets, iDIVA can perform threat analysis on individuals to generate 'trust scores', allowing risk-based targeting of security measures.

**If even a fraction of what is spent on screening was invested in the intelligence services we would take a real step toward making air travel safer and more pleasant.**

This paper discusses the potential of iDIVA to deliver a safer, more secure and efficient airport environment, using IPL's extensive experience of managing, exploiting and disseminating high-value information assets, built on a proven, in-service IPL product - **IP ANPR<sup>ii</sup>** (Intelligent Policing Automatic Number Plate Recognition).

### **IP ANPR background**

The IP ANPR system, which has been in operation since 2008, supports the tracking of vehicles and the identification of suspicious behaviour, when integrated with intelligence from local or national police and security forces.

Analysis of this data enables an intelligence-led approach to the prevention, detection and investigation of criminal and terrorist activity.

IP ANPR has already shown significant benefits to criminal investigations. In the first six months of use at Kent Police, IP ANPR significantly reduced the cost and time required for the collection, preparation and manipulation of crime detection data.

**Unlocking hidden value within data is a process which can take a great deal of effort with conventional investigation methods, but one for which intelligent IT software is ideally suited.<sup>iii</sup>**

### **iDIVA**

iDIVA's capability is based on a modular, configurable and extensible architecture that has already demonstrated operational benefits to end users in the policing domain. iDIVA is unconcerned about the what sources of intelligence are; its power depends on what data is available to it and the connections that can then be made.

### **Building trust scores**

Building detailed pictures of individuals helps to identify the most likely security threats. iDIVA will use all available intelligence and data assets to build trust scores.

The trust score generated by iDIVA is used to perform a threat analysis, resulting in a level of trust (or distrust) associated with an individual. This allows for more efficient targeting of security resources, meaning that the trusted individuals are able to pass through the airport with minimal interference and disruption.

There are several types of information that could currently be used to generate passenger trust scores.



These include booking details (e.g. payment type, destination), car park reservation details, passport details, individual records (criminal, intelligence and security), ANPR and check-in feedback ("Israelification").<sup>iv</sup>



"Israelification"  
- a system that  
protects life and limb  
without annoying you  
to death

### Incorporating situational awareness

iDIVA provides a situational awareness utility that can also be used to help target security resources. This is achieved through a centralised system capable of displaying alerts for events and alarms received from sensors. Data from both within the airport site and its surrounding area can be incorporated, as well as using the national ANPR data centre.

The design of iDIVA means that it can easily be enhanced to incorporate additional datasets including facial or object recognition from CCTV, sensors tracking movement through the airport (e.g. at doorways or escalators), mobile phone positioning and credit card transactions.

There is the potential to increase the level of information associated with individuals by gaining access to intelligence from different agencies and stakeholders.

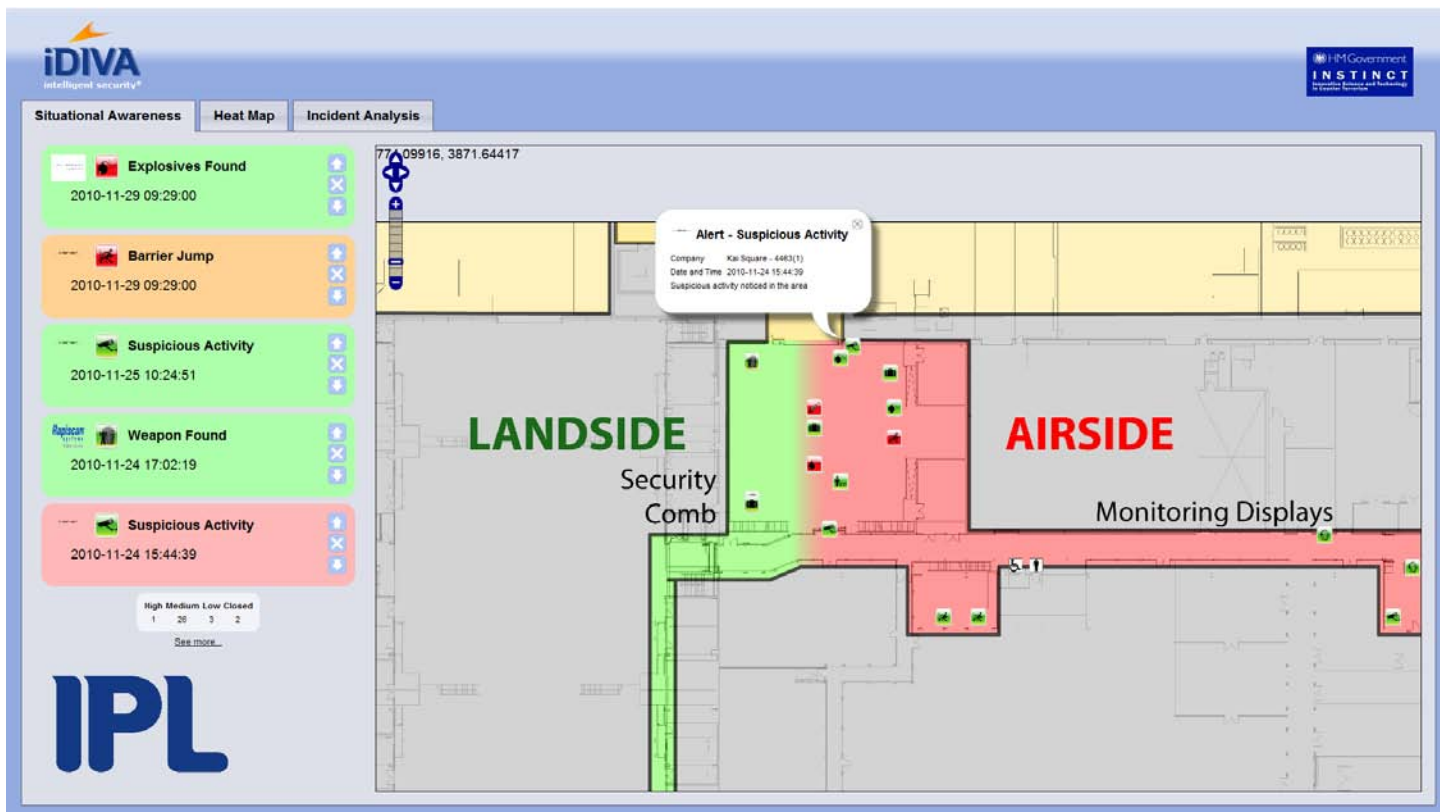
Examples of these include other airports, Customs, the Home Office, financial institutions, ground handling carriers and booking agents. Additionally, it may be possible to incorporate mobile phone records, data from the Police National Computer and previous travel history.

"In Israel, a coordinated intelligence gathering operation produces a constantly evolving series of threat analyses and vulnerability studies"  
  
Rafi Sela,  
Managing Partner at AR Challenges<sup>iv</sup>

Including or connecting to other intelligence databases, can help to identify anomalous or suspicious behaviour. This has the potential to push the security comb further out from the terminal, improving the chances of intercepting threats at a lower risk point in the travel cycle.

Integrating more numerous and varied data sources will result in a more complete picture of an individual, with a higher level of confidence in their calculated trust score.

Finally, the picture built up using iDIVA can be used as a tool for post-incident investigation and analysis. Alerting can be tied into mobile, TETRA and radio networks.

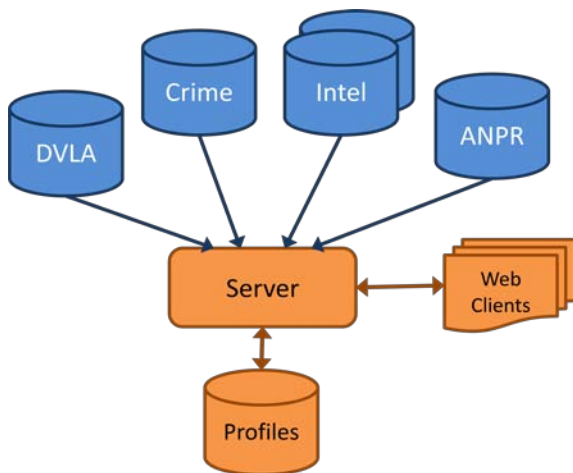


## The underlying technology

The IP ANPR product architecture, upon which iDIVA is based, is designed to access data from multiple database sources and automatically cross-reference this data to provide the best available combined picture.

IP ANPR has an extremely flexible plug-in architecture to ensure ease of connectivity to a wide range of external data sources.

The system is a thin client with a web browser user interface. The back-end server imports, stores and analyses subsets of data retrieved from third party databases. Access routines to the different databases are incorporated during the tailoring phase of system integration. The thin client is supported by a web server, with MapServer providing raster and vector map visualisation. This visualisation layer currently uses OS MasterMap data but can also use GoogleMap data, custom maps, satellite images, etc.



Having been designed in a modular, configurable and extensible manner, the software need not be tied to specific hardware, operating systems or browsers. This allows integration with other data sources, be they sensors or databases.

## Summary

With rising terrorist threats putting greater pressure on our security services, a shift in focus is needed to use intelligence rather than relying on screening alone.

There are already multiple sources of relevant data that exist, but they are disjointed, and without being able to correlate them real threats can be hard to interpret.

iDIVA exploits existing intelligence by integrating a wide range of disparate data sources from multiple stakeholders. It builds up a 'trust score' based on all available information, giving you a clearer picture of potential threats within your airport.

Built on proven technology from IPL, iDIVA is a fast and effective way for your staff to share actionable intelligence and situational awareness, enabling a more efficient security process to improve airport revenue, passenger satisfaction and everyone's security.

**iDIVA**  
**integrates disparate data sources**  
**performs threat analysis on individuals**  
**presents shared situational awareness**  
**provides actionable intelligence**



- i. The Register, 12/11/10, "Airport security boss calls time on tech", [http://www.theregister.co.uk/2010/11/12/airport\\_security\\_scanners/](http://www.theregister.co.uk/2010/11/12/airport_security_scanners/)
- ii. IPL Product Brief: Intelligent Policing (IP) ANPR <http://www.ipl.com/papers/IP%20ANPR%20product%20Obrief.pdf>
- iii. IPL Technology Feature, 12/02/2009, Intelligent policing with next generation ANPR <http://www.ipl.com/papers/Police%20Professional%20Case%20study.pdf>
- iv. Thestar.com, 30/12/09, "The 'Israelification' of airports: High security, little bother", <http://www.thestar.com/news/world/article/744199---israelification-high-security-little-bother>

## About IPL

IPL is a software development and systems integration company with particular expertise in securing, managing, exploiting and visualising high value information assets in business, mission, safety and security contexts.

Founded in 1979, with a turnover of around £30M, IPL is based in its wholly owned premises in the World Heritage City of Bath. We have approximately 280 technical staff, of which more than 90% are security cleared to SC level or above. We also have an additional pool of associates and an offshore partner.

Our track record in software and systems development is exceptional. Our proven development methodology allows us to cut through technical complexity, manage risk and completely focus on delivery. We consistently deliver reliable, efficient and accurate systems to a precise schedule.

Our services are distinguished by clear thinking and exceptional problem solving skills, enabling us to shape innovative and cost effective solutions that address real business needs.

Broadly these services comprise: Business Consulting, Technical Consulting, Solution Delivery and Managed Services (within each of which we offer many more narrowly targeted services):



**IPL's Business Consulting practice provides a range of services to help clients align people, processes and technology with corporate and business unit strategy. Critically, this also involves ensuring that the information acquired, managed and used within the organisation is genuinely treated as a valuable asset.**

**IPL's Technical Consulting practice translates business needs into practical, real-world technical architectures and detailed technical specifications. Getting this transformation right is critical to achieving a system that fulfils its expectations. Our value lies in two key strengths: our proven ability to operate comfortably in both business and technical domains; and our sheer technical depth.**

**For over 30 years, IPL's core business has been its solution delivery service; that is, the development and integration of robust, well engineered software solutions which fulfil our clients' business and technical requirements, supplied on time and within budget.**

**Although Solutions Delivery is a key focus for IPL, we do not stop there. We stay involved throughout the life of a system to ensure that it continues to meet the needs of the business and adapts to the inevitable changes that all enterprises experience.**

IPL is an approved defence contractor and our offices are accredited by the UK MOD for handling classified material. We are also a Microsoft Gold Partner, Investors in People recognised and ISO 9001:2008/TickIT (quality management), ISO 27001:2005 (security management) and ISO 14001:2004 (environmental management) certificated.

For more information on iDIVA or any of our other products and services, please contact:

01225 475000  
[defence@ipl.com](mailto:defence@ipl.com)

or visit [www.ipl.com](http://www.ipl.com)

© IPL Information Processing Limited