



## REAL TIME ALERTING SYSTEM

TODAY'S SENSOR NETWORKS CAN PRODUCE ENORMOUS AMOUNTS OF DATA THAT OVERWHELM USERS LOOKING FOR SPECIFIC PATTERNS.

/// FACT SHEET



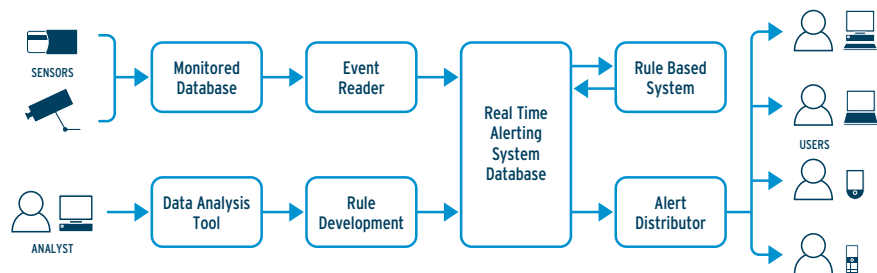
By the time the pattern is discovered, the window of opportunity to act has passed. EDS' Real Time Alerting System (RTAS) detects user-specified patterns in real time streams of data, and instantly alerts the users when a specified pattern has been detected. Therefore action can be taken during the window of opportunity.

### KEY FEATURES

- A Rule Based System (RBS) can run many rules concurrently
- Using a basic PC, a single RBS can process 150 million events each day
- An RBS will watch all incoming data and raise alerts continuously without user intervention
- The RBS can operate on one or more Windows Servers in parallel to provide further scalability
- Users create and maintain rules. There is no extra cost to add new rules, and no knowledge of the programming language is required
- The Rule Development System (RDS) and RBS are independent of the monitored and alerting systems

### Overview

The Real Time Alerting System (RTAS) looks for user-specified patterns in very large volumes of real-time data (millions of records per day) and then instantly sends alerts or makes updates to watch-lists. The RTAS implementation is independent of the system being monitored and the alerting mechanism. It can watch all incoming data and raise alerts continuously without user intervention.



### Your System

Let's assume that a monitored system already exists, such as a network of automated number plate readers, a Passport control system, or a card key system in a school. The system owner can use an analysis tool to discover interesting patterns in the data. These patterns may re-occur, but are generally difficult to detect in a rapidly changing set of real-time data. This is where the Real Time Alerting System solves the problem.

## PERFORMANCE AND SCALABILITY

The performance of the RBS depends on the processor speed and available memory on the host machine. A 2.60Ghz Pentium 4 with 512Mb of RAM running 17 rules handled 150 million events per day (approximately 1700 events per second being written to the system being monitored).

Raising an alert or updating a hotlist is normally achieved within 1 second of inception, although during peak periods this may increase slightly.

To improve scalability the RBS can be installed on multiple Windows hosts (Server 2003 or XP) so that RBS processes run rules in parallel.

## POINT OF CONTACT

For further information on EDS' RTAS solutions please contact:

Ian Brown  
Project Manager  
T: +44 (0)1256 742449  
M: +44 (0)7790 494239  
E: [ian.brown@edl.uk.eds.com](mailto:ian.brown@edl.uk.eds.com)

## Example Rule

The drug squad has identified a pattern of increased trading if at least 3 of a set of 12 suspect passports arrive in the country. They don't arrive on the same flight, nor does any given passport arrive on the same flight each month, and they use several ports of entry. The following rule is developed:

*'Tell me when the last of any three of the 12 suspect passports enters the country within 3 days of the first of the 12 passports arriving'.*

Such a rule is easy for the RTAS to monitor as it never goes off shift, and it can consume enormous amounts of data across a network. It will issue an alert via (e.g.) eMail, SMS or user specific mechanisms within 1 second of detecting the pattern of events.

## RTAS Business Process

Having established a pattern of interest, the user creates rules to match patterns in the incoming data using the Rule Development System (RDS). The Rule Based System (RBS) runs the rules against the live incoming data and raises alerts when rules are satisfied. Alerts can be created in any format required by the end-user and disseminated using whatever technology is available. The RTAS can also update watch-lists, subsequently used as part of the input for future events.

A single RBS process can run multiple rules concurrently, with no noticeable performance penalty. To further improve scalability the RTAS is designed so that multiple RBS processes can run concurrently on separate Windows computers.

## Possible Applications

The RTAS has been designed to be generic so that minimal changes are required to assimilate different data sources. Typical applications are:

- **Electronic Borders (e-borders):** Used in conjunction with a passport monitoring system, RTAS can be used as a component within an intelligence-led border control security framework to monitor people entering and leaving the country, and raise warnings and alerts where necessary.
- **Access Control Systems:** Monitor the movement of people and/or freight through controlled areas.
- **Internet Usage:** Monitor the sites people visit.
- **Financial Transactions:** Monitor the use of Credit and Debit Cards to detect fraudulent use.
- **Automatic Number Plate Recognition (ANPR):** Used in conjunction with an ANPR collection system RTAS can be used as a component of an intelligence gathering, protection or monitoring system.

### Contact

EDS Defence, 1-3 Bartley Wood Business Park  
Bartley Way, Hook, Hampshire RG27 9XA  
phone: +44 (0)1256 742000  
fax: +44 (0)1256 742612  
visit: [www.edsdefence.com](http://www.edsdefence.com)  
visit: [www.eds.com](http://www.eds.com)



EXPERTISE. ANSWERS. RESULTS.