genesys®

ism

Intergrated Security
Manufacturing Limited

Genesys – the power to integrate

A pioneer in integrated security management solutions

"Genesys from ISM has a unique architecture no other system comes close to."

In a world where nothing stands still, the market for integrated security management systems is one of the most active and exciting, and changing at an unprecedented rate.

The days when a disparate security system and a mobile patrol were enough to meet the security needs of an organisation are firmly in the past. Now we are more sophisticated, more technologically advanced, and security managers are rightly demanding significantly higher levels of functionality and integration across all systems.

Today, the industry needs reliable, flexible and powerful integrated management systems, with the highest levels of redundancy and performance. Ease of use and common handling of alarms is no longer desirable – it is essential, for there can be no margin for error in operating multiple systems.

Genesys from ISM has a unique architecture that no other system comes close to. At its heart is intuitive operation; it provides clear and concise information to an operator, every time. It is also scalable, with superior levels of redundancy, which is why Genesys is the leading choice for system integration management across the globe.

It is also a why ISM is deservedly recognised as a true pioneer in world-leading integrated security management solutions.

Stephen Smith
Managing Director ISM

Custody Facilities

Our technology

Genesys – A PSIM system and more, built around intuitive software

Genesys is more than 'just' a PSIM technology. It takes PSIM to another level. It is an Integrated Security Management System (ISMS) that integrates multiple systems from multiple manufacturers – presenting this as one holistic technology.
It means that every electronic security or fire safety device from CCTV to Public Address, and Fire Detectors to BMS – can be monitored and controlled from a single platform.

Most importantly, Genesys includes Migrating 3+™ technology, a patented automatic failover solution that adds higher levels of automatic configurable redundancy and system scalability than conventional PSIMs.

Control is effectively distributed across multiple dedicated workstations so that if one fails, control is migrated to a second workstation seamlessly, with no interruption or downtime. The system is therefore not restricted in its performance by the size or capability of a traditional server, nor does it require the added expense of moving to server farms or utilising clustering software.

Genesys is built around intuitive software that combines a range of industry-leading features and benefits including an enhanced graphical user experience using 3D modelling and a comprehensive event management database. Events and alarms are presented to the operator clearly as and when they happen using flexible cause-and-effect rules and escalation.

Unlike VMS or access control solutions that are centric to their prime function, Genesys ISMS is product agnostic – providing standardised control across all disciplines enhancing ease of use, delivering greater efficiency and offering enhanced ROI.

The ISMS software is totally scalable, from control of just a single building to multi-site, multi-country, Enterprise systems that can operate over local or wide area networks. Events can be transferred to any operating security control room on the network (either local or remote), by site, discipline, or alarm escalation, providing effective monitoring and high level management of any situation.

The ability to roll out a solution from a single site to Enterprise offers end users the ultimate flexibility to expand as their budgets and requirements dictate, or to close down sites or buildings on a temporary basis in an emergency.

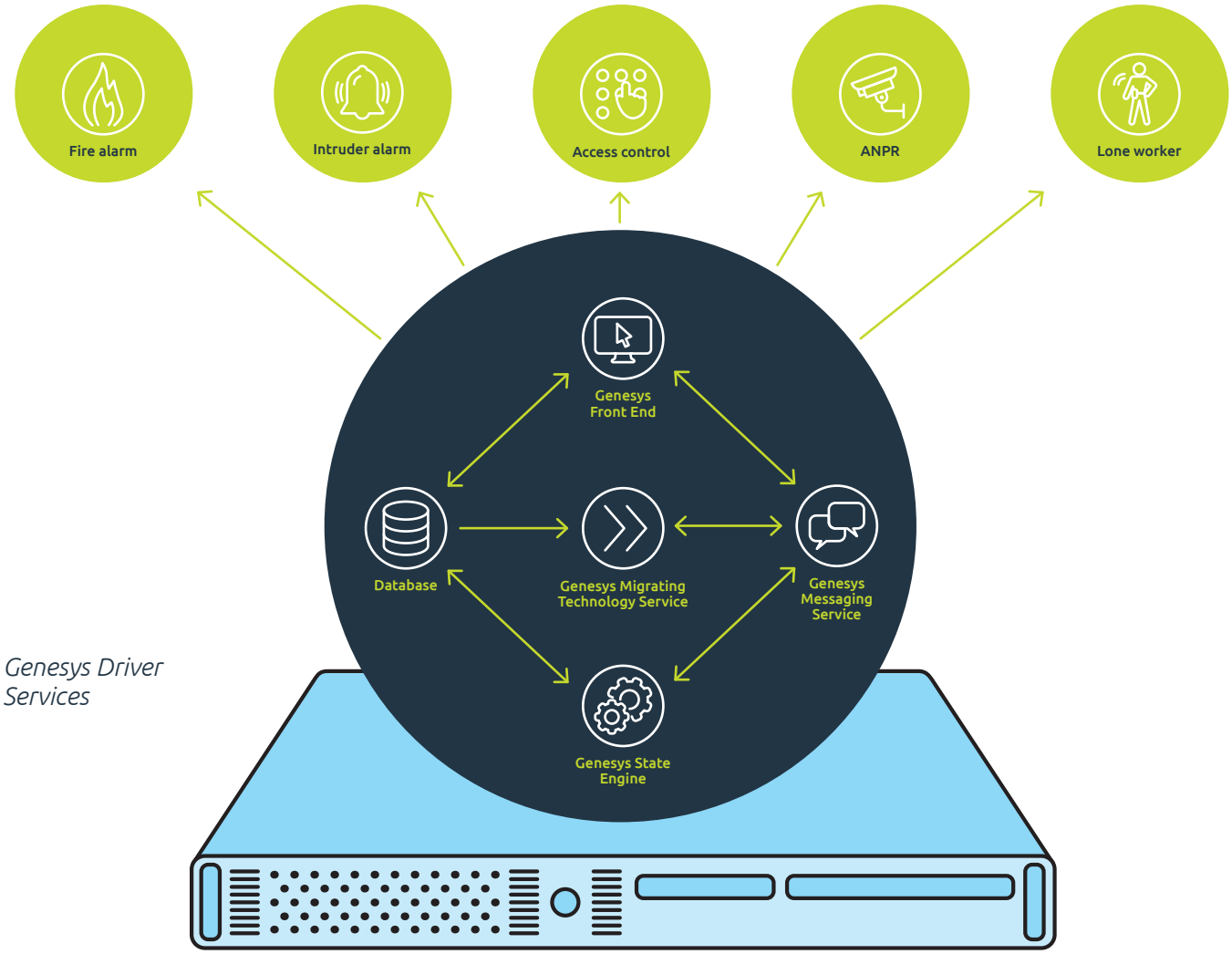
Guaranteed system support

All ISM systems are built to last. They require only the minimum of maintenance and are supported for a minimum of 10 years without the need for costly upgrades.

The trend in the PSIM market is to license software on an annual basis with typical costs of 18% per year and lifecycle of four years before a technology refresh is required. With ISM, this is not the case and there are no 'hidden' costs. The Genesys ISMS provides not only an excellent technical solution, but a truly competitive one especially when the whole lifecycle costs are taken into account.

Genesys has overall control of all electronic security systems installed at each site that includes but is not limited to:

- CCTV and Digital Recording
- Cell Call
- Electronic Locking
- Fire Detection
- Guard Tour
- Intercoms
- Intruder Alarms
- Panic/Affray Alarms
- Perimeter Intruder Detection
- Public Address
- Radio Paging
- Staff Safety Systems
- Trunked Radio
- Video Content Analytics
- Building Management Systems.



Genesys Driver Services

Genesys – a unique approach to systems architecture

Genesys has a unique system architecture, operating on a pier-to-pier principal rather than the old server client topology. This ensures that Genesys is a truly scalable, highly resilient platform. The system is made up of separated software engines for greater control and reliability.

The Genesys Front End

The Genesys Front End (sometimes referred to as a Graphical User Interface or GUI) is one of the engines. Being independent of the rest of the system it can reside on a PC to carry out control functions, or as a main load-carrying PC with driver control. This independence increases the stability of the system and allows it to be easily expanded.

System stability

Within Genesys, individual Driver instances are set up for each system connected within the Genesys Driver Service (GDS). This separation of Drivers is critical as it allows for the load of all the Drivers running to be spread across the system – thereby enabling the connection of a large number of Drivers.

The GDS monitors each Driver instance. If a Driver becomes unstable or fails due to poor third-party software, the GDS can close down the individual Driver (to ensure it does not cause an issue to any other part of the system) at the same time as generating an alarm. The GDS promotes the ability to migrate individual Drivers to other computers in the event of a PC or network failure.

By employing a separate engine, it is possible to run these Drivers on dedicated PCs (or servers if preferred). Genesys incorporates a status engine and an SQL server database. This means that the software remembers the state of all devices, alarms and the current alarm progress of alarm checklists. If an alarm has been accepted on a PC and the PC fails before the alarm has been reset, then the alarm will be sent to the network again.

The state engine

As connected devices change state (some simply from ‘Off’ to ‘On’ or others having multiple states including tamper, fault, door open, insecure, pre-alarm) then the Genesys State Engine (GSE) receives these states and sends a message to update the

icons shown within the Genesys Front End. This provides near real-time status of all devices. This engine also monitors the status of the Genesys computers on the network, what alarms have been acknowledged, and how many actions on the alarm task list have been completed. This keeps each one of the Genesys computers fully up-to-date. If a PC failure or engine fault should occur the other users are made aware that a user is off-line.

Top level encryption

All messages are sent via the Genesys Messaging Service (GMS) between the Genesys engines and services using Transport Layer Security Cryptographic Protocol. The Genesys Migrating Technology Service details the Driver migration and all actions on the system are stored within a SQL server database. When communicating between computers across the network, Genesys employs 256-bit Advanced Encryption Service (AES). This protects information up to the highest security level.

Multiple language communication

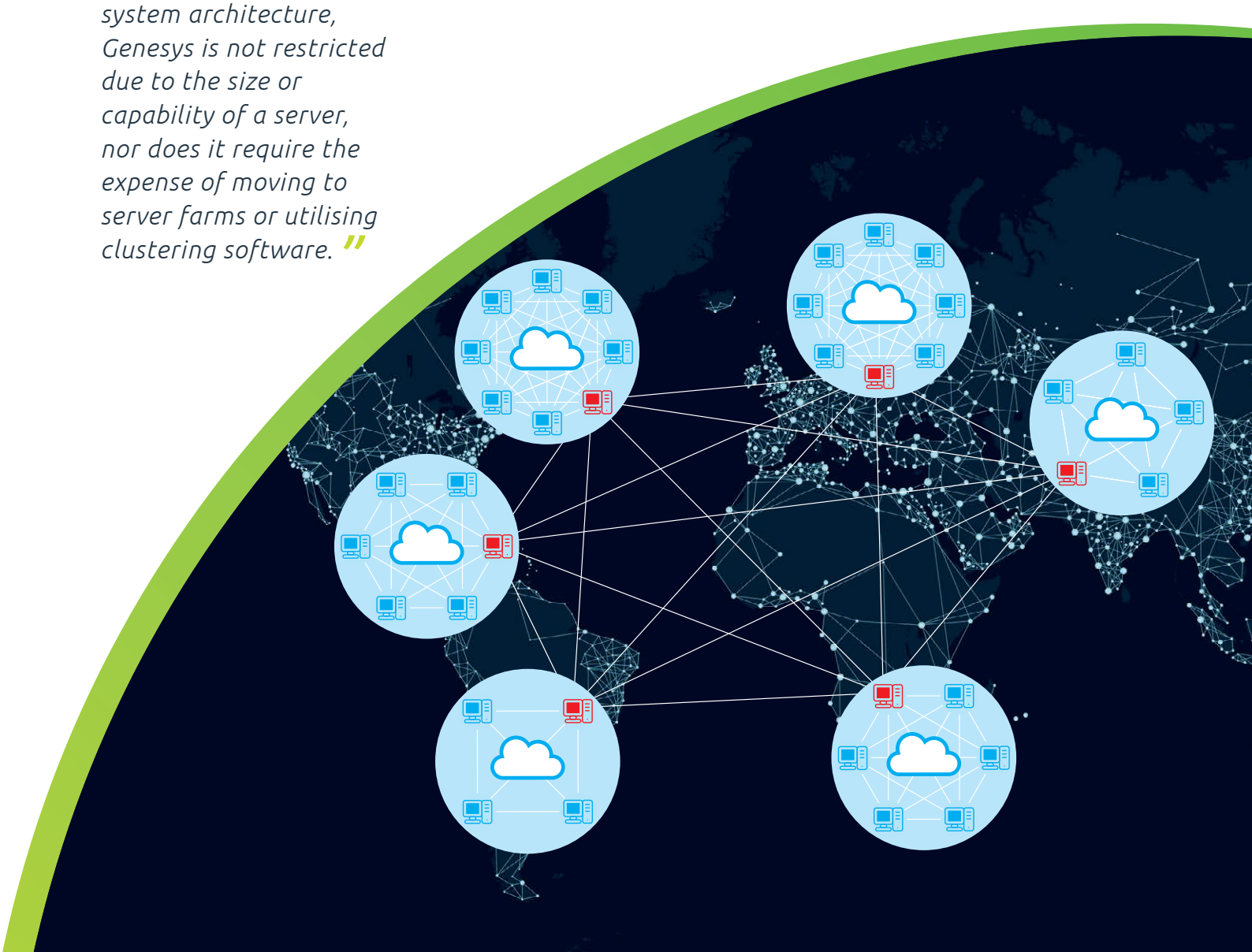
Genesys supports multiple languages, something which is achieved by using a translation database, or databases. When an operator logs on, the correct language is displayed.

Unlimited capabilities

Because of its pioneering system architecture, Genesys is not restricted by the size or capability of a server, nor does it require the expense of moving to server farms or utilising clustering software. Genesys also adds higher levels of automatic configurable redundancy and power, and ensures continued connectivity to all systems at all times.

"Because of its pioneering system architecture, Genesys is not restricted due to the size or capability of a server, nor does it require the expense of moving to server farms or utilising clustering software."

Enterprise Clusters



Uses and applications

Genesys is proven across a broad range of industries and clients including:

- Banks and Financial institutions
- Custodial and Law Enforcement
- Healthcare and Mental Health Units
- Universities, schools and Public Sector buildings
- High security control rooms
- Airports
- Critical infrastructure
- Museums and art galleries
- Oil and gas
- VIP residences.

"The alarm escalation can be triggered automatically from cause and effect rules that are set up in the system configuration."

Scale up to Enterprise level

Genesys offers a completely scalable model from single user/single site to Enterprise version covering multiple control rooms and multiple sites across a country or even across continents.

With its unique architecture, Genesys understands and resolves problems associated with the increasing geographical scope of clients, corporations, governments and institutions while adhering to a multi-tiered hierarchy (or 'federated' system) where total control is centralised, but allows individual sites to maintain local control. This is central for the further development of our industry.

By utilising the pier-to-pier architecture, the absolute reliance on a centralised system is negated as each site can operate automatously in the event of a Wide Area Network (WAN) failure and then re-connect to area or global command centre(s) on restoration of the WAN.

This architecture allows for live, hot redundancy, so if a control room needs to be evacuated operators can just walk into the reserve operation centre without the loss of alarms or functionality and continue to operate immediately. When planning operational control, this element is a vital area where compromise no longer needs to be accepted.

Advanced Alarm Handling

High Security Buildings

Enhanced alarm handling that is easy to operate

Clear and concise alarm management is pivotal for any security management system and to this end Genesys offers a comprehensive event management database.

Events and alarms are presented to the operator concisely along with standard operating procedures, and automated and manual workflow options, that guide the operators through each event. As all events are handled in the same generic way, training is simplified and the efficiency and effectiveness of operators are greatly improved.

Genesys provides enhanced alarm handling incorporating multiple automated actions that can occur due to events being generated or by an operator's actions. Examples of when these actions are triggered are:

1. On receipt of an alarm event
2. When the operator accepts the alarm
3. If the device changes state
4. When the system automatically escalates the alarm
5. When an operator manually escalates an event or alarm
6. When the event is reset

For example, if a PIDS (Perimeter Intrusion Detection System) alarm is triggered Genesys can immediately:

- Increase the frame recording rate and quality on the CCTV system
- Page security staff
- Lock down perimeter doors on the Access Control System
- Switch on perimeter lighting
- Display the alarm event to the operator(s)

When the operator 'accepts' the alarm, they are presented with the live CCTV images together with the pre-and post-event video recording from the time the alarm was generated.

The alarm task list is displayed detailing a workflow for the operator to follow.

The workflow list can detail basic functions for audit purposes such as 'check the CCTV', 'call the supervisor'.

By selecting one of these actions Genesys will carry out the automated function and the item will be checked off the list, enabling the operator to proceed to the next item.

It is possible to add events to the workflow list such as 'lock down doors' or 'add a note to the alarm event'. It is possible to configure Genesys to only allow the alarm to be reset once a note has been added, or when the alarm has been cleared on the hardware, etc.

Once the event has been cleared and the operator has reset the alarm, the system will automatically revert back to a default position for example:

- Sending cameras to their home positions
- Switching the monitors to default view
- Returning the CCTV to normal record state
- Switching off floodlights
- Normalising doors
- Paging staff.

Typical Three Screen Display

Genesys – Key features and benefits

Highly configurable. Most changes can be implemented simply by updating the configuration rather than applying in code.

Enhanced functionality reduces costs.

Alarms can be set to specific users or workstations and can be prioritised.

Alarms can be easily identified and responded to appropriately because of the different alarm sounds and alert/border colours configurable per alarm event.

Emergency Procedures with alarm tick-lists.

Alarm escalation rules and manual activation.

Enhanced graphical user experience and animation from utilising the latest Microsoft technologies i.e. .NET platform and Windows Presentation Foundation (WPF).

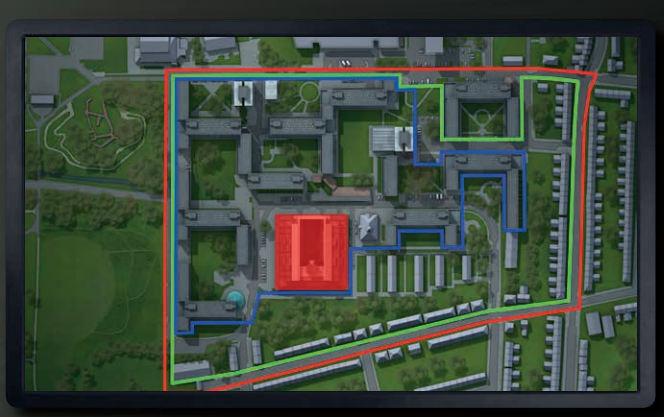
Ease of navigation from the Map control panel in 2D or 3D mode.

Patented Migrating 3+™ Technology: Each Driver can run on any networked PC with its own sequence of migration PCs in the event of failure; Distributed Drivers enable the communication load to be spread across all networked PCs so there is no reliance upon one PC for all communications; because a front-end is not required for the Driver to run, Drivers can run on non-operator PCs. If large numbers of Drivers are required additional PCs can be added to handle the load; each Driver runs in isolation from the front-end and from other system components. A Driver failure will have no effect on the functioning of the rest of the system; Drivers will continue working even when the front-end is not running. When the front-end starts up, any alarms that were activated whilst it was not running will be displayed and any changes to device states (for example doors opening and closing) will be shown.

Multiple monitor support: The front-end can be configured to span across multiple monitors (this is naturally dependent on the capabilities of hardware); different layouts for the Genesys 'panels' (map, video, alarms, control, etc.) can be configured. Layouts can be changed depending on user preference and via Action Lists; advanced Action List system – define powerful and complex cause and effect rules; execute any command on any device; define camera tours; create highly configurable guard tours and cell watches.

Configurable task lists with custom Standard Operating Procedures (SOP) for accepting alarms: uses the Action List system; perform a series of automatic commands; prompt for user input to make alarm notes; alarm can only be reset once tick-list is complete.

New Alarm Window and Alarm Ownership system: dedicated alarm list window shows all alarms, or a filtered selection of alarms; alarms grouped by Accepted, Active and Accepted by Other User. All alarms accepted by the operator are grouped at the top of the list and unaccepted alarms are grouped below; alarms accepted by other users are grouped at the bottom; accepted alarms are allocated to the user and become unavailable to other users. The accepting user's progress through the alarm's reset tick-list is remembered enabling them to return to the alarm later.



Cell Call

The user can also log on to a different workstation to continue processing the alarm; accepted alarms can be escalated causing them to be allocated to a higher-level user and changing the tick-list items, if required; accepted alarms can be un-accepted, allowing another user to continue processing the alarm.

New Multi-State Device Icons: Devices are defined by the state attributed to them. For example, a door device could have a 'Position' state and a 'Locked' state; each value for each state can have a map icon associated with it. A door position's state value of 'Open' can also display a different icon to when it is 'Closed'. Overlaid on top of that will be the icon for the current 'Is Locked' state – an icon for either 'True' or 'False'; the default configuration for the states that have icons and the states that don't is provided by the Driver. However, the user can change any of the defaults and can allocate icons to any state values or remove them.

New State Triggers feature: A trigger can be configured to activate when a device state changes to a particular value. When activated the trigger will run an Action List; the Driver provides full details on the default configuration for its triggers (mainly used to activate alarms). However, it is fully configurable by the user and any actions can be taken when the status of the devices change; a selection of other, more general triggers are also available. For example, an Action List can be run when any of the following activity is selected on the system: Icon Clicked, Menu Shown/Hidden, Module Button Clicked, and Layout Changes.

Critical infrastructure

Genesys – systems, displays and reporting

Mimic Panel Display

Genesys can configure the system to have mimic panel displays. This allows for alarms within a building or zone to be highlighted on an overview map.
In seconds, managers and supervisors can gain a complete overview of the alarm status of the system. What is more, operators are made aware of other activities occurring across the entire system. Initially developed for the prison service to replace conventional line drawn maps with lamp illumination, mimic panels are now utilised in many control rooms as standard. They significantly enhance 'situational awareness.'

Video wall capability

The ability to display video images from different CCTV or VMS manufacturers is an essential element of control room design. Genesys can deliver video walls displaying multiple cameras from differing manufacturers of VMS solutions in different locations onto one holistic monitor wall solution.

System log

Genesys has a full system log. This file records the actions of the system detailing the operator, the action and any automated actions plus any responses to alarms that have been recorded by the operator. This log has a search facility and is capable of producing basic level reports. If a more advanced analysis of the logs is required, then the database can be exported and interrogated by any ODBC program such as ACCESS and Crystal Reports

Case Study

Every Government Department is continually looking to deliver better value for money without impacting services. This is especially true of security, where Departments also need to be assured that the solutions provided do not increase risk.

The brief was to provide central control of a number of high-security sites from a single control room rather than the 'traditional' single control rooms per building approach. To achieve this the Department in question required a solution that was architecturally robust with high levels of system redundancy, and yet was still easy to use by Police Officers and staff who would be responsible for it.

The answer was Genesys, whose patented architecture provided the stability and robust redundancy that made the solution viable for such high-security establishments. Genesys created a platform that not only offers high levels of functionality and power but also unrivalled operational ease.

Lifecycle costs – a big issue in the PSIM market today – was also critical, and was another factor in choosing ISM as we provide support for our Genesys platform for a minimum 10-year period.

Airport

VIP residence

Genesys – from a world-leader in ISMS technologies

ISM is a global pioneer in integrated security management solutions and the UK's leading developer of integrated security management, intercom and cell call systems.

Established in 1989 and today operating from our extensive manufacturing and design facility in Sussex, our global client base encompasses many of the world's most prominent institutions and includes central and local government, critical national infrastructure, healthcare establishments, education campuses, shopping centres, financial institutions and law enforcement agencies.

Our Genesys platform enables the integration of many types and make of equipment including CCTV virtual matrix and digital video recorders, access control systems, fire alarms, intruder alarms, audio matrix, intercoms, public address and paging systems – all from one holistic security management system.

Our investment in R&D

ISM ensures that at least 12.5% of our annual turnover is invested in research and development, undertaken by our dedicated on-site R&D team. Running alongside this tangible commitment is an ongoing dialogue with clients. Only by fully understanding the changing needs of our clients at a granular level can we design, deliver and implement pioneering systems. With the increasing threat from terrorism, the organisations that approach us are looking for a global solution to their security needs; one that can be implemented locally, that is scalable and, crucially, that is easy to use.

"Increased security risks, and threat levels, including heightened risk from Terrorism."

Genesys, a unique patent-protected technology, is the culmination of our internationally-recognised ability to design systems that deliver security management solutions globally. Each of our products is designed, developed and manufactured in-house and supported by a system design team for pre-sales design support. We also have a dedicated project management department to ensure the successful delivery and technical support after-care.

Delivering in all sectors

Increased security risks, and threat levels, including heightened risk from Terrorism.

Working with a world-class technology provider.

Please contact us to discuss your security requirements, request further information or arrange a full system demonstration.

Intergrated Security Manufacturing Limited

25-29 The Bell Centre
Newton Road
Crawley, West Sussex
RH10 9FZ
England

Tel: +44(0) 1293 529990
Email: info@ism-uk.com

ism-uk.com

Intergrated Security
Manufacturing Limited