

Automation in incident management - Security.



Glossary

Scene - Your paper-based risk Matrix or Plan. Merlin can have unlimited "scenes"; and they can interact. Find out more.

Profile - This is Merlin's API; it allows you to set a paper plan to code. Merlin will follow this and make intelligent decisions affecting your risk pathway.

Trigger - Something that invokes a profile. For example, a sensor, human interaction, or an external warning Merlin is monitoring. Find out more.

Response - Interaction with engineers, staff, public or a response agency. Remote control of intelligent devices to control all aspects of a building or process. Find out more.

Computer Intelligence - Is achieved through intelligent control by machine learning, using statistically-driven robots and rules association predictive modelling working with the profile. Find out more.

Statistical Intelligence - This provides meaningful dashboard visualisation, rules association to create the visuals, and reporting of customer KPIs through real-time events, historical analysis, and reactive, predictive modelling (adding some to the profile). Find out more.

IVR - Interactive Voice Response.

Resolution - The conclusion of an incident. Used to quantify and provide historical analysis and as a way of improving the "profile".

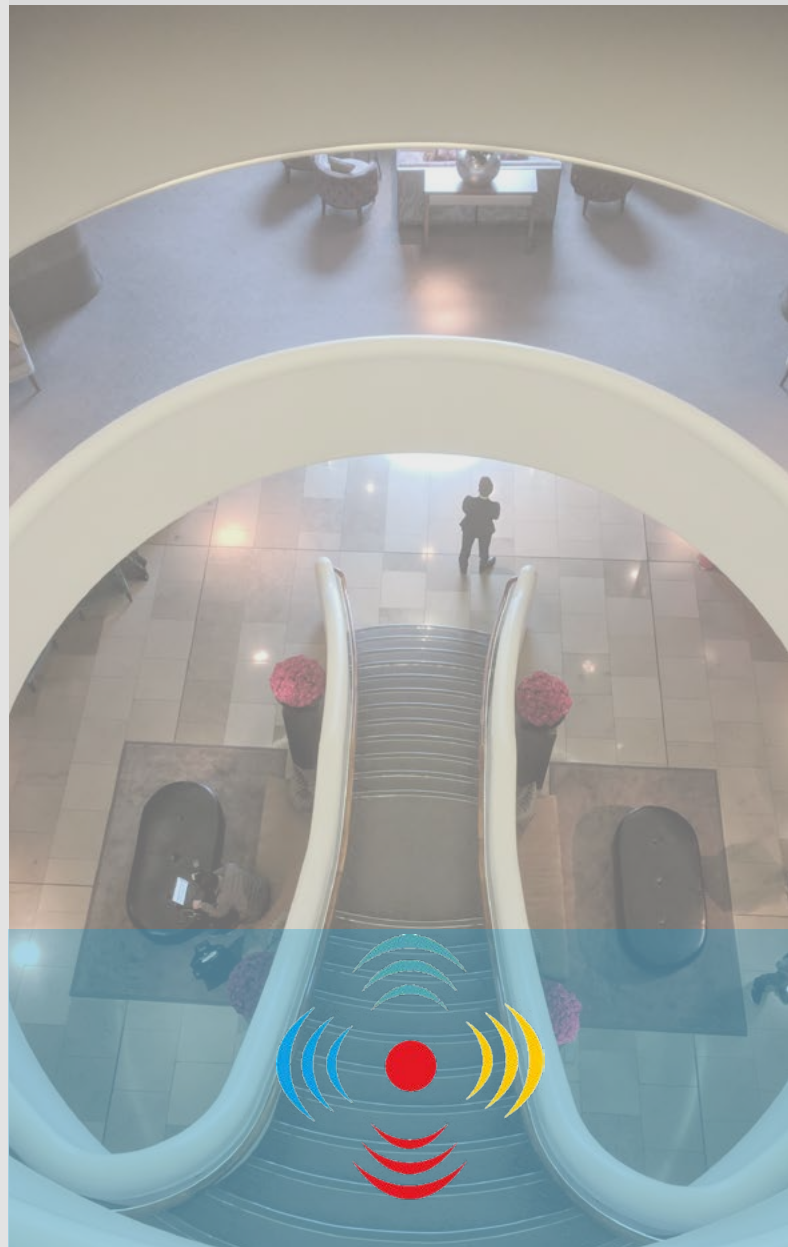
Automation in Security.

Intruder Alarms are a necessary part of everyday life. However, they have an inherent cost way above their monetary value. They are costly to manage when Police Response is required; they are costly for Police - the numbers of false alarms continues to be high - and the insurance industry considers them a deterrent rather than a protection.

Humans have managed the signals from these devices for nearly one hundred years. Initially, a call from an intruder alarm informed the monitoring centre that a warning had triggered.

A new set of standards were produced in 1995 by the US SIA. These standards introduced serial communication of sensors installed in a property. However, due to the necessity for increased human interaction, the SIA standard was not widely supported by security companies in its intended form. Customers would not pay the additional charge for the additional workplace resource, and the monitoring stations did not want the complexity and more opportunity to make mistakes.

The answer has taken almost thirty years. Robotics has reached a stage where monitoring centres can process intruder alarm (and virtually every other alert from any source) automatically. These robots can perform many of the tasks that a human can provide with the added benefit of access to historical data. Machine learning technology and live statistical analysis are now a reality.





Introduction

For more than sixty years, the protection provided by an intruder alarm has been under the control of a human operator. Calls queued in sequence and passed to a response (Police) by telephone.

More recently, automated message passing to the responder has allowed time-saving in the third part of the messaging triangle. However, control room personnel still have to call for additional assistance and follow the incident manually to a conclusion to, at the very least, get the proper resolution to the original call to the Police.

It is all a very costly workforce problem and one that, given the pressures on decreasing margins that the industry faces, must be improved.

Initsys working with specialised algorithm supplier Polaris Telemetry Ltd has built a robotic incident processing system that will allow the complete, truly automated control room.

Merlin "Neon" edition uses a combination of rules engines, state engines, statistical intelligence and computer intelligence, coupled to apps and smart telephony to replace the human operator.

Tests on Intruder, Personal Attack, and VSaaS (Video Surveillance as a Service) indicates that over 90% of incidents can be completely automated using our technology. That would equate to an estimated 60% saving on workforce costs, a significant time-saving in incident processing (a typical alarm would be in the hands of the Police in somewhat less than one second after receipt at the monitoring station). In the case of CCTV biased Video Verification, it gives an almost foolproof security system at a cost that cannot currently be matched at any monitoring station, no matter how small a profit margin they can afford to work.

Testing carried out on real-world scenarios indicates that few incidents require any form of human intervention, and resolution of those that do are within seconds. The ability to have a core of exceptional operations personnel whilst the drudgery of incident processing offloads to our robots means customers have a better experience.

Merlin Neon Edition can outperform a human doing the same job.



History

Initsys Merlin had had an artificial intelligence element since 2017. MerlinAi used an adaptive threat management algorithm to look at each signal in real-time, do a live SQL (a not inconsequential feat) and adapt the rules engine to each threat as it appeared.

This algorithm now builds a live threat profile and forms the Initsys Robot building technology used in NMRE.



- [Primary Approaches.](#)

Intsys Merlin Neon edition uses an advanced Rules Engine known internally as the NMRE (New Merlin Rules Engine). NMRE is more than a simple rules-based processor; it is a programming API capable of processing events and risk management (converting risks templates), Facilities Management (the edges between Security and FM are already blurry) and GSOC applications.

The NMRE uses sub-functions, telephony, mapping (GIS), apps and algorithms to make decisions, all leading to our "Make No Mistake" philosophy, a crucial part of Intsys Mission Statement.

Described by a risk advisor as a sub-field of Artificial Intelligence, NMRE provides a direct link between raw programs and a real-world application.

Merlin Neon Edition is, we believe, quite simply the most advanced processor for security monitoring stations.

- [Supervised Learning.](#)

The NMRE provides a method of categorising incidents and the pathway using input variables and an output target. Achieving Supervised Learning by looking at the type of signal received coupled to additional input such as Machine Learning applied to CCTV signals.

Classification in this context, as real/not real or true/false.

- [Unsupervised Learning.](#)

Using data in a live mode without any prediction of sequencing is more complex; here, information is arriving sequentially, and the NMRE uses its intelligence to increase the threat level from the data it is receiving. It will constantly look at all data streams from a geographic location to calculate the chances of the threat being real or false. Clustering is one indicator of a genuine threat.

NMRE uses Unsupervised Learning to create a supervised category specific to the location to which it applies once a resolution is applied. This technique is known as Adaptive Learning or Self-Supervised learning.

Note:: In the world of Electronic Security, the information is required ideally as a direct live feed from an intruder alarm, achieved by altering the signalling technology.

- [Self Taught Learning.](#)

The NMRE can also adapt to Self Taught Learning, where objects are placed accurately on a map. This intelligence is applied to labelled and unlabelled data either arriving sequentially or as part of a Supervised Learning session.

- [Multi-Tasking Learning.](#)

NMRE will apply its algorithms and alter its profile dependent on the return from any of the Learning algorithms. Of course, it will also increase threat based on the results of interaction with other electronic subsystems.

- [Adversarial Learning.](#)

The NMRE will learn adversarial models as they appear and as they relate to false alarms as described in the resolution stage. In such a way that attempts to surreptitiously manipulate the input data to create a false negative (non-false false alarm) should be detected at any stage. This detection, of course, is one advantage of a machine-based learning process as a human cannot possibly retain information relating to historical events or, indeed, the nature and features of a protected property.

- [Response.](#)

Once an event is categorised, there is a handoff to the despatch manager part of the NMRE. The despatch manager is known as MAA.

The MAA will select the required response and its decision tree based on a traditional rules engine.

Support for both inbound and outbound telephony with near-instant identification and direction of inbound call routing avoids call queuing for situations where "alarm for closure", for example.

IVR is the most convenient tool for this application. However, options exist for email, SMS, and other messaging applications and RSVP, Echo, and various other communication systems based on modern security protocols.

MAA will monitor in real-time the responders and their performance. The design of the "responder" app for non-agency personnel provides real-time location information and attendance recording, and various other specific features. It is available for IOS and Android operating systems.

MAA will update active responders of any change in the threat- for example; an alarm panel reset with a correct keycode or access rights.

- [Resolution.](#)

The resolution to an incident is a critical indicator for future events, and good association is essential. There is no difference here to human action; the proper closure is necessary for either human-based or machine-based monitoring systems.

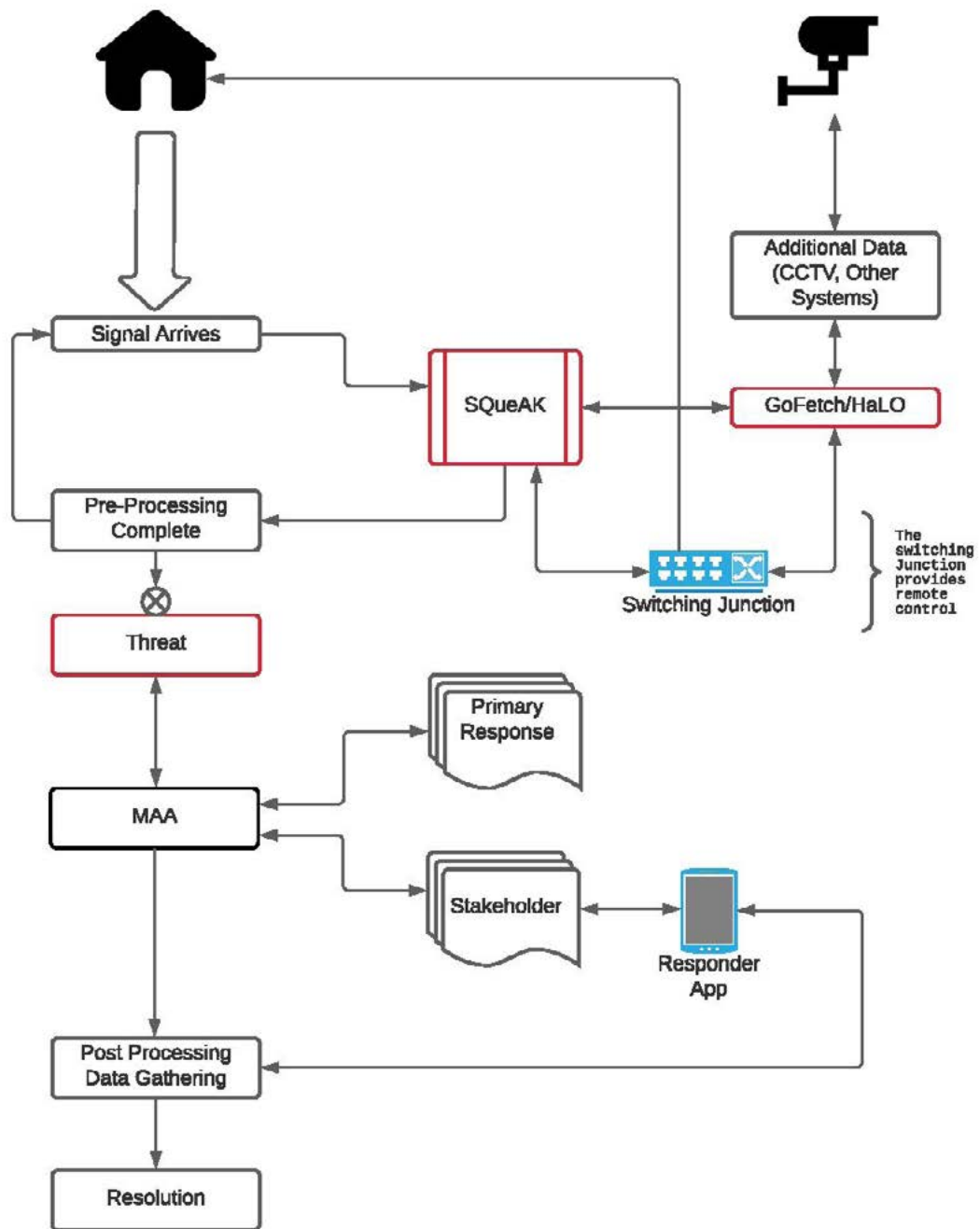
- [Robots.](#)

The following Robots are currently in use in the NMRE.

HaLO - Halt and Look Once, a deep learning algorithm. See separate paper. HaLO examines images either received in small JPG format from CCTV systems or uses the full-frame recovery system iGoLive.

Threat - Threat-(Manager) is a statistical robot that builds an image of "what is happening" at a protected property so that the NMRE can react accordingly and advise response of the state of the incident.

SQueAK - A live SQL robot building live SQL for reaction/check.



The Intruder Alarm Profile demonstrates the capability of the NMRE



www.initsys.net

0845 3301 445

20 - 22 Wenlock Road, London, N1 7GU