Automation in Incident Management -
FM.

INiTSYS

Automation in Incident Management - FM.

Facilities Management in this century revolves around a ticketing system that allows the creation and monitoring of purchases, faults and breakages and tracking the repair or supply process. However, this ticketing system, coupled with some other process monitoring regular maintenance, such as that used for air conditioning, given the threat of legionnaires disease, is time-consuming and workforce-dependent.

Mistakes are often and complaints many. It is, after all, a tedious and often repetitive job, with little liaison with the suppliers and engineers tasked with undertaking the work.

Let's take a simple incident - a leaking tap.

It isn't in isolation a considerable risk. It's a leaking tap, after all. But let's look at the process for getting it repaired, assuming that you don't have the expertise on-site, or indeed do, but the team is busy - or not.

First, you have to raise a ticket, and this goes to the help desk, who research the person responsible for fixing that leak. They then submit a works order (often manually), and there is some interaction with the company.

After the works order, the help desk will ask the company responsible for the repair for an estimated restoration time (return to normality or RTN); this should be within the contract terms.

Then the repair is done, sometimes within the contract terms and sometimes not; who knows and cares? The helpdesk often don't; it is, after all, just a tedious job.

After the repair, you have the task of paying for it. And that in itself is another process that demands attention; however, more often than not, this side of the process has some form of automation.

But what if you could automate the whole process?; this is what the New Merlin Rules Engine can do. By reporting the fault through an app, the NMRE can despatch and monitor the repair process automatically whilst bringing advantages.

- Monitor the RTN in line with the contracted term.
- Escalate the problem if not fixed within the contracted terms.
- Automatically invoke contract penalties.
- Monitor the incident/device and pick up any device-related issues and report on them (is this a faulty tap design or has the location an overpressure on the mains supply).
- These are simply examples, but the NMRE can automatically handle nearly all forms of incidents, saving time and money and enabling your helpdesk workforce to focus on those issues that need that human touch.

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".
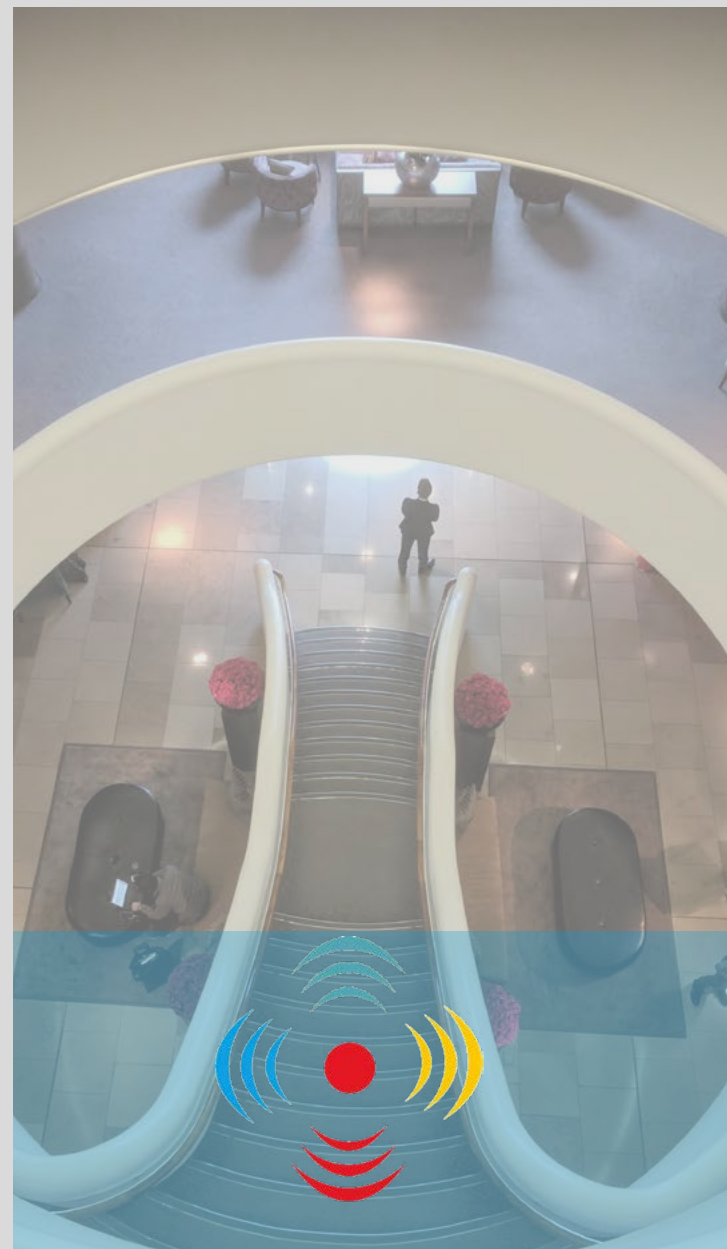
Introduction

One of the last bastions of Facilities Management is the help desk. Unfortunately, they are often staffed by many people handling faults and issues related to business, sometimes with significant risk attached.

People make mistakes.

Sometimes costly mistakes. The Opportunity to make this more automatic, with user-friendly apps as well as links to asset databases, is here.

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

The New Merlin Rules engine (NMRE) uses a combination of rules engines, state engines, statistical intelligence, computer intelligence (machine learning) to allow the robotic helpdesk to be a reality.

Tests on all sorts of incidents, from the leaking tap to recovery after a fire, have shown that Merlin Neon Edition can manage many of today's FM issues entirely automatically. Our robots call and track responders in the same way they have for a long time in the security industry - let's face it, a plumber is just as critical as a Policeman in the correct context.

Once we build the rule, it can be enhanced and improved as required.

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.

The Technology

- **Primary Approaches.**

Initsys 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 Initsys 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.
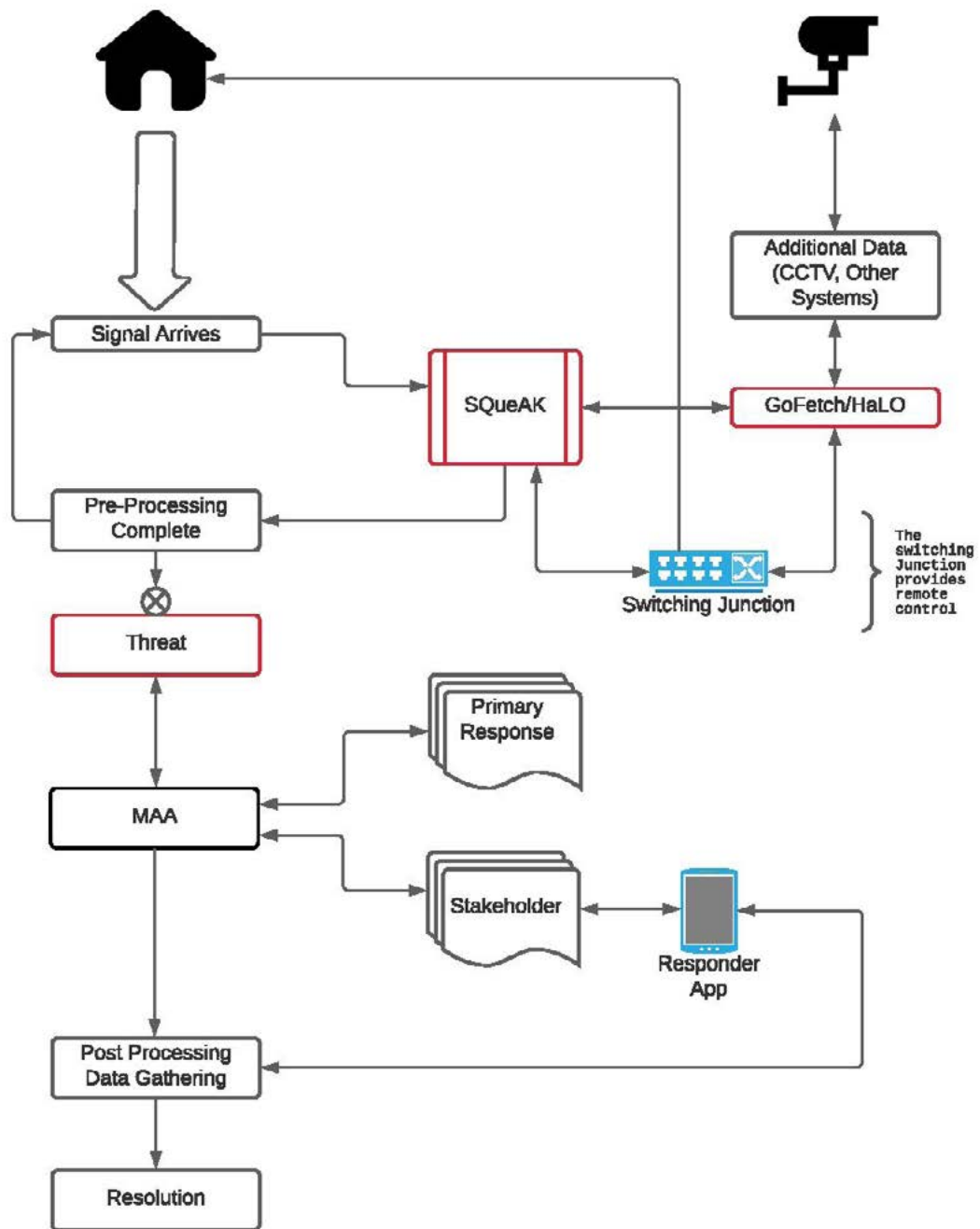
The Intruder Alarm Profile demonstrates the capability of the NMRE