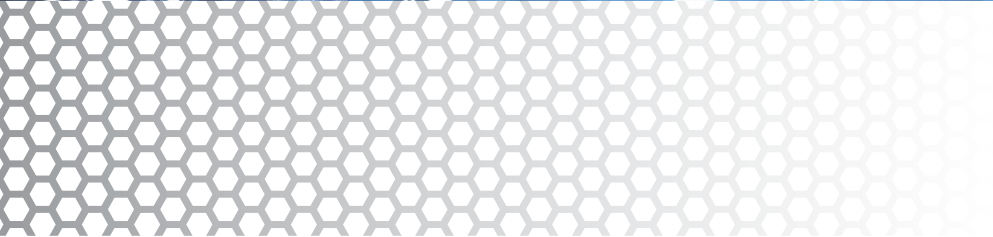


Surveillance as a Communications Center

Integration Enables Smart Site Management



Introduction

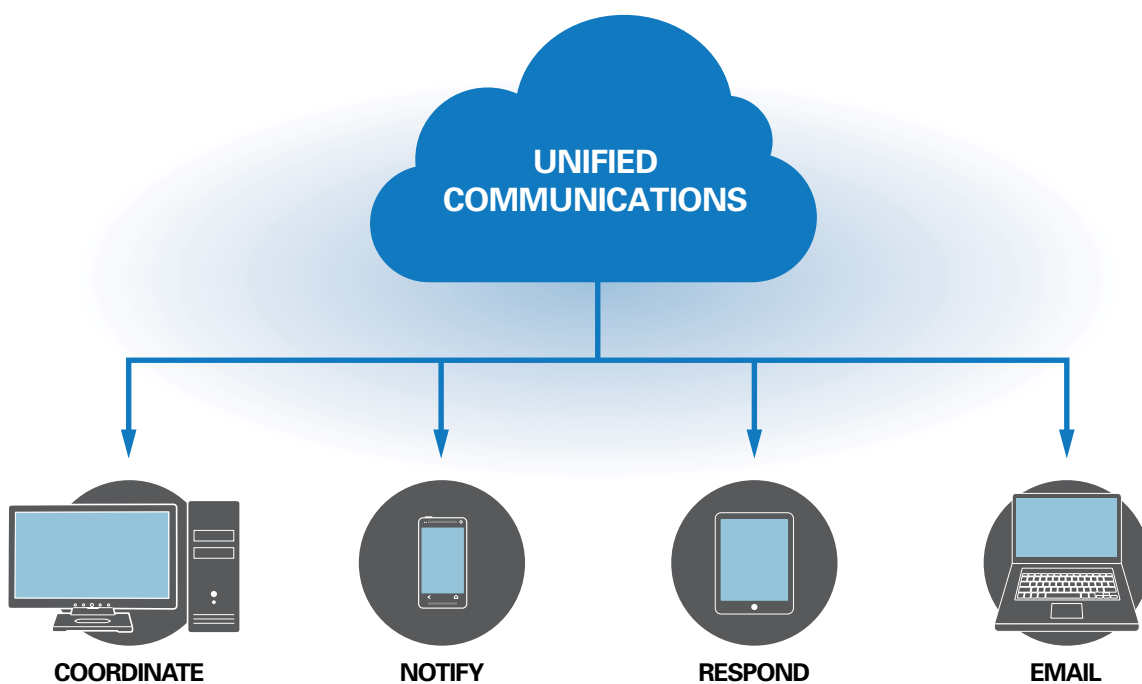
Strategic communications and security go hand-in-hand – a well-planned communications infrastructure can greatly enhance the scope and efficiency of a site’s security mechanisms and processes. It’s the reason that ‘Unified Communications’ has gained so much traction as a concept in recent times.

The term, as the name suggests, refers to the integration of both real-time and non-real-time communications services exchanged via a network. Voice services (including IP telephony), IM, web conferencing (audio and visual), email, SMS, and web-desks (desktops shared via an internet connection); using Session Initiation Protocol (SIP) these communication mediums can all be brought together.

Imagine what could be achieved if Unified Communications could then

be paired with data from other site systems – such as process monitoring, surveillance, threat detection, and access control – and managed in a single environment.

This white paper explores that opportunity in greater depth by looking at the practical requirements and operational benefits of integrating Unified Communications via surveillance command and control technology, particularly in terms of aiding critical decision processes and incident response management.



What is Session Initiation Protocol (SIP)?

With any discussion around Unified Communications, it is first important to understand Session Initiation Protocol (SIP). SIP is a standard open protocol that allows multiple devices to communicate with each other over a shared network. It effectively defines and structures message initiation, transmission, and endpoints. The most common application is for internet telephony or Voice over IP (VoIP) – Skype is perhaps the most well-known example of this.

In addition to facilitating communication, SIP enables redirection services ensuring that physical location is no longer a restriction. Transmissions can be initiated and received from any networked location without losing the

ability to identify the initiating device and, if applicable, its user. This is particularly beneficial in worker safety scenarios – a point addressed in greater detail within this white paper.

VoIP is just one example of SIP-driven communication. With SIP, **any IP-connected devices** – for example tablets, laptops, public address systems, help points, or intercoms – that can receive and transmit audio, numerical, video, or voice data, can ‘talk’ over the network.

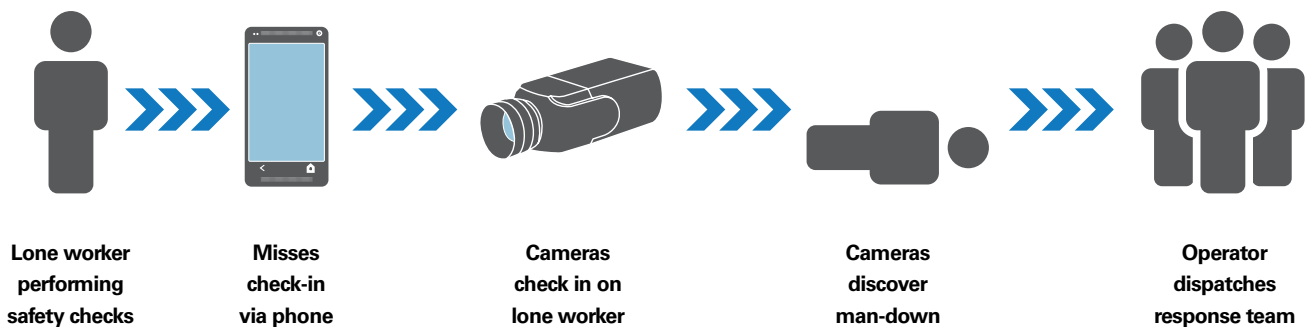
Integrating these vital communication tools, alongside other site systems via a surveillance command and control solution, opens up a powerful set of opportunities.

VoIP through an open integration platform delivers superior communication, improving response times and procedures.



Surveillance Command and Control: The Switchboard of the Future

The best way to demonstrate the effectiveness of adopting this approach to communications is to look at practical examples — real-world scenarios.



STAFF SAFETY – THE LONE WORKER SCENARIO

A lone worker is completing safety checks at various locations on an industrial plant. To complete the task takes several hours and involves inspecting remote areas on site.

Every 20 minutes, they press a button on their mobile. This is programmed to be recognized by the surveillance command and control platform. If the button is not pressed after a certain period of time has elapsed, an alert automatically flags up on the surveillance team’s monitors. Locating

the worker’s edge device, live feeds from the nearest cameras are automatically prioritized on-screen in order to visually verify the safety of the worker.

Footage shows the worker is on the ground and not moving. A ‘man-down’ voice command is routed to the nearest SIP devices to alert support teams located closest to the worker. This also triggers a workflow to guide the surveillance team through further ‘man-down’ protocols.

What this example shows:

Combining communications, visual data, and workflow management delivers a safety resource particularly valuable to organizations operating remote, hazardous, or multi-location sites.

**Unified Communication –
delivered anytime, anywhere,
on any IP device.**



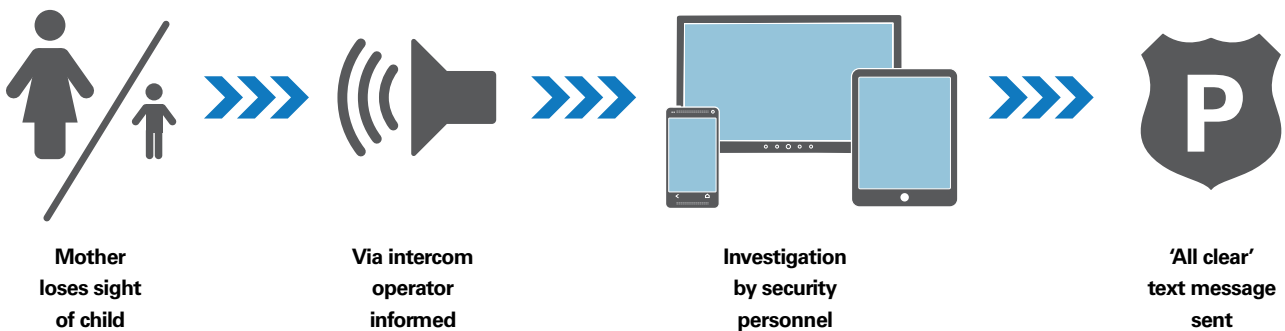
THREAT ANALYSIS – THE INCIDENT INVESTIGATION SCENARIO

A ‘virtual perimeter’ has been established surrounding a large data center, one of several managed from a central location. An intruder detection alarm is triggered, which sets off an automated workflow instructing operatives at the central control center to deploy security personnel to investigate the incident further.

On inspecting the area identified by the intruder detection system, a security operative sees no issues. He sends an ‘all clear’ text message via his phone that feeds back into the command and control platform. This text message automatically resets the intruder detection system, updates a centralized audit trail with confirmation ‘alert investigated’, and notifies the control center team that there is no threat.

What this example shows:

An integrated approach to communications using a command and control platform can enable a single text message to be ‘understood’ and logged/forwarded to multiple settings as required.



PUBLIC ASSISTANCE – THE HELP POINT SCENARIO

At a busy train station, a mother loses sight of her four-year-old child and cannot find him anywhere. She sees a help point, presses the intercom button, and tells the control room operator that she cannot locate her son. The operator takes a description, types this into a message on his terminal, and tags it ‘missing child’. The command and control platform uses the tag to generate multiple actions.

An alert appears on the device screens of the wider surveillance team notifying them of search parameters, a notification is issued to devices held by Transport Police Officers identified as being on site, and an automated text alert appears on electronic public noticeboards around the station.

What this example shows:

A singular point of contact with the public – in this case a help point – can be used to update and involve multiple agencies/individuals quickly in a time-critical scenario.

Looking Beyond the Misconceptions

With so many potential benefits to integrating communications via a unifying command and control platform, why is this a trend yet to gain significant momentum? To answer this, it is useful to look at some common misconceptions.

Cost

New technology often comes with a price tag, prompting many to believe – particularly those with larger, legacy telephony systems in place – that introducing SIP-enabled communications will be expensive.

This is not the case, and in fact it can actually save organizations money. Most organizations considering this option will already have an IP network. A small investment in SIP-enabled Private Branch Exchange (PBX) systems will enable organizations to utilize this resource and avoid both the cost and inflexibility of a separate telephone system with a third-party carrier.

By then integrating telephony, along with messaging and a wide range of additional communication data transmissions, via a central surveillance command and control platform, further efficiencies in terms of resource demands can be achieved.

Hardware Restrictions

A concern linked to cost is that in adopting an integrated IP communications structure, organizations will find themselves restricted to specific hardware and software providers (and their associated fees).

Once again, this is a misconception. Industry standardization and open APIs ensure those adopting IP-based communications benefit from system/device interoperability. Using an open platform command and control solution to converge voice, video, audio, and data communications does not restrict end-users to specific vendors. This safeguards effective buying strategies by allowing organizations to select communications solutions and edge-devices that suit their specific needs, rather than forcing them to purchase specific proprietary technology.

Size

Only large organizations will benefit from integrating communications via a networked command and control platform. A common belief, but a false one. In fact, one of the biggest benefits of adopting this approach to communications is that it is highly scalable. Facilitating and managing communications using an IP-based solution permits end-users of any size to boost or reduce their system to match the organic growth of their business.

Security

Protecting data is a priority for any organization – particularly for those critical to a country's economic or operational infrastructure. Just as a consumer may be wary of communicating their bank details online because of potential hacks or security breaches, so an organization may fear integrating their communications over a networked solution.

In truth, however, hacking is not a key threat. The level of data encryption now available - particularly when using a central command and control platform to manage data - means unauthorized access to communications transmissions is highly improbable.

A more significant threat to security and operations is data loss. An IP-based solution is reliant on network resiliency.

Being aware of this threat is the key to overcoming the hurdle. Organizations looking to network their communications and integrate them with other vital site systems using a surveillance command and control platform, can work with their solution provider to ensure the right level of resiliency and failover is in place.

The Future of Integrated Communications

While integrating communications into a single IP-based command and control environment is not yet widespread, its broader adoption is inevitable – particularly as edge device technology advances within industrial/business settings.

At present, deployments are primarily to be found in CNI, public space, and transport settings, but the range of clear benefits is likely to see gradual penetration into business enterprise, oil & gas, and high-security commercial markets.

With financial, operational, and resource efficiencies achievable, the ‘surveillance communication center’ is a concept certain to attract a great deal of attention in the near future.

For more information about Synectics technology solutions, visit our website: synecticsglobal.com.





Synectics designs integrated end-to-end surveillance control systems for the world's most demanding security environments. We excel at complex projects that require innovative, tailored solutions with high reliability and flexibility, specifically for casinos, oil and gas, marine, public space, banking, transport and critical infrastructure applications.

With over 30 years of high security systems experience, field proven products, and expert support personnel in the UK, US, Europe, UAE and Asia Pacific, Synectics offers its clients turnkey networked solutions for comprehensive protection and peace of mind.

Synectics' Systems division is part of Synectics plc, a global leader in advanced surveillance, security and integration technologies and services.

Synectics

sales@synecticsglobal.com

synecticsglobal.com



Americas Asia Europe Middle East United Kingdom

Specifications subject to change. E & OE.
Literature Reference: SIP-WP/0119/A4 Iss 4