WHITE PAPER

Communications management within your security platform

Genetec™

genetec.com

Executive Summary

In the physical security and public safety industry, communications management systems, such as intercom solutions, are becoming an integral part of developing effective and comprehensive security strategies. This white paper highlights the importance of a standards-based approach to communications, explains the benefits of intercom integration with physical security systems, and outlines key features to look for in a security system when planning to unify communications with access control or video surveillance in a single security platform.

Introduction

Traditionally, communications management systems were viewed as separate and independent solutions from access control (ACS), video surveillance, and intrusion when designing a security solution. That said, the focus in the industry over the past decade has been on allowing end users to integrate or, ideally, to unify these systems into a single security platform.

Currently, there is an increasing demand from end users to unify audio/voice communications together with access control and/or video within a single security platform for both live operations and investigations. Some of the more traditional approaches to integration include:

- Dedicated wiring between an intercom system and an ACS system where the push-to-talk (PTT) function of the intercom station triggers an input on an ACS module, which, in turn, triggers an event in the ACS monitoring interface,
- Dedicated wiring between an intercom system and a video system where the PTT function triggers an input on a video camera or IP encoder, which then triggers an event in the video monitoring interface or live video viewing, or
- Integration through a proprietary protocol that integrates the video or ACS system with the intercom system server using a proprietary Software Development Kit (SDK) or Application Programming Interface (API).

A more recent approach involves leveraging an industry-standard or open protocol like Session Initiated Protocol (SIP) to enable the integration. This approach avoids the use of proprietary intercom manufacturer protocols and allows end users to select, according to their needs, best-of-breed communications and intercom equipment that leverage such standards.

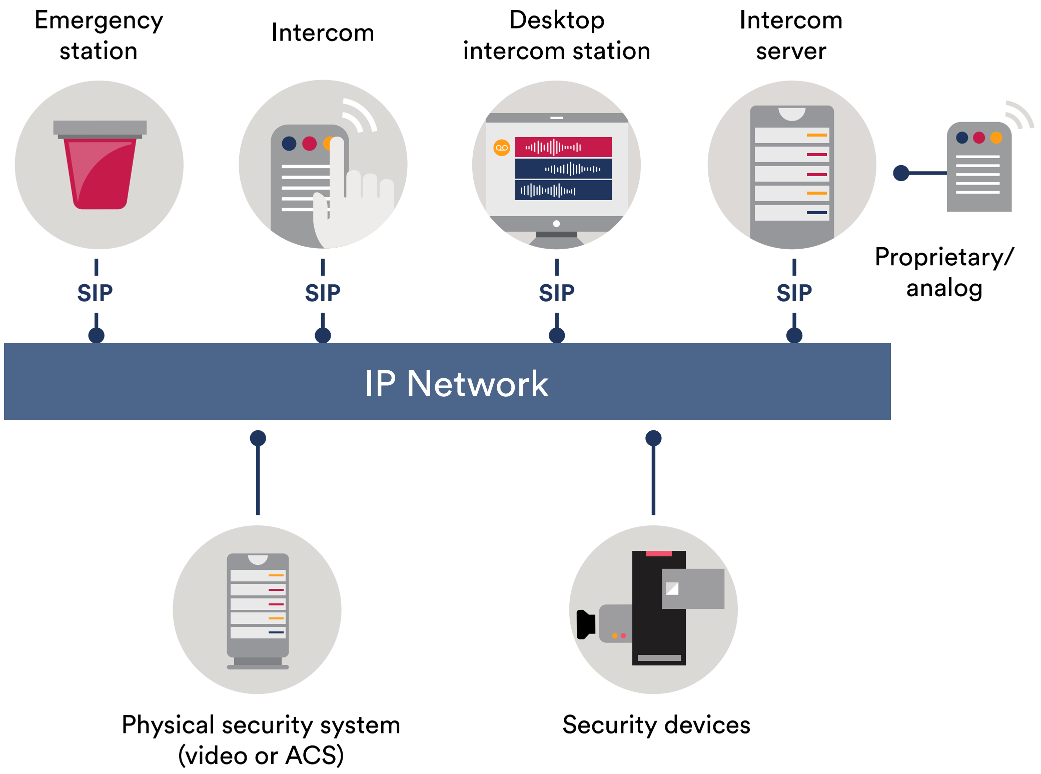
In addition to presenting an overview of intercom management systems, this white paper considers the benefits of intercom integration and explains the importance of a standards-based approach to communications, especially as it applies in the context of security. It also outlines key features to look for in a security system when an organization is planning to unify communications with various security systems.

1. Overview of Intercom Systems

Intercom technology refers to a stand-alone voice communications system mounted permanently in buildings that functions separately from the telephone network. Generally used as a security or safety feature, intercom systems are typically composed of the following components:

- **Master Station**—the primary operator interface component that can control the entire intercom system. Also referred to as a desktop station, this unit can initiate calls to, and receive calls from, any and all other stations, deactivate or mute a specific station, and make announcements over the whole intercom infrastructure.
- **Intercom Server**—the hardware server that is the command and control center of the intercom system. Also known as an intercom exchange server, it provides central administration of the intercoms and master stations in the system and links together devices during a call request through the application of routing and priority rules. Many intercom servers can communicate with both IP-based and analog door stations. Some intercom servers offer interfaces to, or are integrated by, thrid-party systems.
- **Intercom Terminals**—usually fitted with a microphone and designed with a talk button and a power switch. Some terminals are also equipped with a keypad to allow for dialing specifically numbered intercom terminals. There are different types of intercom terminals:
  - › **the door station**, which can only initiate a call with a Master Station but not with any other station,
  - › **the intercom station**, which is capable of initiating and receiving party-line conversations, individual conversations, and signaling and which may be rack-mounted, wall-mounted, or portable,
  - › **the wall-mounted station**, which is a fixed-position intercom station with built-in loudspeaker that may feature a flush-mounted microphone, hand-held PPT microphone, or telephone-style handset.

Traditional intercom systems were composed almost entirely of analog electronic components that were connected together to transmit voice signals. As technology evolved, intercom systems based on digital connections were introduced, offering users new features and interfacing options. Some digital intercom systems can carry both voice and video signals and are composed of dedicated proprietary door stations, a dedicated intercom server that controls the entire system and connects the operator with the individual stations, as well as separate cabling for all stations.



2. Intercom system trends

Two of the main trends driving the intercom industry include (1) a move towards IP-based technology and (2) the need for greater systems integration with security systems.

1. IP-based Technology

The first trend is a growing shift from analog to IP-based technology. Through the use of an organization's existing IP network, communications systems, including intercom systems, can now be operated using far less cabling because of extended bandwidth and other IT advancements.

IP-ready intercom solutions have the capability to use the existing IP infrastructure for communications purposes, thereby significantly lowering Total Cost of Ownership (TCO) by reducing the amount of wiring required and eliminating the need for proprietary wiring. The shift to IP-based technology is also allowing organizations to take advantage of technological advancements in intercom hardware, including intercom or door stations with integrated video cameras and communications session recording.

2. Systems Integration

Integration between communications and physical security systems, including ACS and video surveillance, is the second major trend. Rather than working with separate and independent intercom and physical security solutions, integration allows an organization to manage its communications needs together with its access control and video surveillance systems from a single user application. Such systems integration significantly increases situational awareness and ensures that personnel have a clear picture of their security environment before deciding to act.

With doors, parking gates, and cameras linked to intercom devices, the effectiveness of a security team is enhanced in several ways:

- by using real-time video feeds to view a situation in order to effectively respond to and manage incoming calls, including emergency calls,
- by using video cameras and ACS information to validate the identity of a caller prior to allowing access, such as access requests when employees lose their cards or when visitors arrive on site,
- by enhancing investigations through the replay of recorded call sessions and associated video when reviewing historical events

In addition, integration between communications and physical security systems also means that operators can initiate calls with other users and coordinate activities, such as when responding to a routine call or preparing a response to an emergency situation.

3. Three approaches to systems integration

Currently, there are three main approaches to integration:

1. Wired inputs and relays between intercom systems and the ACS or video surveillance system
2. Using the intercom system manufacturer's API
3. Unification through Standards-based Communication (SIP)

1. Wired inputs and relays between intercom systems and ACS or video surveillance

The more traditional approach to integration between intercom and physical security systems is realized through wiring between systems. For example, if a user would like to trigger video viewing (streaming) or recording when a door station PTT button is pressed, dedicated wiring between a door station and video hardware must be installed. Using this method of integration, the PTT function at the door station triggers an input on an IP camera or IP video encoder, which then triggers an event in the video monitoring interface and starts live camera streaming or recording.

2. Using a Manufacturer's API

As networking technology has evolved and organizations have migrated to IP technology for all of their business needs, vendors have begun to look for more efficient approaches to integrating communications with physical security systems. Many intercom systems manufacturers have developed APIs or SDKs that security vendors can use to develop software-based connectivity between systems over an IP network.

This method of integration eliminates the need for wiring altogether because the intercom system and ACS or video system are connected using a software link over an organization's IP network . However, these APIs and SDKs are developed by individual vendors and are proprietary in nature; as a result, because they vary from vendor to vendor, each system would require a new integration for every vendor. Additionally, compatibility issues can arise when the software of either the intercom system or the physical security system is upgraded and the backward compatibility of the software integration is no longer supported.

3. Unification through Standards-based Communication (SIP)

SIP is a signaling communications protocol that functions by defining the messages that are sent between endpoints, messages that govern the establishment, termination, and other essential elements of a call. SIP can be used for creating, modifying, and terminating sessions consisting of one or several media streams and can be used for two-party (unicast) or multi-party (multicast) sessions.

Newer intercom solutions are now supporting industry-standard protocols and technologies for Voice over IP (VoIP), such as SIP, that allow an organization to easily leverage their existing infrastructure, including its IP network, VoIP infrastructure, and SIP-based devices and apps, for all of their communications needs. In this approach to integration, the software link leverages non-proprietary communications protocols, making it possible for organizations to

- unify their communications and physical security systems in a single platform,
- access a greater selection of standards-based intercom devices,
- avoid the use of proprietary intercom manufacturer-specific protocols.

Used to control the delivery of voice communications and multimedia sessions over IP networks, communications protocols like SIP are at the heart of standards-based telecom technologies. In order to deliver real-time voice and video data, SIP uses the network instead of dedicated telephone lines or proprietary cabling. And, since SIP is widely supported, organizations can easily standardize their communications system and protect their investment in intercom and communication technology.

4. Benefits of unification using standards-based communications

Standardization and interoperability are the two main benefits of unification using standards-based intercom technologies. While the network carries the information, SIP makes it possible for devices to communicate with each other, allowing for seamless communication between operators and intercom devices deployed throughout an organization.

Industry-standard protocols are also essential for ensuring interoperability between different vendors, different devices within a communications system, and between communications and security systems. For example, standards-based intercom integration allows an organization to use its existing network infrastructure and manage video surveillance and full-duplex communication through the Video Management System (VMS) without a dedicated intercom server. Because the intercom system uses an industry-standard protocol like SIP, an intercom unit could be made to behave just like any other camera on the network. In many cases, an integration may not even be required if both the intercom system and the physical security system are SIP-ready.

In addition, the level of interoperability offered by standards-based communications also

- helps to protect the long-term viability of an organization's investment in communications technologies since devices and systems that use industry-standard communication protocols are non-proprietary,
- allows for integration with standards-based devices at a much deeper level, meaning that an organization could upgrade to advanced voice management features independent of 3rd parties,
- reduces an organization's TCO,
- allows an organization to select components from multiple vendors and makes it easy to incorporate those components into its existing system without any additional work,
- makes it possible for an organization to future-proof its communications system because these standards facilitate the seamless integration of the latest technologies, thereby ensuring that the communications system grows along with the needs of the organization,
- allows an organization to unify its intercom system with other business systems, including the phone system, since all SIP-enabled communications devices are compatible with an organization's IP-PBX phone system,
- leads to other new capabilities, such as being able to integrate SIP mobile apps into an organization's security communications strategy.

A unified security and communications system takes it one step further and would also allow an organization to easily address any of the following security applications:

- **Emergency Call Management**

  By leveraging the unification of emergency call stations with the video surveillance system, an organization can better manage emergency calls and more effectively secure a single building or ensure the safety of a town center. A unified security and communication system would allow personnel to answer incoming emergency calls, view live video while responding, and take the right action to address situations as they arise with visual information on hand.

- **Parking Entrance Control**

  Unification would also make it possible for an organization that controls access to parking or to a car park entrance either through access control readers or license plate recognition cameras to exercise greater entrance control. With a unified system, security personnel can respond to incoming requests for assistance and then manually open parking gates from a single unified security application.

- **Employee Lost Card and Other Requests at the Door**

  Unification would also streamline how operators respond to employee lost card requests. Because intercom call stations are linked to access-controlled doors and video cameras, operators can accept incoming calls, confirm caller identity through live video and their cardholder profile, and grant access quickly from a single unified security application.

- **High Security Environments**

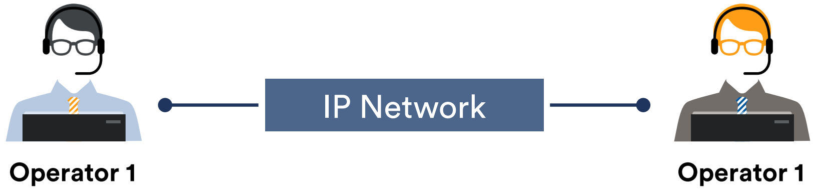
  A unified approach further allows an organization to add another layer of security to their operations by adding intercom communications within a high security environment. Through intercom system integration, operators would be able to grant or deny access to highly secure rooms or areas by validating audio, video, and access control information at the same time.

5. Innovative forms of communication user-to-user video calls

In the context of operator and security team communications, real-time user-to-user calling through the security platform itself can offer significant benefits within a comprehensive security strategy. By allowing operators to communicate with their colleagues both through voice and video over an IP network using a standard off-the-shelf USB headset, microphone, and webcam, an organization will ultimately promote greater collaboration and more efficient communications when responding to security events or during day-to-day activities.

Other benefits include

- intuitive communication because it is embedded in the security system application,
- operators do not have to learn how to use an external 3rd party communications software in order to make user-to-user video calls,
- reduced TCO through the use of inexpensive communications equipment.



Native user-to-user audio and video calls within a security system

6. What to look for in a security system when intercom integration is needed

A successful unification strategy is largely dependent on selecting both the right security platform and a standards-based intercom system. When looking to unify intercom with physical security systems, an organization should choose a non-proprietary off-the-shelf integration over a custom solution because a non-proprietary solution would make it easier to expand and modify the system architecture in the future.

Developed Ecosystem of Partners

It is important to ensure that the security solutions manufacturer or vendor has a developed ecosystem of partners. Choosing a vendor with multiple intercom technology partners gives end users the freedom to choose the intercom solution that best meets their needs or to mix and match hardware from various intercom vendors. Settling on a security solution with a single integration limits the flexibility of an organization in the long run.

User Interface and Overall System Architecture

The user interface and overall architecture of the security system is also a key consideration. For a more efficient operator experience, organizations should look for security solutions that offer embedded intercom control and call management from the same user interface as the one used for access control and video surveillance activities.

It is also important to choose a system with an architecture that supports a standards-based approach to communications management. A security system with native SIP support would allow an organization to reduce TCO by leveraging its IP network for communications and security, and avoid additional proprietary cabling altogether. Since SIP-enabled communications devices are compatible with many IP-based phone systems, choosing a SIP-ready security system may also allow for greater unification between an organization's business and security systems and may also provide access to newer capabilities, such as being able to integrate SIP mobile apps into an organization's security strategy.

Embedded SIP Server Support

A security solution with an embedded SIP server can also achieve much deeper integration with SIP-enabled intercom devices since it is highly likely that it can connect directly to SIP-enabled intercom and door stations, thereby avoiding the need for an intercom server. Ideal for smaller systems, this approach to intercom integration greatly reduces TCO because it eliminates the need for purchasing, installing, and maintaining intercom servers and also makes deployment easier with fewer components to install. In addition, a security system that supports a server-less approach to intercom integration also gives an organization the ability to select components from multiple vendors.

Method of Integration

It is also important to look at how intercom management is integrated with access control and video within the security system. Within a unified security system, intercom devices are likely part of the core architecture of the security system. This usually allows an organization to easily associate call stations with doors, gate control devices, and cameras and to ensure that door-related and camera-related actions are readily available to operators.

Seamless andEmbedded Call Management

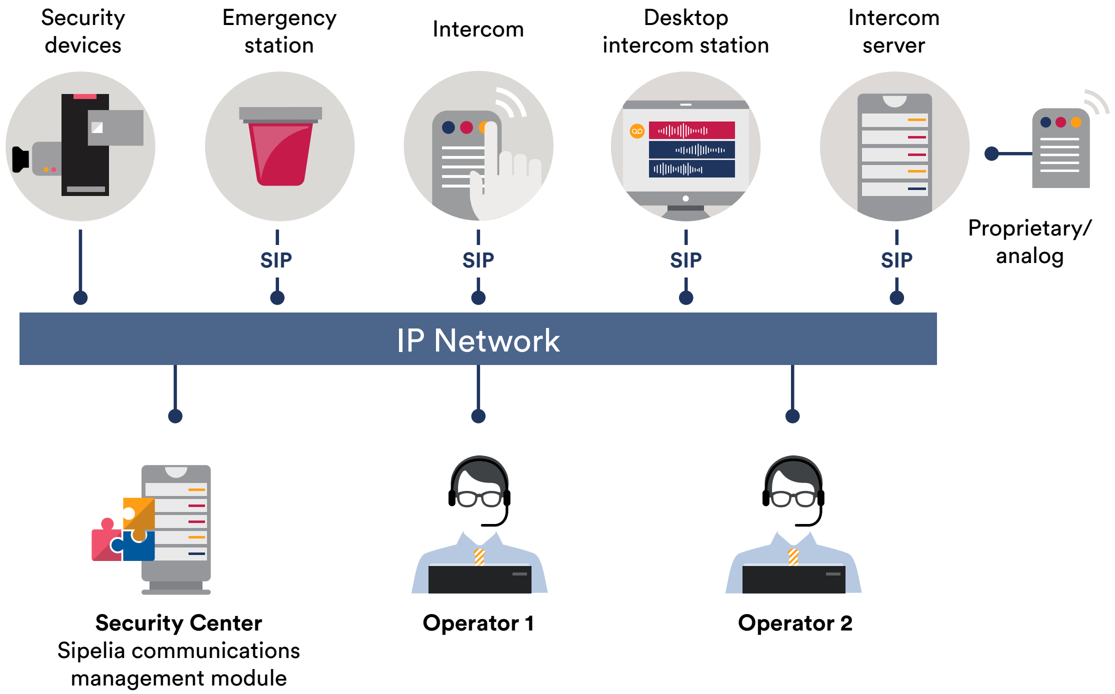
For security personnel and operators, a security system should also provide full call management capabilities, including viewing incoming calls, managing call queues, and running reports. Given that the access control and the video-related interface is unified with communications management, this feature would eliminate the need for external communications applications and would allow users to quickly manage calls with minimum interference while performing other security tasks. It is also important to find a security system that supports call reporting. Using this feature, an operator could quickly review historical call sessions automatically linked with audio and video.

Dynamic Graphical User Interface

The security system should also support communications management via dynamic graphical maps. Such a feature would support the addition of intercom objects within a map that would show the status of the intercom device and all associated actions, including answering a call, forwarding a call, and placing on hold. By being able to manage intercom devices through a map leads to greater oversight and situational awareness for an organization.

7. Overview of Sipelia communications management from Genetec

Genetec offers Sipelia Communications Management as a module of its Security Center unified security platform that guarantees that users are working from a single application for all of their communications and physical security needs. Built on an open-standards approach to communications, Sipelia integrates with SIP-based intercom devices and servers, allowing organizations to enhance their security operations through full communications management.



Benefits of Sipelia Communications Management

Embedded and Scalable SIP Server

A further benefit of Sipelia's use of SIP is that, in some situations, it avoids the need for a dedicated intercom exchange server. The embedded and scalable SIP server in Sipelia directly communicates with a variety of SIP-enabled edge devices from multiple vendors, including door and desktop intercom stations.

Evolving Ecosystem of Partners

With a growing ecosystem of partners, Sipelia supports some of the industry's leading brands of intercom equipment, such as Zenitel (Stentophon), Commend, and Castel. And, since call management is embedded within Security Center, end users do not need to rely on third-party vendor applications for call management.

Dynamic Graphical Map Interface

When Security Center's mapping functionality (Plan Manager) is enabled, Sipelia functionalities can be accessed from an easy to use dynamic graphical map interface, allowing operators to view the real-time status of intercom devices and answer calls directly from a map.

Innovative User-to-User Video Call Functionality

Rather than deploy third-party video call applications, the Security Center interface now includes user-to-user video call functionality to facilitate communications between users from the same interface used to monitoring the Genetec access control and video systems. Users can now initiate live audio or video communications with one another using off-the-shelf headsets and microphone and a webcam or standard security camera.

Benefits of Sipelia Communications Management

Additional functionalities in Sipelia

Sipelia Communications Management also allows an organization to

- **Seamlessly link intercom devices with doors and/or cameras.**
  - Linking intercom devices to one or more doors enhances efficiency because operators have quick access to door-related controls. And, since associations are defined in advance, operators do not have to look for associated doors and door-related actions when answering a call.
- **Leverage cameras built-into intercom devices with SIP video support in Sipelia.**
  - This provides another layer of visual information and guarantees that operators do not have to look for associated cameras and camera-related actions when answering a call.
- **Receive visual notifications of incoming calls in the Security Center interface notification tray while personnel are operating the security system.**
  - Once an operator is visually notified of a call, the call window dialog is easily and directly accessible no matter what the operator is doing.
- **Have instant access to all intercom devices, Security Center users, and ring groups with the Sipelia phone book feature.**
  - Users can search and access recipients, quickly place calls, and identify frequently contacted recipients.
- **Be available for all calls, including for workstation to intercom station, workstation to workstation, and intercom to intercom calls, with no exchange server.**
  - In addition, Sipelia offers bidirectional call recording, logging, and playback that can also include any associated video linked to a call.

Learn more about communications management solutions from Genetec:

genetec.com/sipelia

Genetec™

© Genetec Inc., 2017. Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.