AN-VOIP-102

Security Systems: Migration to Cloud-Enabled IP-Based Solutions

Introduction

Security systems are used in a variety of applications: residential, office buildings, hospitals, industrial facilities, and campuses such as schools and universities. In general, security systems include a wide range of functions including access control, computer security, video surveillance, and public safety. The focus of this document is on security systems for building structures intended to prevent harm to assets and persons from accidental or malicious causes.

Legacy security systems typically consist of multiple monitoring elements connected to a monitoring unit which is managed from a control panel (see Figure 1). The monitoring unit is connected via an analog phone line to a remote Monitoring Station, which operates 24x7 and responds to alarm conditions. The figure also shows a Local Area Network (LAN) connected to the Internet; but the security system is not connected to the LAN (and hence grayed out). These systems can have a wide range of installation locations, starting with one unit, such as in a single-family home, to many tens of units, such as in a multi-site commercial deployment.

Migration to IP-Based System

Security system manufacturers are changing their products to meet customer demand, evolving from traditional analog systems to IP-based products to leverage widespread innovation in IP-based communication systems and to make them ready for Cloud services. Emerging security systems are much more than just intruder alarms; their functionality, connectivity, and access options continue to evolve as new technologies emerge. They provide a much richer set of features including Voice over IP (VoIP), call routing, rule-based response, and access via mobile devices.

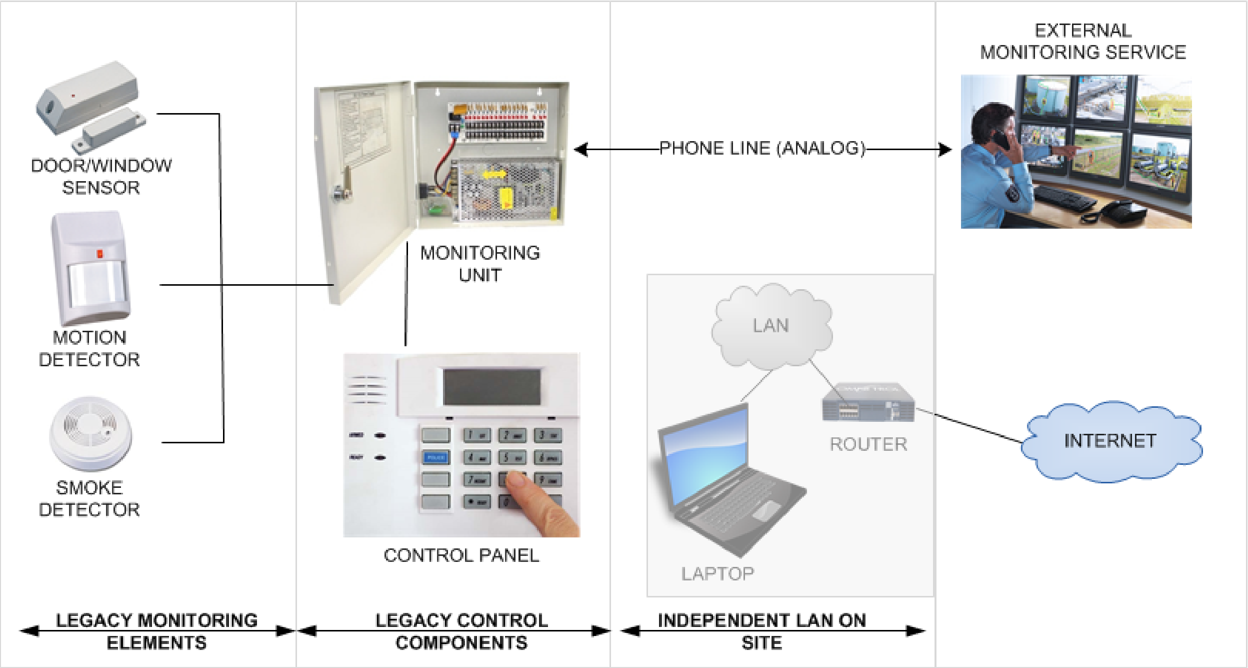

Figure 1: An example of a Security System

Migration Paths to IP-based Systems

Customers want the features of IP-based security system but also often want to leverage their investment in installed security system; hence, manufacturers are providing migration and upgrade paths which enable existing analog components to coexist with new IP-based components in multiple ways. For example:

1) **Basic upgrade**: in this scenario, the legacy system is upgraded to use a VoIP connection to the external Monitoring Station (see Figure 2). There is significant market pull in this direction since many customers are already moving away from “landlines” and using their cellular phones.

2) **Advanced upgrade**: in this scenario, the local monitoring unit and control panel are upgraded to an IP-based system while leveraging existing monitoring elements (see Figure 3). This option allows customers to enjoy a full complement of IP-based monitoring services since the monitoring unit and control panel can be access over the internet allowing a wider range of services.

Basic Upgrade: VoIP Connection

An immediate migration path to an IP-based security system is to connect the local monitoring unit to the remote Monitoring Station via Internet. In this scenario, rather than using an analog phone line, customers can leverage their existing internet connection to connect the monitoring unit to an Analog Telephone Adaptor (ATA) as shown in Figure 2. Security system manufacturers realize that there is significant market pull in this direction since many customers are moving away from “landlines” and using their cellular phones instead. In addition, many customers already have a connection to the Internet making installation an easy process.

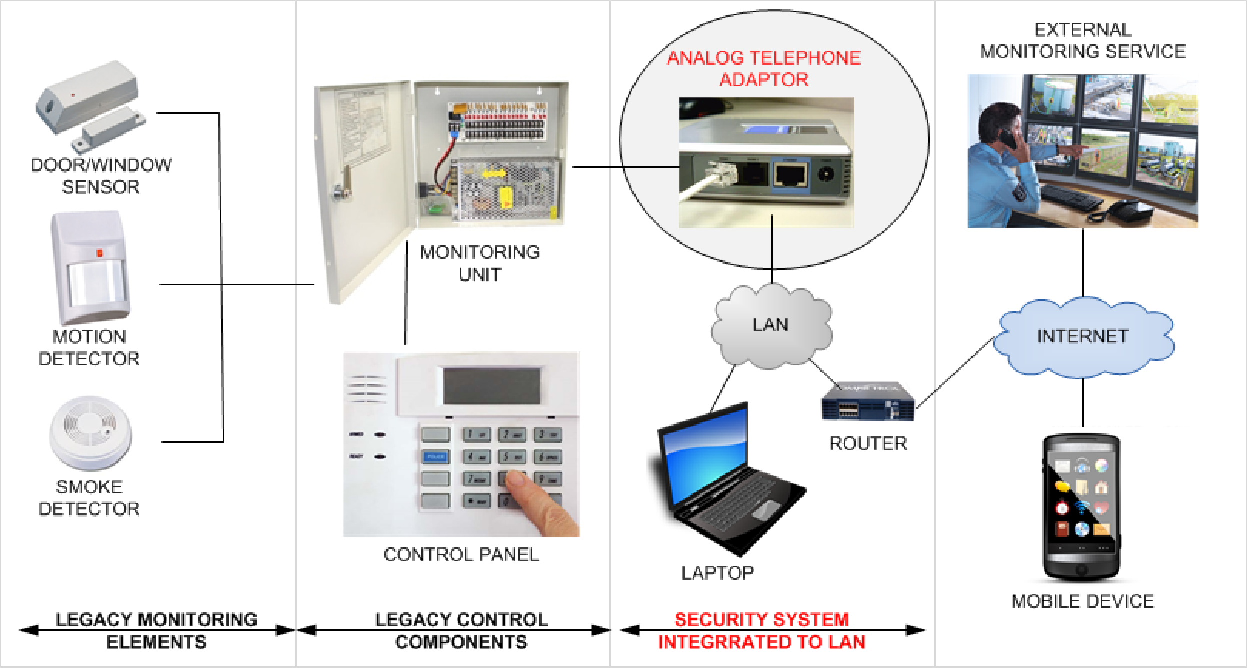

Figure 2: An example of Basic Upgrade: VoIP connection.

Advanced Upgrade: IP-based Monitoring

Often customers want to remotely verify and control status of the security system in addition to simply receiving alarms and text messages. This scenario calls for an advanced migration where the monitoring unit and control panel are upgraded to an IP-based system; however, the new components continue to leverage the existing analog monitoring elements thus reducing installation cost. As shown in Figure 3, an IP-based monitoring unit is deployed and connected directly to the LAN; legacy monitoring elements already installed are simply connected to the new monitoring unit since the wiring is already in place. The new IP-based control unit is also directly connected to the LAN. This option allows customers to enjoy a full complement of IP-based monitoring services since the monitoring unit and control panel can be accessed over the internet allowing a wider range of services.

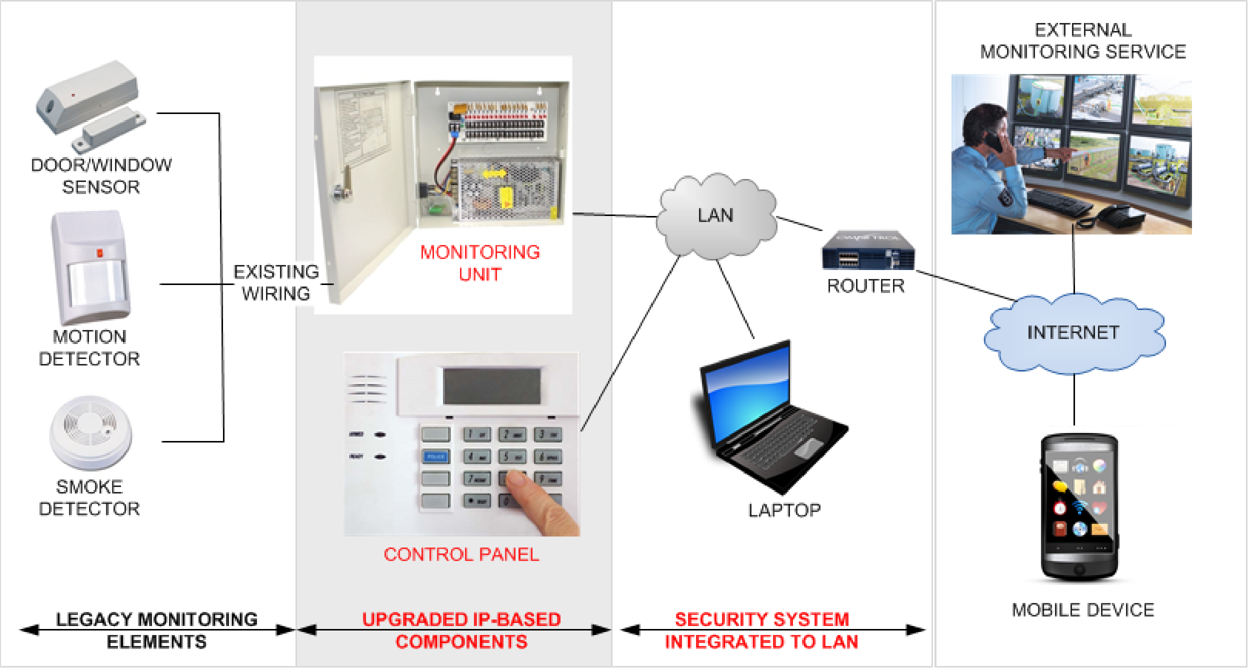

Figure 3: An example of Advanced upgrade: IP-based Monitoring

IP-based Security Solutions

For new construction or major remodeling, a complete IP-based security system can be deployed. Components of an IP-based security system are network-enabled including the monitoring unit, control panel, access control, and monitoring elements (see Figure 4). Advances in wireless technologies are also enabling easy integration of a variety of wireless monitoring elements. In addition, IP-based system also allow for integration with a range of other “Home Automation” function including intercoms, appliances, and thermostats.

IP-based security systems provide a much richer set of features including VoIP, call routing, rule-based response, and access via mobile devices. More importantly, IP-based systems enable use of emerging **Cloud-based Services**.

- Multi-modal communication: text, e-mail, Instant Messaging, in addition to voice communication
- Access Control: enable or disable access to assets or buildings
- Remote Control: ability to remotely configure and monitor

In general, these services allow customers to remotely configure and control the system from any web browser or internet enabled smartphone. They can send out instant text message and/or email notifications based on any system event.

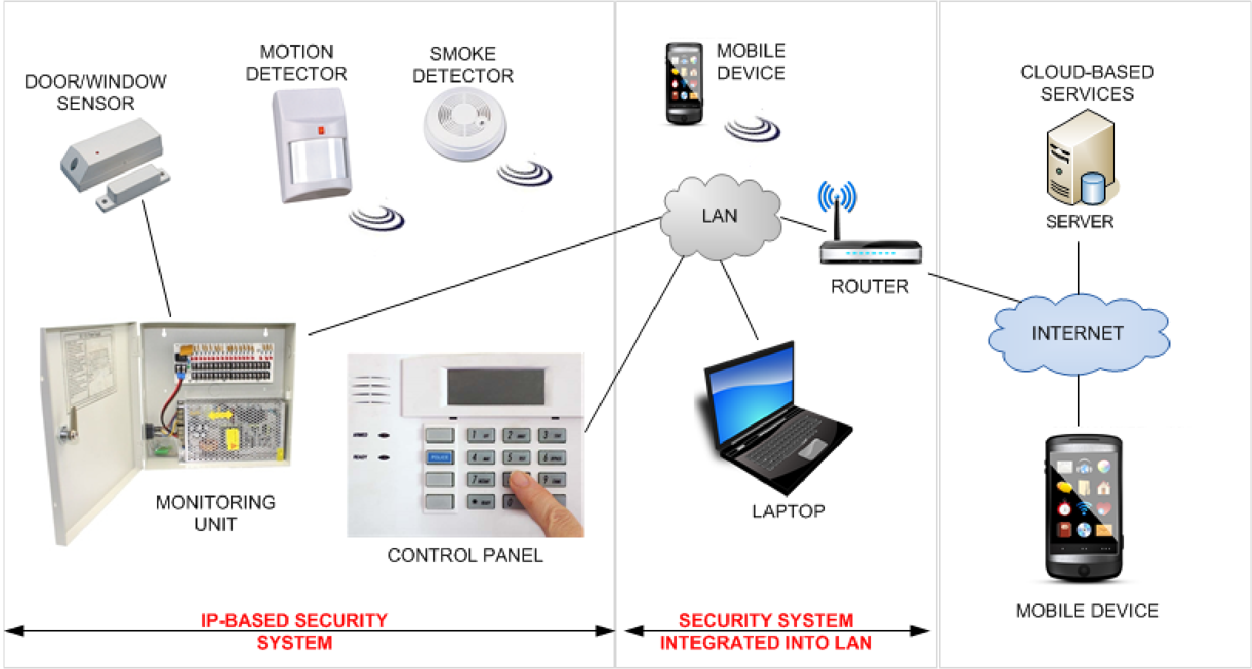

Figure 4: An example of IP-based Security System

Benefits of IP-based Security Solutions

IP-based security systems provide significant benefits in terms of new services, deployment efficiency, and operational efficiency; for example:

- Services:
  - **Access**: remote access and control via mobile and network devices
  - **Real-time information**: status, alarms, and alerts delivered in real-time
  - **Cloud Services**: enables a variety of services delivered via the cloud
- Deployment Efficiency:
  - **Lower cost**: use power over Ethernet (PoE) to simplify installation and reduced wiring cost
  - **Ease of Integration**: Internet and LAN standards make integration easy
  - **Scalability**: can be scaled from a single site to multiple sites and functionality
- Operational Efficiency:
  - **Lower cost**: reduced power consumption through the use of EEE and other “green” enabling standards
  - **Lower operation cost**: eliminates recurring cost of analog telephone connection
  - **Lower maintenance cost**: fewer disparate elements to maintain and monitor

Components of IP-based Security Systems

IP-based security systems employ a range of components depending on the requirements for a particular installation. At the core of these components is the ability to provide network connectivity and VoIP functionality. These components can be broadly classified as follows:

- **Embedded components**: these are components that bridge operating domains, such as analog-to-digital, and are often configured via a web or serial port interface and usually do not require a local interface. Examples of such components include an Analog Telephone Adaptor (ATA), which is used to connect analog phone systems to an IP network.
- **Endpoint components**: these components are connected to the network and provide a rich user interface often including display, keypad, microphone, and speaker. Examples of these components include control panels, access control, and intercoms.

Embedded Components

Embedded components bridge operating domains, such as analog-to-digital, and are often configured via a web or serial port interface and usually do not require a local interface. Examples of such components include an Analog Telephone Adaptor (ATA), which is used to connect analog phone systems to an IP network.

ATAs can have one or more “FXS” ports where the analog phone line is plugged in (instead of the phone jack), a network connection to connect to the Internet, and may have an additional network connection to connect a local device for convenience (see Figure 5). Many units are built with a Power-over-Ethernet (PoE) option in which case the unit can be powered using a PoE enabled Ethernet switch.

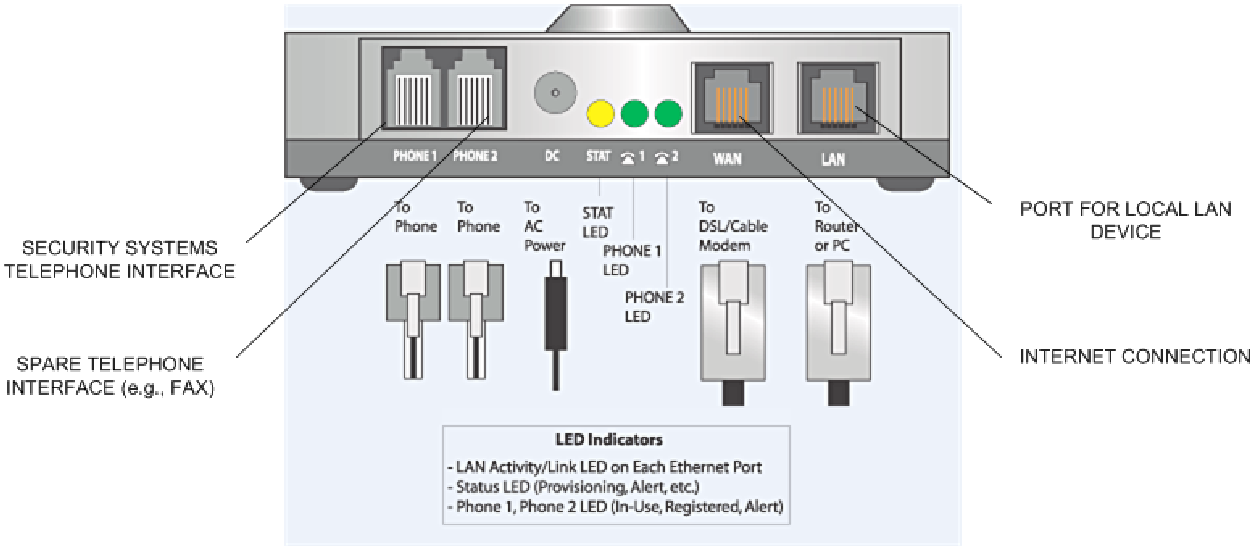
PHONE 1
PHONE 2
DC
STAT
☎ 1
☎ 2
WAN
LAN
To Phone
To Phone
To AC Power
STAT LED
PHONE 1 LED
PHONE 2 LED
To DSL/Cable Modem
To Router or PC
SECURITY SYSTEMS TELEPHONE INTERFACE
SPARE TELEPHONE INTERFACE (e.g., FAX)
PORT FOR LOCAL LAN DEVICE
INTERNET CONNECTION
LED Indicators
- LAN Activity/Link LED on Each Ethernet Port
- Status LED (Provisioning, Alert, etc.)
- Phone 1, Phone 2 LED (In-Use, Registered, Alert)

Figure 5: An example Analog Telephone Adaptor for an IP-based Security System

Endpoint Components

Endpoint components are connected to the network and provide a rich user interface often including display, keypad, microphone, and speaker. Examples of these components include control panels, access control, and intercoms.

For example, consider a basic control panel for an IP-based security system shown in Figure 6; the control panel consists of an LCD display used to indicate status and alarm conditions, a keypad for configuration and control, and a microphone and speaker which are typically driven via VoIP for communication. Typically, the back panel has one or two network interfaces to connect to a LAN. Some endpoints also include digital control of external devices, such as door lock, sensors, cameras, and other security devices.

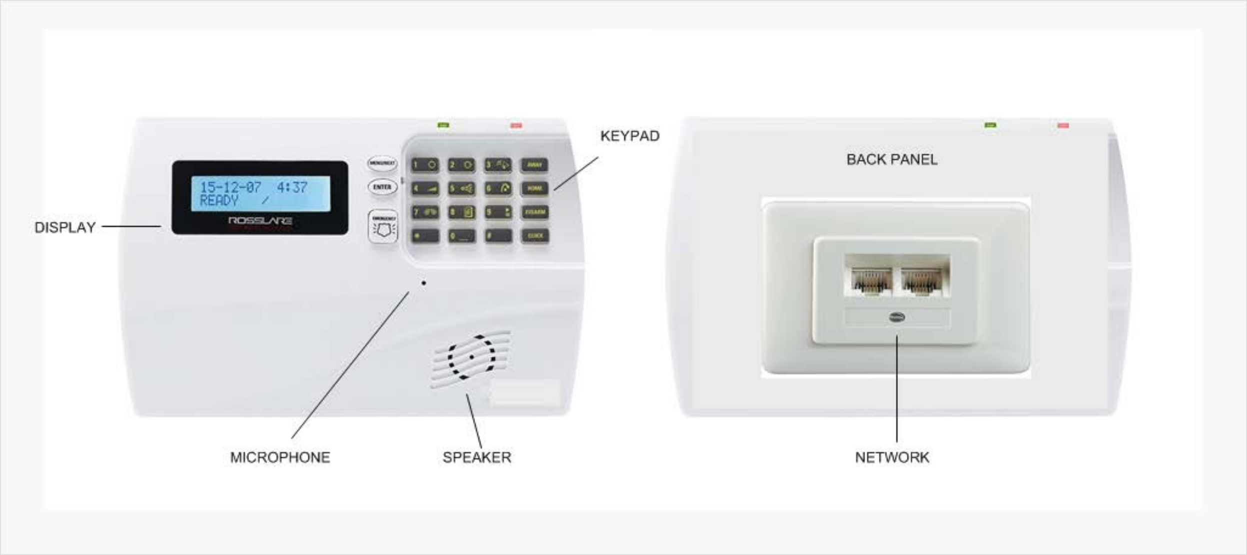

Figure 6: An example Control Panel for an IP-based Security System

Another example is an intercom endpoint (see Figure 7). The form factors and functions are different than the control panel, but the basic architecture still consist of a display, keypad, microphone, speaker, and network connections. These endpoints can typically be installed efficiently since they only need Cat 5 wiring with power over Ethernet (PoE).

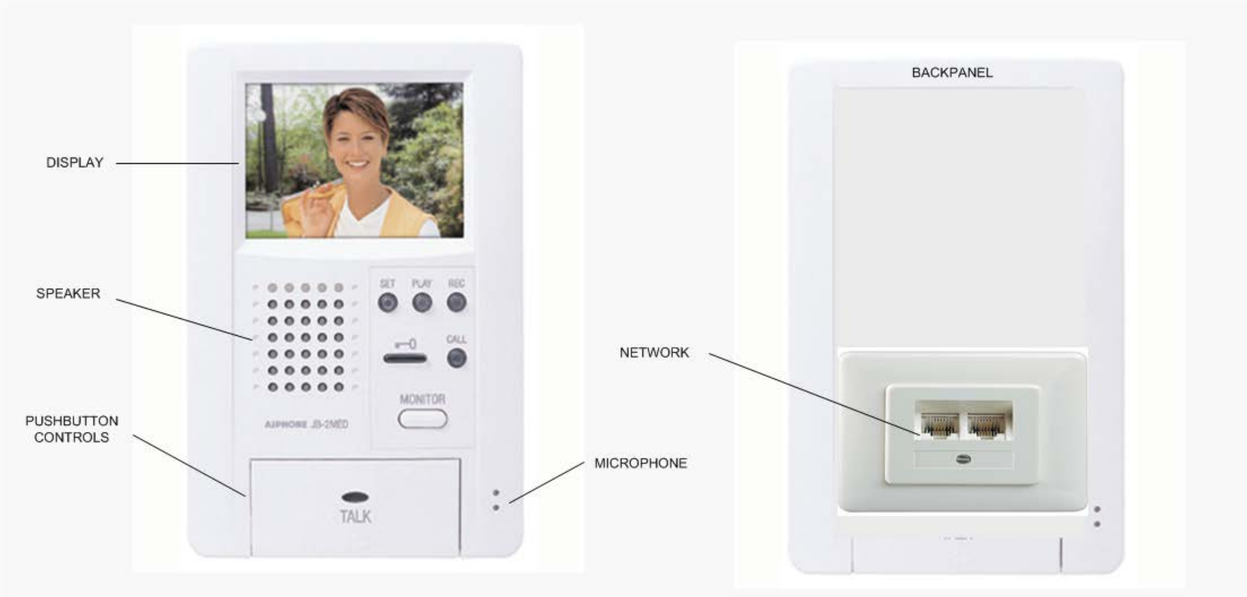

Figure 7: An example Intercom for an IP-based Security System

Micrel's System-on-chip (SoC) for IP-based Security Systems

Micrel's KSZ8342 and KSZ8382 families of System-on-chip (SoCs) provide complete solutions for components of an IP-based security system. These SoCs have built-in support for interfaces required for these components–hence only a few additional external devices are needed to create a fully functional component. Micrel's SoCs are the ideal choice for IP-based security systems, backed by Micrel's high-reliability and solution robustness proven in commercial, industrial, and automotive applications around the globe.

Both the SoC families implement a multiprocessor architecture with embedded RISC CPU and powerful DSP, providing a flexible VoIP platform with narrowband and wideband voice processing and excellent voice quality.

Embedded Processing Resources

- CPU and memory: Micrel's SoCs embed MIPS32 RISC processor for configuration and network protocol processing, SDRAM and DDR2 interfaces, and Flash interface
- DSP: Micrel's SoCs embed a ZSP400 Digital Signal Process which offers high-quality voice/audio processing, 8kHz/16kHz 16-bit ADC/DAC with integrated amplifiers, Narrowband and Wideband CODECs

Network

- Network: 3-port 10/100BaseT Ethernet Switch; Integrated low-power PHY transceivers
- IGMP snooping to handle multicast traffic (RFC 4541)
- VLAN support (IEEE 802.1Q)
- Energy Efficient Ethernet (IEEE 802.3az)

KSZ8342 SoC Family

Micrel's KSZ8342Q System-on-Chip (SoC) provides a complete solution embedded components of an IP-based security system. The chip bridges Digital and Analog systems enabling IP-based communication. It addresses a wide range of applications including Analog Telephone Adapters (ATA) and gateways. The highly-integrated SoC has built-in support for interfaces which reduces the need for external components. As shown in Figure 8, the KSZ8342 includes a PCM Controller which can be coupled with a SLIC interface to create FXS and FXO ports as needed.

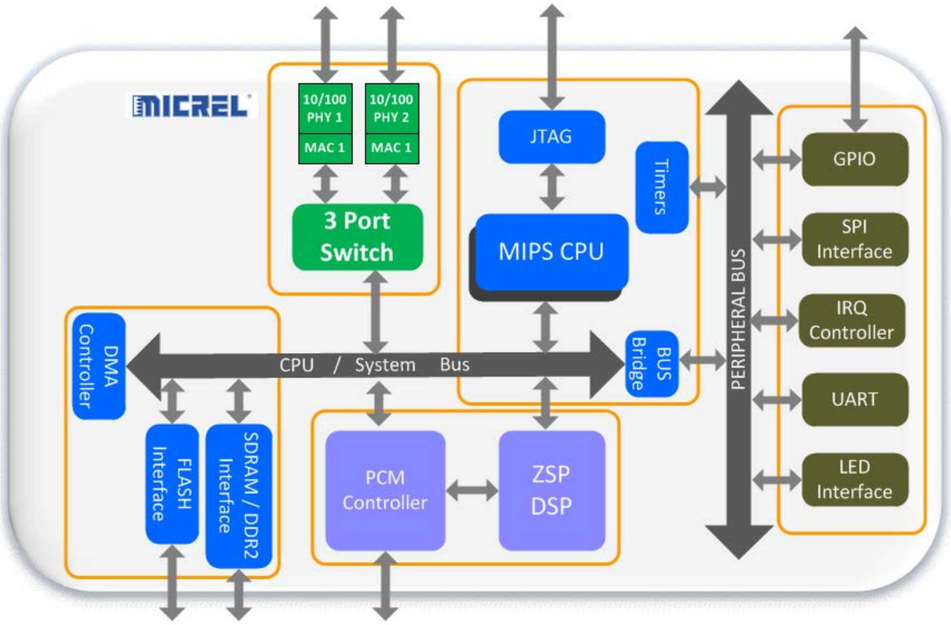

Figure 8: Micrel's KSZ8342 SoC block diagram

KSZ8382 SoC Family

The KSZ8382 SoC is the ideal choice for endpoints components of an IP-based security system. The chip's extensive integration increases performance and reduces BOM cost, featuring a high-performance audio subsystem, LCD interface, keypad scanner, memory controllers for both SDRAM and DDR2, and flexible GPIO. The LCD Interface supports SPI (8-bit parallel interface). The keypad scanner can be used to support push buttons and even a full telephony keypad. GPIO can be used for a variety of functions including monitoring elements, door controls, indicators, etc.

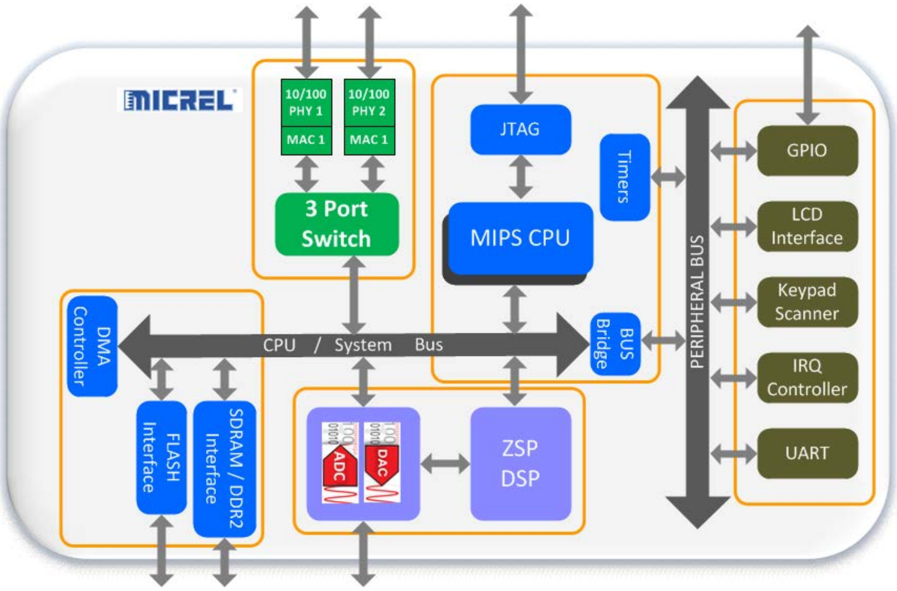

Figure 9: Micrel's KSZ8382 SoC block diagram

Firmware: CPU and DSP

The firmware for Micrel's KSZ8382 has a modular architecture to provide developers with variety of choices in developing their Endpoint Application.

- Access at Call Control: For a turnkey solution, developers can leverage the built-in SIP call manager from the Endpoint Application. The layers below handle media transport and DSP functionality.
- Access at Media Transport: For developers who have their own SIP software (or want to implement other call control protocols) can use the RTP/RTCP access for media transport. As described above, the layers below handle network and DSP functionality.
- Access at DSP Resources: For developers who want their own call control and media transport (standards-based or even proprietary) can access the DSP resources directly.

The firmware supports a wide range of security features including signaling protection using SIP TLS, media encryption using SRTP, and STUN for working across firewalls.

Conclusion

Innovation in IP-based communication systems is driving the rapid pace of migration from analog to IP-based security systems. Micrel's KSZ8342 and KSZ8382 families of SoC provide a complete solution for IP-based security system components that can be used to upgrade legacy security systems in an efficient and cost-effective manner and to add cloud services or to build a completely new IP/VoIP based application. These SoCs have a high level of integration through the integration of a 3-Port switch, PHY, amplifiers, audio interface, and PCM interface. Because of their built-in support for interfaces required for embedded and endpoint components, only a few additional external devices are needed to create a full-featured component. The firmware for these SoCs has a modular architecture to enable developers many choices in developing application software for these IP-based security components. Together, these SoCs and associated firmware can be used to create a wide range of IP-based security solutions.

Revision History

Date	Change Description/Edits by:	Rev.
	Initial Release	

MICREL, INC. 2180 FORTUNE DRIVE SAN JOSE, CA 95131 USA
TEL +1 (408) 944-0800 FAX +1 (408) 474-1000 WEB http://www.micrel.com

Micrel makes no representations or warranties with respect to the accuracy or completeness of the information furnished in this data sheet. This information is not intended as a warranty and Micrel does not assume responsibility for its use. Micrel reserves the right to change circuitry, specifications and descriptions at any time without notice. No license, whether express, implied, arising by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Micrel's terms and conditions of sale for such products, Micrel assumes no liability whatsoever, and Micrel disclaims any express or implied warranty relating to the sale and/or use of Micrel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

Micrel Products are not designed or authorized for use as components in life support appliances, devices or systems where malfunction of a product can reasonably be expected to result in personal injury. Life support devices or systems are devices or systems that (a) are intended for surgical implant into the body or (b) support or sustain life, and whose failure to perform can be reasonably expected to result in a significant injury to the user. A Purchaser's use or sale of Micrel Products for use in life support appliances, devices or systems is a Purchaser's own risk and Purchaser agrees to fully indemnify Micrel for any damages resulting from such use or sale.