Michael Long
Smart Building and Smart City Strategy Manager, Analog Devices, Inc.

IN-BUILDING SECURITY SYSTEM EVOLUTION AND NEW AGE SOLUTIONS

Share on Twitter | Share on LinkedIn | Email

In recent years the user experience of consumer electronics, new government legislation, and the push for increased system efficiency have conspired to drive significant advances within the in-building security or intrusion detection system solutions market requirements and functional design targets. Traditional sensor types, connectivity, control interfaces, and power sourcing have all been affected to a varying degree, driving a significant shift in the look, feel, and operation of these somewhat ubiquitous applications. Historically, intrusion detection systems were mostly a simple wired set of hardware consisting of control panels, door/window contacts, and perhaps a passive motion sensor (or two) that carried minimal software integration and/or operational intricacy. Over the past decade, however, both residential and commercial building customer demands have influenced the complexity and utility of the individual components and the complete functionality of these system solutions.

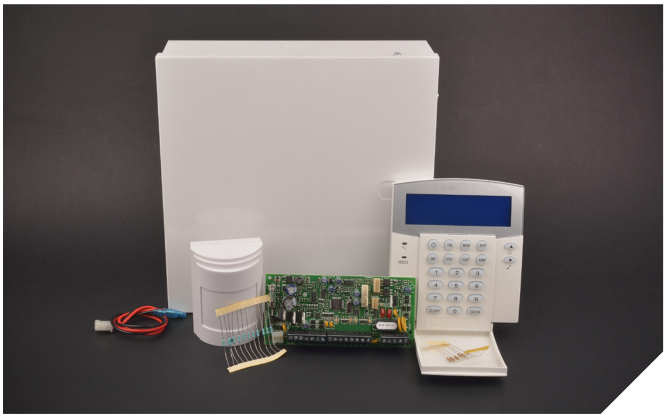

Figure 1. Traditional intrusion detection system solution deployment hardware package.

One of the first drivers of this evolution was new government legislation being enacted in many regions of the world specifically in the developing world and countries where there is a large chasm between the classes of population. Most impactful has been a mandate that first-order threat verification must be conducted prior to dispatching emergency services. This was due to a significant increase in the false alarm rates and erroneous deployments of municipal resources (police, fire, EMS). In order to adhere to this mandate, two separate but connected actions were undertaken. First, the system development OEMs added new sensor technology to the hardware itself, and second, the system service providers enhanced the level of remote monitoring by human personnel.

Here is an example of how these actions have manifested themselves: traditional motion sensors were based on a single or dual pixel passive infrared (PIR) sensor element. PIR sensors operate by identifying changes in heat signatures within a field of view. Though quite acceptable for some use cases, PIR sensors are limited to the mere detection or presence of stimuli (humans, pets, vehicles) but they cannot identify the type of source that has been detected. In order to distinguish or classify the detected objects, additional sensor technology must be added to the system. In an effort to address this need and to increase the overall accuracy, reliability, and performance of the entire system, image capture capability has been added to an increasing percentage of security motion sensor nodes. The PIR sensing element remains present but in this advanced configuration, the PIR acts as a trigger to wake up the image capture subsystem, which then grabs an image frame or two and they are then sent to a remote monitoring station for verification. Upon receipt at the service provider's operations center, round-the-clock human security employees are tasked with checking the transported images in order to verify the stimuli that tripped the alarm, which presents a threat or alarm condition; only after this verification step has been completed will emergency services be dispatched. As an extension to the functionality of the image capture capability being included at the edge of the network within individual sensor nodes, local processing integration is also now being deployed to enable local threat analysis and verification. This additional layer of intelligence provides reduced decision making latency and enables the data transmission bandwidth to be significantly lower, as mere bits of data (flags, interrupts, and notifications) need to be transmitted rather than bytes of data (multiple image frames).

Another major advance in the in-building security solutions sector has been a large move from wired to wireless interfacing, not only between the individual sensor nodes and the control panel, but also from the entire system deployment to its associated remote monitoring station or operations center. For many decades the sensor to panel connection was made using low voltage serial wiring, most often of the RS-485 variety commonly found in many other building control applications. This hardwired interfacing required significant effort and an increasing level of cost for system installation. With the advent of very low power and short range wireless technology, a number of manufacturers have extended their hardware system portfolios to include wireless system versions enabling much simpler and easier initial deployments. This shift in turn has reduced implementation time as well as cost, and by extension has opened a significantly larger market size by allowing reasonable retrofit installations rather than the market continuing to be driven by new construction sales as it has in the past. Additionally, in the area of back-end connectivity, the intrusion detection system market, which was once exclusively aligned to a phone line or POTS connection to the remote monitoring station or operations center, has evolved to leverage Wi-Fi/gateway Internet links, as well as terrestrial mobile phone network connections, widening the playing field of deployment options while also eliminating the hard requirement of landline phone connections being present for intrusion detection system installations.

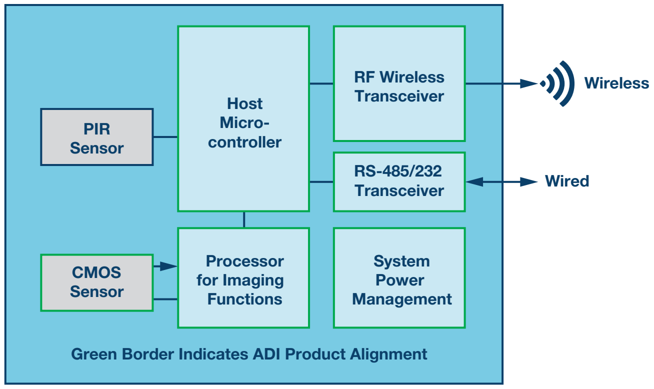

Figure 2. A high level internal system block diagram of a next-generation intelligent motion sensor.

The final area of major evolution in the in-building security equipment space has been that of the user interface. Only a short time ago, intrusion detection system control panels were comprised of simple push button and dial interfaces. However, now with smartphone and tablet use pervasive among almost all of the target consumer demographics, the user experience of residential and commercial building control equipment, including intrusion detection systems as well as thermostats and smoke detectors, has leaped into the 21st century. Although most OEMs still offer entry level, no-frills equipment options, the midrange and high end offerings now include such features as touchscreens, backlit keypads, ambient light sensing, and voice control capabilities. Most of these features clearly address the look and feel elements of the system performance and the utility. Operational value of features such as ambient light sensing can also address the critical areas of system power consumption and operating expenses over the life of the product or as sometimes referred to as "total cost of ownership." While these features can be viewed as having an incremental drive on overall system cost, the public demand necessitates feature additions to match expectations set through 24/7 consumer electronics utilization. The OEMs have responded by integrating consumer electronics related features into their hardware materials. Today's top-of-the-line system would be largely unrecognizable to the consumer public of a mere 20 years ago. Real-time, on-demand activation, local threat verification, wireless connectivity, high resolution control panel displays, advanced user interfaces including voice control, remote monitoring capabilities complete with streaming video feeds, and a new array of sensor elements offering such functionality as shock, vibration, and acoustic event detection have significantly transformed the landscape of this industry in a relatively short period of time.

All of the improvements and advances previously outlined cannot come at the expense of an increase in system power consumption. As the data and control interfaces between sensors and panels moves from wired to wireless as explained within this article, a continued reliance on ac power sources and wired tethering is a complete and utter nonstarter. Using stacked batteries for increased capacitance while operating certain portions of the system in a duty cycled manner are merely two ways in which OEMs are enabling increased value and utility of in-building security systems while maintaining power budgets—possibly to be served through battery/dc power sources, whether standalone or combined with energy harvesting capabilities such as subsystems based on high efficiency photovoltaic cell harvesting elements.

When reviewing the multiple areas of upgrade and evolution of in-building security or intrusion detection system covered herein, a strong push can be made to generate new technology platforms in order to integrate and promote many or all of these innovative advances within a single vehicle.

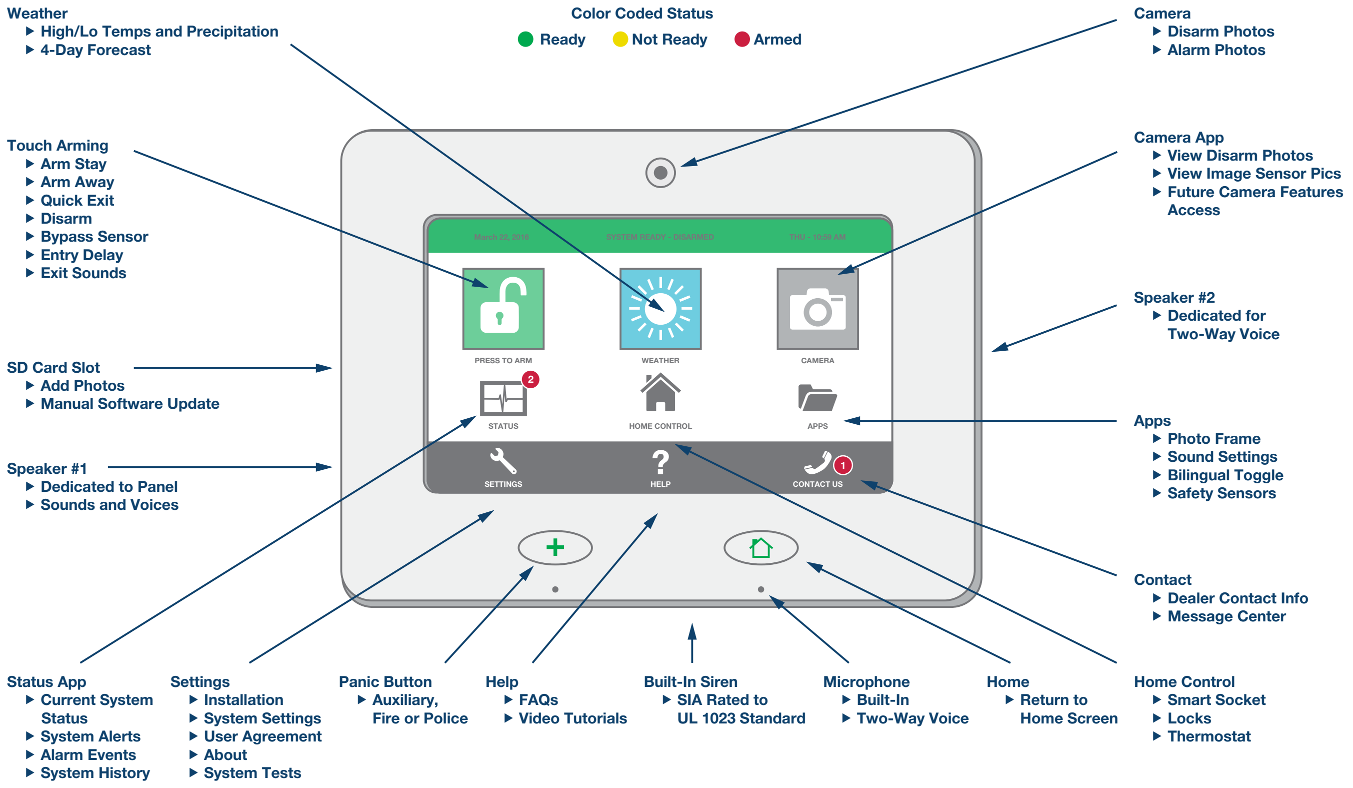

Figure 3. High performance, feature rich intrusion detection system user interface control panel.

This is true for both the end equipment manufacturers themselves as well as for the solution providers to the intrusion detection system equipment market. These platforms can serve as the foundation of next-generation hardware projects within the manufacturers and/or as a reference design from solution providers aimed at enabling smooth transition from existing technology to some of the advances outlined in this article while in parallel speeding time to market for adopting customers.

Clear alignment between many of the innovations and technology advances included in this piece, as well as the underlying market requirements, can be drawn with the innovative technologies being delivered by Analog Devices. Whether rooted in the signal conditioning and signal conversion functions, which are traditional strongholds of ADI, or the more recent focus areas of digital processing and power management, ADI has the industry-leading technology and robust solutions to enable the scaled requirements that in-building security/intrusion detection system equipment manufacturers face when developing their next-generation platform architectures.

About the Author

Michael Long is the strategy manager for the Smart Buildings market segment within the Industrial Sensing business unit at Analog Devices, Inc. Previously he served in product line management capacities across various technology groups at ADI.

Analog Devices, Inc.
Worldwide Headquarters

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters

Analog Devices, Inc.
Wilhelm-Wagenfeld-Str. 6
80807 Munich
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Asia Pacific Headquarters

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™