White Paper

Panel-Based vs. Remote Cell Communicators

Many security system suppliers continue to believe that the practice of locating cellular communicators remotely from the panel provides a necessary or higher level of security. This is true for installers that are still using old-style slave cellular communicators. When using the current generation of communicators, which are tightly integrated with and installed internal to the panel, the greatest security is created by locating the communicator in the panel enclosure. Remotely locating the communicator merely increases the complexity and cost of the installation, with absolutely no benefit to security. In fact, it could make the system less secure, particularly with the older slave or slow retransmission-type cell communicators.

Old School Thinking

The fundamental fallacy of the remote-from-panel theory is that the security is in the communicator. The theory holds that if you protect the communicator, you ensure it will be able to transmit an alarm even if the panel is attacked. Therefore, the theory claims, isolating the communicator at some distance from the panel or carefully hiding the communicator enhances the security of the system.

This incorrect belief goes back to older slave communicators that are/were not designed specifically to work with a particular panel. This was the first generation of cellular communicators that have been widely used for many years in our industry. For applications that demand the highest levels of security, like financial institutions, this older technology is no longer the best method. The current generation of cellular communicators is designed specifically for a particular control panel, and offers many improvements over slave type-systems. In these newer systems, the panel programming provides for regular check-in messages. Included are device-to panel check-ins, as well as supervised check-ins between the panel and the Central Station.

In such systems, if any component in the system is attacked, the Central Station will become aware of the issue immediately or as soon as the expected check-in message is missed. If a perpetrator attacks the panel and renders it unable to communicate, an alarm will be triggered by the receiver in the Central Station. The security at that point is in the receiver, not in the panel.

When an intruder trips one of the premise's sensors, whether a door or window contact, glass-break, or motion detector, the panel will immediately signal the Central Station. This alarm may be received much faster than that provided by a missed check-in (depending on the Supervision Programming). Therefore, it is still a recommended practice to design your installations so the panel is wrapped in multiple layers of protection. The attack-grade panel enclosure is installed in a locked room protected by door contacts, motion detectors, etc.

But in the event of an attack on the system, security is still ensured. In most cases, the panel will have sufficient time to transmit an alarm to the Central Station since it needs less than a second to communicate via network. Even if the intruder is successful in destroying the panel and/or the communicator before an alarm can be sent, the Central Station still becomes aware of the situation when the next-scheduled check-in fails to occur.

The location of the communicator has no bearing on the level of security or speed of the response in the event of an assault on the panel. In fact, having the cell communicator in the attack-grade enclosure, powered by the panel and backed up by the full system battery, provides fewer points of potential system failure.

Multi-layer Communication

The most capable panels permit the creation of a multi-layer communication approach that provides in-depth security with reduced communication costs. In these panels, the primary path for panel-to-Central Station communication is network. If that path becomes unavailable for any reason, the panel switches to a secondary path. Additional paths can also be created and programmed in these panels. This approach makes it virtually impossible to disrupt all panel communications. It also minimizes cellular signaling and the related cost, because the cellular communicator is sending data only when needed.

A more advanced implementation of this backup-path approach is DMP's Adaptive Communication. For most panels, the failure of a communication path generates a Panel-Missing message before the backup path connects to the Central Station. This is because the device/path is too slow or the retransmission of the signal creates a delay. DMP panels adapt more quickly to the new backup cell path, which continues to fulfill the check-ins at the receiver and therefore avoids that panel missing message. The rapid switch to an alternate communication path avoids the need to respond or, in some high-security applications, saves the responsibility of sending a runner to the alarm premises.

When the primary path is restored, the panel again adapts and reverts back to that primary path. In the meantime, the Central Station will receive a trouble message for the failed communication path, notifying them of a switch in the communication paths.

DMP's large commercial panels provide as many as eight communication paths. Users of these systems have tremendous confidence in the availability of reliable, unbroken connections to their Central Stations.

Added Costs of Remote Installation

Systems buyers who employ the remote-communicator approach not only fail to improve their security but also pay more for their systems than necessary. Locating the cellular communicator remotely means they will typically buy a second, hardened enclosure for it. They also have the cost of installing the communicator and running the necessary wires and conduit to connect it to the panel.

When installed remotely, the communicator requires its own battery, adding to the initial costs. The second battery also has to be maintained and replaced on a maintenance schedule, adding service costs. When located inside the panel, the cellular communicator relies on the panel's backup battery for power.

From a hardware, installation, and wall-space perspective, housing the communicator inside the panel is clearly preferable.

Other Speed and Reliability Concerns

Users interested in the fastest and most secure communications should be aware that most older cellular communicators actually communicate via a third-party network operations center (NOC). These communicators send the cellular message to the NOC which may convert it into a Contact ID message and relay that via dialer or some other method.

While these intermediary communication points are generally secure and reliable, they nevertheless represent additional retransmissions in the communication process that create delays and are subject to potential failure. The DMP cellular communicator connects directly from the panel to the receiver at the Central Station, without any relaying or retransmission providing a shorter, faster, and more reliable messaging approach.

A More Effective Approach

Old habits die hard and so many end users continue to be sold on the idea that the most-effective security approach is to locate their cellular communicators remotely from the panel. Smart system integrators are aware that the security isn't in the communicator; it's at the Central Station. With the current generation of communicators, locating the communicator inside the control panel optimizes security while minimizing the cost to remotely install, wire, and maintain their cellular communicator.

Function, Feature and/or Listings	DMP 263LTE Cell	Telular TG-4 Cell	DSC 3G3070	Uplink 4550 Cell
Upload DMP Panel Programming via cell connection	YES	NO	NO	NO
Download DMP Panel Programming via cell connection	YES	NO	NO	NO
Make programming changes while connected	YES	NO	NO	NO
Arm/disarm, update time, lock/unlock doors, control outputs/Z-wave over cell	YES	NO	NO	NO
Able to perform diagnostics & send test signal through keypad via Diagnostics menu.	YES	NO	NO	NO
Able to provide Installer/Service Cell Signal	Yes (built into Diagnostics actual dB level)	Yes (jumper into test mode, LED bars only)	Yes, LED indicator	Yes (jumper into test mode, LED only)
Networks	Verizon, AT&T, FirstNet	AT&T, T-Mobile	AT&T, T-Mobile	AT&T, T-Mobile
Anti-jamming technology?	YES	NO	NO	NO
Time for message transmission to monitoring center after primary failure	less than 10 seconds	minutes	minutes	minutes
VPN Communication	Either way, customer's preference	Required	NA (not able to support DMP format, IP Data)	NA (not able to support DMP format, IP Data)
Extra power supply required?	No (utilizes panel power)	NO (built-In Battery Charger, Battery no included)	Yes & No (Unit does not ship with AC Transformer or battery, but has built-In Battery Charger)	Yes & No (Unit does not ship with AC Transformer or battery, but has built-In Battery Charger)
Phone line required?	NO	NO, but uses dialer capture in DMP format	No, but uses dialer capture in CID format for DMP panel.	No, but uses dialer capture in CID format for DMP panel.
Direct communication to Monitoring Center?	YES	NO, re-transmitted	YES	NO, re-transmitted
Adaptive Technology™, cell changes from back-up to primary with same check-ins	YES	NO	NO	NO
Programmable Check-In & Failure (from 2 to 240 minutes) as primary and/or back-up	YES	NO	NO	NO
Supports SMS messaging and SMS commands	YES	NO (not with DMP)	NO (not with DMP)	NO (not with DMP)
Full data with complete area, zone, user names	YES	YES (w/DMP format)	NO (not with DMP)	NO (not with DMP)
Able to be primary or back-up	YES with extensive programmable options	YES with limited options	Yes with limited options	YES with limited options
Able to change from back-up to primary, when primary fails	Yes (when programmed)	NO	NO	NO
Listings/Approval California State Fire Marshal (CSFM)	YES	NO	NO	NO
Listings/Approval New York City (FDNY COA #6123)	YES	NO	NO	NO
Listings/Approval Industry Canada: (4160A-CNN0301 263C/463C)	YES	NO	YES	NO
Listings/Approval ANSI/UL 365 Police Station Connect Burglar Alarm Systems	YES	YES	YES	NO
Listings/Approval ANSI/UL 985 Household Fire Warning System Units	YES	YES	YES	NO
Listings/Approval ANSI/UL 1023 Household Burglar Alarm System Units	YES	YES	NO	NO
Listings/Approval ANSI/UL 1076 Proprietary Burglar Alarm Units & Systems	YES	NO	NO	NO
Listings/Approval ANSI/UL 1610 Central Station Burglar Alarm Units	YES	YES	NO	NO
Listings/Approval ANSI/UL 864 Control Units for Fire-Protective Signaling Systems	YES	NO	NO	NO
Listings/Approval ULC Subject-C1023 Household Burglar	YES	NO	YES	NO
Listings/Approval ULC/ORD-C1076 Proprietary Burglar	YES	NO	NO	NO
Listings/Approval ULC S304 Central Station Burglar	YES	NO	YES	NO
Listings/Approval ULC S545 Household Fire	YES	NO	YES	NO
Listings/Approval ULC S559-04 Fire Signal Receiving Centers & Systems	YES	NO	NO	NO

800-641-4282
INTRUSION • FIRE • ACCESS • NETWORKS
www.dmp.com
2500 North Partnership Boulevard
Designed, Engineered and Assembled in the USA
Springfield, Missouri 65803-8877