ARTICLE

UL's Fire and Security Service Solutions

Understanding Line Security

The full value of a security alarm system can only be realized if the detection of an intruder is made known to people who can take action in response. UL Standards provide requirements for Line Supervision and Line Security that address this critical element of a security system.

- **Line Supervision** requirements provide increased assurance of a functioning communication path between protected property and monitoring center
- **Line Security** requirements provide increased assurance that even surreptitious attacks will be detected and announced at the monitoring center

As the level of risk increases at a protected property, so does the value of resiliency and reliability in alarm signal communications.

- For lower risk applications, where the threat of surreptitious attack is low, a non-Line Security rated system that checks the integrity of the communication path once every 24 hours may be adequate
- For higher risk applications, where the threat of surreptitious attack is high, a Line Security rated system that checks the integrity of the communication path once every few minutes may be more appropriate based on a review the individual environment

Selecting an appropriate system is about balancing the level of risk against the total cost of ownership, which includes the options available from both your security and communications service providers, as well as any consequences of signaling false alarms.

Line Supervision

Line Supervision is the occasional signal confirmation of a communication path accomplished by regularly sending and receiving messages over the path in a specified timeframe. It is a foundational requirement in all UL Alarm System Standards. The 2-way exchange between the protected property and the monitoring station is often referred to as a 'check-in'.

The frequency of check-ins required by UL Standards is driven by risk determination. Relatively low risk residential scenarios may require one check-in every 24 hours. Higher risk commercial applications, e.g. a jewelry operation, may require a check-in as often as once every 200 seconds.

When the alarm system at a protected property fails to check-in with the monitoring station within the specified timeframe, the cause is usually uncertain. Since criminals frequently try to disrupt alarm communications prior to entering a

building by cutting cables or damaging radio antennas, there is reason to treat the event as a sign of an intrusion.

On the other hand, a failed check-in could have nothing to do with a surreptitious attack, but rather a communications network problem. In this case, requesting a law enforcement response could result in false alarm fines and other negative consequences incurred by the property owner.

For this reason, many contemporary system designs provide multiple communication paths, often using different technologies. For example, a system that uses both a wired and wireless communication method can

remain in contact with a monitoring station even if one network goes down, thus maintaining the desired level of communication path assurance and reducing the chances of initiating a false alarm.

"Mission Impossible" Attacks

While a simple signal check-in may verify the existence of a communication path, it does not provide assurance that the received signals are authentic.

A staple of the popular Hollywood heist movie is the trusty "alligator clip connection" that feeds a prerecorded video loop of an empty room to a guard station. The bad guys cut the real camera wires, attach the alligator clips, and go about their dastardly deeds undetected while the guard station sees a vacant room and assumes everything is normal. This is known as a substitution attack. Early intrusion detection systems were susceptible to similar kinds of substitution attacks, where batteries, signal generators, or carefully prepared replacement control units could be swapped for legitimately installed units.

Smash-and-grab, or social engineering based attacks, may be more frequent than "Mission Impossible" style technical attacks. However, high value targets like jewelry stores, are more likely to attract criminals that possess the high-level technical skills needed to successfully carry out such attacks.

UL Line Security Requirements

To address these higher level technical vulnerabilities, surreptitious attack testing and a Line Security

designation/rating, for products that meet the test requirements, were added to UL Alarm Equipment Standards. Understanding that these advanced safeguards would be used to protect high risk accounts, the consensus of stakeholders was that the check-in frequency for a system in Line Security mode should be 200 seconds or less.

Additionally, UL Alarm Service Standards gave alarm companies the ability to declare Standard Line Security service on certificates covering protected properties, when a Line Security rated product is installed and properly configured to operate in Line Security mode. When technological advances made encryption of alarm signals feasible, the Encrypted Line Security designation was made available for products that could add encrypted messaging on top of the ability to detect surreptitious substitution attacks.

Note that the complete Line Security 2-way communication protocol requires an "always on" type communication path. Line Security requirements cannot be met by systems that communicate using 10 digit dial-up service over wired or wireless public switched telephone network (digital alarm communicator transmitters — DACTs — in alarm industry terminology).

The Many Flavors of Line Security and How to Choose

The concepts underlying Line Security are relatively simple and straight forward — check-in often, detect and annunciate surreptitious attacks in real time.

Line Security Rated equipment can be

configured to detect attack straight out of the box; a user pays for the capability as part of the product price. However, the cost of check-in frequency depends on carrier pricing plans and can change as newer technologies and/or pricing models are introduced.

When requirements were first developed, telecommunications systems were much simpler and limited in variety. Consensus among UL Standard stakeholders, that balanced risk with available technology and costs, established the 200 second check-in frequency for commercial burglar alarm systems.

As telecommunication technologies have evolved, the 200 second check-in frequency requirement became difficult to do at reasonable cost. In response, the industry developed systems that utilize multiple communication paths and support less frequent check-ins. These types of systems still maintain a high level of communication resiliency, due to the use of multiple communication paths, but can reduce the long term telecommunication costs associated with frequent check-ins.

That cycle of innovation has occurred several times and is reflected in the set of Line Security options recognized in today's UL Standards. The cost effectiveness of some of these configurations depends on the telecommunication provider's pricing plans. In general, the configurations offer reduced check-in times for additional ('back-up') communication paths. Selecting an appropriate arrangement is about balancing the level of risk against the total cost of ownership, which would include the options available from both your security and communications service providers, as well as any consequences of false alarms in your community.

Line Security

When working with your alarm service provider, be sure that your expectation of receiving Line Security service is specified in your contractual agreements. Most contemporary commercial security systems can be configured or programed to provide Line Security, but that Line Security configuration is generally not the default mode. The system will need to be programmed appropriately by your installation technician.

UL Standard requirements call for annual or more frequent inspection and testing by your service provider. Asking your technician to verify Line Security during each inspection can help to provide added assurance that your expectations are being met.

Communication Method Options

Communication method options for Line Security are described in the UL Standard UL 681, The Standard for Installation of Burglar alarm Systems. A UL Listed alarm service provider will be familiar with UL Standards and can help clarify requirements to help ensure the choice you make meets your needs and expectations.

The following descriptions start with the Single Path configuration, a simple arrangement that forms a baseline which can be added to for increased security.

Single Path

Control unit   Transmitter   Communication cloud

(Boundary of the protected property)
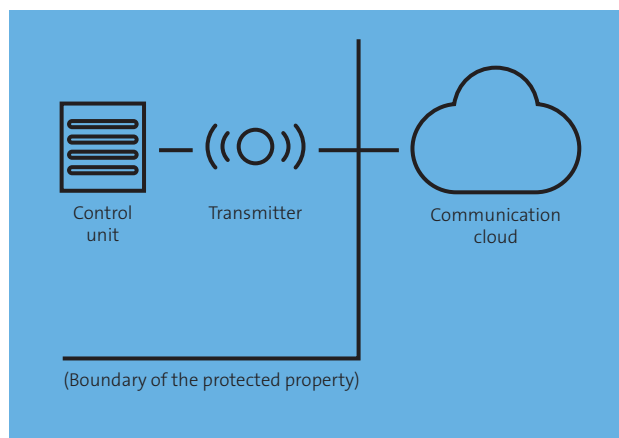
Single path Line Security requires a communication technology that can support the required 2-way communication protocols and have sufficient bandwidth to check-in with the monitoring center every 200 seconds. Both wired and wireless data networks can generally support Line Security. The public switched telephone network, used by auto-dialers (DACTs), cannot.

The use of a single path can help to minimize communication costs, however, the arrangement is more susceptible to network interruptions. If a network interruption occurs while the alarm system is armed, the monitoring station is required to treat it as an 'intrusion in progress' and initiate the proper protocols. In many cases, this would mean dispatching law enforcement, which brings the risk of false alarm fines or other local measures/penalties.

Pros:
- Minimizes initial cost of equipment and cost of maintenance

Cons:
- Lack of a backup communication path in the event of a network interruption

In some cases, the alarm system subscriber could end up paying multiple false alarm fines or other penalties, negating the cost savings of this option.

Dual Path

Control unit   Modem*

DACT

(Boundary of the protected property)

Communication cloud
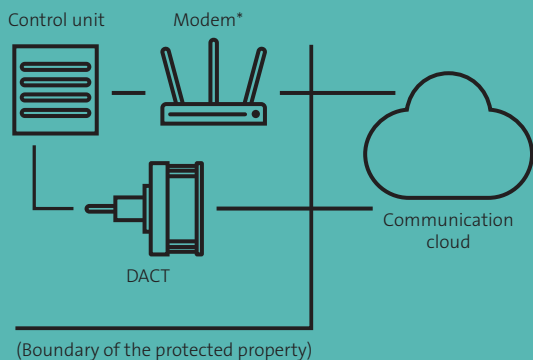
A dual path system uses a communication path that supports the required 2-way protocols as its primary means of communicating to the monitoring station (the modem line in the above illustration). It also uses a second communication path as a secondary means of communicating. The secondary path is not required to support Line Security and is typically a phone line (10 digit dial-up number, voice grade, wired or wireless).

This configuration may help reduce communication costs in situations where communication costs are bandwidth sensitive. Providing a dual path reduces the frequency of required check-ins on the primary path from once every 200 seconds to once every 360 seconds. Check-in on the secondary path is only once every 24 hours.

In a Dual Path system, a communication failure on the primary path results in a signal being transmitted on the secondary path. If this event happens when the system is armed, it would be handled as an alarm signal. If the system is unarmed, it would be a trouble signal and a service technician would be dispatched.

Until the primary path is restored, the alarm system would still be able to communicate via the secondary path, but in a degraded, non-line security mode.

Pros:
- In the event of a communication failure on the primary path, the signal is transmitted on the secondary path (back-up). This signal is treated as a trouble signal if the system is unarmed, which results in the dispatch of a service technician, rather than the local law enforcement.
- May help reduce communication costs in situations where communication costs are bandwidth sensitive
- Reduces the frequency of required check-ins on the primary path from once every 200 seconds to once every 360 seconds; check-in on the secondary path is only once every 24 hours

Cons:
- Initial installation costs for two communication paths
- Until the primary path is restored, the alarm system would still be able to communicate via the secondary path, but in a degraded, non-line security mode

Alternate Primary Path

Alternate primary path employs two communication channels, both of which support the required 2-way communication protocols and have sufficient bandwidth to check-in every 200 seconds. Use of a wired and wireless technology reduces the risk of total communication interruption in the event of outage on one of the communication networks.

Alternate Primary Path systems can reduce the risk of unnecessary law enforcement dispatch in the event of interruption of the preferred communication path. These systems monitor communication path integrity and if the

Control unit   Wireless data network

Modem*

Communication cloud

(Boundary of the protected property)
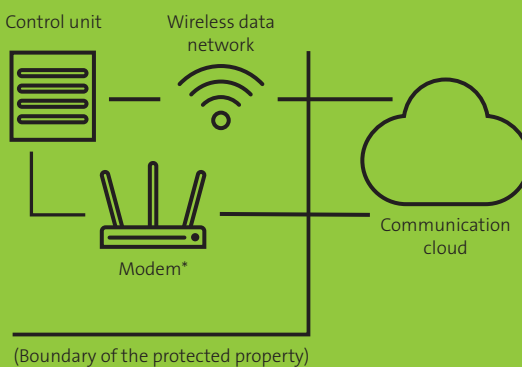
preferred path is not available, can switch to the other path quickly enough to check-in with the monitoring station on schedule. Under these conditions:
- The monitoring station does not treat the signal as an alarm and law enforcement dispatch is not required
- Line Security service is still in place - although until full communications are restored, it is of the Single Path variety
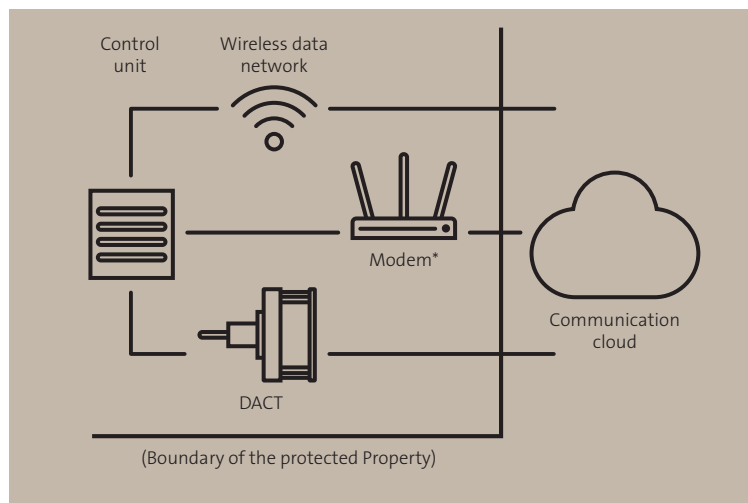
Pros:
- Use of a wired and wireless technology reduces the risk of total communication interruption in the event of outage on one of the communication networks
- can reduce the risk of unnecessary law enforcement dispatch in the event of interruption of the preferred communication path
- Consistent Line Security Service, even if the preferred communication path is interrupted

Cons:
- Cost of equipment
- Costs associated with check-ins

Alternate Primary with Dual Signal Path

Control unit
Wireless data network
Modem*
DACT
Communication cloud
(Boundary of the protected Property)

Alternate Primary with Dual Signal Path configuration provides the highest level of resiliency currently described in UL Standards. It uses two communication paths both of which support the required 2-way communication protocols. The third path is not required to support the required 2-way protocols, and is typically a phone line.

The addition of a third path reduces the required check-in frequency on the Line Security path in use from once every 200 seconds to once every 360 seconds. Check-in on the 3rd path is once every 24 hours.

Pros:
- Provides the highest level of resiliency currently described in UL Standards
- The addition of a third path reduces the required check-in frequency on the Line Security path in use from once every 200 seconds to once every 360 seconds
- Check-in on the third path is once every 24 hours

Cons:
- Cost of equipment
- Telecommunications cost for 3 lines

To learn more about UL's Fire and Security Solutions program, please visit UL.com/AlarmService or contact alarmservice@UL.com.

Empowering Trust™