Alarm Confirmation, Verification and Notification Procedures

TMA CS-V-01-2022 (Version April 01, 2022)

Sponsor
The Monitoring Association (TMA)

Left Intentionally Blank

Printed in the United States of America

Published by

The Monitoring Association

7918 Jones Branch Drive, Suite 510, McLean, VA 22102

www.tma.us

Table of Contents Page

Foreword

This standards document is published by the The Monitoring Association (TMA) and was developed and adopted by a consensus of industry volunteers in accordance with TMA's standards development policies and procedures.

TMA assumes no responsibility for the use, application or misapplication of this document. Industry members using this document, particularly those having participated in its development and adoption, are considered by TMA to have waived any right they might otherwise have had to assert claims against TMA regarding the development process of this standard.

TMA reserves the right to revise this document at any time. Because TMA policy requires that every standard be reviewed periodically and be revised, reaffirmed, or withdrawn, users of this document are cautioned to obtain and use the most recent edition of this standard. Current information regarding the revision level or status of this or any other TMA standard may be obtained by contacting TMA.

Requests to modify this document are welcome at any time from any party, regardless of membership affiliation with TMA. Such requests, which must be in writing and sent to the address set forth below, must clearly identify the document and text subject to the proposed modification and should include a draft of proposed changes with supporting comments. Such requests will be considered in accordance with TMA's standards development policies and procedures.

Written requests for interpretations of a TMA standard will be considered in accordance with TMA's standards development policies and procedures. While it is the practice of TMA staff to process an interpretation request quickly, immediate responses may not be possible since it is often necessary for the appropriate standards subcommittee to review the request and develop an appropriate interpretation.

Requests to modify a standard, requests for interpretations of a standard, or any other comments are welcome and may be sent to:

The Monitoring Association
7918 Jones Branch Drive, Suite 510
McLean, VA 22102
Tel: 703-242-4670
email: Membership@tma.us

Acknowledgements

TMA Standards Chairman: Glenn Schroeder, NetOne International

TMA Staff Administrator: Celia T. Besore, Executive Director, TMA
Bryan Ginn, Information Systems Mgr., ASAP Svc. Mgr.

Sub-committee Membership 2020

Louis T. Fiore, Sub-committee Chair
Robert Bonifas, ADS Alarm of IL
Robert Bean, Alert Alarm of Hawaii
Heather Peterson, COPS Monitoring
Larry Dischert, Johnson Controls, Inc.
Peter Giacalone, Giacalone Associates, LLC
Mark McCall, Stanley Security
Larry Folsom, I-View NOW
Anita Ostrowski, Vector Security
Glen Schroeder, NetOne, Inc.
Steven Schmit, UL, LLC.

Sub-committee Membership 2022

The Monitoring Association UL-Subcommittee

This standard was approved by the Security Industry Standards Council in March 2022

Revision History:

Original Version 2004

Revised-New Edition 2016

1) Reorganized to include CS-V-01, CS-V-02 and CS-AUD-01
2) Minor modifications
3) Minor clarifications

Revised-New Edition 2020

1) Major changes in support of smart devices.
2) Language modified in recognition of today's many communications methods.
3) Language modified to align with law enforcement's recognizing resolutions
4) Minor clean-ups.

Revised-New Edition 2022

1) Modify to Remove the General Prohibition of a NRTL System Being Treated Differently
2) Minor typo’s

Introduction

This standard has been prepared under the direction of the Security Industry Standards Council (SISC) members with the participation of The Monitoring Association (TMA) members, Security Industry Association (SIA) members, Electronic Security Association (ESA) members, ASIS members and the Canadian Alarm Association (CANASA) members. This standard is to be used by alarm monitoring facilities and by state and local units of government in their development of consistent administration criteria for alarms. New technologies and successful efforts to reduce false alarms have led to this standard. This standard, adopted by the various states and local units of government, recognizes the lifesaving benefits monitored security and fire alarm systems provide. The intent of this standard is to achieve increased efficiencies by reducing costs and eliminating wasteful efforts associated with potential false notifications.

Alarm Confirmation, Verification and Notification Procedures

1. Scope

This standard defines methods by which notifications for signals received from security systems that are eventually classified as false alarms can be greatly reduced. It has been proven that confirming and verifying an alarm signal by a supervising station will drastically reduce false alarm notifications. This standard takes confirmation to its next level by defining multiple attempt confirmation, biometric, audio and video confirmation.

Additionally, beyond the use of confirmation in standard or basic security systems, this document defines methods by which it can be determined an unauthorized activity is in progress and cannot be identified, thus false alarm notifications can be greatly reduced. Supervising station's customers, that use video and audio technologies to assess that unauthorized activity is possible, helps law enforcement to prioritize their resources and drastically reduce false alarm notifications. This standard takes verification to its next level by defining audio and video verification techniques as well as multiple attempt confirmation and multi-trip notifications.

"Methods defined herein have been tested and proven to achieve higher apprehension rates[1] and lower levels of false alarm notifications. Further reduction is possible to achieve using a combination of the methods defined herein."

Actions related to commercial and residential fire alarm systems, are found in NFPA 72.

[1] Police Chief Magazine March 2012 and SDM Magazine June, 2012

1.1. General

1.1.1 If differences exist between this document and other Special Instructions with the monitored premises, the Special Instructions shall take precedence.

1.1.2 If a Notification was made and subsequent information indicates no emergency exists, contact shall be made to the emergency agency in an attempt to cancel their response.

1.2. Exceptions

1.2.1. Signals received from systems that are approved under the listing(s) that follows, shall be handled in accordance with the procedures defined within the applicable standard.

1.2.1.1. UL Standard for Safety for National Industrial Security Systems, UL 2050

1.2.1.2. Standard for Signal Receiving Centres Configurations And Operations, ULC S301

1.3. Definitions

1.3.1. * Alarm Abort

The process that an alarm company shall consider the receipt of an "Authorized user", "Automatic cancel", " "Abort", "User cancel," or "Opening" signal from the alarm system as valid authorization and will not be required to make a Notification.

1.3.2. Alarm Confirmation

Alarm confirmation is a generic name given to many techniques used (1) to permit authorized personnel to appropriately identify themselves, thereby preventing emergency response agencies from being requested to respond to situations that do not represent an emergency; and (2) to confirm or deny the validity of alarm signals received at a supervising station.

1.3.3. Alarm Verification

Alarm verification is a generic name given to techniques used to determine whether or not suspicious and unauthorized activity is occurring, and to confirm or deny the validity of alarm signals received at a supervising station.

1.3.4. Answering System

A mechanism that will answer incoming calls and will then instruct callers to leave a message. It records the message from the caller, typically keeping track of the exact date and time of each.

1.3.5. Archived Video

Video images that have been recorded and stored for later viewing.

1.3.6. Audio Device

Mechanism that produces or hears sounds

1.3.7. Audio Verification Types

An event activated method that provides recorded audio associated with alarm activation and/or live real time audio from the protected premises to the supervising station that enables the monitoring company to verify whether activity is occurring that appears to warrant the immediate emergency response of responding agencies.

1.3.7.1. Listen-In

An audio device capable of being activated by the initiation of another security device. A one-way audio feed will be available to the supervising station when a device such as a hold-up button, audio detector or door contact has come into alarm. (See 1.2.6)

1.3.7.2. One-Way Audio

One- way audio is the term commonly referred to when a mic or microphone is installed at the protected premise. A microphone is a device that converts sound into an electronic signal. A signal accompanied by audio, when accessed by the operator, will assist him or her to better determine if an individual is present at a protected premise. (See 1.2.6)

1.3.7.3. Two-Way Audio

An event driven, two-way, hands free communications session at the premise with the supervising station caused by the activation of an alarm event at the premise for the purpose of verifying the validity of an alarm condition and/or gain additional information regarding the cause of the condition.

1.3.7.4. Impact Activated Audio

An audio device capable of being activated by the sounds of an intrusion or unauthorized entry. The audio device after activation will cause the control panel to contact the supervising station and provide the premise sound

1.3.8. Call Back Mode

The state of readiness, by an audio verification system, .to permit a two-way voice interval.

1.3.9. Captured Video

Captured Video is associated video information aligned with the alarm event and/or identified by the supervising station personnel while viewing video. Examples include the following: the presence of video aligned with the alarm, the identification of a human or humans, or any other information germane to the alarm scene (broken window, smashed door, or other physical characteristics) at the time of the alarm event.

1.3.10. Capture Mode

The means of the audio verification system holding the communication path open after the communication device has received an acknowledgment from the supervising station.

1.3.11. Code

Code as applied within this standard is used to identify a person on the other end of a verbal conversation or verified electronic receipt of a personal identifier as being valid. Code can be anything that uniquely assures the person seeking the identity of the individual at the other end, is in fact, the individual they are claiming to be.

1.3.12. Confirmation Methods

1.3.12.1. Electronic

An electronic signal transmitted to the supervising station that indicates to its personnel or to its notification computer that no emergency appears to exist or confirms that an emergency does exist.

1.3.12.2. Verbal

A personal contact by means of telephone or audio conversation with an authorized code holder or other authorized person for the protected premises to confirm that no emergency exists.

1.3.12.3. Video

An electronic picture, pictures or images viewing an area of the protected premises from which an alarm signal has been received which permits supervising station personnel to view the area which has an alarm to confirm suspicious and unauthorized activity is occurring.

1.3.13. Confirmation Types

Two broad forms of confirmation may be employed. These include:

1.3.13.1. Standard Confirmation

Standard confirmation is the attempt by supervising station personnel to confirm that an emergency does not appear to exist at the monitored premises, by means of a telephone call, voice contact or other electronic means.

1.3.13.2. Enhanced Confirmation

Enhanced Confirmation is the attempt by supervising station personnel to confirm that no emergency appears to exist at the monitored premises by means of more thorough procedures such as two (2) or more investigative phone calls, Data Message other means or a combination of these procedures. (Formerly known as ECV)

1.3.14. Data Message

Any form of electronic communication that conveys an appropriate message. (Examples would be, texting, recorded messaging, email, push notification, and the like)

1.3.15. Discernible Image

A video picture, still or live, that supports being able to accurately view and identify objects within the camera's view

1.3.16. Dispatch

Notification (See 1.3.19 below) of a law enforcement agency, a guard, guards, a runner, multiple runners, other response entities or predetermined combination of the above to respond to the premises.

1.3.17. Interactive Audio/Video System (Interactive A/V)

A security system, that by design, when an alarm occurs, is both an audio and a visual (video) interface with the protected premises.

1.3.18. Multi-Trip (MT)

The application of redundant detection devices such that one motion detector or one photo-electric beam paired with some other device such as another motion detector, photo-electric beam, door contact or door contacts, to cover generally the same area. An alarm is recognized when both detectors in the pair are triggered within a predetermined. defined period of time

1.3.19. Notification

A call or Data Message to the law enforcement authority, such as 911 or the telephone number used to reach the responding law enforcement agency.

1.3.20. Notification Cancel

The process that may occur after the contacting authority is complete and the supervising station learns that the alarm is false and notifies them.

1.3.21. Security Device

Hardware that detects a change in a protective status such as a motion detector, video camera, door contact, or other sensor.

1.3.22. Special instructions

Separate documented directions, from the monitoring contract document, that specifies a specific set of instructions to be followed in the event of an alarm, between the monitored premises and the supervising station.

1.3.23. Supervising Station

A facility that receives signals from protected premises alarm systems and at which personnel are in attendance at all times to act upon to these signals

1.3.24. Verified Alarm (VA)

Is the result of alarm verification procedures, which indicate to an operator who, sees, hears or otherwise confirms, with a degree of certainty, there is suspicious and unauthorized activity.

1.3.25. Video

Video Information that is available at the time an alarm event was annunciated by the alarm system control unit.

2. Standard Confirmation Procedures for Burglar Alarm Signals

2.1. Procedures for Alarm Signals

2.1.1. * Initial Attempt

Unless Special Instructions exist, supervising station personnel shall attempt to reach designated contacts for identification and confirmation of persons authorized to be on the customer's premises.

2.1.2. If No Contact

If there is no response, the supervising station personnel shall make a Notification, unless the supervising station personnel have reason to believe no emergency exists.

2.1.3. If Attempt is Answered

If the attempt is answered, the supervising station personnel shall obtain a code that the person is authorized to be on the premises. Upon receipt of correct identification, and the authorized person states that no emergency exists, responding entities shall not be notified or shall be recalled, if already notified, and the alarm is considered aborted.

2.1.3.1. * No Code

If no code or authorization is provided, the supervising station personnel shall attempt to reach an authorized person off premises to confirm the authenticity of the on-premises person, and failing that shall make a Notification. Further explanatory material on this can be found in Annex A.

2.1.3.2. * Wrong Code

If the person(s) contacted cannot be identified by a valid identification code within a reasonable time after the contact as defined in 2.1.3, the supervising station personnel shall make a Notification.

3. Enhanced Confirmation of Burglar Alarm Signals

3.1. Procedures for Alarm Signals

3.1.2 Procedure

For security systems signals received from non-certificated commercial systems or any residential system, the following procedures shall be followed.

3.1.2.1 Initial Attempt

The supervising station shall attempt to obtain confirmation by contacting the protected premises after receipt of the alarm signal. The procedure defined in 2.1.3 above shall be followed if the premises attempt is answered. Otherwise proceed to 3.1.2.2 or 3.1.2.3 whichever is applicable.

3.1.2.2 Second Attempt to the Premises

When supervising station personnel get a busy signal or no response on the first attempt to the protected premises, a second attempt(s) shall be made to an alternate at the protected premises when such is available. The procedure defined in 2.1.2 above shall be followed.

3.1.2.3 Second Attempt, Other Than Premises

When supervising station personnel have no response on the first attempt to the protected premises, a second attempt shall be made by an alternate means or number to contact an authorized person.

3.1.3 Alarm Abort

The Alarm Company shall consider the receipt of an "Authorized user", Automatic cancel", or "Abort" signal from the security system as validation that no emergency exists and Notification shall not occur.

3.1.4 Answering System

Each supervising station shall establish written procedure to be followed when an answering system is encountered as to whether or not to leave a message, including the message content.

3.1.5 Scheduled Events

If an alarm signal is received in connection with a scheduled opening or closing event, additional attempts shall be made to the call list in order to determine whether the alarm signal is caused by an opening or closing error. If there is no response or no determination can be made that a false alarm exists, a Notification shall occur.

3.1.6 Confirmed False

If the alarm is confirmed as being false during the first or second attempts, supervising station personnel shall suspend activities relating to the specific signal being worked.

3.1.7 Use of Call List

Following the Notification, attention shall be placed on contacting the emergency call list, to achieve a cancellation of the Notification if it is then determined that no emergency exists.

4. Standard Audio Verification Procedures for Burglar Alarm Signals

4.1. Procedures for Alarm Signals

4.1.1. If the cause of the alarm cannot be determined through the use of pre-recorded or live audio received from the protected property, and in the absence of special instructions to the contrary, the supervising station personnel shall communicate with the protected property through the use of the audio verification system to attempt to determine if authorized persons are present. If authorized persons are not determined to be present, it shall be treated as a verified alarm.

4.1.2 Personal engaged in audio verification shall be trained in the practice.

4.2. Two-Way Audio Verification

To ensure all reasonable efforts are expended in attaining a confirmation of an alarm condition and avoiding the necessity for a notification the following best practices shall be carried out:

4.2.1. Initial Verification Session

Upon receipt of an alarm condition the supervising station operator will initiate the audio session via capture mode, call back mode or impact activated audio according to the manufacturers stated command set Upon initiation the supervising station operator will challenge the user on the premises for a valid code. Upon acknowledgment of valid code, alarm notification will be avoided and the supervising station operator can continue to communicate with the verified, valid user on premises.

4.2.1.1. If No Contact

If there is no response or non-communication with the premises via the two-way audio session, the supervising station personnel shall make a second attempt, using an alternate method, and if the authorized person states that no emergency exists, responding entities shall not be notified or shall be recalled. The operator will disconnect the two-way audio session via manufacturers stated command set.

4.2.1.2. *Wrong Code

If communication is established with the premise and a valid code is not communicated by the person (s) on premise via the two-way audio session, the operator will disconnect the two-way audio session via

manufacturers stated command set. Upon proper termination the operator will notify the responding agency.

4.2.2. If Audio Communication is Established

If contact is made, the supervising station personnel shall obtain a code that the person is authorized to be on the premises. Upon receipt of correct identification, and the authorized person states that no emergency exists, responding agencies shall not be notified or shall be recalled, if already notified, and the alarm is considered aborted.

4.2.2.1. *No Code

If no code or authorization is provided, the supervising station personnel shall attempt to reach an authorized person off premises to verify the authenticity of the on-premises person, and failing that shall make Notification.

4.3. Listen-In One-Way Audio Systems

The general purpose of this technology and service is to allow the supervising station to gain additional information from the protected premise on certain alarm conditions that are not verified conditions.

4.3.1. Alarm Processing Session

4.3.1.1. Upon receipt of an alarm condition the supervising station operator will initiate the audio session according to the manufacturers stated command set.

4.3.1.2. Upon initiation the supervising station operator will be in a “Listen Only” status and will not communicate with the premise and will continue to maintain the “Listen In” session.

4.3.1.3 Should the operator, listening to the premises, hear a valid code, an effort to cancel or abort Notification will be attempted.

4.4. Enhanced Audio Verification of Burglar Alarm Signals

4.4.1. Procedures for Alarm Signals

4.4.1.1. Procedure

For burglary alarm signals received from commercial burglary security systems or residential security systems, the following procedures shall be followed.

4.4.1.1.1. Audio Verification Session - Attempt #1

The supervising station shall attempt audio confirmation with the protected premises after receipt of the alarm signal. The procedure defined in 4.2.2 above shall be followed if audio contact is made with premises. Otherwise proceed to 4.5.1.3.2.

4.4.1.1.2. Audio Verification Session - Attempt #2

When supervising station personnel cannot attain contact or confirmation during the first attempt to the protected premises, a second attempt shall be made to an alternate phone number(s) such as a premise, cellular or work number and if the authorized person states that no emergency exists, responding entities shall not be notified or shall be recalled, if already notified, and the alarm considered aborted.

4.4.1.2. Compliance with Enhanced Confirmation

4.4.1.2.1. The Audio verification procedure defined in **Error! Reference source not found.** shall be in compliance with section 2 Standard Confirmation Procedures for Burglar Alarm Signals

5. *Standard Video Verification Procedures for Burglar Alarm Signals

5.1. Procedures for Alarm Signals

5.1.1. *Video Verification Procedures

5.1.2. Upon receipt of an alarm activation the operator shall review any special instructions, and where they apply to the alarm activation, and follow as required.

5.1.3. Based upon the image(s) contained within the video presented, the operator shall select one of the following:

5.1.3.1. Follow the appropriate subsection within section 3. Enhanced Confirmation of Burglar Alarm Signals. and/or:

5.1.3.2. Proceed with analyzing the image(s) presented and determine which of the categorizations applies as enumerated in section 5.1.5

5.1.4. Upon completing the steps within 5.1.2 and no determination reached, the operator, shall view any Captured Video Information (video clip(s)) attached in order to determine if the video contains discernible human image(s).

5.1.4.1. At any time within this section, if the operator determines, that communications with the subscriber is appropriate, he/she may do so.

5.1.4.2. * If there is no discernible human activity, or if there is evidence of recent human activity, contained in the clip the operator shall attempt to access the video alarm system.

5.1.4.2.1. Upon accessing the Video System, the operator shall view live video. If live video does not indicate a discernible human image, then the operator shall view archived video if available.

5.1.4.2.2. If the Video System cannot be accessed or if upon access no discernible human image is seen, then the alarm shall be handled as indicated in section 5.1.5.

5.1.4.3. If the initial video contains a discernible human image(s), then the operator shall determine which of the two choices applies:

5.1.4.3.1. If human activity is observed or if there is evidence of recent human activity, then the operator shall handle the alarm as indicated in the choices within section 5.1.5.

5.1.4.3.2. If no current or recent human activity is observed, then the operator shall handle the alarm as indicated in the choices within section 5.1.5.

Note: Personal engaged in video verification, shall be trained in the practice.

5.1.5. Categorization and Notification

5.1.6. Upon the completion of the steps within 5.1.1 Video Verification Procedures the operator, with the knowledge developed during those steps, shall select the appropriate categorization l as listed below:

5.1.6.1. No human activity is apparent and supervising station personnel have been unable to contact the subscriber. An alarm has been received along with video images of the area where the alarm occurred. There are no human images seen and several

attempts have failed to contact the subscriber.

5.1.6.2. No human activity is apparent, but supervising station personnel have been able to contact the subscriber who indicates no-one is expected to be there. An alarm has been received along with video images of the area where the alarm occurred. There are no human images seen and attempts have verified that the subscriber is not present nor expects someone to be present.

5.1.6.3. A human(s) is present, or there is evidence of recent human activity, but unable to be identified, and supervising station personnel have not been able to contact the subscriber. An alarm has been received along with video images of the area where the alarm occurred. There are human images seen, but several attempts have failed to have someone on the premised answer and there has been no answer(s) to other attempted contacts.

5.1.6.4. A human(s) is present, or if there is evidence of recent human activity, but unable to be identified. and a contact with the subscriber indicates no-one is expected to be there. An alarm has been received along with video images of the area where the alarm occurred. There are human images seen, but no one answered at the premises and attempts to other subscriber locations have resulted in being informed that no one is expected to be on the premises.

5.1.6.5. No human activity is apparent and non-human activity appears to have caused the signal. The image being viewed clearly shows what caused the signal to be transmitted, but there is no threat to the premises.

5.1.6.6. A human(s) is present, and there is suspicious activity occurring. Upon viewing the image, it is clearly being demonstrated that the action, taking place, is suspect.

Once the appropriate categorization has been chosen, notification shall be done using the descriptions as documented within the categorizations above.

5.2. Interactive A/V

Follow the processes found in section 4.1 Procedures for Alarm Signals and 4.2 Two-Way Audio Verification, while being aided by the data and information, that is presented by the video images

6. Smart Device Alarm Verification

When an alarm system supports smart device interfacing and the subscriber has chosen to use their smart device for signal verification the following shall be the method implemented.

6.1. Signals normally requiring supervising station action (alarms, supervisory, and trouble).

6.1.1. These types of signals shall first be transmitted to the mobile device or as a result of the central station automation system, to the mobile device.

6.1.1.1. The smart device and alarm system shall start a “count-down” of an amount of time agreed upon between the subscriber and the supervising station.

6.1.1.1.1. Should the “count-down” period end and no action has been taken by the subscriber, the signal, shall be processed by one of the following procedures;:.

a) Where the use of smart verification is known to the supervising station, the operator shall proceed with Notification

b) Where the use of smart verification is not known to the supervising station, then the operator shall proceed with Verification.

6.1.1.2. The subscriber shall take whatever action(s) they choose and when they have completed their analysis, they shall inform the supervising station of the action to be taken.

6.1.1.3. If the subscriber determines the supervising station should take action, the supervising-station shall be notified immediately and take appropriate action for the signal received.

6.1.1.4. If the subscriber determines that no action is needed, no further activity shall occur.

6.2. Signals not normally requiring supervising-station action (arming, disarming, bypassing, etc.)

6.2.1. These types of signals shall be transmitted and recorded as agreed upon between the subscriber and alarm company.

7. Additional Confirmation and Verification Factors

7.1. Answering Systems

Each supervising station shall establish written procedure to be followed when an answering system is encountered as to whether or not to leave a message, including the message content.

7.3. Verified False

If the alarm is verified as being false during the first, second or succeeding attempts, supervising station personnel shall suspend activities relating to the specific signal being worked.

7.4. Use of Call list

Following the Notification, attention shall be placed on contacting the entire emergency call list, to achieve a cancellation of the Notification if it is determined that no emergency exists.

7.5. Notification Cancel

After Notification, the alarm company shall continue the effort to contact the remaining designated persons on the emergency call list and upon contact and upon learning that the alarm is false update the AHJ with a “cancel” Notification unless modified by Special Instructions.

7.6. Unexpected Openings/Closing

Conditions considered as Unauthorized Opening, Late to Open or Late to Close shall not be considered as alarm conditions and no Notification shall occur unless verbally requested to do so at the time of the event by a designated emergency contact or unless modified by special instructions.

8. Multiple Trip Procedure

Multiple Trip (MT) can be accomplished in two ways:

8.1 One alarm signal from multiple sensors:

8.1.1. Multiple independent sensor trips are analyzed on site by the alarm system and a single MT signal (identified as such on the operator's terminal) is sent to the supervising station.

8.1.2. When the MT alarm is received, the supervising station operator immediately initiates the Enhanced Confirmation procedure.

8.1.3. At the conclusion of the Enhanced Confirmation procedure, if a need for police response is determined, the operator shall notify the responding agency, that multiple trips occurred and that the Enhanced Confirmation procedure was followed.

8.2 Two alarm signal

Multiple alarm signals from more than one sensor(s) at the same building, structure or area within a building or structure are received at the supervising station.

8.2.1. The supervising station operator initiates the Enhanced Confirmation procedure immediately after the first of the two signals has been received.

8.2.2. When a second alarm signal from a different sensor is received from the same location during the Enhanced Confirmation procedure, and if a need for response is determined, the operator shall notify the responding agency, that multiple trips occurred and that the Enhanced Confirmation procedures were followed.

9. Hold-Up

9.1 Hold-Up Alarm

Unless otherwise noted by Special Instructions, the supervising station shall not attempt any verification but shall first make a Notification to allow emergency responders to investigate the protected premises prior to any attempts of communicating with the customer.

9.2 Residential Panic/Duress/Emergency Alarm

The supervising station shall follow the Standard Confirmation Procedures as defined in section 2.0.

Annex A (Informative)

A.1.2.1 The supervising station can receive alarm abort or cancel signals and or messages in multiple ways. Intrusion, video systems, cloud-based solutions can successfully and reliably transmit this information to a supervising station using email or some form of electronic notification. When one of these methods is received by the supervising station as valid authorization. With this information, the supervising station can complete the signal and additionally related signals to avoid initiating a notification. If a notification has been made prior to receiving the abort or cancel, the supervising station should contact the responding agency to cancel the need for a response.

A.2.1.1., 2.1.3.1., 2.1.3.2., 4.2.1.2, & 4.2.2.1 If the supervising station personnel reach the protected premises on the first or second call and the person answering the phone does not have the proper code then, if possible, the personnel may attempt to make a 3-way call with the premises person retained as a party to the call. The supervising station personnel may attempt to reach others on the call list to confirm the authenticity and authorization of the person on the protected premises. If this process fails to resolve the issue then the supervising station personnel should follow any special instructions if present and/or proceed to make a Notification.

A. 2.1.1 and 3.2 Premises Confirmation Phone Accessibility Guideline
Care should be taken to verify that the phone line(s) used by the digital communicator do not have a call waiting feature, or alternately that *70 is programmed in front of the supervising station receiver phone number(s). The confirmation phones at the protected premises should be accessible after hours in the vicinity of commonly used entrances and not be locked up in an office, or have inbound calls sent to voice mail after hours. This is so the after-hours users and cleaning people can hear and answer the confirmation phone call made by the monitoring facility personnel.

A. 5. Monitoring Facilities Video Availability
It is recommended that the Captured Video be transmitted and available to the supervising station when the alarm event is transmitted. The alarm event and captured video do not need to be transmitted over the same medium. For example, it may be transmitted via an Internet feed. The supervising station personnel shall have the Captured Video presented in a manner that is easily accessible

A 5 Video Verification
Video verification adds complexity to the operators' response. Because someone is present in a live or recorded video clip does not mean a crime has occurred. A large percentage of false alarms are caused by employees or family members entering a protected premise or property. To simplify an operator’s response, it is recommended that a supervising station classify areas when providing video verification/ video monitoring services. It is best that for this purpose of this technique, the phrase “secure area” and an “unsecure “area“ be referenced. Where possible provide instructions for each area so an operator has a clear understanding while viewing the video camera.

SECURE AREA
A secure area is to be entirely enclosed on all sides by walls or fences that are secured and lockable. All the walls, fences and gates should be of an adequate height and of a robust enough construction to require any individuals who enters without authorization to make purposeful actions to gain entry. If a wall or fence can be easily stepped over or scaled, then the area should not be considered a secure area.

UNSECURE AREA
An unsecure area is an area which is not entirely enclosed on all sides and allows individuals unrestricted access to the property.

DUAL SITE
Some protected premises may have areas that are both considered open and closed. Notating these areas during the initial contract negations is important, so the supervising station personnel know how to respond properly in each area.

Video verification/video monitoring are solutions that are both complimentary and often solve issue's that traditional intrusion systems can face. Understanding the purpose of why a video solution was installed should be understood by the supervising station and should be notated on the customer's account record. Examples include crowd control, theft, unauthorized entry, public safety, and vandalism.

When the supervising station views event video an operator should understand that the area is secure or unsecure. This information will aid the operator to respond to the event accurately. Also, having documentation that includes response instructions is recommended.

A.5 System Maintenance
Video verification/video monitoring requires the video system to be partly responsible for the operator's ability to respond appropriately to the received signal. Periodic maintenance should be provided to ensure the proper cameras operation. Examples: dirty camera lens or globe, IP address change, camera angle or tilt changes so the camera no longer covers the desired area.

A.5.1.2. During this upfront review, look for other means of verification, such as smart device.

A. 5.1.1 Examples
As an example, if the minimums are implemented, at least 5 frames of captured video spanning five seconds starting no more than 100 milliseconds after the actual alarm event will be captured and transmitted. Alternately, in applications where the time between alarm initiation and recording of the first of the required five frames cannot be assured to be within 100 milliseconds, then 5 (five) frames would be distributed over 5 (five) seconds 1 (one) second between full frames) with two frames containing pre-alarm video, the event frame being the third, and two frames of post event video

A 5.1.4.2
Efforts should be made to simplify the operator's ability to accurate determine is a person or persons is on the protected premise. If video analytics or AI are being utilized a visual indication should be displayed in the video event allowing the operators attention to be drawn to the specific area that generated the event.

When utilizing an intrusion detector with video verification it is required that the video cameras field of view overlooks the entire detection pattern to ensure the supervising station personnel can accurately determine if a person is present at the time the signal was generated. When using intrusion detection with video verification, efforts should also be made to draw the operator's attention to the area of concern.

A. 5 Premises Camera Position
The camera should be placed to provide a clean view of the protected area. Care should be taken to avoid Cameras that can be repositioned for other purposes (ex. Review product displays or check customer traffic).

A. 5 Video Equipment Configurations
The type of camera, video transmission, placement of equipment and views provided by such video equipment may serve different multiple needs for the consumer. If determined by the consumer that a different configuration is desired, deviation from the placement and functionalities described in this standard should not prohibit the supervising station from utilizing such video information in its course of performing a Notification to the law enforcement agency if appropriate.

A. 5 Video Implementation Techniques
The quality of the video received shall be of a nature that a person will at a minimum, be able to decipher between a human and non-human based on the attributes of human form or any other information germane

to the alarm scene (broken window, smashed door, or other physical characteristics) at the time of the alarm event.

A 5 System Maintenance

Video verification/video monitoring requires the video system to be partly responsible for the operator's ability to respond appropriately to the received signal. Periodic maintenance should be provided to ensure the proper cameras operation. Examples: dirty camera lens or globe, IP address change, camera angle or tilt changes so the camera no longer covers the desired area.

.