PARTNERSHIP FOR Priority VERIFIED ALARM RESPONSE

Audio Verified Alarms
Best Practices

September 2022

PPVAR Audio Verification Committee

Table of Contents

PPVAR Audio Verification Committee

Participating Parties in Developing Best Practices

Security Industry

- Alarm New England
- Red Hawk Fire & Security
- Redwire
- Sonitrol of Lexington
- Sonitrol - Kimberlite
- Sonitrol Pacific
- Stanley Security
- Sureview Systems
- Sonitrol of Delaware

Law Enforcement

- Sheriff's Office – Kern County
- Phoenix PD, Arizona
- Sheriff's Office, Harris County, Texas
- Sheriff's Office, Story County, Iowa

PPVAR Audio Verification Committee
Recommendations for Audio Verification Standard for Burglar Alarms

1. Introduction

1.1. Positioning of PPVAR on Topic

2. Scope

2.1. This standard establishes the policies and procedures used by a central monitoring station:

- To assess audio sounds that originate from equipment used to form electronic security systems that are installed at protected properties in accordance with manufacturers' instructions;
- To gather related information regarding the protected property and its current state;
- To communicate information to law enforcement or other responders, when deemed appropriate.

The objective is to provide law enforcement with a minimum acceptable level of confidence that unauthorized activity is or has occurred at a protected property. The goal is that law enforcement will increase the priority level of response based upon the information provided by the central monitoring station.

2.2. This standard does establish criteria for the operability of the audio equipment that creates the audio used in verification, the manner in which it is assessed, and the manner in which the information is communicated to the responding entity while preserving the chain of evidence and protection of privacy issues.

2.3. The standard does not establish requirements for the installation of audio equipment used in verification beyond the manufacturer's instructions; nor does it establish requirements for the installation and operation of other electronic security equipment installed at a protected property.

2.4. This standard does not establish requirements for the use of alarm verification techniques such as electronic verification, enhanced call verification, and the like that are commonly associated with false alarm reduction programs, except as described in Section 6.

3. Glossary

General – The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. Merriam-Webster's Collegiate Dictionary, 11th edition, shall be the source for the ordinarily accepted meaning.

3.1. **Alarm Verification** – A generic name given to false alarm reduction 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 Central Station or monitoring facility.

- **Electronic Cancellation –** An electronic signal transmitted to the central monitoring station that indicates to personnel or to its dispatch computer that no emergency appears to exist.

3.2. **Alarm Event** – An event that is either initiated by the control panel at the premise or through the Central Monitoring Station automation programming indicating the need for further investigation.

3.3. **Archived Audio** - Audible sounds generated from a premise that have been recorded or stored for later listening.

3.4. **Audio Verification –** A method in which an audible sound that was captured at the same time an alarm event was detected by the alarm system control unit is compared with the signal(s) received form the alarm system to determine if a response to the protected property is required.

3.5. **Authority Having Jurisdiction (AHJ)** – An organization, office, or individual responsible for enforcing the requirements of Local laws and ordinances.

3.6. **Call lists** – A list of personnel associated with a protected property that are to be contacted in the event an alarm signal or other emergency event at the protected property is received in the central monitoring station.

3.7. **Central Monitoring Station (CMS)** – A building or distributed group of buildings or enclosed area within a building that houses an operating room and / or equipment used to provide monitoring service to protected properties.

3.8. **Dispatch (reference ANSI/TMA CS-V-01)** – Notification of law enforcement agency as defined in 3.4 or a guard, guards, a runner, runners, other response entities or predetermined combination of the above to respond to the premises.

3.9. **Emergency Response Agency** – Organizations providing law enforcement, emergency medical, fire, rescue, communications, and related support services.

3.10. **Enhanced Call Confirmation (ECC**) – Enhanced Call Confirmation is the attempt by monitoring facility personnel to verify that no emergency appears to exist, at the monitored premises, by means of procedures such as two (2) or more verification calls.

3.11. **Live Audio** – Audible sound that is presented to the central monitoring station operators for listening in near real time or real time.

3.12. Notification Call (reference ANSI/TMA CS-V-01) – The call to the law enforcement authority, such as 911 or the telephone number used to reach the responding law enforcement agency.

3.13. Public Safety Answering Point (PSAP) or Emergency Communications Center – A facility staffed with trained personnel that are responsible for answering calls to an emergency telephone number for police, firefighting, and Emergency Medical Services.

3.14. Scheduled Events – Openings, closings, or other such events that occur on a prearranged schedule.

3.15. Secured Area – An enclosed locked space without public access that has a sufficient perimeter to inhibit unauthorized entry which is protected by electronic security devices.

3.16. Shall – Indicates a mandatory requirement.

3.17. Should – Indicates a recommendation or that which is advised but not required.

3.18. Special Instructions – A written, separate document 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 alarm/monitoring company. This may also be made available to the operator on screen automatically on activation of the alarm. In no case shall special instruction violate local laws.

3.19. Threat Level – A numeric system by which the audio heard indicates the presence or lack of presence of human activity basis for the actions taken by an operator.

- **3.19.1. Threat Level 3** – Audio activity is heard indicating that a human is present, and suspicious or possible criminal activity is taking place, appears to have taken place or appears about to take place.
- **3.19.2. Threat Level 2** – Audio activity is heard indicating that a human is present but there is no discernable suspicious or criminal activity and no apparent criminal activity is about to take place.
- **3.19.3. Threat Level 1** – No audio activity is heard indicating that human activity is apparent.

3.20. Two Call Confirmation (TCC) – Two Call Confirmation is the attempt by monitoring facility personnel to verify that no emergency appears to exist, at the monitored premises, by means of procedures such as two (2) or more verification calls previously known as Enhanced Call Confirmation (ECC).

3.21. Unsecured Area – A non-enclosed space without a sufficient perimeter to inhibit unauthorized entry where entry by persons into the space is to be detected by electronic security devices. Once detected, the person's activity in the unsecured area is to be scrutinized by CMS personnel using audio, video, or other technology to determine if criminal activity is occurring or about to occur.

3.22. Common Area – An indoor unsecured space that is enclosed within a building without a secured perimeter that has public or limited access to persons at times when the rest of the building may be secure. Once detected, the person's activity in the common area is to be scrutinized by CMS personnel using audio, video, or other technology to determine if criminal activity is occurring or about to occur.

3.23. Verified Audio Alarm – An alarm signal that, through the use of audio technology, has been determined to require investigation by a designated organization such as law enforcement.

4. Training – Central Station

4.1. Central Station

4.1.1. The central station shall train and test their operators in accordance to the TMA Five Diamond Program, manufacturer certified training, state mandated training, or equivalent training sources for audio verification.

4.2. Training requirements

4.2.1. Training shall include general awareness and familiarization of the different audio threat levels.

4.2.2. Training shall include function-specific training for the different equipment being used for audio monitoring in the CMS.

4.2.3. Training shall include situational awareness and escalation procedures for the different audio threat levels.

4.2.4. Training shall include some type of exercise related to the material presented that requires the operator show proficiency with the subject matter.

4.3. Initial Training

4.3.1. A new employee, or employee who changes job functions, may handle audio alarms before completing training, provided:

4.3.1.1. The employee does so under the direct supervision of a properly trained and knowledgeable staff member; and

4.3.1.2. The training is completed within 90 days of employment or change in job function.

4.4. Periodic Training

4.4.1. Training and/or reference materials shall be made available at all times to the audio operators.

4.4.2. Periodic training shall be done with the introduction of new technology and as needed to meet any revisions in policies and procedures.

4.4.3. The training program shall be reviewed by the CMS with the introduction of new technologies, or the policies or procedures of the CMS change, or as it otherwise deems necessary to maintain relevant content.

4.4.4. Relevant training received from another source may be used to satisfy the requirements, provided a record of training is obtained from the other source and maintained as described in 4.5.

4.4.5. Training shall be provided to new operators or to existing operators as needed to maintain an adequate skill level.

4.5. Training Records

4.5.1. Shall include the employee's name.

4.5.2. Shall include the completion date of the most recent training.

4.5.3. Shall include as a minimum a description of the training materials (Copy, description, or location).

4.5.4. Shall include the name of the trainer.

4.5.5. Shall include any training credentials that the employee has been trained and tested.

Alarm Verification and Notification Procedures

5. Threat evaluation

5.1. The most important evaluation is at the listening of the initial audible sounds transmitted where an immediate decision is required as to whether possible criminal activity has

taken place, is taking place or is likely to take place.

5.2. The simple presence of a person at the premises does NOT constitute probable cause to believe a crime is in progress and thus does not warrant an elevated response by law enforcement. However, once the property owner or responsible party has been contacted through Enhanced Call Verification or calls to the party notification list and confirms that there should not be anybody there, then the presence of the person does constitute suspicious activity.

5.3. In cases where there is clear and evident knowledge that a crime is in progress an immediate dispatch should be made and all information available to the central station dispatcher should be relayed to the PSAP/Emergency Communications Center.

5.4. In instances where the audible sound(s) heard do NOT provide clear and evident knowledge that a crime is in progress verification processes as described in this document shall be performed prior to contacting the PSAP/Emergency Communications Center. At the time of dispatch the central station operator should explain all of the facts to the PSAP/Emergency Communications Center.

5.5. In instances where there is no audible representation of any human activation of the alarm signal, then NO reference of "audio alarm" activation or "audio alarm" should be made to the PSAP/Emergency Communications Center.

5.6. The level of information available to the monitoring personnel as to specific microphone or audio sensor location and what audio coverage area is must be as detailed as possible. Merely having audible sound(s) heard that indicates a person should never be the sole criteria for a dispatch. If there is no clear evidence that criminal activity is taking place then verification processes as described in this document shall be made prior to dispatch.

5.7. What must be done in all cases is to provide all of the evidence available to the PSAP/Emergency Communications Center operator and allow them to determine the level of response.

5.8. If additional information is received after the initial dispatch this information shall be forwarded to the PSAP/Emergency Communications Center.

6. Central Monitoring Station Actions

6.1. CMS audio alarm action steps defined

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

6.1.2. In no case shall special instruction violate local laws.

6.1.3. When special instructions are used, this information must also be told to the responding agency at the time of dispatch.

6.1.4. In each instance below the monitoring facility personnel shall listen to enough audio to make a reasonable determination at their sole discretion as to whether suspicious activity is occurring, or not.

6.2. Audio Verification Procedures

6.2.1. Upon receipt of an alarm activation from a Audio Alarm System the CMS operator shall listen any live or recorded audio information (audio clip(s))associated the event in order to determine if the audio heard is discernable.

6.2.1.1. If no audio is received or if there is no discernable activity contained in the

clip the CMS operator shall attempt to access the Audio Alarm System.

6.2.1.1.1. Upon accessing the Audio Alarm System the CMS operator shall listen to live audio and may listen to archived or recorded audio in order to determine if there is actionable audio as prescribed by 5.1.

6.2.1.1.2. If the Audio Alarm System cannot be accessed or if upon access no actionable audio is heard then the alarm shall be handled as a non-audio verified incident following the CMS procedures.

6.2.1.2. If the initial audio is discernable then the CMS operator shall determine if the audio is actionable.

6.2.1.2.1. If human activity is heard or if there is evidence of recent human activity then the CMS operator shall attempt to determine the Threat Level of the activity as prescribed by 3.19.

6.2.1.2.2. If no current or recent human activity is heard then the CMS operator may close incident or continue with additional non-audio verification procedures as required by the CMS.

6.2.2. Determine if Actionable Audio is Threat Level 3

6.2.2.1.1. If the CMS operator determines there is a requirement to dispatch because audio activity is determined to be Threat Level 3 the operator shall dispatch the event by efficiently communicating relevant details of what was heard in the clip(s) or live or archived audio without unnecessary delay.

6.2.2.1.2. After dispatching the CMS operator shall notify Contacts

6.2.2.2. If the CMS operator determines the human activity is a Threat Level 2 the operator shall attempt to access the Audio Alarm System. Upon accessing the Audio Alarm System the operator shall listen using live audio and may listen to archived or recorded audio in order to determine:

6.2.2.2.1. If the Threat Level should be raised to a Level 3 and take action as prescribed by 6.2.2.1.1

6.2.2.2.2. If the Audio Alarm System cannot be accessed or the additional audio activity heard does not raise the threat level to level 3 then the CMS Operator shall attempt verification by contacting someone on site using any appropriate or available means of communication and if unable to verify at the site by contacting an authorized Contact in order to determine if the activity observed is authorized.

6.2.2.2.2.1 If the activity is authorized then the incident is closed.

6.2.2.2.2.2 If the activity cannot be verified then the CMS operator shall determine if the audio activity is from an Secured Area or from an Unsecured Outdoor Area or Unsecured Indoor Area.

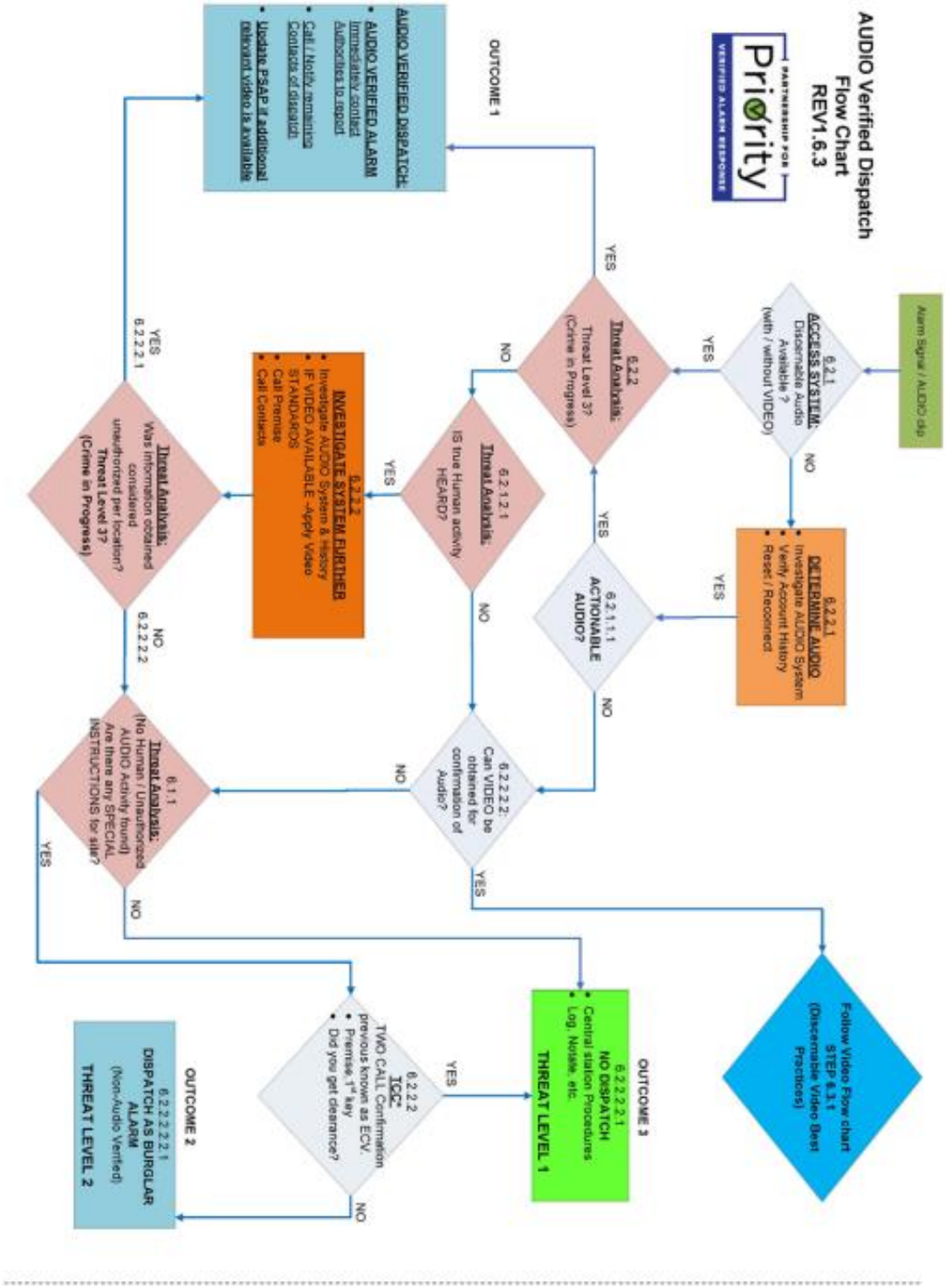
6.2.2.2.2.2.1 If the audio is from a Secured Area the CMS operator shall dispatch the incident to the AHJ, describing in detail the actions taken and what was heard

in the clip(s) or live or archived audio.

6.2.2.2.2.2.2 After dispatching the CMS operator shall notify Contacts.

6.2.2.2.2.2.3 If the audio activity is from an Unsecured Outdoor area or Unsecured Indoor Area the CMS operator may close the incident.

7. ANNEX:


AUDIO Verified Dispatch
Flow Chart
REV1.6.3
Priority
Alarm Signal / AUDIO clip
6.2.1 ACCESS SYSTEM: Discernable Audio Available ? (with / without VIDEO)
YES
NO
6.2.2.1 DETERMINE AUDIO
Investigate AUDIO System
Verify Account History
Reset / Reconnect
YES
6.2.2 Threat Analysis: Threat Level 3? (Crime in Progress)
YES
NO
6.2.1.1.1 ACTIONABLE AUDIO?
YES
NO
6.2.1.2.1 Threat Analysis: IS true Human activity HEARD?
YES
NO
6.2.2.2 INVESTIGATE SYSTEM FURTHER
Investigate AUDIO System & History
IF VIDEO AVAILABLE -Apply Video STANDARDS
Call Premise
Call Contacts
6.2.2.2: Can VIDEO be obtained for confirmation of Audio?
YES
NO
Threat Analysis: Was information obtained consistent/ unauthorized per location? Threat Level 3? (Crime in Progress)
YES 6.2.2.1
NO 6.2.2.2
6.1.1 Threat Analysis: (No Human / Unauthorized AUDIO Activity found) Are there any SPECIAL INSTRUCTIONS for site?
YES
NO
AUDIO VERIFIED DISPATCH:
AUDIO VERIFIED ALARM
Immediately contact Authorities to report
Call / Notify remaining Contacts of cessation
Update PSAP if additional relevant video is available
OUTCOME 1
Follow Video Flow chart STEP 6.1.1 (Discernable Video Best Practices)
OUTCOME 3
6.2.2.2.1 NO DISPATCH
Central station Procedures
Log, Notate, etc.
THREAT LEVEL 1
6.2.2.2 TCC: TWO CALL Confirmation
previous known as ECV.
Premise 1st key
Did you get clearance?
YES
NO
OUTCOME 2
6.2.2.2.2.1 DISPATCH AS BURGLAR ALARM (Non-Audio Verified)
THREAT LEVEL 2