PARTNERSHIP FOR Priority VERIFIED ALARM RESPONSE

Video Verified Alarms
Best Practices

September 2022

PPVAR Video Verification Committee

Table of Contents

PPVAR Video Verification Committee

Participating Parties in Developing Best Practices

Security Industry

- Acme Protective
- Alarm Detection Systems (ADS)
- Alarm New England
- ATT Digital Life
- Axis Communications
- Bold Group
- COPS Monitoring
- Emergency 24
- First Alarm
- Guardian Alarm
- Honeywell
- Integrated Security Group (ISG)
- I-View Now
- Protection 1
- Rapid Response (RRMS)
- Red Hawk Fire & Security
- Redwire
- Security Central
- Security Partners
- Sonitrol SW of Ohio
- Sonitrol of Lexington
- SSD Systems
- SW24 Security
- Stanley Security
- Sureview Systems
- Telular
- Titan Protection & Consulting
- United Central Control (UCC)
- Universal Monitoring
- Vancouver Fire
- Videofied
- VideoIQ
- Xtralis

Law Enforcement

- California Police Chiefs Association
- Indiana Association of Chiefs of Police
- Michigan Association of Chiefs of Police
- Texas Police Chiefs Association
- Chicago PD, Illinois
- Grand Prairie PD, Texas
- Highland Park PD, Texas
- Houston PD, Texas
- Los Angeles County Sheriff's Dept.
- Phoenix PD, Arizona
- Sheriff's Office, Harris County, Texas
- Sheriff's Office, Story County, Iowa

Insurance

- Intertek (ETL)
- National Insurance Crime Bureau (NICB)
- Underwriters Laboratories (UL)
- Verisk Crime Analytics

PPVAR Video Verification Committee
Recommendations for Video 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 video images 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 video equipment that creates the images 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 video 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. Actionable Video – Video information aligned with the alarm event that shows the presence of a human or humans, or any other information germane to the alarm scene such as a broken window, smashed door, or other physical characteristics at the time of the alarm event that would indicate suspicious activity.

3.2. Alarm Confirmation– 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.

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

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

3.5. 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.

3.6. 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.

3.7. 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.

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

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 confirm 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 Video – Video images that is presented to the central monitoring station operators for viewing 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. Remote Video Investigation – A procedure where CMS personnel use a live video connection or recorded video clips, pictures, and other methods to remotely view the premises as a follow up method after an alarm event has been transmitted. The viewing of video and associated information about the premises occurs after the initial alarm.

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

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 observed presence or lack of presence of human activity basis for the actions taken by an operator.

3.19.1. Threat Level 3 – Human activity is observed or appears to have taken place, 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 – Human activity is observed 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 human activity is apparent.

3.20. Verified Video Alarm – An alarm signal that, through the use of video data, has been determined to require investigation by a designated organization such as law enforcement.

3.21. Video Verification – A method in which video data that was created at the same time an alarm event was annunciated by the alarm system control unit is compared with signals received from the alarm system to determine if a response to the protected property is required.

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, or equivalent training sources for video verification.

4.2. Training requirements

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

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

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

4.3. Initial Training

4.3.1. A new employee, or employee who changes job functions, may handle video 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 video 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 first viewing of the transmitted video 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 Confirmation 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 video images 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 video representation of any human activation of the alarm

signal, then NO reference of “video alarm” activation or “video alarm” should be made to the PSAP/Emergency Communications Center.

5.6. The level of information available to the monitoring personnel as to specific camera location and what is in the field of view must be as detailed as possible. Merely having a view that shows 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 video 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 instruction 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 view enough video to make a reasonable determination at their sole discretion as to whether suspicious activity is occurring, or not.

6.2. Standard & Enhanced Video Verification Procedures

6.2.1. Upon receipt of an alarm activation from a Video Alarm System the CMS operator shall view any Captured Video Information (video clip(s)) attached in order to determine if the video is discernable.

6.2.1.1. If no clip is received or if there is no discernable activity contained in the clip the CMS operator shall attempt to access the video alarm system.

6.2.1.1.1. Upon accessing the Video System the operator shall view live video and may view archived video in order to determine if there is actionable video as prescribed by 3.1.

6.2.1.1.2. If the Video System cannot be accessed or if upon access no actionable video is seen then the alarm shall be handled as a non-Video incident following the CMS procedures for such.

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

6.2.1.2.1. If human activity is observed 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 observed then the CMS operator may close incident or continue with additional non-video procedures as required by the CMS.

6.2.2. Determine if Actionable Video is Threat Level 3

6.2.2.1. If the CMS operator determines there is a requirement to dispatch because video is determined to be Threat Level 3 the operator shall dispatch the event

by efficiently communicating relevant details of what was observed in the clip(s) or live or archived video without unnecessary delay.

6.2.2.1.1. 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 Video System Upon accessing the Video System the operator shall view live video and may view archived video 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.

6.2.2.2.2. If the Video System cannot be accessed (Standard System) or the additional viewed video 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.

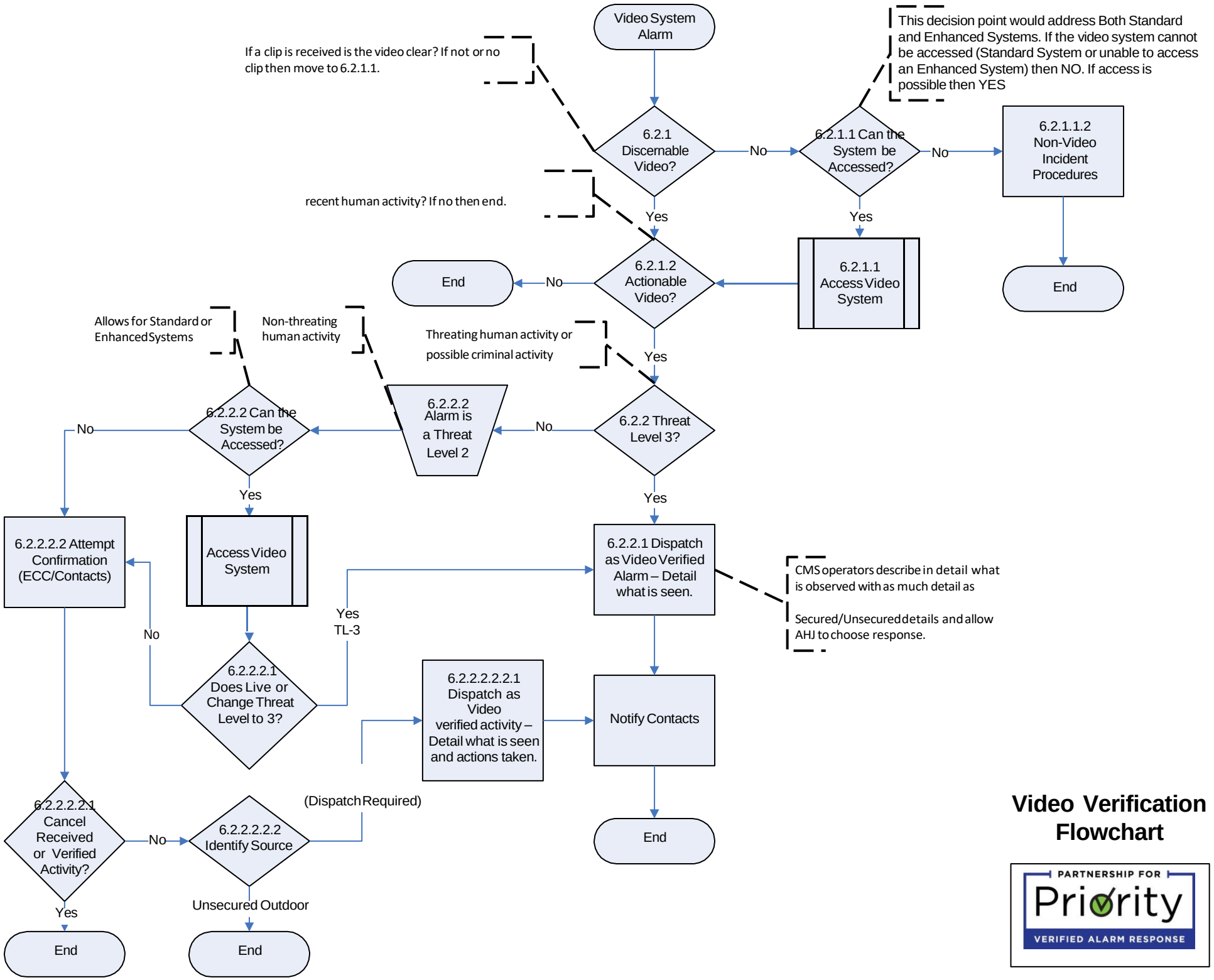
6.2.2.2.2.2. If the activity cannot be verified then the CMS operator shall determine if the video is from an Indoor or Secured Outdoor source or from an Unsecured Outdoor source.

6.2.2.2.2.2.1. If the video is from an Indoor or Secured Outdoor source the CMS operator shall dispatch the incident to the AHJ, describing in detail the actions taken and what was observed in the clip(s) or live or archived video.

6.2.2.2.2.2.2. After dispatching the CMS operator shall notify Contacts.

6.2.2.2.2.2.3. If the video is from an Unsecured Outdoor source the CMS operator may close the incident.

7. ANNEX:



Video Verification Flowchart

PARTNERSHIP FOR Priority VERIFIED ALARM RESPONSE