



Alarm Validation Scoring (AVS) Standard

TMA AVS-01-2022 Revision 1

Sponsor
The Monitoring Association (TMA)

Left Intentionally Blank

Copyright notice

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered and that effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he or she has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give interpretation on any American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

The developers of this standard have requested that holders of patents that may be required for the implementation of the standard disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard.

As of the date of publication of this standard and following calls for the identification of patents that may be required for the implementation of the standard, no such claims have been made. No further patent search is conducted by the developer or the publisher in respect to any standard it processes. No representation is made or implied that licenses are not required to avoid infringement in the use of this standard.

Printed in the United States of America

Published by

The Monitoring Association

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

www.tma.us

© TMA 2022 — All rights reserved

Contents

Foreword and Limitation of Liability	iv
Acknowledgements	v
Sub-committee Membership 2021	v
Revision History:	vi
Introduction	1
Preface	1
Alarm Validation Scoring (AVS) Standard Procedures	2
1. Scope	2
1.1. General	2
1.2. Definitions (Defined Terms are Italicized)	2
2. <i>Burglar Alarm</i> Processing	5
2.1. <i>Fundamental</i> Weighting	5
Intrusion Signals (D,1)	8
Reporting Categories	9
Intrusion <i>Alarm Level 4</i> Life Threatening Event	10
Intrusion <i>Alarm Level 3</i> Threat to Property	10
Intrusion <i>Alarm Level 2</i>	10
Intrusion <i>Alarm Level 1</i>	11
Intrusion <i>Alarm Level 0</i> (No Call for Service to ECC/PSAP)	11
3. ECC/PSAP Call for Service	11
3.1. <i>Intrusion Alarm</i>	11
ECC/PSAP Call for Service	11
Intrusion Alarm Request for Service Data Elements (*5.3)	12
4. Compliance Management	12
4.1. Record	12
4.2. Process Monitoring and Corrective Action	13
5. Appendices	15
Annex A (Informative)	15
5.1. Data Privacy and Retention Considerations	15
Annex B (Informative)	16
5.2. Example of an Operator Assistant Card	16
Annex C (Informative)	17
5.3. Intrusion Alarm Script	17
Annex D (Informative)	18
5.4. The Entire Swimlane Flow Diagram	18
Annex E (Informative)	19
5.5. Compliance Management	19

Annex F (Informative)	22
5.6. Common Industry Terms	22
Annex G (Informative).....	24
5.7. Available Forms for Download	24

Foreword and Limitation of Liability

This standards document is published by 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 or the standard described herein. TMA provides this standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

Use of this document or the standard described herein constitutes agreement that in no event will TMA be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this standard, even if TMA or an authorized TMA representative has been advised of the possibility of such damage. In no event shall TMA's liability for any damage ever exceed the price paid for this standard, regardless of the form of the claim.

Use of this document or the standard described herein constitutes agreement to defend, indemnify, and hold TMA harmless from and against any loss, expense, liability, damage, claim, or judgment (including reasonable attorney's fees) arising out of the use of or the inability to use this standard, even if TMA or an authorized TMA representative has been advised of the possibility of such damage.

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 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: standards@tma.us

This document is owned by The Monitoring Association and may not be reproduced, in whole or part, without the prior written permission from TMA.

Acknowledgements

TMA Standards Chairman: Glenn Schroeder, NetOne, Inc.

TMA Staff Administrator: Celia T. Besore, Executive Director, TMA

Bryan Ginn, Information Systems Mgr., ASAP Svc. Mgr.

Sub-committee Membership 2021

Committee Membership 2021-22			
Sam	Bauder		Intrado
Michael	Brown		National Sheriffs Association
Chris	Brown		Immix Software
Steve	Butkovich		CPI Security Systems
Alison	Chase		Alarm.com
Shane M.	Clary, Ph.D.	Alternate	Bay Alarm Company
Don	Crowder		G4S
Louis	Dekmar, Chief	IACP	LaGrange Police Department
Rick	Denos		MAS
Matthew	Depoint	Alternate	Rapid Response Monitoring
Larry Robert	Dischert	Recording Secretary	LRD Consulting-JCI/Tyco
Tony	Dunsworth	NENA	City of Alexandria
Jay	English		APCO
Greg	Eusden		Simplisafe
Frank	Fernandez		Miami Police (Ret.) Reserve Officer
Bob	Finney		Collier County
Bob	Finocchioli	Alternate	Evolon Technology
Larry	Folsom	Co-Chair	I-ViewNow
Ryan	Fouts		RapidDeploy
Randall	Gellens		Core Technology Consulting
JoeAllen	Gentry		Washington Alarm Inc
Sean	Githens		Redwire
Teresa	Gonzalez		Lydia Security Monitoring, Inc. dba: COPS & UCC
Lucinda	Guerrero		Bay Alarm Company
Jay	Hauhn		
Morgan	Hertel		Rapid Response Monitoring
David	Holl	Co-Chair	Lower Allen Dept of Public Safety
Alberto F.	Hook	FARA	Montgomery County PD & FARA, President
Anthony	Iannone		Affiliated Monitoring
John	Jon Adams		Digital Monitoring Products
Andy	King	IAFC	City of Franklin Fire Department

Committee Membership 2021-22			
Sascha	Kylau		OneTel
Avi	Lupo		Dice Corporation
Kirk	MacDowell		MacGuard Security Advisors Inc
Stan	Martin		SIAC
Mark E	McCall	Chair	Immix Software
Kerri	McDonald	FARA	City of Riverside, PD, Alarm Unit
Thom	Meyer		Bold Group
Thomas	Nakatani		ADT
Chris	Newhook		American Alarm and Communications, Inc.
Suzie	Nye		AvantGuard
Anita	Ostrowski		Vector Security, Inc.
Joe	Pereira	Alternate	Stanley Security
Joey	Rao-Russell		Kimberlite
John	Romanowich		SightLogix
Steve	Schmit		UL LLC
Glenn	Schroeder		NetOne, Inc.
Anthony	Sharpy		Guardian Alarm
Mark	Skeen		JCI/Qolsys
Kevin	Stadler		Evolon Technology
Nicola	Tidey		Mission Critical Partners, Inc.
Tim	Tracy		Resideo Technologies, Inc.
Wes	Usle		

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

Revision History:

Original Version 2022

Introduction

This standard has been prepared by The Monitoring Association, an ANSI accredited Standards Development Organization (SDO), under the auspices of Security Industry Standards Council (SISC.) The creation of this standard is congruent with the ever-increasing operational use of data by businesses and public safety. For an alarm activation, alarm monitoring centers will perform a standardized assessment of applicable data to create an alarm scoring metric. The metric, also in a standardized manner, will be provided to Emergency Communications Centers (ECCs)/Public Safety Answering Points (PSAPs) when creating an alarm *Call for Service*.

The methods defined herein are at a minimum intended to result in higher criminal apprehension rates, improve law enforcement safety via data driven situational awareness and assist in the reduction of alarm calls for service that are ultimately categorized as false alarms.

Preface

This standard defines a process for burglar alarm activations where data received at a monitoring center associated with alarm activations, enable a monitoring center agent, either manually or assisted by the automation system, to use applicable data to generate standardized alarm scoring metrics. Relevant data may be video and/or audio, or other high confidence Human Presence technologies. This standard is aggregate to existing *Alarm Confirmation* processes.

A standardized method of creating an alarm scoring metric that grades the probability of unauthorized activity detected by alarm systems will assist law enforcement with resource allocation and *Call for Service* prioritization.

Alarm Validation Scoring (AVS) Standard Procedures

1. Scope

Establish standardized methods for calculating an alarm score that results in a repeatable metric that estimates the validity of a burglar alarm activation using historical and real-time data. *Calls for Service* to *Emergency Communications Centers* (ECCs)/*Public Safety Answering Points* (PSAPs) that include such a standardized scoring metric will assist public safety departments with their alarm response policies.

Note: Actions related to commercial and residential Fire Alarm systems, are found in NFPA 72.

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 *Call for Service* was made and subsequent information indicates no emergency exists, contact shall be made to the emergency agency in an attempt to cancel their response.

1.1.3. When an item is marked with an asterisk (*) it indicates there is explanatory material within the annex.

1.2. Definitions (Defined Terms are Italicized)

1.2.1. Alarm Abort/Cancel

An electronic or verbal *Call for Service* by an authorized person for the alarm location that occurs within a specified time frame after an alarm event that indicates the response to an alarm event should be aborted or canceled. There is this same type of event that occurs, within the protect premises control unit that is compliant with ANSI SIA CP-01, whereby the panel has a timed window between an alarm activation and the transmission to the central-station, that should an “disarming” occur, during the window, the transmission is aborted.

1.2.2. Alarm Confirmation (See CS-V-01) *

Alarm confirmation is a generic name given to many techniques used (1) to permit authorized personnel, at the protected premises, 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.

1.2.3. Alarm Level(s) (0, 1, 2, 3, 4)

Levels are a system designed to add some meaning to the supervising center's *Call for Service*. They are a result of operator observations and/or a combination of observations and automation assistance.

Defined as;

Level 0: No *Call for Service*

Level 1: A *Call for Service* with no other information.

Level 2: A *Call for Service*, with proof of or a high probability of knowing person or persons are present at the alarm site.

Level 3: A *Call for Service*, knowing person or persons are present at the alarm site and it appears there is a threat to property.

Level 4: A *Call for Service*, knowing person or persons are present at the alarm site and it appears there is threat to life.

1.2.4. Analytical Data

Information that is the result of raw data being analyzed by program algorithms that have been developed to give understanding to the events being presented.

1.2.5. Analytical Data Confirmation

An automated process whereby raw elements of data, when put into context, result in the determination that there is a high probability that an event is occurring that warrants a *Call for Service* to the *ECC/PSAP*

1.2.6. Asset (Artifact)

Any media or *Metadata* used in the scoring process. This shall be the original unaltered media or *Metadata* used in the evaluation of the event, and could include video, audio or other information describing the activity that is associated with the alarm event.

1.2.7. Automated Secure Alarm Protocol (ASAP)

A form of electronic communication utilizing ANSI standard protocols developed cooperatively by the Association of Public-Safety Communications Officials (APCO) and The Monitoring Association. With ASAP, life safety signals are processed through the Nlets system of state-to-state *ECC/PSAP* communication.

1.2.8. Automation Data

Data that is presented to the operator that is the result of the supervising station's automation system.

1.2.9. Biometrics

The measurement and/or analysis of physical, biological, behavioral, and other human characteristics typically used in verifying the identity of a person or that a person is present.

1.2.10. Burglar Tools

Any object that could criminally be used to harm an individual and/or burglarize a premises, i.e., crowbar, hammer, pipe, knife, and the like.

1.2.11. Burglar Alarm (Intrusion Alarm)

An event that is received by the monitoring center that indicates a sensor(s) has detected an entry into a protected premises, that occurs when the alarm system is "armed."

1.2.12. Business, Type of (Jeweler, Gun shop, Bank)

The primary business that is conducted at the protected premises, i.e., jeweler, car showroom, motorcycle sales, firearms, bank, check cashing, and the like.

1.2.13. Call for Service (Notification (See 5.6.14)

A call or *Data Message* to the law enforcement authority, such as *ECC/PSAP/911* or the telephone number used to reach the responding law enforcement agency, that the *Supervising Station* is in receipt of an alarm.

1.2.14. CS-V-01 (Alarm Confirmation, Verification and Notification Procedures)

A standard that was first developed and published in 2004, by the then CSAA (now TMA) by a committee which had representatives from; security industry, national trade associations, a sheriff's office, an insurance company, and UL. It was based on industry best practices that had been used in industry supported studies. It has gone through several upgrades over the years and just has been updated in 2021.

The standard spells out the "best practices", in alarm handling, in the attempt to reduce false *Calls for Service*. And with the integration of it within AVS-01, AVS-01 builds upon that foundation.

CS-V-01 is also suggested to be a part of municipal ordinances, as suggested by it's being incorporated into the "Model Ordinance" of the Security Industry Alarm Coalition (SIAC).

1.2.15. Customer Confirmed Event

Monitoring station personnel in contact with the customer and/or customer-representative, receive information from same that the alarm event is valid.

a. **Electronic**

An electronic signal transmitted to the *Supervising Station* that indicates to its personnel or to its *Call for Service* computer that no emergency appears to exist or confirms that an emergency does exist.

b. **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.

c. **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.

1.2.16. Custodian of Record

The entity that holds the Asset of alarm events, as identified within 4.1.3. a) & b), used in the decision process that led to a *Call for Service*.

1.2.17. Data Message

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

1.2.18. Dispatch (see 1.2.14 *Call for Service*)

1.2.19. End User (Customer/subscriber)

The person who is using the alarm system. Very often not the owner/customer/subscriber, but a person who is authorized to operate the “*End User*” interface.

1.2.20. Emergency Communications Center/Public Service Answering Point (ECC/PSAP)

A facility responsible for receiving and processing Calls for Service (1.2.14) for emergency service organizations such as fire departments, law enforcement departments, and emergency medical service organizations.

1.2.21. Enhanced Call Confirmation (ECC, formally ECV – Enhanced Call Verification)

A process, described within the ANSI TMA CS-V-01 standard, whereby the supervising-station will make multiple attempts to confirm or deny that an alarm is or is not false.

1.2.22. Enhanced Call Verification (ECV, See 1.2.22)

1.2.23. Human Activity

There are indications that humans are and/or have recently been in the area of the alarm event.

1.2.24. Human Presence

Data presented that would indicate there is a human(s) present on the protected property.

1.2.25. Metadata - Data about the content, quality, condition, and other characteristics associated with media or other data. Examples including, but not limited to, date/time of creation, source, versioning.

1.2.26. Sensor Type

The type of detector that activated, causing an alarm signal to be sent to the monitoring center, i.e., glass-break detector, motion sensor, door sensor, and the like.

1.2.27. Special instructions

Instructions that are in addition to the normal data that each account contains/maintains. Typically, 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. They fall into different categories as follows:

- a. Customer supplied in writing:
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.
- b. AHJ supplied in writing:
A situation whereby the local Authority Having Jurisdiction (AHJ) has instructed the supervising station, with a specific set of instructions to be followed, upon the occurrence of an identified event.
- c. Third-party supplied:
Instructions added by someone, such as the entity that contractually owns the account and has contracted-out "monitoring" to an outside monitoring station.

1.2.28. Structural Damage

Damage that is evident to the very structure of the protected premises. (Window broken, door forced open)

1.2.29. 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.

1.2.30. Trip/Tripped

The act or current state of a detector that has been violated by a condition which it was designed to detect, i.e.; opening of a door, motion detector "seeing" motion in its field of view, heat detector's temperature being at a level it was designed to detect, and the like.

1.2.31. Unknown Persons Onsite

Within the Artifact, unidentified persons are detected, cannot identify themselves, and cannot be identified to or by the monitoring station personnel.

2. Burglar Alarm Processing

Note: Throughout this section, at the ending of most headings you will see a reference to this chart and the "row and column" as the ID convention specifies the letter/row first, column/number second (i.e. B,2)

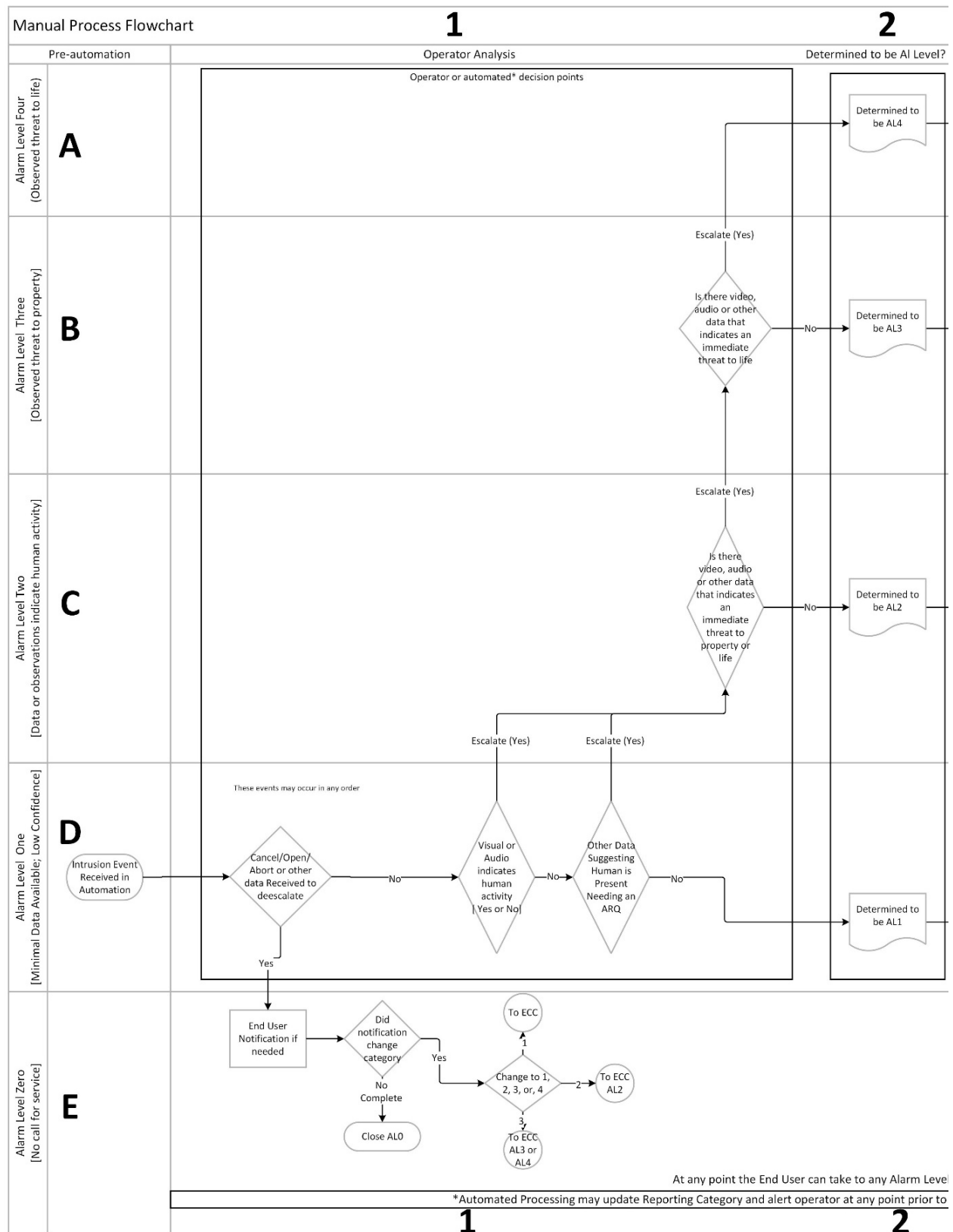
2.1. Fundamental Weighting

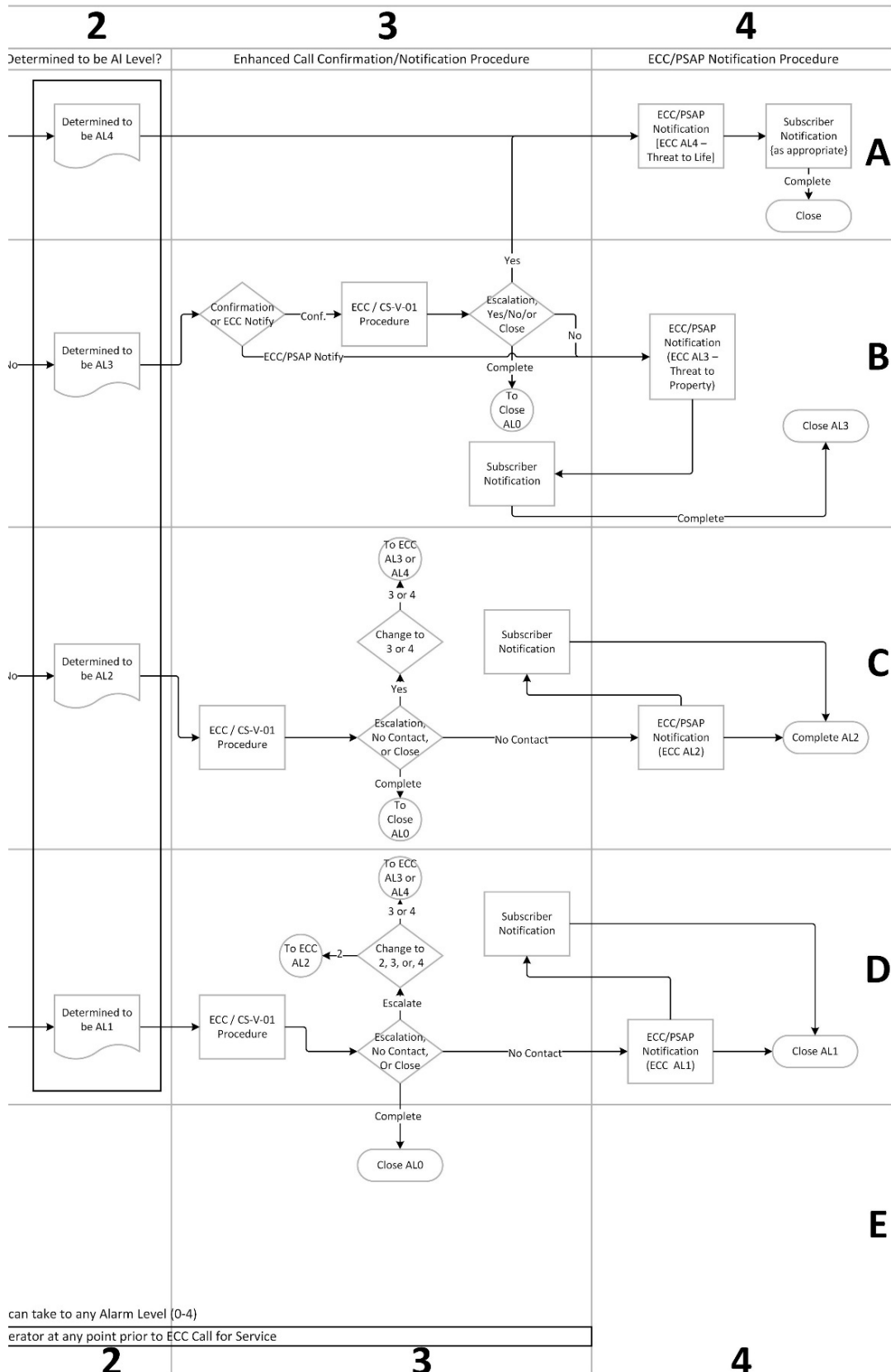
The following chart depicts the fundamental steps that occur when processing an alarm.

An intrusion alarm is considered an *Alarm Level One* in the absence of modifying factors.

During the CS-V-01 process, as additional data is learned, the intrusion alarm is escalated, deescalated, or unchanged, followed by the *Call for Service*.

Details are in the following sections.





Intrusion Signals (D,1)

2.1.1. Signal is handled as follows:

Note: All intrusion signals are initially considered to be *Alarm Level 1*. The *Alarm Level* may escalate or deescalate based on Automation Data, data analytics and operator observation.

- a. If an *Alarm Cancel/Abort*, Opening, or other items as described in Section *Intrusion Alarm Level 0* are received prior to making a *Call for Service*, the signal is Determined to be *Alarm Level 0 (E)*, the *Call for Service* is not made, and the event is completed as prescribed by company procedures.
 - i. Proceed to identify the appropriate *Alarm Level* for *Call for Service* by the following:
 - ii. *Alarm Level 1* processing (D): Are there visual/audio indicators of *Human Presence*?
 - iii. Yes – Escalate to AL2 (C,1) and move to 2.1.1.b
 - iv. No – Continue
 - v. Are there any series of events as described in the Section *Alarm Level 2*?
 - vi. Yes – Escalate to AL2 (C,1) and move to 2.1.1.b
 - vii. No – Signal is Determined to be *Alarm Level 1 (D)*, move to 2.1.2
 - viii. *Alarm Level 2* processing (C): Is there an observed and immediate threat to life or to property?

Note: *Special instructions*

- 1) Customer or Customer's Service Provider *Special instructions* alone cannot escalate *Alarm Level*.
- 2) Public Safety Authorities may provide *Special instructions* based on known circumstances that may modify the process.

- i. Escalate and move on to the appropriate "Determined *Alarm Level*" as described below
 - i. Unchanged and proceed to *Call for Service* to the ECC/PSAP (C,4)
 - ii. Deescalate to a lower *Alarm Level* as appropriate and complete the event.
- b. With no additional information the signal is then handled in the identified categories below.

2.1.2. Determined to be *Alarm Level 0 (E,1)*

(See: *Intrusion Alarm Level 0 (No Call for Service to ECC/PSAP)*)

- a. If, during the process, the CS-V-01 escalates the Alarm, process signal accordingly, otherwise
 - 1) No *Call for Service* is to be made
 - 2) Process signal according to company procedures.

2.1.3. Determined to be *Alarm Level 1 (D,3 & 4)*

(See *Intrusion Alarm Level 1*)

- a. *End User* Confirmation Procedure
 - 1) Proceed to the *Enhanced Call Confirmation (ECC/CS-V-01)* procedure(s) (D,3)

2) Based on the findings of the ECC/CS-V-01 procedure, the outcome will be one of the following:

- i. Escalate and move on to the appropriate “Determined *Alarm Level*” as described below.
 - i. Unchanged and proceed to *Call for Service* to ECC/PSAP (D,4)
 - ii. Deescalate to *Alarm Level* zero with no *Call for Service* and complete the event.

2.1.4. Determined to be *Alarm Level 2* (C,3 & 4)

(See: Intrusion *Alarm Level 2*)

a. End User Confirmation Procedure

- 1) Proceed to the *Enhanced Call Confirmation* (ECC /CS-V-01) procedure(s) (C3).
- 2) Based on the findings of the *End User* Confirmation procedure, the outcome will be one of the following:
 - i. Escalate and move on to the appropriate “Determined *Alarm Level*” as described below
 - i. Unchanged and proceed to *Call for Service* to ECC/PSAP (C,4).
 - ii. Deescalate to a lower *Alarm Level* as appropriate and complete the event.

2.1.5. Determined to be *Alarm Level 3* (B,3)

(See: Intrusion *Alarm Level 3* Threat to Property)

a. CS-V-01 Confirmation Procedure

- 1) Based on the available information, make a determination that the data supports one of the following:
 - i. Proceed to do the *Enhanced Call Confirmation* (ECC/CS-V-01) (B,3) procedure(s).
 - ii. If allowed by local jurisdiction and provided *Special instructions*, initiate *Immediate Call for Service* to the ECC/PSAP (C,4)
- 2) Based on the findings of the *End User* Confirmation procedure, the outcome will be one of the following:
 - i. Escalate and move on to “*Alarm Level 4.*” (A,4).
 - ii. Unchanged and proceed to *Call for Service* to the ECC/PSAP (B,4).
 - iii. Deescalate to *Alarm Level 0* and complete the event.

2.1.6. Determined to be *Alarm Level 4* (A,2)

(See: Intrusion *Alarm Level 4* Life Threatening Event)

- a. Proceed to *Call for Service* to the ECC/PSAP (A,4).
- b. Close event as prescribed by company procedures

Reporting Categories

An intrusion alarm is considered an *Alarm Level One* in the absence of modifying factors.

During the *CS-V-01* process, as additional data is learned, the intrusion alarm is escalated, deescalated, or unchanged, followed by the *Call for Service*.

Intrusion Alarm Level 4 Life Threatening Event

2.1.7. Visible, audible, eyewitness or *Analytical Data* confirmation of a threat to life.

Examples: Observation by operator or through analytics, potential life-threatening language or sounds heard, physical altercation seen, authorized user confirms or perceives a threat to life, analytic confirmation of pre-determined threat, e.g., Weapons presented in a life-threatening manner, firearms heard, and the like.

Intrusion Alarm Level 3 Threat to Property

2.1.8. Visible, audible, eyewitness or Analytical Data Confirmation of a threat to property

Examples: Observation of broken glass or other *Structural Damage*, obvious/likely criminal activity, heard, detected, or confirmed.

Intrusion Alarm Level 2

2.1.9. There is proof, or the very high probability, of non-validated or non-authorized *Human Presence* with unknown intent.

Examples of defined events Manual process:

- a. Video of person(s) on premises that cannot be validated or authorized to be onsite, and there is no additional data present that raises to AL3 or AL4.
- b. Audio of person(s) on premises that cannot be validated or authorized to be onsite, and there is no additional data present that raises to AL3 or AL4.
- c. Open/Close/Cancel/Bypass by unauthorized user code.
- d. Seismic detection with ATM, Vaults and the like.
- e. License Plate Recognition activation of 'known foe' (list supplied by the subscriber) within protected area, plus an intrusion alarm.
- f. Confirmation of presence of human(s) with unknown intent. (e.g., cell application, any technology that allows observation of premises, and the like)
- g. Manual Fire Pull/Emergency phone signal, in addition to intrusion alarm.
- h. Eyewitness call that states person is at premise.
- i. And the like

Automation Examples:

- a. Video/Audio analytics or data, where the video/audio is not presented to an operator, but that indicate high probability of *Human Presence*.
- b. Presence detection analytics that determine human device (e.g., cell phone, Bluetooth) is on premises.
- c. Lidar/Radar/WIFI or other platforms to indicate that human movement inside is occurring.
- d. And the like.

Intrusion Alarm Level 1

2.1.10. The default category for an intrusion alarm absent any contributing factors listed for Categories 0, 2, 3, or 4

Intrusion Alarm Level 0 (No Call for Service to ECC/PSAP)

2.1.11. An intrusion alarm where it is determined a *Call for Service* to *ECC/PSAP* is not warranted.

This may be determined by:

- a. Receipt of a *CANCEL/OPEN/CLOSE*, a recently armed system
- b. Verbal confirmation from the Contact List
- c. Visible, audible, eyewitness or *Analytical Data* confirmation that no threat is present
- d. An event, from the site, that could only be the result of an authorized individual. Such as bypass, late to open, and the like.
- e. A Data Message, such as from an *End User* interface, from an authorized individual, indicating there is no emergency at the protected premises.

3. ECC/PSAP Call for Service

With the categorizing established in 2 above, and the data obtained during the process, this section provides the mechanics of a *Call for Service* to the *ECC/PSAP*.

3.1. Intrusion Alarm

When executing the procedures, as indicated within *CS-V-01* and described in Section 2, only alarms that cannot be categorized as *Intrusion Alarm Level 0*, continue to this point;

ECC/PSAP Call for Service

Communications shall be established with the appropriate *ECC/PSAP*. Once communication is established, data is exchanged as directed by the *ECC/PSAP* and supported by the *Central Station*. (See: *Intrusion Alarm Request for Service Data Elements (*5.3)*) Data may be conveyed electronically or verbally.

3.1.1 Electronic Data Transmission

- a. Data is conveyed electronically to the *ECC/PSAP* specific to the conveyance mechanism.

Examples are *ASAP* to *PSAP*, *NG9-1-1*, and the like.

3.1.2 Verbal Data Transmission

- a. Generally, the *ECC/PSAP* will “ask” for this information using their own style, order, and screening process after the opening introduction by the central station operator. The opening statement to the *ECC/PSAP* shall use the following format: “This is [company name] calling with an [Commercial/Residential] *Intrusion Alarm Level* [X, description].” E.g., “This is John with ABC Security calling with a Commercial *Intrusion Alarm Level 2* with confirmed *Human Presence*.” The other information listed below, if available, should be provided to the *ECC/PSAP* as requested.

Intrusion Alarm Request for Service Data Elements (*5.3)

ID	Event Data
a.	Company Greeting
b.	Alarm company name
c.	Intrusion <i>Alarm Level X</i> , with the added description for <i>Alarm Levels</i> .
d.	Address (including Apt. No.; Suite No.)
e.	Persons in Possession “Burglar Tools”, “Weapons”, etc.
f.	Audible or Silent
g.	<i>Sounds</i> heard (Describe)
h.	Commercial Business Type (Jeweler, Gun shop, etc.)
i.	Residential or Commercial Business Name
j.	Alarm company operator number
k.	Anyone en-route to premises
l.	Signal type, Location(s), (Burglary Front Door)
m.	Permit Information
n.	Directions to the site
o.	Site Information
p.	Alarm center call back number
q.	Alarm company incident number
r.	CS-V-01

4. Compliance Management

With the alarm event categorization and *ECC/PSAP Call for Service* defined in Sections 2 and 3, this section defines ongoing compliance management responsibilities of stations using AVS to process intrusion detection system alarm events.

Central-stations that want to claim compliance with this standard must have a Nationally Recognized Testing Laboratory (*NRTL*) certificate in force and therefore follows confirmation procedures outlined in UL 827, UL 2050, ULC S301 or ULC S304 Standards and have a subset certificate meeting the requirements of this standard

4.1. Record

4.1.1. *The alarm event record for signals handled as described in Section 2.1 shall include the detailed information which formed the basis of any escalate or de-escalate decision.

4.1.2. *Records of alarm event handling shall be kept for a minimum of 12 months.

4.1.3. *When handling an alarm event includes analyzing a video clip, audio clip, or other data stream captured in real time during the intrusion event, the *Custodian of Record* (see 1.2.17) shall be notified that the subject event record shall include information sufficient to reconstruct the analytic automation, such as the version number(s) of the analytic(s). The event record shall also include:

- a) The video clip, audio clip, or other data stream itself, or

- b) Sufficient *Metadata* to enable understanding of decisions made during alarm event processing. The *Metadata* shall include the details upon which an escalation/de-escalation decision was made., or
- c) Operator recorded description of event that includes the details upon which an escalation/de-escalation decision was made

4.1.4. *When the *Custodian of Record* for data specified in 4.1.3 is not the central station, the central station company shall implement a) and b);

- a) Have a contract or agreement in place with the *Custodian of Record* that commits the *Custodian of Record* to retaining the data in compliance with 4.1.2, and
- b) The central station's alarm event handling record shall identify the *Custodian of Record*

4.2. Process Monitoring and Corrective Action

4.2.1. AVS Scoring Process

- a. A central station shall implement a process by which compliance with Sec 2.1 is continuously measured and monitored by the station
- b. The length of time between self-assessments shall not exceed 90 days
- c. The periodic assessment described in 4.2.1, b) shall be made by analyzing a random sampling of signals processed in the covered time span, according to the following
 - 1) Sampling shall be randomized across all intrusion detection signals received.
 - 2) Target sample size is 10% of intrusion detection alarm signals received in the assessment time frame
 - 3) Minimum sample size shall be 50 alarm events and shall include samplings of all *Alarm Levels*. If available, the sampling shall be a minimum of 10 and a maximum of 25 alarm events that are *Alarm Level 2* and above.
 - 4) Maximum sample size shall be 200 alarm events and shall include samplings of all *Alarm Levels*. If available, the sampling shall be a minimum of 40 and a maximum of 100alarm events that are *Alarm Level 2* and above.
- d. The Sec 2.1 compliance monitoring process shall include periodic self-assessment by the central station of alarm event records described in 4.1 to determine:
 - 1) *Completeness of records for the purpose of understanding how the event was handled
 - 2) *Compliance with Sec 2.1 for each *Alarm Level* determination
 - 3) *Accuracy of *Alarm Level* determinations based on information and *Additional Risk Qualifiers* available at the time the event was handled
- e. If compliance with 4.2.1 d) 1) or 2) falls below 80%, the station shall take action to retrain staff, adjust system program or other action that mitigates the root cause(s) of noncompliance
- f. If compliance with 4.2.1 d.3) falls below 80% the station shall take action to retrain staff, adjust system programing or other action that mitigates the root cause(s) of noncompliance
- g. The effectiveness of corrective actions described in 4.2.1 e and 4.2.1,f shall be monitored and adjusted as necessary until the process operates within the compliance requirements specified

5. Appendices

Annex A (Informative)

5.1. Data Privacy and Retention Considerations

As a system that will house and transfer data, there are privacy and retention concerns that should be addressed.

Annex A is not a part of the requirements of this TMA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

Some components of a privacy policy might include:

- The types of information collected by the website or application
- The purpose for collecting the data
- Data storage, security and access
- Details of data transfers
- Affiliated websites or organizations (third parties included)
- Use of cookies

A few rules of thumb for a data retention policy include:

- Identifying and classifying the data your organization holds (or transfers)
- Knowing which governing bodies have regulations that apply to you
- Deleting data once it is no longer required or after the data retention period has been met
- Less data retained, and shorter storage requirements are desired

Annex B (Informative)

5.2. Example of an Operator Assistant Card

ALARM LEVELS				
LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
No Notification	Notification	Person(s) Present Notification	Threat to Property	Threat to Life
No person(s) seen or heard	No person(s) seen or heard	Person(s) seen and/or heard	Visible/auditable evidence of threat to property	Visible/auditable evidence to threat to life
Automation clears alarm	Automation does not clear alarm	Signal caused by unauthorized person(s)		
CS-V-01 clears alarm	CS-V-01 does not clear alarm	Automation indicates human caused event(s) (Seismic, presence TBD)		
		CS-V-01 confirms unknown person(s) with unknown intent		
		Eyewitness confirms person(s) on prem		

ALARM LEVELS				
LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
No Notification	Notification	Person(s) Present Notification	Threat to Property	Threat to Life
No person(s) seen or heard	No person(s) seen or heard	Person(s) seen and/or heard	Visible/auditable evidence of threat to property	Visible/auditable evidence to threat to life
Automation clears alarm	Automation does not clear alarm	Signal caused by unauthorized person(s)		
CS-V-01 clears alarm	CS-V-01 does not clear alarm	Automation indicates human caused event(s) (Seismic, presence TBD)		
		CS-V-01 confirms unknown person(s) with unknown intent		
		Eyewitness confirms person(s) on prem		

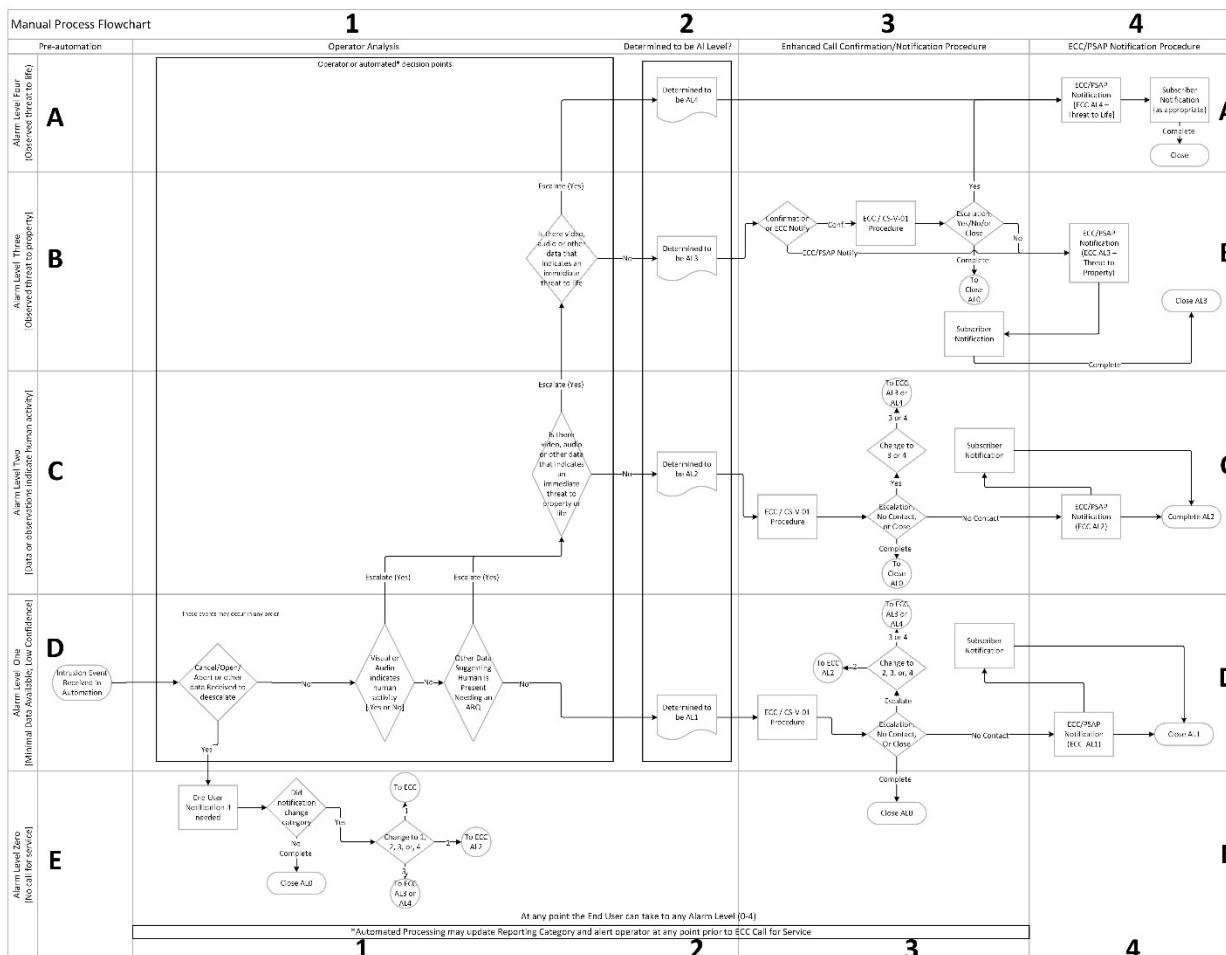
Annex C (Informative)

5.3. Intrusion Alarm Script

No,	Event Data	Suggested Dialogue / Examples
a.	Company Greeting	Dia: Hello, I have an [commercial/residential] intrusion alarm to report.
b.	Alarm company name	Dia: Calling from ABC Alarm Company
c.	Intrusion <i>Alarm Level X</i> , with the added description for <i>Alarm Levels</i> .	Dia: We have received an Intrusion Alarm, Level 2, unknown persons on premises.
d.	Address (including Apt. No.)	Dia: Address is 123 Main St., second floor apartment 203.
e.	Persons in Possession “Burglar Tools”, “Weapons”, etc.	Dia: The unknown person appears to have a firearm. Ex: Firearm, crowbar, hammer, rifle, pipe, knife, wearing body armor, and the like.
f.	Audible or Silent	Dia: There is an audible alarm siren on the exterior.
g.	Sounds heard (Describe)	Dia: We can hear what sounds like things being pounded and broken. Ex: Breaking glass, loud pounding on surfaces, persons shouting threatening words, screaming, yelling for help, and the like.
h.	Comm (Bus type; Jeweler, Gun shop, etc.)	Dia: The premises is a Pawn Shop
i.	Residential or Commercial Business Name	Dia: This is a multistory, twin house.
j.	Alarm company operator number	Dia: This is Operator 25
k.	Anyone en route to premises	Dia: The apartment owner is responding.
l.	Signal type, Location(s)	Dia: We received an alarm from the apartment door and an image from the video camera. Ex: Door contact, glass break detector, interior motion detector, video camera, and the like. Ex: Front door, warehouse south rear door, fire exit-north side, roof hatch, show room, and the like.
m.	Permit Information	Dia: The premises has a permit No. 12345.
n.	Directions to the site	Dia: The premises in on the south side of Main Street and 2 nd avenue.
o.	Site Information	Dia: The owner does have a safe within the master bedroom closet.
p.	Alarm center call back number	Dia: Our call back number is 123-123-1234
q.	Alarm company incident number	Dia: Our ticket number is: A1234-59
r.	CS-V-01	Dia: Customer reports, seeing their video and they do not know the person seen.

Annex D (Informative)

5.4. The Entire Swimlane Flow Diagram



Annex E (Informative)

5.5. Compliance Management

A 4.1.1 The intent of Section 4.1 is to assure 1) that sufficient information is captured during alarm event handling to allow post-event analysis and 2) that data upon which an escalate/deescalate decision was made is retained for use by public safety, *NRTL* auditor, or another stakeholder.

When a video clip, audio clip or other data stream that may raise privacy concerns is retained, the station should take measures that assure compliance with applicable statutory and regulatory requirements See Appendix A, 5.1 Data Privacy and Retention Considerations.

A 4.1.2 The 12-month record retention period is consistent with alarm event record retention requirements in ANSI/UL827, Central Station Services, and the needs of this Standard's public safety development partners

A 4.1.3 After-event access controls or rights, to a video clip, audio clip or other data stream may impede efficient central station analysis or *NRTL* audit of compliance. In such cases, the intent of 4.1.3 b) and c) is to allow the central station alarm event record to include *Metadata* or an operator recorded description of the event as an alternative to placing the actual video clip, audio, clip, or other data stream in the record.

Example A central station has access to a subscriber's camera video stream during an alarm event, but the video recording is stored by the camera's manufacturer and post-event access to the video recording requires a lengthy and/or complex subscriber authorization procedure. To facilitate station analysis and *NRTL* audit, the central station operator enters a descriptive narrative that may be similar to:

- a. Observed a human form walking across the front office, headed toward the production area door. The picture was very poor, so unable to further define.
- b. Saw what appeared to be a tall male in dark pants and dark hoody covering the face in view of the camera facing the back employee's entrance.
- c. Seeing a short male, in blue jeans, red plaid shirt, with a face mask, crossing the production floor.
- d. Saw three individuals running out the rear entrance, but the picture was very poor, so no further details.
- e. See what appears to be juveniles ransacking showroom cases.
- f. Male individual could be seen answering call to premises, but gave wrong passcode, and hung up. Then proceeded into the warehouse. He was wearing black pants, and dark blue jacket.
- g. Heard sounds of multiple voices (male and/or female), discussing where to go "next", then moved out of range of audio.

A 4.1.4 The intent is to assure a) that the data upon which an escalate/deescalate determination was made is retained for a period long enough to meet the needs of this Standard's public safety development partners and b) that the 3rd party *Custodian of Record* is documented and readily discoverable in the event of public safety need.

A4.2.1.c.1) – Contemporary automation systems can programmatically add many record elements. However, focus on record completeness becomes critically important when a central station uses AVS methods that rely on human operator action to document parts, or all, of alarm event handling.

A 4.2.1 b – Scripted, automation driven AVS processes may simplify management and audit of compliance with *Enhanced Call Confirmation* and *ECC/PSAP Call for Service* requirements.

A4.2.1 d – Quality control procedures that include documented supervisor monitoring of event handling can be effective in identifying and correcting errors in *Alarm Level 1*/escalate/deescalate decision making.

Note: The form that follows can be used as a work sheet for documenting the compliance audit. It is also available for download from the TMA website (See Annex 5.7)

Date: ____/____/____

Compliant Audit-Work Sheet

Comp by: _____

Number	System Number	Time/ Date	Flowchart Columns 1 - 2							Flowchart Column 3				Flowch Column 4		
			A	B	C	D	E	F	G	H	I	J	K			
			Recorded Level	Cancel/ Abort	Audio/ Video	Human Present	Property Threat	Life Threat	Audited Level	ECC CS-V-01	Escalate D-Escla	Changed Level	ECC/ PSAP	Complaint Y/N		
1																
2																
3																
4																
5																
6																
7																
8																
9																
10																
11																
12																
13																
14																
15																
16																
17																
18																
19																
20																

AVS Audit Ck Sheet Rev 2.xlsx

Process and Description(s)			
Enter recorded level			
A	Y - Yes Cancel, Abort, Close, etc. Cont to "L" Level=0	E	Y - Yes Threat to Life - Cont to "G" Level=3
	N - No Continue to "B"		N - No No Threat to Life Cont to "G" Level=2
B	Y - Yes Audio/Video-Human Cont to "C"	G	Y - Yes Confirm Threat to Life - Cont to "J" Level=4
	N - No Continue to "D"		Y - Yes CS-V-01 Clears Event Cont to "K" Close Ev
C	Y - Yes Human Presence - Cont to "D"	H	N - No CS-V-01 Does Not Cl Evt Cont to "H" Level=2/3
	N - No Continue to "E"		1 - Nothing Additional - Cont to "J" Level=2/3
D	Y - Yes Threat to Property - Cont to "E"	J	2 - New Info Observed - Cont to "J" Adj Level=2/3
	N - No - Continue to "G"		Call for Service Cont to "K"
		K	Event is compliant? (Y or N)

Level 0 (No Notification to ECC/PSAP)

An intrusion alarm where it is determined a Call for Service to ECC/PSAP is not warranted. This determination could be due to the receipt of a CANCEL/OPEN/CLOSE, a recently armed system, verbally from the Contact List, electronically from an End User Interface.

Level 1

After the Enhanced Call Confirmation Procedure an intrusion alarm absent any contributing factors listed above for Categories 0, 2, 3, or 4.

Level 2

Visual, audible, eyewitness or analytical data indicates non-authorized human presence, but determination of intent of said humans does not support increase to "Intrusion Level 3, and/or additional analytical data that would lower event to "Intrusion Level 1 or Level 0"

Level 3 Threat to Property

Visible, audible, eyewitness or Analytical Data Confirmation of a threat to property

Level 4 Life Threatening Event

Visible, audible, eyewitness or analytical data confirmation of a threat to life.

Quarterly/Sampling Compliance Guidance

Sample size: 10% of intrusion events

Min 50 events, (min=10, max=25 2 & above)

Max 200 events, (min=40, max=100 2 & above)

Annex F (Informative)

5.6. Common Industry Terms

5.6.1. 24-hour zone

Identification of areas that are always armed, e.g., emergency exits.

5.6.2. Actual Alarm

A confirmed documentable alarm event initiated by the detection of either an attempted or successful unauthorized entry of, or actions upon, a protected property by a person or persons.

5.6.3. Additional Risk Qualifiers (ARQ)

There are other data such as, higher risk account type and time, non-verified human or *Human Activity* seen or heard, site specific knowledge or data that indicates suspicious activity.

5.6.4. Alarm Verification (See CS-V-01)

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.

5.6.5. Audio Activity (Walking, Doors)

The protected area has a listen-in feature where non-verbal audio is received at the monitoring center indicating *Human Activity*, e.g., footsteps, doors opened and/or closed, other sounds of activity.

5.6.6. Automated AVS Procedure

A process that is a part of the supervision station monitoring automation system that assesses the circumstances surrounding the alarm event, and then presents a summary of them along with the likelihood of what *Alarm Level* (see Reporting Categories) the event belongs in.

5.6.7. Communication Failure (from/to Panel at Protected Property)

An event that indicates the communications path from the protected premises to the monitoring center has been disrupted. Could be caused by physical phone line cut, ISP failure, cellular service failure, and the like.

5.6.8. Computer Aided Dispatch (CAD) System

Computer-aided dispatch (CAD) systems, used by dispatchers, call-takers, and 911 operators to prioritize and record incident calls, identify the status and location of responders in the field, and effectively dispatch responders. Responders in the field can receive messages initiated by CAD systems via their mobile data terminals, radios, and cell phones

5.6.9. Destructive Sounds

The protected area has a listen-in feature with audio received at the monitoring center indicating destructive activity, e.g., doors being kicked in, glass breaking, and the like

5.6.10. Facial Recognition (Known/Unknown)

A customer owned/operated "facial recognition" system reporting to the monitoring center, recognized, or non-recognized person(s) within the area where alarm activation occurred.

5.6.11. Interior Alarm Reporting Zone

A Reporting Zone that identifies an interior area of protection, such as a showroom motion, warehouse office door, bedroom motion, hall motion, and the like. (See 1.2.66 Zone)

5.6.12. Interior Alarm followed by Perimeter Alarm

An order of receipt from sensors (points of protection), such that it is known an interior sensor activated first, followed by a perimeter or exterior sensor activation. (See Interior Alarm 1.2.35 and Perimeter alarm 1.2.43)

5.6.13. Multiple Trips – Different Reporting Zones

A *Burglar Alarm* event from the protected premises that includes activations from more than one uniquely identifiable Reporting Zone.

5.6.14. Multiple Trips – Single Reporting Zone

A *Burglar Alarm* event from the protected premises where there is more than one activation from a single uniquely identifiable Reporting Zone

5.6.15. Notification (See 1.2.18 Call for Service)

5.6.16. Call for Service Cancel

The process that may occur after the contacting the *ECC/PSAP/911* is complete and the *Supervising Station* learns that the alarm is false and notifies them.

5.6.17. NRTL (Nationally Recognized Testing Laboratory) “Certificated” Alarm System

The term *NRTL* Certificated Service, as used in this document, refers to *Burglar Alarm* systems that have a Nationally Recognized Testing Laboratory (*NRTL*) certificate in force and therefore follows confirmation procedures outlined in UL 827, UL 2050, ULC S301 or ULC S304 Standards.

5.6.18. Occupants Phones/GPS on/off Premises

Phone location technology providing location information of authorized persons at the protected premises.

5.6.19. Recent Activity (Opening, Closing)

An arming (Closing) or disarming (Open) has occurred within several minutes of the alarm event.

5.6.20. Visual Images

Video or still image(s) Information that is available and relevant to the alarm event.

5.6.21. Zone Type (Gun safe, ATM, Safe(money))

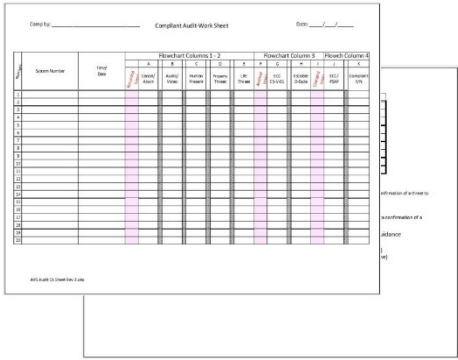
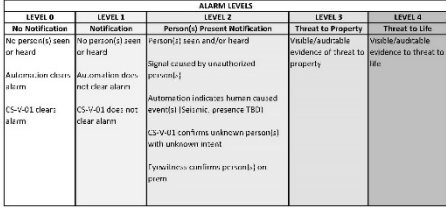
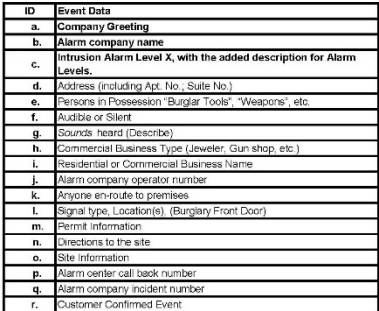
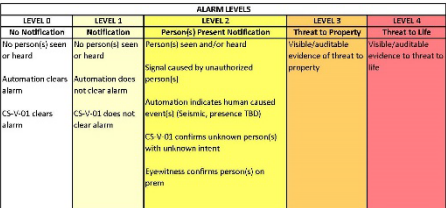
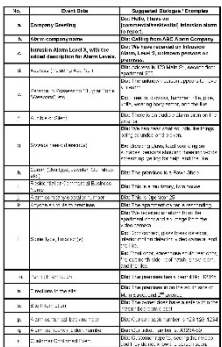
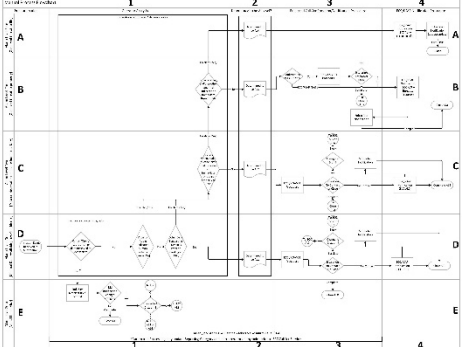
The area, or item that is being protected, like gun safe, ATM, vault, jewelry safe, and the like.

5.6.22. Zone

The description given to a sensor or group of sensors, describing what is being protected. e. g. a single sensor on the door of a gun safe, vault, roof hatch and/or a group of sensors that protect several windows and doors comprising a zone of a “perimeter zone or an individual room with several openings to be protected. (See Sensor Type 1.2.27)

Annex G (Informative)

5.7. Available Forms for Download

	
<p>Compliant Audit Work Sheet PDF (Portable Doc) Compliant Audit Work Sheet XLSX (Excel)</p>	<p>Operator Assistant Card Blk-Wht PDF (Portable Doc) Operator Assistant Card Blk-Wht XLSX (Excel)</p>
<p>Intrusion Alarm Request for Service Data Elements</p> 	
<p>Intrusion Alarm Req for Svc Data Elements PDF (Portable Doc) Intrusion Alarm Req for Svc Data Elements XLSX (Excel)</p>	<p>Operator Assistant Card Color PDF (Portable Doc) Operator Assistant Card Color XLSX (Excel)</p>
	
<p>Intrusion Alarm Script Sheet PDF (Portable Doc) Intrusion Alarm Script Sheet XLSX (Excel)</p>	<p>Swimlane as JPG (Image) Swimlane as PDF (Portable Doc) Swimlane as VSDX (Visio)</p>