



Active Threat (Detection) Notification (ATN) Standard

TMA ATN-01-2025 Revision 1



Sponsor
The Monitoring Association (TMA)

Left Intentionally Blank

Copyright notice

Approval of an American National Standard requires verification by the American National Standards Institute (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 that do not conform to the standards.

ANSI does not develop standards and will in no circumstances give an interpretation of any American National Standard in the name of ANSI. 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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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 ANSI 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 ANSI.

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 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 220, McLean, VA 22102

www.tma.us

© TMA 2025 — All rights reserved

Contents

Page

Foreword and Limitation of Liability	iv
Acknowledgements	v
Sub-committee Membership	v
Revision History:	vii
Introduction	1
Preface	1
Active Threat Notification (ATN) Standard Procedures	2
1. Scope	2
1.1. General	2
1.2. Definitions (Defined Terms are Italicized in the body)	2
2. Active Threat Alarm Processing	6
2.1. Fundamental Grouping	6
Active Threat Signals	2
2.1.1. Signal is handled as follows:	2
2.1.2. Active Threat Alarm Group A (A)	2
2.1.3. Active Threat Alarm Group B	2
2.1.4. Active Threat Alarm Group C	3
2.1.5. Active Threat Alarm Group D	3
Reporting Categories	4
Active Threat Alarm Group A – <i>Active Shooter</i>	4
Active Threat Alarm Group B – <i>Weapon Present-Human confirmed</i>	4
Active Threat Alarm Group C – <i>Weapon Detected-Not Human confirmed</i>	4
Active Threat Alarm Group D – <i>Threat Present-Not Human confirmed</i>	5
Active Threat Alarm Group E – <i>No Call for Service to ECC/PSAP</i>	5
3. ECC/PSAP Call for Service	5
3.1. Active Threat Alarm	5
ECC/PSAP Call for Service	5
Active Threat Alarm Request for Service Data Elements (*5.3)	6
4. Compliance Management	6
4.1. Record	7
4.2. Process Monitoring and Corrective Action	7
5. Appendices	9
Annex A (Informative)	9
5.1. Data Privacy and Retention Considerations	9
Annex B (Informative)	10
5.2. Example of an Operator Assistant Card	10

Annex C (Informative).....	11
5.3. Active Threat Alarm Script.....	11
Annex D (Informative).....	12
5.4. The Entire Swim Lane Flow Diagram	12
Annex E (Informative)	13
5.5. Compliance Management.....	13
Annex F (Informative)	16
5.6. Common Industry Terms	16
Annex G (Informative).....	17
5.7. Available Forms for Download	17

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 or visiting the TMA website, www.tma.us.

Requests to modify this document are welcome at any time from any party, regardless of membership affiliation with TMA. Such requests must be in writing and sent to the address set forth below. They must clearly identify the document and text subject to the proposed modification and include a draft of the 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 220
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 prior written permission from TMA.

Acknowledgements

TMA Standards Chairman: Glenn Schroeder, GLS Strategies, LLC

TMA Staff Administrator: Celia T. Besore, Executive Director

Bryan Ginn, IS, Standards, Operations Manager

Sub-committee Membership

Committee Membership 2023-2024			
Name (First)	Name (Last)	Voting Member	Company Name
Nina	Agnew	Principal	A3 Smart Home
Cameron	Anderson	Principal	A3 Smart Home
Celia	Besore	Principal	TMA
Megan	Bixler	Principal	APCO
Erica	Broome	Principal	Comporium SMA Solutions Inc.
Chris	Brown	Alternate	Immix
Steve	Butkovich	Principal	CPI Security Systems
Amber	Carter	Non-Vote	Everon
Allison	Chase	Alternate	Shooter Detection Systems/Alarm.com
Alex	Chermak	Principal	Databuoy
Ernie	Cole	Principal	Doyle Security
Jerry	Cordasco	Principal	Tech Systems
Tammy	Cozby	Non-Vote	Everon
Dan	Crowe	Principal	Noonlight
Larry	Dischert	Prog. Mgr.	LRD Consulting/JCI North America
Amy	Estey	Principal	Security Industry Alarm Coalition (SIAC)
Victoria	Ferro	Principal	Micro Key Solutions
Bob	Finney	Principal	Collier County Sheriff's Office
Dianne	Flanigan	Alternate	Collier County Sheriff's Office
Richard	Flores IV	Principal	Puget Sound Energy
Randall	Gellens	Principal	Core Technology Consulting
Bryan	Ginn	Non-Vote	The Monitoring Association
Jay	Hauhn	Non-Vote	Hauhn and Associates
Chris	Hawkins	Principal	IACP
Morgan	Hertel	Principal	Rapid Response Monitoring / TMA
Mark	Hillenburg	Principal	DMP
Stephanie	Hochstetler	Alternate	Securitas
Dave	Holl	Co-Chair	Lower Allen Township
Alexandria	Keen	Principal	EPS SECURITY

Rocky	Khullar	Principal	Bold Group
Jeff	Lippert	Alternate	Rapid Response Monitoring
Arthur	Martins	Principal	State of Rhode Island E-911 Director
Mark	McCall	Co-Chair	Immix
Caroline	McGrath	Alternate	Johnson Controls
John	McNutt	Principal	BluePoint Alert Solutions LLC
Tony	Mucci	Alternate	Johnson Controls
Colin	Murray	Alternate	Alarm.com
Thomas	Nakatani	Principal	ADT
Javier	Olarte	Principal	UL Solutions
Richard	Onofrio	Principal	Shooter Detection Systems
Anita	Ostrowski	Co-Chair	Vector Security
Joseph	Pereira	Principal	Securitas Technology
Michael	Picciola	Alternate	ADT Security
Al	Policano	Alternate	UL Solutions
Mindy	Pretzman	Principal	Federal Law Enforcement Officers Association
Chelsea	Prophete	Principal	Stanley Convergent Security / Securitas Technologies
Keith	Puckett	Principal	Ubiety Technologies, Inc.
Joey	Raorussell	Principal	Kimberlite
Michael	Riley	Principal	Vigilante Security
Glenn	Schroeder	Principal	GLS Strategies, LLC
Karen	Shaver	Non-Vote	ADT
Edison	Shen	Principal	Security Industry Association
Brooke	Smith	Non-Vote	ADT Security
Chuck	Speck	Alternate	Micro Key Solutions
David	Stonhill	Principal	Battelle Energy Alliance
Josh	Studeney	Principal	Vector Security, Inc.
Stephen	Surfaro	Alternate	Security Industry Association
Russell	Vail	Principal	Alula, LLC
Tommy	Whisnant	Alternate	CPI SECURITY SYSTEMS, INC.
Steve	White	Alternate	Vector Security, Inc.
Tony	Wilson	Principal	Criticom Monitoring Services - CMS
Jeffrey	Zwirn	Principal	IDS Research & Development, Incorporated

This standard was approved by the Security Industry Standards Council in **July 2025**

Revision History:

[Original Version](#)

Introduction

This standard has been prepared by The Monitoring Association, an ANSI-accredited Standards Development Organization (SDO), under the auspices of the 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 a standardized alarm 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 increase safety via data-driven situational awareness and reduce alarm calls for service that are ultimately categorized as false alarms.

Preface

This standard defines a process for Active Threat activations, where the data received at a monitoring center associated with alarm activations, enables a monitoring center agent, either manually or assisted by the automation system, to generate standardized alarm metrics using applicable data. Relevant data may be video and/or audio or other high-confidence technologies.

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

Active Threat Notification (ATN) Standard Procedures

1. Scope

Establish methods for standardizing metrics that result in a repeatable process. *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.

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 to cancel their response.

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

1.2. Definitions (Defined Terms are Italicized in the body)

1.2.1. Active Threat Alarms

a. Active Shooter, Human and/or Analytics Confirmed

The discharge of a firearm weapon has been detected and confirmed by a human or Analytics.

b. Explosives Detected - Video Analytics

Explosive devices, bombs, or grenades detected through video *analytics*.

c. Explosives Detected - Video Analytics, and/or Human Confirmed

Explosive devices, bombs, or grenades detected through video *analytics* and confirmed by a human or *analytics*.

d. Firearm Detected – Video Analytics

The presence of a firearm on a person, in a position to be used, detected by video *analytics*.

e. Firearm Detected – Video Analytics, and/or Human Confirmed

The presence of a firearm on a person, in a position to be used, detected by video *analytics* and confirmed by a human or *analytics*.

f. Firearm Detected – Weapons Detection System

The presence of a firearm on a person or within a bag detected by a metal detector, millimeter-wave scanner, or similar system.

g. Firearm Detected – Weapons Detection System, Human and/or Analytics Confirmed

The presence of a firearm on a person or within a bag detected by a metal detector, millimeter-wave scanner, or similar system and confirmed by a human or *Analytics*.

h. Gunshot Detected - Acoustic Only Sensor

The discharge of a *firearm detected* by an automated sensor using only acoustics.

i. Gunshot Detected - Acoustic Only Sensor, Human or Analytics Confirmed

The discharge of a *firearm detected* by an automated sensor using only acoustics and confirmed by a human or *analytics*.

- j. **Gunshot Detected - Multi-Technologies**
The discharge of a *firearm detected* by an automated sensor using multi-technologies.
- k. **Gunshot Detected - Multi-Technologies, Human and/or Analytics Confirmed**
The discharge of a *firearm detected* by an automated sensor using multi-technologies and confirmed by a human or *analytics*.
- l. **Lockdown Alarm, Human and/or Analytics Confirmed**
A threat within the facility or facility grounds where immediate emergency protocols are executed (i.e. locked exterior doors/gates, locked interior/classroom doors, shelter in place).
- m. **Lockout Alarm, Human and/or Analytics Confirmed**
A threat outside of the facility/property in the immediate vicinity or surrounding areas where certain emergency protocols may be enacted (i.e. locked exterior doors), but the facility is mainly operating as usual.
- n. **Non-Firearm Weapon Detected - Video Analytics, and/or Human Confirmed**
Knife, sword, edged weapon, or other non-firearm weapon detected through video *analytics* and confirmed by a human or *analytics*.
- o. **Non-Firearm Weapon Detected - Video Analytics**
Knife, sword, edged weapon, or other non-firearm weapon detected through video *analytics*.
- p. **Person Claims to Have Firearm - Audio Analytics Speech Detection**
A person verbally expresses having a firearm as a means to threaten others.
- q. **Person Claims to Have Firearm - Audio Analytics Speech Detection - Human or Analytics Confirmed**
A person verbally expresses having a firearm as a means to threaten others, and possession is confirmed by a human or *analytics*.
- r. **Video - Observed by Monitoring Personnel**
An individual is observed holding a firearm (and confirmed by another at the monitoring facility).
- s. **Video - Observed by Monitoring Personnel, Human and/or Analytics Confirmed**
An individual is observed discharging a firearm (and confirmed by another at the monitoring facility).

1.2.2. Active Threat Definitions

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

Defined as;

Group A: A *Call for Service*, knowing a person or persons are present and there is an active threat to life, confirmed by a human or *analytics*.

Group B: A *Call for Service*, knowing a person or persons are present and are a threat to life, confirmed by a human or by a human and *analytics*.

Group C: A *Call for Service*, with a high probability (but no human confirmation) that a person or persons present a threat to life.

Group D: A *Call for Service* where there are signs of a potential threat to life.

Group E No *Call for Service*

1.2.3. Alarm Confirmation

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 an *Alarm Monitoring Center*.

1.2.4. Alarm Monitoring Center (AMC)

A facility that receives signals from protected premises alarm systems and at which personnel are in attendance at all times to act upon these signals. (Also known as Central Station, Monitoring Center, Supervising Station)

1.2.5. Analytics

A set of technical activities that define, create, collect, verify or transform digital data into reporting, analyses, recommendations, and predictions. It can be valuable in areas with recorded information; analytics relies on the simultaneous application of statistics, computer programming, and operations research.

1.2.6. 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.

1.2.7. 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*

1.2.8. Asset (Artifact)

Any media or *Metadata* used in this Alarm Confirmation process (See 1.2.3). This shall be the original unaltered media or *Metadata* used in the evaluation of the event which could include video, audio, or other information describing the activity associated with the alarm event.

1.2.9. 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 and electronically dispatched participating ECCs/PSAPs.

1.2.10. Automation Data

Data that is presented to the operator that is the result of the *Alarm Monitoring Center's* automation system.

1.2.11. Call for Service (Notification (See 5.6.7))

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

1.2.12. 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*.

1.2.13. 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).

1.2.14. 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.

1.2.15. Emergency Communications Center/Public Safety Answering Point (ECC/PSAP)

A facility that –

- A. is designated to receive a 9-1-1 request for emergency assistance and
- B. performs one or more of the following functions:
 - 1. process and analyze 9-1-1 requests for emergency assistance and information and data related to such requests;
 - 2. dispatch appropriate emergency response providers;
 - 3. transfer or exchange 9-1-1 requests for emergency assistance and information and data related to such requests with one or more facilities described in this paragraph and emergency response providers;
 - 4. analyze any communications received from emergency response providers; and
 - 5. support incident command functions; or
 - 6. may be a public safety answering point, as defined in the Communications Act of 1934 (47 U.S.C.).

1.2.16. Human Confirmed Event

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

a. Electronic

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

c. Video

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

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

1.2.18. NRTL (Nationally Recognized Testing Laboratory) “Certificated” Alarm System - The term NRTL Certificated Service, as used in this document, refers to alarm systems that have a Nationally

Recognized Testing Laboratory (NRTL) certificate in force and therefore follow confirmation procedures per the UL 827 standard and the like.

1.2.19. Sensor (Type)

The type of detector activated, causing an alarm signal to be sent to the monitoring center, i.e., *firearm detected*, video *analytics*, acoustic, weapon detected, and the like.

1.2.20. Special Instructions

Instructions that are in addition to the normal data each account contains/maintains. Typically, separate documented directions, from the monitoring contract document, that specifies a specific set of instructions to be followed between the monitored premises and the *AMC* in the event of an alarm. They fall into different categories as follows:

- a. Customer supplied in writing:
Separate documented directions from the monitoring contract document that specify a specific set of instructions to be followed between the monitored premises and the *AMC* in the event of an alarm.
- b. AHJ supplied in writing:
A situation whereby the local Authority Having Jurisdiction (AHJ) has instructed the *AMC* 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.

2. Active Threat Alarm Processing

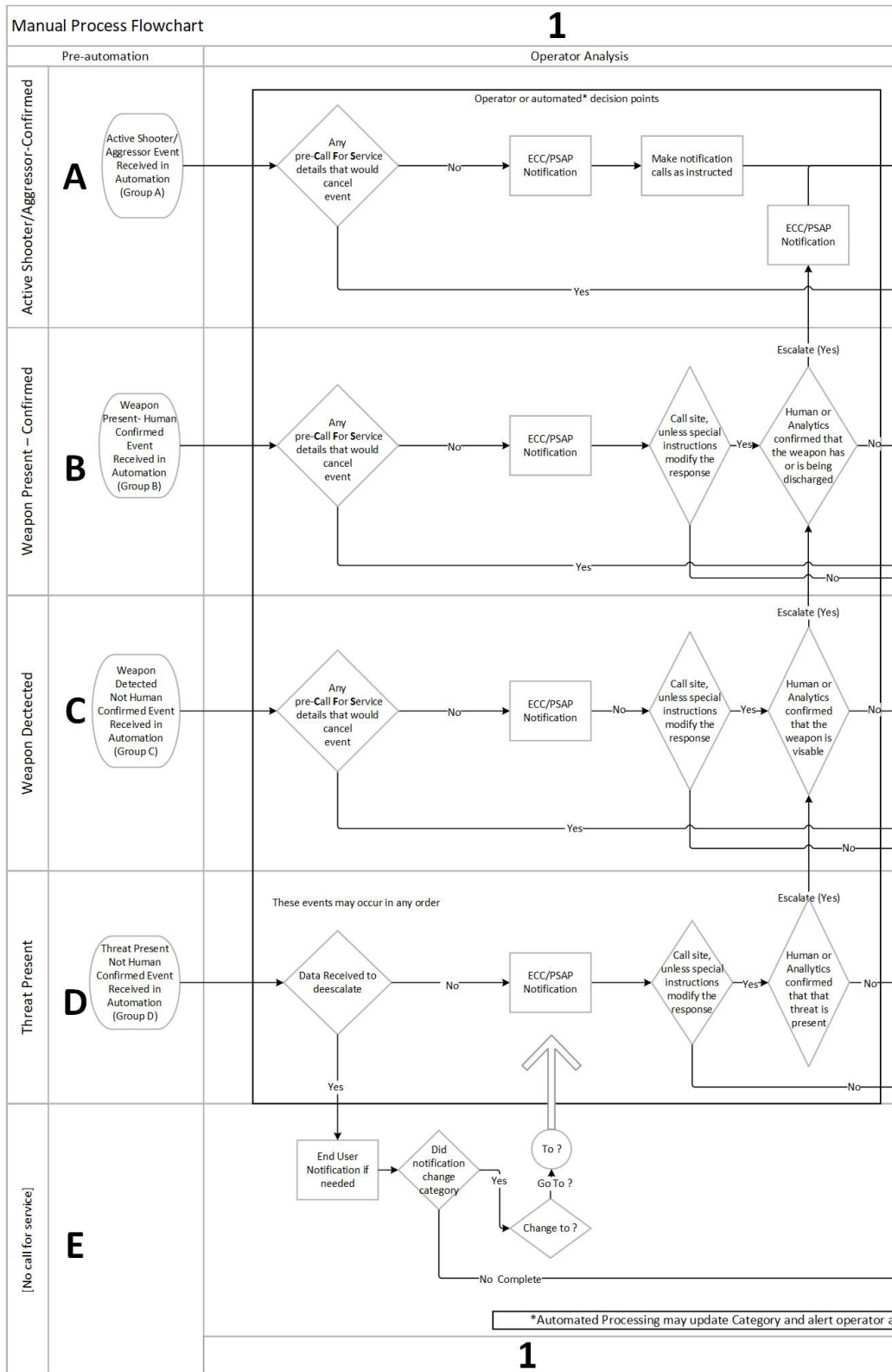
Note: Throughout this section, at the ending of most headings, you will see a cross-reference to the chart that follows, and the “row and column” as the ID convention specifies the letter/row first, column/number second (i.e., B,2).

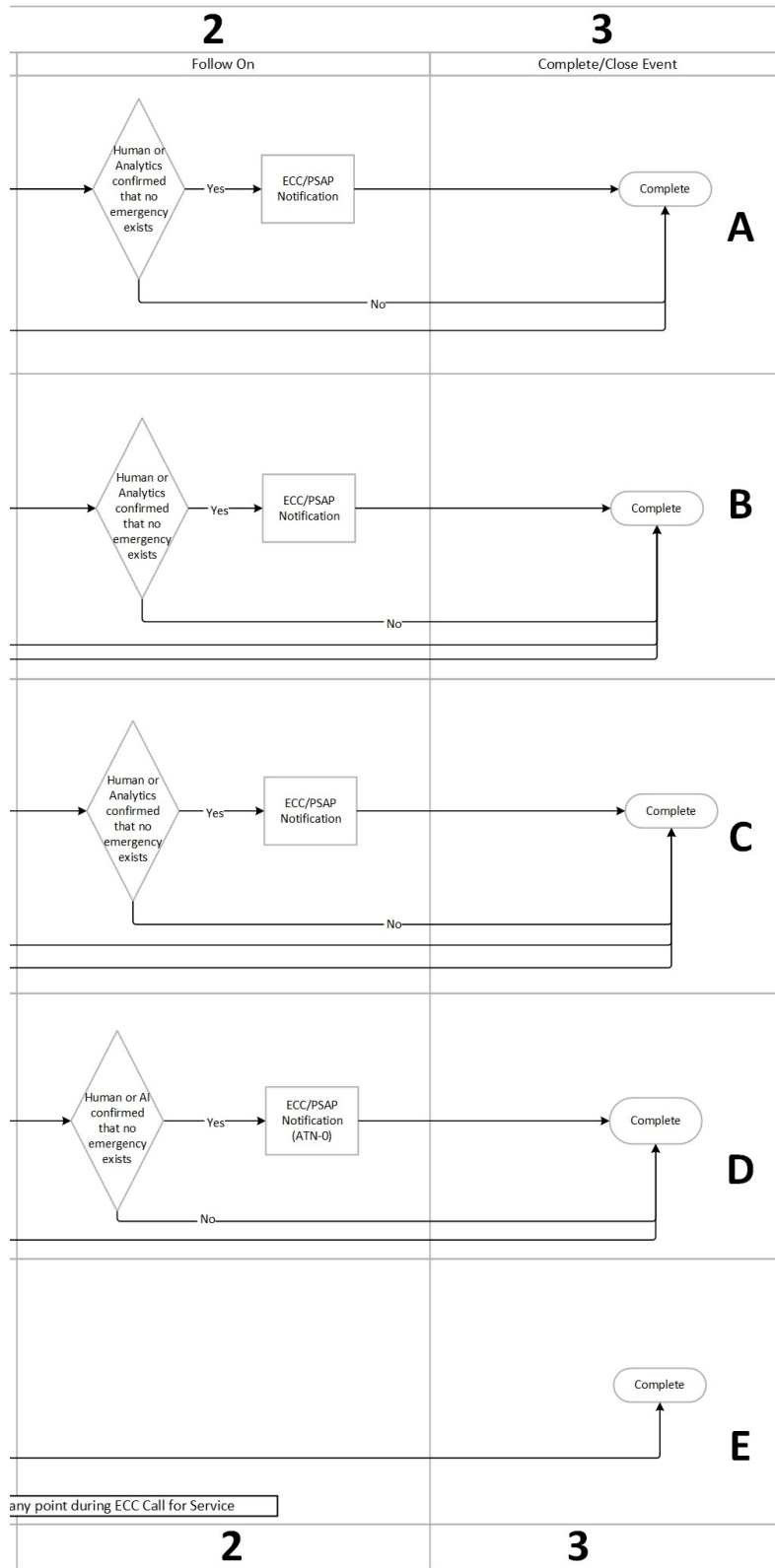
2.1. Fundamental Grouping

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

An active threat alarm is considered a *Call for Service* in one of four groups, which determines the content of the message passed in the *Call for service* to the *ECC/PSAP*.

Details are in the following sections.





Active Threat Signals

2.1.1. Signal is handled as follows:

- a. The following instructions follow the “swim lane diagram” shown above.

Note: All active threat signals initially enter the alarm queue in a predetermined group. The *Alarm Group* may escalate or de-escalate based on *Automation data*, human input, data *analytics*, and operator observation(s).

Note: Although the following follows the order of the “swim lane” there can be an interruption at any point that alters the course and changes the group upward and/or downward.

Note: *Special Instructions*

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

2.1.2. Active Threat Alarm Group A (A)

(See Active Threat Alarm Group A – *Active Shooter*)

Entry of a Group A event, is defined as there is an active-shooter and it has been confirmed by human or *analytics*.

- a. At any time during the processing of this signal, there may be communications that de-escalate the threat group. The operator will take whatever action is appropriate. (A)
- b. A *Call for service* is made by the AMC to the *ECC/PSAP* indicating that an *active shooter* has been confirmed by a human or *analytics*. (A,1)
- c. At some time after the Call for Service is completed, the AMC will reach out to the premises in a time frame based on the customer's instructions, and/or AMC policy. That contact will result in one of the following choices: (A, 1):
 - 1) Confirmation of the event that was reported, or:
 - 2) The event was a false alarm. The *ECC/PSAP* is then contacted and updated. (A,2)
- d. Once completed, the event is closed/completed based on the AMC policy. (A,3)

2.1.3. Active Threat Alarm Group B (B)

(See Active Threat Alarm Group B – *Weapon Present-Human confirmed*)

Entry of a Group B event is defined as having a weapon present and having the event confirmed by humans or *analytics*.

- a. At any time during the processing of any signal, communications may escalate or de-escalate the threat group. The operator will take whatever action is appropriate. (B,1)
- b. A *Call for Service* made by the AMC to the *ECC/PSAP* indicating that a weapon is present and has been confirmed by a human or *analytics*. (B,1)

- c. At some time after the *Call for Service* is completed, the AMC will reach out to the premises in a time frame that is based on the customer's instructions and/or AMC policy. That contact will result in one of the following choices: (B,1):
 - 1. Confirmation of the event that was reported, or:
 - 2. The event was a false alarm. The *ECC/PSAP* is then contacted and updated. (B,2) or:
 - 3. The event has escalated to a higher group. The *ECC/PSAP* is then contacted and updated. (A,1)
- d. Once completed, the event is closed/completed based on the AMC policy. (B,3)

2.1.4. Active Threat Alarm Group C (C)

See (Active Threat Alarm Group C – Weapon Detected-Not *Human confirmed*)

Entry of a Group C event is defined as a weapon being detected that has not been confirmed by humans or *analytics*.

- a. At any time during any signal processing, communications may escalate or de-escalate the threat group. The operator will take whatever action is appropriate. (C,1)
- b. A *Call for Service* made by the AMC to the *ECC/PSAP* indicating that a weapon has been detected and the detection has been received at the AMC. (C,1)
- c. At some time after the *Call for Service* is completed, the AMC will reach out to the premises in a time frame that is based on the customer's instructions and/or AMC policy. That contact will result in one of the following choices: (C,1)
 - 1) Confirmation of the event that was reported, or:
 - 2) The event was a false alarm. The *ECC/PSAP* is then contacted and updated. (C,2) or:
 - 3) The event has escalated to a higher group (B,2) and acted upon accordingly.
- d. Once completed, the event is closed/completed based on the AMC policy. (C,3)

2.1.5. Active Threat Alarm Group D (D)

See (Active Threat Alarm Group D – Threat Present-Not *Human confirmed*)

Entry of a Group D is defined as a threat detected that has not been confirmed by human or *analytics*.

- a. At any time during any signal processing, communications may escalate or de-escalate the threat group. The operator will take whatever action is appropriate. (D,1)
- b. A *Call for Service* made by the AMC to the *ECC/PSAP* indicating that a threat has been detected, and the information has been received at the AMC. (D,1)
- c. At some time after the *Call for Service* is completed, the AMC will reach out to the premises in a time frame that is based on the customer's instructions and/or AMC policy. That contact will result in one of the following choices: (D,1):
 - 1) Confirmation of the event that was reported, or:
 - 2) The event was a false alarm. Then the *ECC/PSAP* is contacted and updated. (D,2) or:
 - 3) The event has escalated to a higher group. Then the *ECC/PSAP* is contacted and updated.
- d. Once completed, the event is closed/completed based on the AMC policy. (D,3)

Reporting Categories

Active Threat Alarm Group A – *Active Shooter*

2.1.6. A *Call for service*, knowing there is an ongoing *active shooter* event.

Examples:

- a. *Gunshot detected* - multi-technologies, *analytics* and/or *human confirmed*
The discharge of a firearm has been detected by an automated *sensor* using multi-technologies.
- b. *Gunshot detected* - Acoustic Only *Sensor*, *analytics* and/or *human confirmed*
The discharge of a firearm has been detected by an automated *sensor* using only acoustics.
- c. Video - Observed by Monitoring Personnel, *analytics* and/or *human confirmed*
An individual is observed discharging a firearm (and confirmed by another at the monitoring facility).

Active Threat Alarm Group B – *Weapon Present-Human confirmed*

2.1.7. A *Call for service*, knowing that a weapon(s) is present and is *human confirmed*.

Examples:

- a. *Firearm detected* – Weapons Detection System, human and/or analytics confirmed
The presence of a firearm on a person or within a bag, detected by a metal detector, millimeter wave scanner, or similar system and confirmed by human and/or analytics.
- b. *Firearm detected* – Video Analytics, human, and/or analytics confirmed
The presence of a firearm on a person, in a position to be used in a threatening manner, detected and *confirmed* using video analytics and *human*.
- c. Video - Observed by Monitoring Personnel
An individual is observed and confirmed holding a firearm.
- e. *Explosives Detected* - Video Analytics and *human confirmed*
Explosive devices, bombs, or grenades detected and confirmed through video analytics.
- d. *Non-firearm weapon* Detected - Video Analytics and *human confirmed*
Non-firearm (e.g., edged weapon, bat, and the like) weapon being used in a threatening manner detected and *confirmed* through video analytics and *human*.

Active Threat Alarm Group C – *Weapon Detected-Not Human confirmed*

2.1.8. A *Call for service*, with a weapon(s) detected but not *human confirmed*.

Examples:

- a. *Firearm detected* – Weapons Detection System
The presence of a firearm on a person or within a bag detected by a metal detector, millimeter wave scanner, or similar system.
- b. *Gunshot detected* - Acoustic Only *Sensor*
The discharge of a firearm has been detected by an automated *sensor* using only acoustics.
- c. *Gunshot detected* - multi-technologies

The discharge of a firearm has been detected by an automated *sensor* using a single or multiple *sensor(s)* using multi-technologies.

- d. Person Claims to Have Firearm - Audio Analytics Speech Detection - *Human confirmed*
A person verbally expresses having a firearm as a means to threaten others. Confirmed by a human.

Active Threat Alarm Group D – Threat Present-Not *Human confirmed*

2.1.9. A *Call for Service* that there are signs of a threat to life.

Examples:

- a. Person Claims to Have Firearm - Audio Analytics Speech Detection
A person verbally expresses having a firearm as a means to threaten others.
- b. *Lockout alarm*
A threat outside of the facility/property in the immediate vicinity or surrounding areas where certain emergency protocols may be enacted (i.e. locked exterior doors), but the facility is mainly operating as usual.
- e. *Lockdown alarm*
A threat within the facility or on facility grounds where immediate emergency protocols are executed (i.e. locked exterior doors/gates, locked interior/classroom doors, shelter in place).

Active Threat Alarm Group E – No Call for Service to *ECC/PSAP*

2.1.10. An Active Threat alarm where it is determined a *Call for Service* to *ECC/PSAP* is not warranted.

This may be determined by:

- a. Verbal confirmation from the Contact List
- b. Visible, audible, eyewitness, or *Analytical Data* confirmation that no threat is present
A data message, such as from an end-user interface or 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. Active Threat Alarm

When executing the procedures, as described in Section 2, only signals that are categorized as Active Threat Alarm Groups A - D, 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 *AMC*.

(See:

[Active Threat 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 *AMC* operator. The opening statement to the *ECC/PSAP* shall use the following format: “This is (Operator ID), [company name] calling with an Active Threat Notification., i.e. “This is John with ABC Security calling with a **(Human or Human and Analytics Confirmed)** Active Threat Notification, Weapon Detected.” The other information listed below should be provided to the *ECC/PSAP* as requested, if available.
- b. Examples:
 - 1) Group A – *Active shooter*: “This is John with ABC Security calling with an **Active shooter event**.”
 - 2) Group B - *Weapon(s) Present – Human Confirmed*: “This is John with ABC Security calling with a **(Human Confirmed)** Active Threat Notification, Weapon Detected.”
 - 3) Group C - *Weapon Detected-Not Human Confirmed*: “This is John with ABC Security calling with an **(Analytics Confirmed)** Active Threat Notification, Weapon Detected.”
 - 4) Group D - *Threat Present-Not Human Confirmed*: “This is John with ABC Security calling with a **(Non-Confirmed)** Active Threat Notification, **[Describe the situation]**.”

Active Threat Alarm Request for Service Data Elements (*5.3)

Example: based on section: Group B. [a](#) or B. [b](#)

ID	Event Data
a.	Company Greeting
b.	Alarm company name
c.	(Human or Human and Analytics Confirmed), Active Threat Notification Weapon Detected
d.	Address
e.	Location/area information
f.	Persons in Possession of “Weapons”, “Active shooter”, etc.
g.	Sounds heard / visible observations (body armor) (Describe)
h.	Type of premises, (School, Multi FI building, campus, etc.)
i.	Video, meta-data and/or audio available,
j.	Alarm company operator number
k.	Anyone enroute to premises
l.	Permit Information
m.	Directions to the site
n.	Site Information
o.	Alarm center call back number
p.	Alarm company incident number

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 ATN-01 to process Active Threat detection system alarm events.

4.1. Record

4.1.1. *The alarm event record for signals handled as described in Section 2.1 shall include the detailed information that 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 by the AMC during the Active Threat event, the *Custodian of Record* (see 1.2.12) shall be notified that the event record includes 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 the 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 Section 4.1.3 is not the AMC. The AMC 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 retain the data in compliance with Section 4.1.2, and
- b) The AMC's alarm event handling record shall identify the *Custodian of Record*.

4.2. Process Monitoring and Corrective Action

4.2.1. ATN Analyzing Process

- a. An AMC shall implement a process by which compliance with Section 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 Section 4.2.1. 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 Active Threat detection signals received.
 - 2) Target size is 100% of Active Threat detection alarm signals received in the assessment time frame.
 - 3) Minimum sample size shall be 5 alarm events, up to a maximum of 15, or any sample available if less than 5, and shall include samplings of all *Alarm Groups*.
 - 4) Documentation of any remedial training conducted shall be kept and be available for inspection.
- d. The Section 2.1 Compliance Monitoring Process shall include periodic self-assessment by the AMC of alarm event records described in Section 4.1 to determine:
 - 1) *Completeness of records to understand how the event was handled.
 - 2) *Compliance with Section 2.1 for each *Alarm Group* determination.

3) *Accuracy of *Alarm Group* determinations based on the information and *Additional Risk Qualifiers* available at the time the event was handled.

- e. If compliance with Section 4.2.1 d) 1) or 2) falls below 80%, the station shall take action to retrain staff, adjust the system program, or other action that mitigates the root cause(s) of noncompliance.
- f. If compliance with Section 4.2.1 d.3) falls below 80%, the station shall retrain staff, adjust the system programming or other action that mitigates the root cause(s) of noncompliance.
- g. The effectiveness of corrective actions described in Sections 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)

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, when appropriate.

5.1. Data Privacy and Retention Considerations

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

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 GROUPS				
GROUP A	GROUP B	GROUP C	GROUP D	GROUP E
Active Shooter/ Aggressor	Weapon - Present	Weapon Detected Not Human Confirmed	Threat Present	No Notification
All Confirmed	Firearm Detected	Firearm Detected	No human confirmation	Communications: Human or Analytics
Gunshots Detected	Video Analytics Firearm Detected	Gunshot Detected	Person claims to have weapon	There is no threat present
Video Observed Gunshots	Explosives Detected	Person claims to have weapon - Human and/or Analytics confirmed	Lockout alarm Threat outside of facility. Exterior doors secured	
Active Shooter	Non-firearm Detected		Lockdown alarm A threat within the facility	
Active Aggressor				

ALARM GROUPS				
GROUP A	GROUP B	GROUP C	GROUP D	GROUP E
Active Shooter/ Aggressor	Weapon - Present	Weapon Detected Not Human Confirmed	Threat Present	No Notification
All Confirmed	Firearm Detected	Firearm Detected	No human confirmation	Communications: Human or Analytics
Gunshots Detected	Video Analytics Firearm Detected	Gunshot Detected	Person claims to have weapon	There is no threat present
Video Observed Gunshots	Explosives Detected	Person claims to have weapon - Human and/or Analytics confirmed	Lockout alarm Threat outside of facility. Exterior doors secured	
Active Shooter	Non-firearm Detected		Lockdown alarm A threat within the facility	
Active Aggressor				

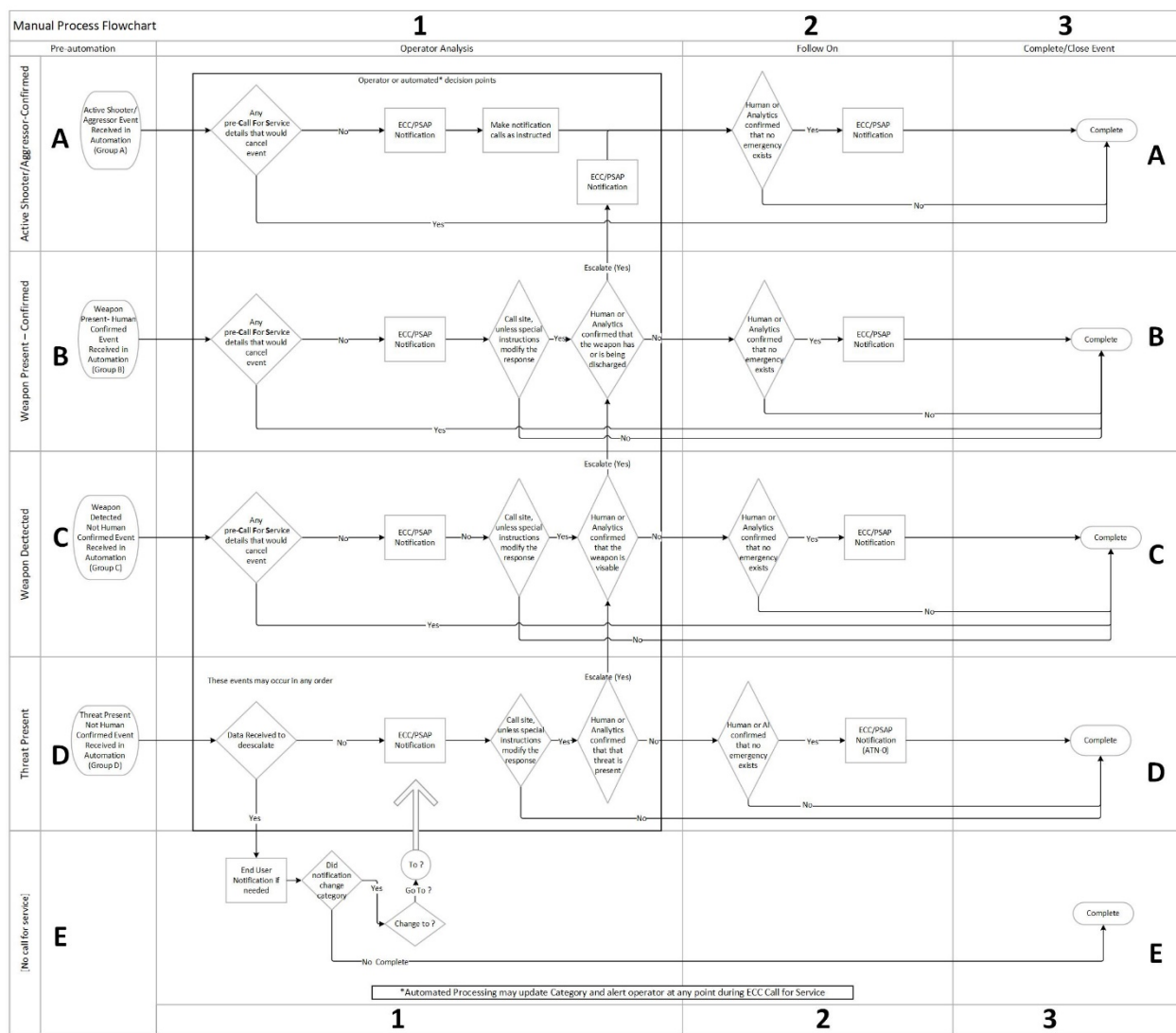
Annex C (Informative)

5.3. Active Threat Alarm Script

No,	Event Data	Suggested Dialogue / Examples
a.	Company Greeting	Dia: Hello this is operator XX,
b.	Alarm company name	Dia: Calling from ABC Alarm Company
c.	Active Threat notification.	Dia: We have received a Human Confirmed, Active Threat Notification, Weapons detected.
d.	Address (including Apt. No.)	Dia: Address is 123 Main St.
e.	Location/area information	Dia: The weapon is detected in the main lobby.
f.	Persons in Possession of “Weapons”, “Active shooter”, etc.	Dia: No persons seen in possession.
g.	Sounds heard (Describe)	Dia: We can hear what sounds like threats being made.
h.	Type of premises, (School, Multi FI building, campus, etc.)	Dia: The premises is a high school.
i.	Video, <i>metadata</i> , and/or audio available,	Dia: We don’t have any video or audio.
j.	Alarm company operator number	Dia: This is Operator 25.
k.	Anyone enroute to premises	Dia: The building security is responding.
l.	Permit Information	Dia: The premises has a permit No. 12345.
m.	Directions to the site	Dia: The premises is on the south side of Main Street and 2 nd avenue.
n.	Site Information	Dia: The school is on a “lockout” condition.
o.	Alarm center call back number	Dia: Our call back number is 123-123-1234.
p.	Alarm company incident number	Dia: Our ticket number is: A1234-59.

Annex D (Informative)

5.4. The Entire Swim Lane Flow Diagram



Annex E (Informative)

5.5. Compliance Management

A 4.1.1 The intent of Section 4.1 is to ensure 1) that sufficient information is captured during alarm event handling to allow post-event analysis and 2) that data upon which an escalate/de-escalate decision was made is retained for use by public safety, the *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 *AMC* analysis or *NRTL* audit of compliance. In such cases, the intent of 4.1.3.b)) and c)) is to allow the *AMC* 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: An *AMC* 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 the *AMC*’s analysis and *NRTL* audit, the *AMC* 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. With what appears to be a rifle.
- c. Seeing a short male, in blue jeans, red plaid shirt, with a face mask, with a revolver, crossing the production floor.
- d. Saw three individuals running out the rear entrance, but the picture was very poor, so no further details.
- e. Heard sounds of multiple voices (male and/or female), discussing where to go “next,” then moved out of range of audio.
- f. Observed an individual with a handgun entering the main lobby.
- g. Received *metadata* that a weapon had been detected.

A 4.1.4 The intent is to ensure a) that the data upon which an escalate/de-escalate 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, an *AMC* focused on record completeness becomes critically important when an *AMC* uses ATN-01 methods that rely on human operator action to document parts or all of an alarm event handling.

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

A4.2.1 d Quality control procedures that include documented supervisor monitoring of event handling can effectively identify and correct errors in the decision making of the *Alarm Group* escalation/de-escalation.

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

Comp by: _____ Date: ____/____/____

Compliant Audit-Work Sheet

Number	System Number	Time/ Date	Flowchart Columns 1					Flowchart Column 2				Flowchart Column 3	
			A	B	C	D	E	F	G	H	I	J	K
			Confirmed No Emergency	ECC/PSAP Notified	Call to Site Mod-Y/N	Escalate Yes/No	Group Determine d	Audited Ground	Confirmed Yes/No Emergency	ECC/ PSAP Yes/No	Changed Level	Complete	Complaint Y/N
1			Recorded Ground										
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													

Process and Description(s)				
Enter AMC Answer & Whether or Not Correct				
Question	Ans're	Correct	Question	Ans're
Recorded Group			Recorded Group	
Yes/No Emergency Exist			Yes/No Emergency Exist	
Yes/No ECC/PSAP Notified			Yes/No ECC/PSAP Notified	
Yes/No Call to Site			Yes/No Group Change	
Yes/No Escalate			Recorded Group	
Yes/No Group Change			Yes/No Completed	
Recorded Group			Yes/No Complaint	

Group A-Active Shooter/Aggressor - Confirmed

A Call for Service, knowing person or persons are present and there is an active threat to life, confirmed by a human or analytics.

Group B- Weapon Present - Confirmed

There is a weapon present and it has been confirmed by human or analytics.

Group C- Weapon Detected

Weapon had been detected and it has not been confirmed by human or analytics.

Group D-Threat Present

There are signs of a threat to life and it has not been confirmed by human or analytics.

Group E - No Call for Service

Annex F (Informative)

5.6. Common Industry Terms

5.6.1. 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.

5.6.2. Alarm Verification (See ANSI/TMA 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 an *AMC*.

5.6.3. 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.

5.6.4. Computer Aided Dispatch (CAD) System

A computer-based system that aids Public Safety Telecommunicators (PSTs) by automating selected dispatching and record-keeping activities. The use of a computer-based system by a PST electronically transmits incident details to the computers in emergency vehicles.

5.6.5. 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

5.6.6. 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.

5.6.7. Notification (See [1.2.11 Call for Service](#))

5.6.8. Call for Service Cancel

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

5.6.9. Occupant's Phones, or other location services - /GPS on/off Premises

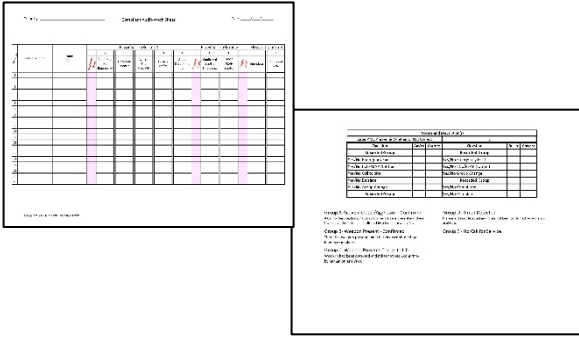
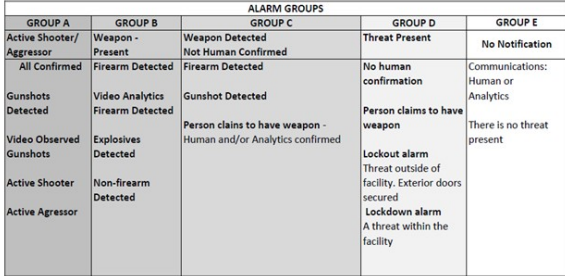
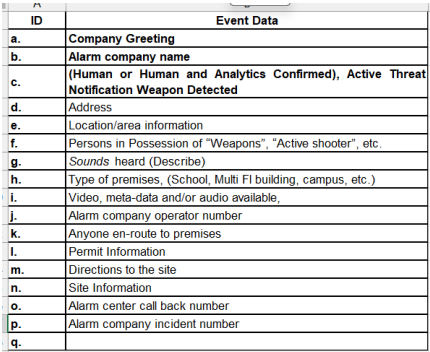


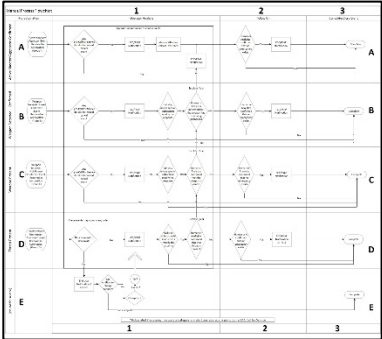
Technology that provides location information of authorized person(s) at the protected premises.

5.6.10. Visual Images

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

Annex G (Informative)

5.7. Available Forms for Download

	
<p>Compliant Audit Work Sheet PDF (Portable Doc) Compliant Audit Work Sheet XLXS (Excel)</p>	<p>Operator Assistant Card Blk-Wht PDF (Portable Doc) Operator Assistant Card Blk-Wht XLXS (Excel)</p>
	
	
<p>Active Threat Alarm Script Sheet PDF (Portable Doc) Active Threat Alarm Script Sheet XLXS (Excel)</p>	<p>Swim lane as ATN (JPG (Image)) Swim lane as ATN (PDF (Portable Doc)) Swim lane as ATN (VSDX (Visio))</p>