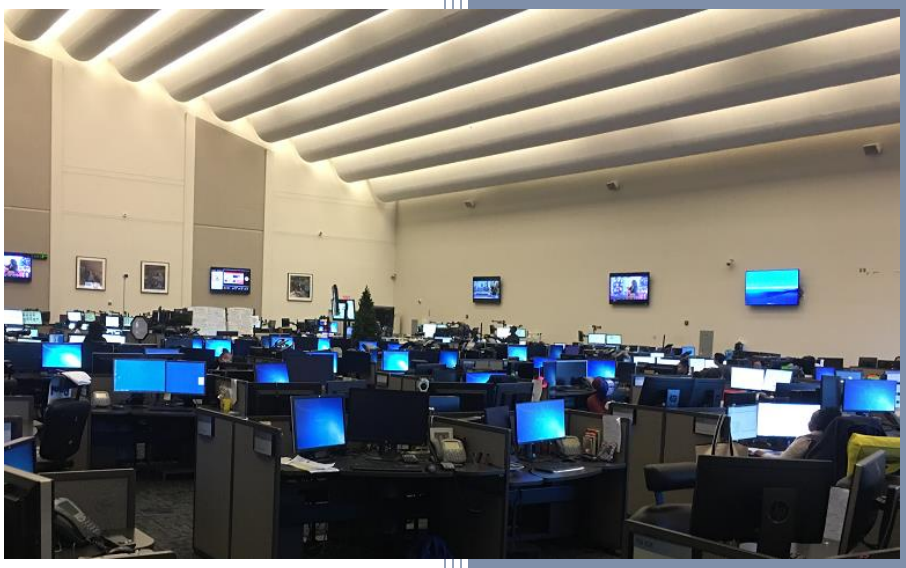
IJIS Institute

ASAP-to-PSAP Case Study on Standards and Outcomes



IJIS Institute

Public Safety Technical Standards Committee

November 2017

Principal Authors
Bill Hobgood, City of Richmond, Virginia
Becky Ward, FATPOT Technologies

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following IJIS Institute Public Safety Technical Standards Committee (IPSTSC) authors and contributors and their sponsoring companies and organizations for supporting the creation of this document:

Principal Authors

- Bill Hobgood, City of Richmond, Virginia
- Becky Ward, FATPOT Technologies

Principal Contributors

- Nate Daniels, Northrop Grumman
- Rochelle Danielson, Versaterm
- Valeria Ferrell, TriTech Software Systems
- Anita Ostrowski, Vector Security

Contributors

- Mike Alagna, The IJIS Institute
- Tom Dewey, Advanced Justice Systems
- Jay Hauhn, The Monitoring Association
- Steve Hoggard, Spillman Technologies, a Motorola Solutions Company
- Charles Stortz, Logistic Systems Inc.

Important Notice:

The information contained in this paper is believed to be accurate at the time the paper was prepared. However, some of the information contained herein will become outdated as soon as the last sentence is typed as new CAD providers begin to participate in the ASAP program, as new alarm monitoring companies join the program, and as more PSAPs go live. Likely some of the processes and procedures may also be modified. The reader is encouraged to visit the referenced websites at the end of this paper for the most current information.

TABLE OF CONTENTS

INTRODUCTION

Automated Secure Alarm Protocol (ASAP) was launched in 2011 as a public-private partnership designed to increase the efficiency and reliability of emergency electronic signals from alarm monitoring companies to public safety answering points (PSAPs). ASAP uses ANSI-standard protocols developed cooperatively by the Association of Public Communications Officials and Central Station Alarm Association (now named The Monitoring Association).

According to the National Emergency Number Association (NENA), as of January 2017, the United States had 5,874 primary and secondary PSAPs with an estimated 250 million calls made to 911 each year. The Security Industry Alarm Coalition reports that Central Stations (herein after called alarm monitoring companies) that are connected to alarms at homes and businesses relay 22,800,000 alarm notifications to local PSAPs annually to facilitate the dispatch of public safety responders.

PSAPs are faced with an ever-increasing volume of 911 calls, which require human interaction to obtain the information necessary to send the right help to the right location. While priority must be given to answering 911 calls, PSAPs also must answer their non-emergency lines as well. Alarm monitoring companies that deliver alarm notifications via telephone to PSAPs must use 7-digit (10-digit when long distance) non-emergency numbers as assigned by the PSAPs. Those lines experience frequent answering delays due to 911 calls of emergency events having priority.

The sheer number of PSAP call volumes prompted the desire to automate those incoming calls that had consistent, structured and limited data: call type, location, and reporting party. Verbal information originating from alarm monitoring companies was a perfect fit – if these calls could be entered directly into CAD, skipping the call answering stage and the interrogation stage by PSAP call-takers, time could be saved on every call.

If a standard data exchange format for electronically transmitting information between an alarm monitoring company and a PSAP could be developed, then this data exchange could replace the telephone calls between the

ACRONYMS

ANS – American National Standard

APCO – Association of Public Safety Communications Officials

ASAP – Automated Secure Alarm Protocol

CAD – Computer Aided Dispatch

CMS – Central Monitoring Station

CSAA – Central Station Alarm Association, now called The Monitoring Association

GJXDM – Global Justice XML Data Model

IEPD – Information Exchange Package Documentation

NENA - National Emergency Number Association

NIEM – National Information Exchange Model

NLETS – The International Justice & Public Safety Sharing Network (formerly known as the National Law Enforcement Telecommunications System

PSAP – Public Safety Answering Point, or 911 Center

TMA – The Monitoring Association

alarm monitoring company operator and the 911 PSAP call-taker. This was the idea behind ASAP. It was developed over a nearly five-year period with three goals in mind:

1. Eliminate the telephone calls between the alarm monitoring company and the 911 PSAP.

2. Eliminate miscommunication between the alarm monitoring company operators and the 911 PSAP call-takers.

> *"When phone lines are overloaded, PSAPs give priority to 9-1-1 calls before calls that come in on the seven-digit administrative lines used by alarm monitoring companies' operators to report alarm signals from their customers. This means some alarm monitoring companies experience long waiting times or may even see calls go unanswered."*
>
> ~ Bill Hobgood, City of Richmond, Virginia

3. Decrease processing and response times to alarm-related calls for service with the objective of an increase in law enforcement apprehensions made, a decrease in fire duration and damage, and better medical outcomes with lives saved.

This is exactly what the ASAP program provides.

Purpose

This paper will provide background on why Automated Secure Alarm Protocol (ASAP) to Public Safety Answering Point (PSAP), referred herein as ASAP-to-PSAP, is important, and what it takes to get started. Although several papers and presentations exist on the ASAP project, no one paper compiles all relevant information together in one place. The paper will answer questions not covered in other articles and illuminates a path for CAD service providers, consultants, practitioners, and systems integrators to understand ASAP benefits and begin to take the steps to gain greater participation in the ASAP-to-PSAP program.

Intended Audience

This paper is intended for practitioners desiring ASAP, CAD service providers being asked to engineer an ASAP-to-PSAP interface, middleware providers, consultants, alarm monitoring companies not yet participating in ASAP, and the alarm monitoring automation providers that have not developed an ASAP interface.

WHAT IS ASAP?

Of the 250 million calls to America's PSAPs annually, nearly 23 million are calls from alarm monitoring companies. While local alarm service organizations often sell and install alarm systems to homeowners and businesses, there is usually an alarm monitoring company that provides the actual monitoring of these systems and is charged with initiating and coordinating the appropriate notifications if an alarm is received. Typically, the alarms they receive are electronic but they may also be from an involved person.

The alarm monitoring company has alarm location data, event type data (i.e., intrusion alarm, fire alarm, personal alarm, etc.) when they initiate the call to the 911 center. With the thought to automate the transfer of this information directly into the CAD system, the vision of ASAP was born.

With ASAP, critical and accurate information is relayed and processed very quickly via a network transport consisting of the International Justice & Public Safety Sharing Network, (formerly known as the National Law Enforcement Telecommunications System or Nlets) as the core hub with a message broker, and each of the fifty state switches as a spoke, with the ASAP-participating alarm monitoring companies and PSAPs as the end points. This topology ensures that complete and precise information is transmitted to the PSAP every time. The ASAP program has the potential to save PSAPs and emergency services millions of dollars and save lives, by reducing manpower costs for answering alarm calls and speeding emergency response to these events.

The ASAP community includes:

- Alarm monitoring companies,
- 911 PSAPS and their CAD providers,
- Nlets as the main transport method coupled with each state's message switch, and
- The Monitoring Association (formerly known as the Central Station Alarm Association) providing the Message Broker.

Standards

ASAP is an American National Standards Institute (ANSI)-standard, based on open standards. One size fits all, no matter how large or small the agency. CAD providers who develop the interface once can market it continuously to their client base.

> The original official American National Standard (ANS) name is ***APCO/CSAA 2.101.1-2008 ANS Alarm Monitoring Company to PSAP CAD External Alarm Interface Exchange*** and it was originally called External Alarm Interface Exchange ANS. It was formerly adopted as a standard on January 15, 2009, after nearly five years of work by PSAP practitioners, the Central Station Alarm Association (CSAA) now called The Monitoring Association (TMA), alarm monitoring companies, and CAD providers. It was rebranded in April 2011 as the *Automated Secure Alarm Protocol (ASAP)*. The renewed ANS name is ***ANSI/APCO/CSAA 2.101.2-2014 APCO / CSAA Standard (ANS) for Alarm Monitoring Company to PSAP CAD Automated Secure Alarm Protocol (ASAP)*** and it was renewed on August 5, 2014. ANSI requires that all standards be renewed no less often than every five years. Generally, renewals do include updates to the standard. Such was the case in 2014.

ASAP uses XML and was initially converted from custom template to GJXDM then to NIEM 2.0. The current ASAP schema version is 3.3. Today, the ASAP standard has been certified and deployed by 8 CAD providers with many more in development, and in 30 PSAPs across in 11 states plus the District of Columbia. An equal number of PSAPs are in queue to implement ASAP soon.

FLOW DIAGRAM: WITH ASAP AND WITHOUT ASAP

Without ASAP

Figure 1 depicts the standard processing and response times for alarm handoffs to 911 by alarm monitoring companies using the traditional method of delivery via telephone.

Upon receipt of an alarm signal by the alarm monitoring company, the company initiates its contracted verification procedures to verify the legitimacy of the alarm. It then calls the appropriate PSAP to report the incident type and location. The PSAP's call taker interrogates the alarm monitoring company caller and verifies the information, and enters the call into its CAD system. Telecommunicators see the incident in their dispatch waiting or pending call queue and dispatch the appropriate units.

FIGURE 1: STANDARD PROCESSING COMPONENTS WITHOUT ASAP

While the alarm monitoring company processing remains constant in this scenario as well as the one below (i.e., with and without ASAP), the two middle pieces are most impacted by implementing ASAP. The ringing phone and the time to answer it goes completely away, and the gathering of information is transformed into simplify processing the data electronically received.

The process depicted above (from the time the alarm monitoring company initiates the transmission of the alarm notification to call-for-service creation) can take anywhere from 1½ minutes to 3 minutes or more!

With ASAP

The difference in the traditional method using the telephone versus using the new alarm exchange standard becomes apparent very quickly. Figure 2 depicts the significant reduction in processing and response times using ASAP for alarm handoffs to 911 by alarm monitoring companies compared to the traditional method of delivery via telephone.

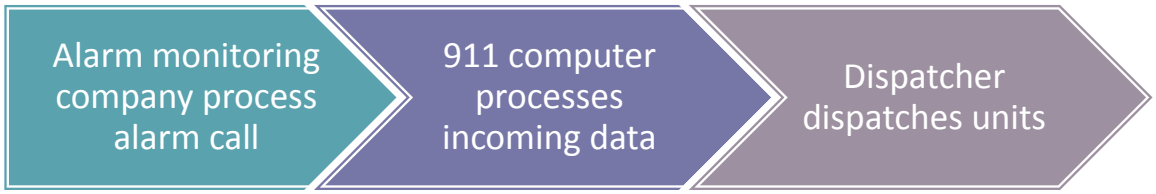


FIGURE 2: STANDARD PROCESSING COMPONENTS WITH ASAP

The process depicted above usually takes 15 seconds or less, usually 5 seconds on average!

How ASAP Works – The Details

The process on how ASAP works is straightforward. Once an alarm monitoring company operator determines that an event must be handed off to 9-1-1, the new alarm event is electronically sent from the alarm monitoring company over a secure, dedicated network to the designated 9-1-1 center for dispatch of public safety resources. It is important to mention that ASAP in no way changes the steps that an alarm operator must take before notifying the PSAP. For example, enhanced call verification (ECV) is required of all alarm monitoring companies, and the alarm monitoring company operator still performs these procedures (two attempts to reach the key contact) prior to notifying the PSAP through the use of ASAP.

The information that is sent to the PSAP includes all data about the premise monitored by the alarm system, such as address, event type, directions to the location (for rural areas), alarm trigger points, contact information, permit info, etc. Data transmitted also includes information about the alarm monitoring company, such as the name of the company, operator ID, contact information, alarm service company info, as well as the alarm monitoring company's incident number.

Next, the PSAP's CAD system responds with the appropriate **Accept** or **Reject message** and a PSAP incident number is created automatically if the event has been accepted. Two things are required from the alarm monitoring company by the PSAP: a valid address within the jurisdiction and a valid event type such as *Burglary*, or *Holdup*, etc. There is a standardized event type list with the ASAP standard.[1] Failure to transmit a valid street address or a valid event type will result in the CAD system sending a Reject message back to the alarm operator. Keep in mind that the CAD system is performing these steps automatically without any 9-1-1 staff intervention and without a telephone call.

As soon as the CAD accepts the incident as valid, it appears in the dispatcher's pending calls queue ready for dispatch of the appropriate resources. The internal computer processing takes only seconds. Note that some CAD providers can further automate the dispatch process by enabling the computer to automatically recommend and dispatch units for certain types of incidents.

[1] Alarm Event Types, Translation Worksheet, and Richmond VA Example

An **Update** message can be used by the CAD user or the alarm operator for the following situations including but not limited to:

- Requests for cancellation by the alarm monitoring company,
- Updates concerning key-holder information by the alarm monitoring company, and
- Updates from the PSAP telecommunicator or field resource requesting additional information such as an estimated time of arrival for the key-holder.

As an example, if the radio dispatcher or even a field resource has a question for the alarm operator, they can send the question to the alarm operator as an **Update** transaction and ask their question. Examples could include: "Do you have an ETA for the key-holder?" or "What is the key-holder's name and what will they be wearing?" All CAD providers having an ASAP interface solution must provide this capability to the CAD users. Some CAD providers may extend this capability to the mobile users to enable field personnel to transmit questions to the alarm operator.

All **Update** messages are logged to the CAD call-for-service regardless of the origin of the message.

CAD systems can send a **CADUpdate** to the alarm monitoring company when emergency responders are dispatched, arrive on the scene, and clear from the scene along with disposition information.

The figure below depicts the two-way, bidirectional flow of information throughout the system. The TMA Message Broker co-exists with the Nlets Message Switch in Phoenix, Arizona.

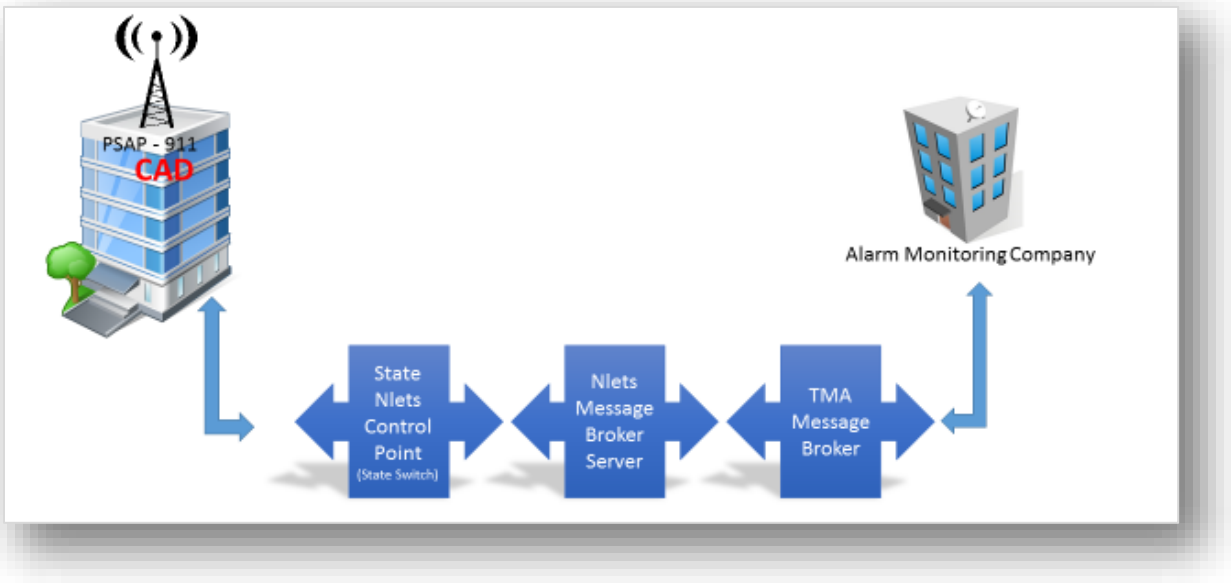


FIGURE 3:TWO-WAY, BIDIRECTIONAL FLOW OF INFORMATION THROUGHOUT THE SYSTEM.

BENEFITS AND HARD SAVINGS

The achievement of three goals of ASAP will:

1. Eliminate the telephone calls between the alarm monitoring companies and the PSAP;

2. Eliminate miscommunication between the alarm monitoring companies and the PSAP; and

3. Decrease call processing and response time and increase favorable outcomes for alarm originating calls using ASAP are quantifiable by agencies capturing relevant statistics.

Eliminating telephone calls from the alarm monitoring companies to the PSAP saves not only call answering time but also call processing time. Busy PSAPs trying to adhere to NENA's recommendations on call answering time (90% of calls within 10 seconds during the busy hour and 95% within 20 seconds) may have to ignore calls coming in on the 7-digit line when things get really busy. Additionally, it's often hard to hear callers and accurately capture the information they are trying to relay. Spelling mistakes occur at the best of times, and understanding caller's speech due to accents or audio quality of the connection impacts call processing time. ASAP works efficiently regardless of how inundated the PSAP may be. Saving time in any part of the 911 process translates into saving lives in medical events, reducing property damage in fire events, and apprehending perpetrators in law enforcement events.

Save Time – Save Lives

How does the time regained benefit the community? By bypassing the routine and time-consuming data capture of information from third-party callers (alarm monitoring companies), call takers can focus on human interaction 911 calls. For a medical alarm call where a victim is having a heart attack, each minute of delay decreases a person's chance of survival by 10%. If processing alarm monitoring company calls at the PSAP takes 1½ to 3 minutes, the cardiac arrest victim's chances of survival just decreased by 15% to 30%. For fire alarm incidents involving fires, a delay of 1½ to 3 minutes can allow a fire to more than quadruple in size, making it harder to extinguish and endangering lives.

Save Money

How does the time regained benefit the 911 center? By automating calls originating from alarm monitoring companies from human (telecommunicator) processing, additional staff in Full-time Equivalents (FTE) is effectively created. Staff normally tasked with handling alarm calls can be reassigned to other duties in the PSAP or other departments. A large PSAP with a plethora of alarm calls can be transformed from being understaffed to being adequately staffed.

Another benefit that is difficult to measure is the avoidance of litigation. Mistakes by telecommunicators do happen, and sometimes the results are tragic. Civil suits are frequently filed against the accountable jurisdiction and the payment to the litigant can be in the millions of dollars. Because the ASAP program provides some of the most accurate data and concise calls-

for-service in the PSAP, there is a strong likelihood that lawsuits have been avoided because human intervention and error in miscommunication are removed.

ASAP has the potential to improve the jurisdiction's International Organization for Standardization (ISO) rating and potentially lower its insurance costs. ISO collects information useful for many aspects of insurance underwriting, including public fire protection. Through the Public Protection Classification (PPC) program, ISO evaluates municipal fire-protection efforts throughout the United States. Insurance companies use PPC information to help establish fair premiums for fire insurance and generally offering lower premiums with better protection. Part of the ISO rating is an evaluation of the emergency communications center and how effectively, efficiently, and reliably fire alarms are received and processed. Find out more about ISO at https://www.isomitigation.com.

Better Service to the Community

Guilford County, North Carolina, stated in January 2016 that ASAP will not only save lives but will reduce the number of calls received by 911 operators by about 20,000 a year. This should potentially free up the emergency lines and get residents help much faster. Residents had a positive reaction to the program and said the time savings was crucial, and getting help more quickly was better for everyone.[2]

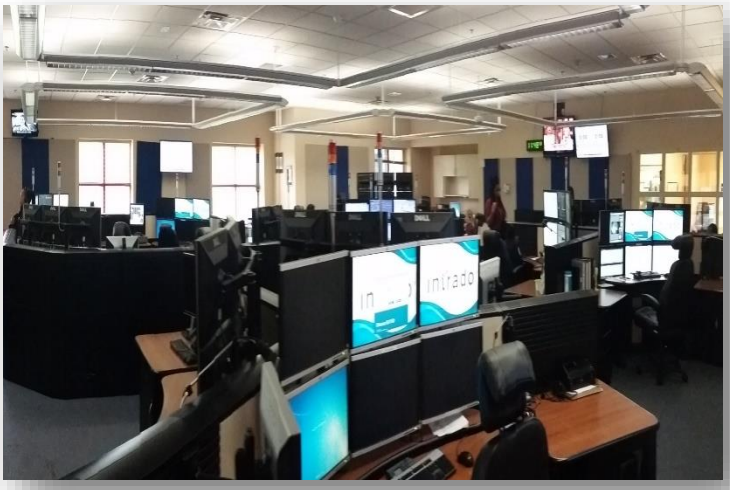
Sample Outcomes

The following data has been self-reported by each agency.

Richmond, Virginia

Richmond, Virginia, provided the following statistics for its PSAP operation regarding the ASAP program:

- 50,000+ alarms exchanges have been transmitted.
- 1½ minutes was the average process time before ASAP.
- Some calls took 3 minutes or more to process.
- Alarm operators sometimes placed these calls on hold for 8-10 minutes.



[2] See a video, Guilford County Sees Faster Response, at http://www.wfmynews2.com/news/guilford-metro-911-homeowners-could-see-faster-response-times/51911611.

- Telephone calls from alarm operators to the PSAP was considered the worse call in the PSAP.
- With ASAP, these calls now take 15 seconds or less.
- With ASAP, these calls are the most accurate, and are considered the best call in the PSAP.

The outcome of this project at the City of Richmond and another early adopter, York County, Virginia, has been a huge success, resulting in several thousand alarm events transmitted electronically to Richmond's 911 center while the 911 center itself had several thousand less telephone calls to handle. Now:

- Call processing takes 15 seconds or less.
- Is the most accurate and concise call in the PSAP.
- Not a single mistake has occurred – no spelling mistakes, no accidental transposition of street address numbers, no low-volume headset issues, and no need to try to interpret accents.

ASAP works efficiently regardless of how inundated 9-1-1 call takers may be. During storms and other natural events (like the Virginia earthquake in August 2011), call-takers are inundated with 9-1-1 calls, and resources to answer the 7-digit lines are often lacking. With ASAP, there is no delay and no dependency waiting on a call taker to answer the telephone.

Houston, Texas

Houston, Texas, is the fourth-largest PSAP in the U.S. and provided the following information about its PSAP operation before and after adopting ASAP:

- In CY 2015, the Houston Emergency Center (HEC) created 155,000 alarm calls:
  - Only 16% (24,600) were received via ASAP with 84% (131,000) initiated by telephone.
- Non-ASAP dispatched alarm calls were received through the non-emergency number:
  - Each alarm calls typically required 2.5 phone calls to process the call from start to finish, equaling 330,000+ calls added to the workload.
  - The 330,000+ non-ASAP calls represented 40% of the 800,000 non-emergency calls to the HEC.

- The HEC's non-emergency line is typically staffed with eight call takers present 24-hour-a-day/seven-days-a-week.
- With the additional of ADT in March 2016, ASAP is currently processing 150 alarm calls day, equating to 55,000 calls per year.
- This equates to eliminating 140,000 phone calls to the HEC.
- Hard savings to date is about $400,000.
- With the addition of ADT and other big players, the hard savings is anticipated to exceed $1M.

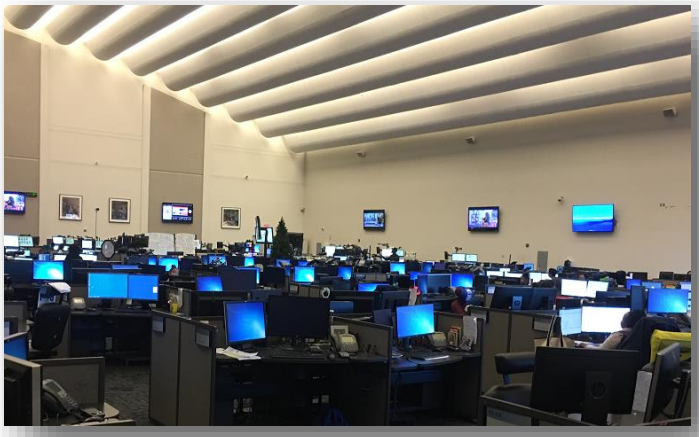
Houston's projected savings of $1 million annually is due to the reduction in staff dedicated to answering non-911 lines. As Houston's non-emergency call volumes drop, some of these staff can be reassigned to other departments and agencies within Houston's government.

Washington, DC

The Office of Unified Communications (OUC) in Washington, DC, provided the following information about its PSAP operation before and after adopting ASAP:

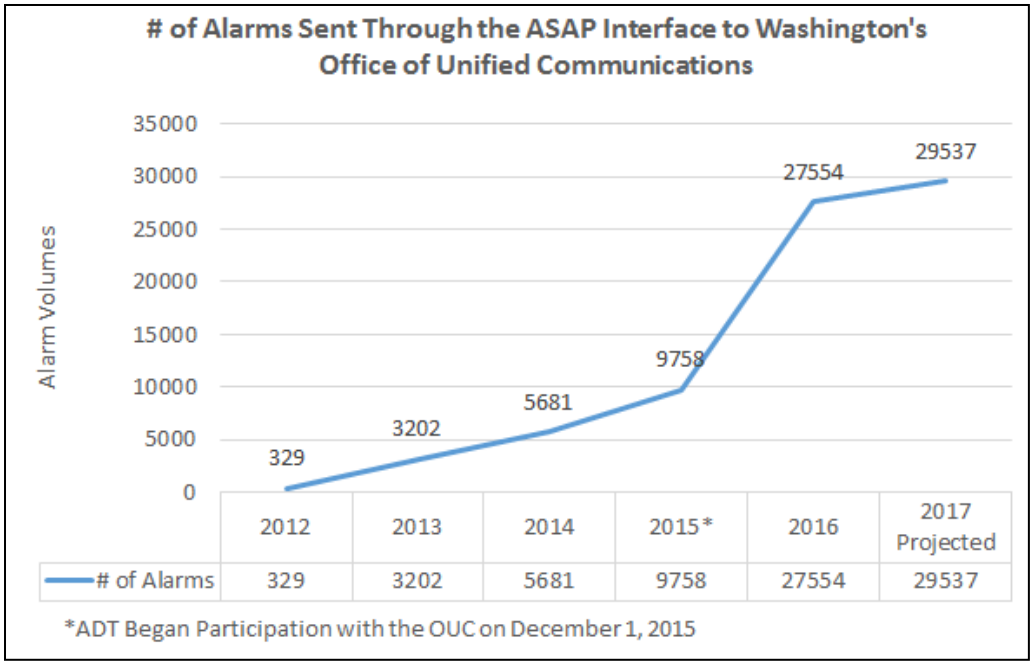
- OUC receives 50,000 call-in alarms annually from alarm monitoring companies, resulting in:
  - Two minute average processing time for each alarm call.
  - Three phone call average needed to process each call.
  - Negative impact to the center by tying up phone lines and needlessly engaging 911 call takers.

OUC reports the following results after implementing ASAP:



- 59,950 total alarm notifications since October 2012.
- Alarm call composition:
  - 79.9% Burglar alarms,
  - 9.4% Fire alarms,
  - 2.2% Medical alarms, and
  - 8.5% Holdup/panic alarms.

The graphic below depicts the rapid rise of alarms handled using the ASAP interface, and reflects the impact of additional alarm monitoring company participation.



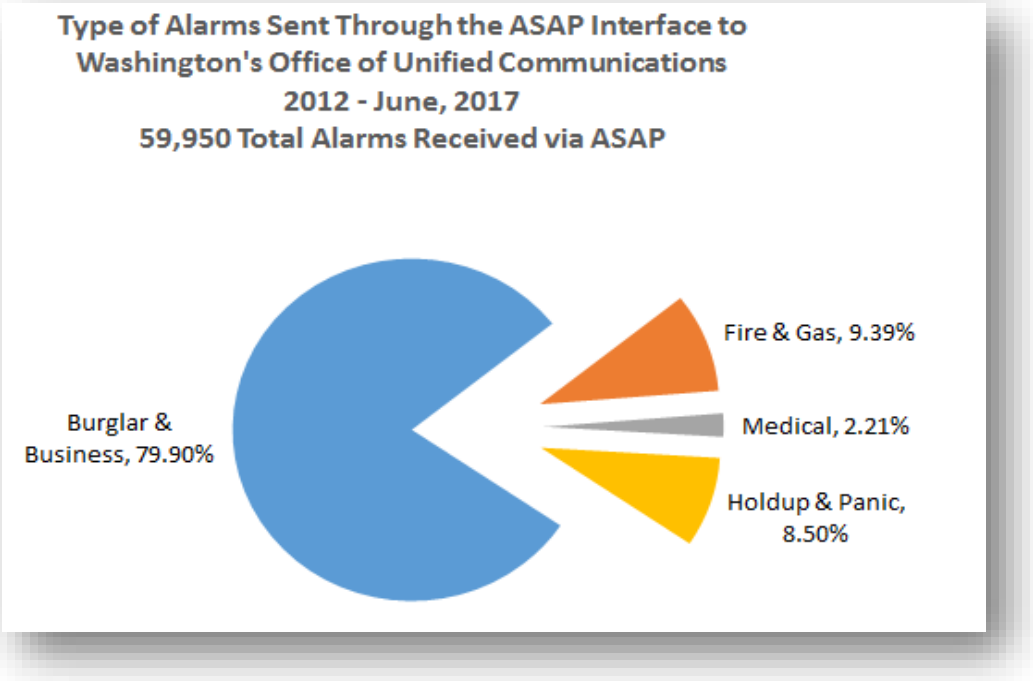


FIGURE 4: RAPID RISE OF ALARMS HANDLED USING THE ASAP INTERFACE.

Boca Raton, Florida

The City of Boca Raton, Florida, reported that with only eight alarm monitoring companies connected, 37% of all alarm calls were coming in through ASAP at the outset.

FIGURE 5: OUTCOMES IN BOCA RATON, FLORIDA.

James City County, Virginia

James City County, Virginia, is in the tidewater area of Virginia, borders York County, Virginia, and is about 40 miles east of Richmond, Virginia. The following data was provided by the PSAP.

	2013	2014	2015	2016	2017							Grand Total	%
Alarms Rcvd Via ASAP	Total	Total	Total	Total	Jan	Feb	Mar	Apr	May	Jun	Total	Grand Total	%
Burglar	75	153	269	617	45	52	55	61	61	48	322	1266	72.72%
Fire	30	36	43	77	6	3	5	11	7	8	40	200	11.49%
Tamper	2	3	6	4	0	0	0	0	1	0	1	15	0.86%
Medical	1	4	24	36	1	3	2	1	3	0	10	71	4.08%
Gas	1		1	6	5	6	4	0	1	0	16	23	1.32%
Holdup	1		5	12	2	2	2	0	1	3	10	24	1.38%
Panic / Duress		11	31	68	6	4	3	5	7	4	29	142	8.16%
Total	110	207	379	820	65	70	71	78	81	63	428	1741	

FIGURE 6: ASAP ALARM NOTIFICATION VOLUMES IN JAMES CITY COUNTY SINCE JANUARY 2013.

ASAP-TO-PSAP STATE STATUS MAP

Figure 7 indicates where ASAP is in production as well as each state's readiness that encompasses the status of the state message switch upgrade necessary to handle ASAP transactions.

Note that California has a unique environment, notated as *special*, as several counties have county message switches that connect to the state switch. The state switches already conform to Nlets and CJIS Security policies. Each state must have the switch vendor configure the switch to accommodate Nlets Message Keys ALQ (Alarm Exchange Query), and ALR (Alarm Exchange Response).

Note that the state readiness status map changes frequently – view the most current version online at http://tma.us/asapdocs/ASAPReadinessMap10162017.pdf.

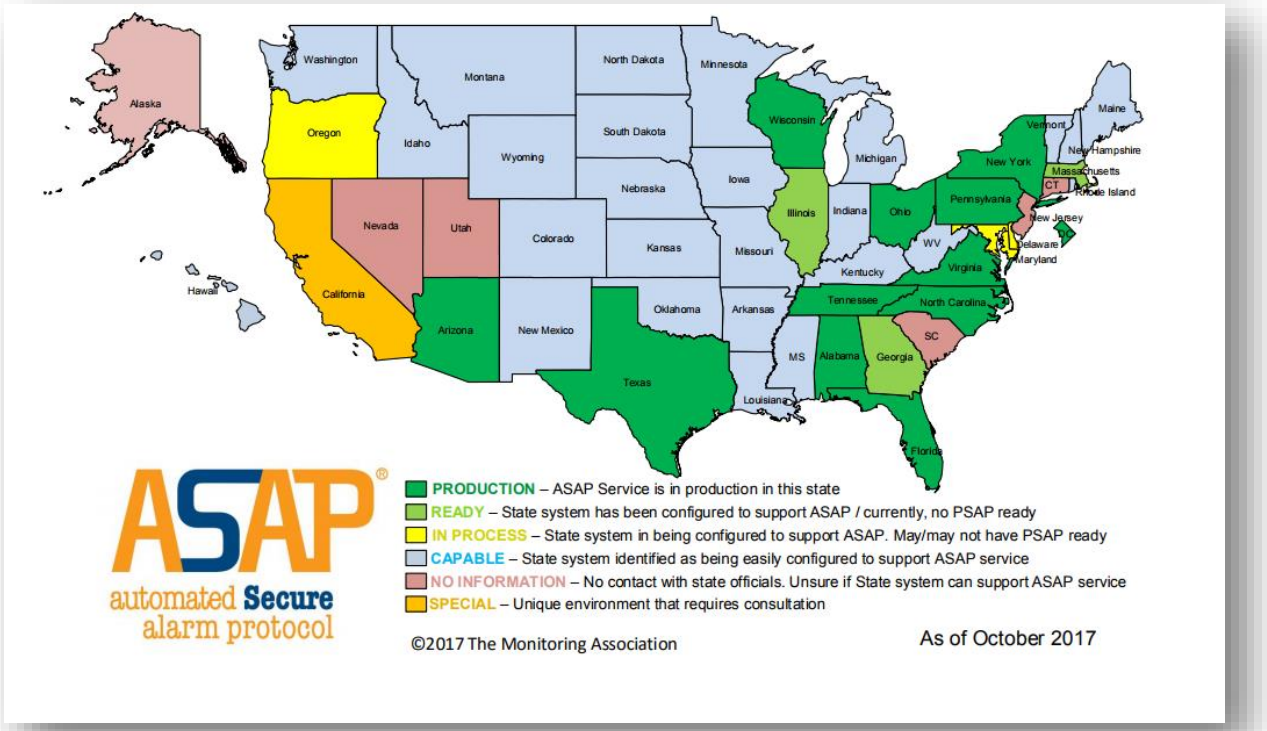


FIGURE 7: ASAP-TO-PSAP STATE SERVICE READINESS.

INVOLVED PARTIES

The ASAP program is expanding daily, and by the time you read this paper, the information below be out of date. Please check the resource section of this paper for links to the latest information.

PSAPS

The following table indicates PSAPs that are operational with ASAP:

PSAP Name/Location	Go Live
Boca Raton FL	12-2015
Bucks County PA	01-2017
Cary NC	05-2013
Chandler AZ	06-2012
Dane County WI	07-2017
Delaware County OH	07-2016
Denton County TX	10-2013
Durham City – Durham County NC	05-2016
Grand Prairie TX	03-2016
Guilford County – Greensboro NC	01-2016
Hamilton County TN	11-2017
Henrico County VA	11-2014
High Point NC	11-2016
Highland Park TX	04-2017
Houston TX	04-2011
James City County VA	12-2012
Johnston County NC	11-2016
Kernersville NC	05-2016
Loudoun County VA	10-2017
Manatee County FL	06-2017
Monroe County NY	04-2017
Morgan County AL	04-2012
Newport News VA	07-2017
Richmond VA (*ASAP's first pilot in 07-2006*)	12-2008
Rochester/Monroe County NY	04-2017
Tempe Police Department AZ	04-2014
Union County NC	09-2017
Washington DC	10-2012
Williamson County TX	01-2017
Wilson County NC	05-2017
York County – Williamsburg – Poquoson VA	07-2006 (pilot) 12-2008

The following PSAPs are in testing or implementation:

PSAP Name/Location	
Alpharetta GA	Mansfield OH
Beaumont, TX	Missouri City TX
Brentwood TN	Monroeville PA
Broome County NY	Onondaga County NY
Burleson TX	Pasadena TX

Chesapeake VA	Phoenix AZ
Chester PA	Prince George's County MD
Collier County FL	Riviera Beach FL
Dublin OH	Sarasota County FL
Erie County NY	Saratoga County NY
Hamilton County TN	Virginia Beach VA

Participating CAD Companies

The table below presents CAD provider companies that have implemented the interface as of the date of this paper's publication. There are additional CAD providers who have expressed interest or are under development.

Company	States Where Live	Product Certified
Hexagon (Intergraph)	DC, FL, VA	I/CAD (EdgeFrontier)
Northrop Grumman	NY, PA, TX	NG CAD (cobol) & Altaris
Versaterm	AZ	Versadex CAD
SunGard Public Sector	AL, NC, TX, VA	OneSolution CAD
Motorola	VA	Premier One
Alert Public Safety	OH	APSS Responder
TriTech	TN, WI	Inform CAD
Tyler (New World)	TX	Enterprise CAD
Developed in-House	Henrico County, VA	

Active Alarm Monitoring Companies

An alarm monitoring company is a company that provides services to monitor burglar, fire, and residential alarm systems. Note that one hundred alarm monitoring companies signed on as charter members with the TMA to participate in the ASAP-to-PSAP program. The following alarm monitoring companies are actively participating in the ASAP program.

Active Alarm Monitoring Companies
ADS Security (Nashville)
ADT
Affiliated
American Alarm
Central Security Group
Criticom Monitoring (CMS)

ESC
Guardian Protection Services
Johnson Controls Home Solutions, North America (formerly Tyco)
Monitronics
National Monitoring Center (NMC)
Protection 1 (recently merged with ADT)
Rapid Response Monitoring
Safeguard Security
Securitas US (purchased Diebold)
Stanley
United Central Control
Vector Security
Vivint

Please see http://tma.us/asap-status/ for the latest active status list as the list changes frequently.

Each alarm monitoring company must collaborate and test with each PSAP. A Traffic Authorization Letter (TAL) to enable the transmission of ASAP transactions to the PSAP must be signed by an authorized official representing the PSAP and submitted to the ASAP Service which manages the TMA's Message Broker.

Future Participating Alarm Monitoring Companies

The following alarm monitoring companies have signed a contract to participate in ASAP. They are either in testing or in the onboarding process.

Alarm Monitoring Company Name	
Arcadian	Guardian Alarm Co of Michigan
Ackerman	iWatch
Alarm Center, Inc	Kastle Systems
Alarm Central Station	Kings III
Alarm Detection Systems	LDS Church
ASG	MACE
AT&T	Monitoring America
AvantGuard	Peak Alarm
Buckeye Protective Service	PER MAR
CentraLarm	Richmond Alarm
Checkpoint	Security Central (Lake Norman)
CPI	Security Solutions
COPS	SEI
Devcon	Sentry Net
DGA	Tyco
DMC Security	Washington Alarm
Doyle	Watchlight
FE Moran	Wayne Alarm

STEPS FOR A PSAP TO GET STARTED

The PSAP is the primary driver and owner of the project. They must take ownership of all the steps involved in getting ASAP up and running.

1. First, PSAPs must make sure that they have executive stakeholder buy-in. This includes the director or CEO of the communications center as well as the political powers who hold the purse strings. It is also helpful to present information to the public to gain their support that will influence the executive and financial decision makers. Find out the status of your state's readiness for ASAP so that you can include this information in your report to the executives (see the map in the status section in this paper and also check the TMA website for the most up-to-date information).

2. Second, touch base with your state's Nlets representative to ensure that the PSAP can be allowed to receive and transmit ASAP transmissions over the state's connection to Nlets.

3. Third, contact your CAD provider to obtain a quote for the PSAP interface. The quote should include development and/or licensing cost, project management, training, iterative testing, and support/maintenance.

4. Fourth, complete the online contact form[3] or email asap@tma.us. TMA staff will forward the *ASAP Terms of Service*, the *ASAP-to-PSAP Readiness Questionnaire*, the *PSAP Information Form*, and an example initiation letter which acknowledges that PSAP's commitment and agreement with the ASAP Terms of Service. These forms should be completed and returned to TMA. TMA staff will schedule an on-boarding with the PSAP.

5. Fifth, hire a TMA-approved consultant with ASAP expertise for project management and coordination services.

The PSAP should also appoint a staff member to manage the project and the program after it is initially deployed. Familiarity with CAD and addressing systems are prerequisite qualifications for this individual. Support from the information technology department as well as a network engineer is also essential.

ASAP IMPLEMENTATION PROCESS

Each CAD provider's ASAP interface solution must be certified once upon completion of development. The certification process usually occurs at the CAD provider's first beta site. Once the product has been certified, the CAD provider may deploy the solution to multiple sites.

The PSAP's go-live is scheduled after the CAD provider's interface is tested in a test/training environment and then in the production environment with a seasoned alarm monitoring company. The contracted consultant will be on-site to conduct training and be on hand for the

[3] http://tma.us/asap-contact-us/

ASAP go-live. Testing leading up to the scheduled go-live is usually handled remotely. The consultant will oversee testing with each alarm monitoring company in a test environment. This testing is a prerequisite that leads to a Traffic Authorization Letter that must be signed by the agency to permit each alarm monitoring company to be moved to production with the agency. The consultant will issue a solicitation for address lists from each alarm monitoring company for pre-screening purposes and will provide the alarm monitoring company's information to create a test account that will be used for testing. The address on the test account is usually the address of the PSAP. Alarm monitoring companies are tested in the order they respond to the solicitation on a first-in, first-out (FIFO) basis.

At the time of go-live with each company, all addresses monitored by the alarm monitoring company will be transmitted to the agency's CAD system. The bulk address verification process includes all addresses being sent to the PSAP's CAD system as an ALQ transaction. When the alarm company begins this process, they are considered to be live with the PSAP simultaneously.

The CAD System will validate each address to be a valid address within the jurisdiction's response area, or will reject a bad address. The alarm monitoring company will work with the PSAP to resolve any rejected addresses. As each address is validated successfully, the address becomes eligible to be transmitted as an alarm notification. Occasionally, an alarm has been triggered within minutes or even seconds of the successful address validation, and is pretty exciting and rewarding.

Often, however, there are issues that come up during testing, and the consultant and agency personnel work with the CAD provider to correct any errors and retest. When everything is running smoothly, the system is moved into the production environment.

The consultant is normally onsite for two to three days. The morning of the first day is usually set aside for training the telecommunicators. Information is provided about the ASAP program with specific information about the changes that they will experience with their CAD, and how to send messages to the alarm monitoring companies. The afternoon of the first day involves bring up the alarm monitoring companies and testing.

Normally, the second day the system is switched into the production environment and goes live. The third day is needed for larger PSAPs with many alarm monitoring companies and perhaps for a new CAD provider with its first ASAP client.

CAD PROVIDER LEVEL OF EFFORT

The following CAD providers were interviewed and provided information about their development and implementation efforts for ASAP.

Versaterm

Versaterm completed their first implementation of the ASAP Alarms Interface with their Versadex CAD system in summer of 2012. The first client was Tempe Police Department in Arizona. The interface was very seamless to complete due to the great documentation and support from the police department and its consultant, Bill Hobgood.

Only one Versaterm developer was needed to complete the interface, and this individual had less than five years of development experience. This developer found the interface very straightforward to write due to the extensive documentation provided and also the assistance from the project consultant. With the availability of a knowledgeable person development went very smooth. Additionally, the first client, Tempe PD, had a technical and knowledgeable point of contact that was key to testing and implementation support.

The complicated pieces revolved around testing the interface in the live environment. Testing could be done in development very easily through Nlets and test calls but often additional testing with new alarm monitoring companies was required. There were occasional issues when new alarm monitoring companies came on board. Sometimes the new companies did not follow the protocol exactly as specified or they exposed an issue with the CAD interface. Testing with a specific alarm monitoring company was the hardest to coordinate between all the parties involved.

After a successful implementation in Tempe, it was very easy to implement at other areas in the State (Chandler PD, AZ is now also live). The biggest issue in rolling out to other clients is that their state may or may not be ready with the connection to Nlets. A CAD provider can only deliver if the state is ready on their end. Versaterm clients in Washington, California and Oregon are waiting for their state to be ready. Each new Agency will be simple to install because at this point it is just configuration if they are on the latest version of CAD. A new state would require more testing than a client in an existing state but should be still a very smooth implementation.

TriTech Software Systems

TriTech invested nine weeks of total effort for development, testing, initial implementation, and certification. TriTech hired consultant, Bill Hobgood. The initial phase was a telephone consultation after which time the engineer began working on the interface. After approximately six weeks of development time, the consultant travelled to our San Diego headquarters for two days to work with development and product management to evaluate the interface progress. During this time we tested specific scenarios and messages that would be received and sent by the interface. We worked to identify any gaps in the interface or expected CAD functionality. Once the initial testing was completed, engineering continued to work on the interface and make changes identified during testing. The consultant continued to provide remote developer support during this process.

TriTech used three engineers at various points in this process: a state-provider engineer to add and support the ALQ/ALR message keys, a second engineer to work on the interface and CAD functionality, and a QA engineer for internal testing efforts.

During TriTech's first implementation at a customer site, the consultant, TriTech's CAD product management, and TriTech's engineering, along with the customer representative and representative from a security company, worked over the course of two days to complete certification testing. Testing encompassed receiving various types of CAD alarm events via the ASAP interface, bi-directional alarm event updates and closures, address verification requests sent from the alarm monitoring company, error messages received in cases where the state connection was down, or other types of interface disruptions.

First and foremost, CAD vendors should approach this interface like a CAD-to-CAD interface. It will require translation tables and configurable options based on a specific client's needs much like a CAD-to-CAD interface would. Build a simulator to properly test incoming and outgoing messages. Special attention should be placed on various address scenarios, i.e., intersections, coordinate-based addressing, as well as looking at how PSAP map data can sometimes follow a local or CAD-centric convention where the alarm monitoring companies may use a more traditional style address format. This may lead you to have to translate a short names used for things like cities, counties, etc. in CAD to a full name value used by the alarm monitoring companies. ASAP consulting services are key during this process, so be prepared to accept and implement suggestions made during this process. Following the advice received during consultation will lead to a smooth and successful certification.

Northrop Grumman

Northrop Grumman has two CAD platforms certified with the ASAP Service.

Houston's ASAP Synopsis

Houston's ASAP viability discussions were held in 2009. In 2010 Houston purchased the ASAP solution from Northrop Grumman for implementation into the Altaris™ CAD system. The ASAP solution went live in approximately April 2011.

Houston had to first work with the state to allow the Texas Law Enforcement Telecommunications System (TLETS) access for the ASAP transactions. Houston has a message switch that is in front of the CAD system that attaches and receives the TLETS transactions. Houston's effort was a little more complex given multiple interface layers. Northrop Grumman has not implemented the ASAP solution at another Altaris™ CAD to date. The initial development effort was approximately 900 hours between four developers over approximately five months. Not all the development labor was continuous given the different skillsets that were used. Understand the 900 hours for all the development from making the application changes, interface development, alarm company access and location validation, to implementing the City of Houston specialized alarm permitting. Voluntary consulting was used to guide the implementation.

The Houston implementation also entailed City processes that had to approve the permits for the various alarm companies before allowing alarms to be processed by the CAD system. Specific process and protocols had to be put into place. The implementation also called for the City agency to provide a daily upload of approved alarm companies. As part of the ASAP implementation, the CAD system tracks the number of false alarms from the CAD system and bills the citizens for those.

Lessons learned is to scope all the components including the interface access depending on where your agency sits in the state interface hierarchy for access to the state and ASAP transactions. Make sure you provide a test CAD system interface for testing and validation of the alarm addresses.

Bucks County (PA) and Monroe County (NY) ASAP Synopsis

Bucks County, PA, and Monroe County, NY, had the same version of the CAD system. Northrop Grumman developed a new interface that was compatible with Bucks County and Monroe County version of their CAD system. Both sites would become the first agency to come into production with the ASAP interface in their state (CLEAN for Pennsylvania and NYSPIN for New York). Both Bucks County and Monroe County dispatch alarms for a number of police, fire and EMS agencies.

Bucks County and Monroe County worked with alarm companies to verify the address and ensure that the city code/municipality code sent in with the alarm message would validate in the CAD system. Often the alarm company would use the mailing address city/municipality code which was not the same code used for CAD. This was the most time consuming process for the county to resolve. The same process had to be done with each alarm company that was planning to send ASAP alarm data.

The CAD system has a table to translate the city/municipality name from the alarm company into a city code in the CAD system. A similar table was set up to translate the alarm type (i.e., burglary) into a valid CAD incident type. Depending on the location of the alarm and the setup of the CAD system, one alarm notification may generate up to three incidents (police, fire, and EMS).

Interface development took approximately 20 hours to receive the alarm notification and parse the data. Application development took approximately 120 hours to update the applications to process the alarm data in the CAD system (create incidents, update incidents, send updates to alarm company) and format the responses back to the alarm company. End-to-end throughput testing from alarm monitoring company to PSAP took 16 hours to process any XML formatting issues or problems with the various switches/networks the message must pass through.

The certification process took approximately eight hours to complete. ASAP follows a multi-step process of scenarios to verify the data exchange between the CAD system, the state network and the alarm company. In the case of Bucks County and Monroe County, we encountered some minor issues with configuration and ORI routing due to both of these sites being the first ASAP installation in their respective state.

Lessons learned include:

1. Using common terms such as city/municipality as the CAD system has multiple municipalities that are not in alignment with the alarm company city names;

2. Confirming the abbreviations used in the CAD system for the street types (i.e., AV or AVE, BL or BLVD); and

3. Getting test transactions from the alarm company through TMA Message Broker, through NLETS, and through the state switch to the local PSAP can have any of a number of connectivity issues.

Each step in the transport layer must be analyzed when there is no clear indication of where a problem might be. The state may reject a message due to improper XML formatting or may allow it through to be rejected or not properly received by the alarm company.

ALARM INDUSTRY LEVEL OF EFFORT

Some of the smaller alarm sales and installation companies contract with a larger company that serves as the alarm monitoring company that creates and relays ASAP alarm messages.

Each alarm monitoring company has a modest level of effort required to ensure seamless operations. First, they must ensure that the addresses within their files sync to PSAP's address file (MSAG/Geo-file). Address validation can be accomplished in bulk and includes addresses:

- From a new participating alarm monitoring company to PSAPs already participating with the ASAP program.
- To a new participating PSAP from alarm monitoring companies already participating with the ASAP program.

Address validations confirm that the address is correct within the participating jurisdiction only. It does not account for addresses assigned to the wrong PSAP in the alarm monitoring company's database, nor does it account for new account address validations. New account address validations are usually performed automatically by the alarm monitoring company's automation software when new account added.

Alarm monitoring companies are responsible for using a third-party service for Emergency Service Number (ESN) resolution to determine the proper Authority Having Jurisdiction.

Alarm monitoring companies must use event types from standardized list. Note that each PSAP, not the alarm monitoring company, decides up front which alarm types it will receive (e.g., law, fire, and/or EMS), and each PSAP decides how to translate each alarm event type.

NLETS LEVEL OF EFFORT

Nlets is the preferred transport method for ASAP traffic – the infrastructure is already in place, and it provides safe and secure communications to thousands of PSAPs. It offers an intelligent routing scheme that enables a fairly simple pass through via the Nlets network to the states, then via the state network to the PSAPs. CAD providers are engineering ASAP-specific application programming interfaces (API) to handle ASAP message traffic bi-directionally.

The TMA was approved as an Nlets Strategic Partner Organization (SPO) in May 2011 and implemented a TMA-managed message broker server at Nlets. Testing was completed and updated IEPD and schema were quickly released to CAD providers.

Nlets has assigned two new Message Keys for alarm traffic while providing ORIs & unique TMA IDs used for routing messages:

- ALQ = Alarm Exchange Query sent by the alarm monitoring company to the PSAP consisting of the following message types:
  - "Address Verification" is requesting verification that an address is a valid address within the PSAP's jurisdiction
  - "Alarm" is the initial notification of an alarm event
  - Update Messages
    - Request for cancellation by the alarm monitoring company
    - Update concerning key-holder information by the alarm monitoring company
- ALR = Alarm Exchange Response from the PSAP to the alarm monitoring company consisting of the following message types:
  - Update of status by the PSAP's Computer-Aided Dispatch (CAD) system to the alarm monitoring company:
    - "Accept" means the alarm notification is accepted and call-for-service created
    - "Reject" means the alarm notification is rejected due to invalid alarm location address, invalid event type, alarm notification too old, or other reason(s)
    - "CADUpdate";
      - Notice by the PSAP that the primary response agency has been dispatched
      - Notice by the PSAP that the primary response agency has arrived on scene
      - Notice by the PSAP that the event has been closed (with a disposition if applicable)
  - "UPDATE" is an update from the PSAP telecommunicator or field resource requesting additional information such as an estimated time of arrival for the key-holder
  - "UPD ACCEPT" is confirmation by the CAD system that an "update" from the alarm monitoring company was successfully received and added to the CAD event
  - "UPD REJECT" is confirmation by the CAD system that an "update" from the alarm monitoring company was received by could not be added to the CAD event, usually due to the CAD event having been already closed

Figure 3 depicts the high level Nlets-TMA design. The XML firewall is housed within Nlets' facility. Nlets also provides secure certificate authenticated hardware-based VPN to the alarm monitoring companies. The TMA Message Broker server acts to consolidate alarm monitoring company's traffic housed within Nlets' site. Each alarm monitoring company connects to the single TMA Message Broker. The Message Broker confirms that each alarm monitoring company has permission to send a message to a PSAP. If not, the message broker will stop the message.

Of interest is that the ASAP Service is capable of many interesting reports including transaction over time for the ORIs.

PSAPS LEVEL OF EFFORT

Project Management

As mentioned above, the PSAP is the primary driver and owner of the project. They must take ownership of all the steps involved in getting ASAP project up and running. While this is not a full time project management position, it will require an individual with strong project management expertise with good communications, technical, and organizational skills to drive the effort. Many players are involved but all are acting at the behest of the PSAP's project manager. Usually this individual is from the IT department that supports PSAP operations.

Program Management

After ASAP is in live operations, a staff member department should be appointed to manage the program. Again, this is not a full time, exclusive position for most agencies but could be for very large metropolitan areas serviced by many alarm monitoring companies. New alarm monitoring companies may desire to join the program and will require coordination, testing and certification. Usually this person is from the IT department as well and may indeed be the original project manager. Note that the alarm monitoring company's automation must be certified by a TMA-approved consultant.

Typical Costs

The following tables presents expenses that are typical to implement an ASAP-to-PSAP program:

Cost Types	Who Pays	Investment (time/dollars)
CAD provider to develop, install and test ASAP interface	Most often the Agency/PSAP pays for the development but costs might be shared with the CAD provider who can resell it to other clients	Cost examples (one time cost) Vendor A $16,000 Vendor B $40,000
CAD provider on-going support/maintenance	Agency/PSAP	Costs normally range between 15% and 25% of the software license cost; highly vendor dependent

Consultant – required, per TMA rules	On average a 40 hours engagement plus travel Large PSAPs are evaluated on a case by case basis	To bring up one alarm monitoring company (limited engagement) or all companies in the region Usually $5,000 for small to medium PSAPs

CAN'T USE NLETS? OTHER OPTIONS

There are some entities that may not be able to use the data flow depicted in Figure 3. These entities may include PSAPs with CAD systems that are fire-only dispatch, EMS-only dispatch, and federal entities. Access to the Nlets network is controlled by the State's Nlets Control Point, usually the state police or other similarly-named state law enforcement agency.

Dispatch operations at these centers should contact the State Nlets Control Point to inquire about using the existing network. It's helpful to have data on alarm volume and incident types (i.e., number and types of alarms) when scheduling these discussions. This approach still has to be coordinated with TMA and has not been implemented at the time this paper was published although there has been significant interest. This topology must still undergo the certification process.

If access to the state switch is denied, some agencies look to CAD middleware data exchange hub providers who can connect a number of PSAPs in a region to the Message Broker. This approach can leverage existing CAD-to-CAD infrastructure, and potentially lower costs if the CAD connection to the middleware broker is already a bidirectional data exchange.

EXPANDING ASAP

There is an ongoing effort for continuous improvement of the ASAP Program because of the desire to include more information valuable to PSAP and their first responders.

Additional fields have been added to the schema, including:

- Video confirmation link for PSAPs and field responders.
- Alarm service organization name.
- X/Y coordinates in decimal degrees.
- Uniform list of information messages :
  - Reject messages from the Message Broker or the PSAP.
  - Accept message from the PSAP.

The above fields can be used before next release of ANS, which is projected to be published by Spring 2019.

CONCLUSION

The key fact of ASAP is that it saves time in emergency call processing in dispatch centers. The key benefit is that the time savings realized – from 1 ½ to 3 minutes or more – is used to save lives, reduce property damage, and apprehend perpetrators.

The investment by the PSAP is minimal in hard dollars: the procurement of the CAD provider ASAP API is the main expense. The investment of time is more burdensome and impactful of the IT staff, although managing the project is not a full time imposition. Since the process is ongoing to the extent that all or at least a majority of the alarm monitoring companies serving a jurisdiction should participate, the duration of this effort can take many months or even years. If a state is ready, the process goes much faster.

Because of the proven hard and soft benefits of the ASAP program, PSAP Chief Technology Officers or executive directors across the country should push for activation of the ASAP-to-PSAP program. The steps are pretty clear although they do take time. PSAP managers owe it to the community, the first responders and their staff to do so.

RESOURCES

Organizations and individuals that can assist with ASAP-to-PSAP information or efforts include:

APCO	www.apco911.org https://www.apcointl.org/resources/interoperability/asap.html asap@apcointl.org External Alarm Interface Exchange ANSI, Fact Sheet, FAQs, IEPD ❖ https://www.apcointl.org/resources/interoperability/asap/asap-resources.html ❖ IEPD available at www.niem.gov (Tools > Work with IEPDs > Search for IEPD (Keyword "Alarm")
The Monitoring Association (formerly the Central Station Alarm Association)	State status http://csaaintl.org/asap-status/ www.csaaintl.org CSAA Video: csaaintl.org/asap or www.youtube.com/watch?v=6K0g-VyXrxg psap@csaa-asap.org
Nlets	www.nlets.org
Bill Hobgood, Project Manager, Public Safety Team City of Richmond, Dept. of Information Technology	City of Richmond, Dept. of Information Technology 900 E. Broad St., Room G-2 Richmond, Va. 23219 (804) 646-5140 Cell (804) 240-0744 Bill.Hobgood@Richmondgov.com

ASAP Program Awards

ASAP Program Awards to date include:

- ✓ 2009 Virginia Governor's Technology Award for Innovation in Local Government
- ✓ Inaugural IJIS Institute's Innovation Award
- ✓ American City & County Magazine's 2009 Crown Community Award for Excellence in Local Government
- ✓ Center of Digital Government 2009 Digital Government Achievement Award
- ✓ Accepted into the 2009 City Showcase sponsored by the National League of Cities
- ✓ Alliance for Innovation 2010 Award for Innovation in Local Government
- ✓ 2013 Computerworld Honors Laureate Award for Safety & Security
- ✓ 2013 Virginia Governor's Technology Award for IT as an Efficiency Driver, Government to Business
- ✓ 2013 Government Computer News (GCN) Award for Outstanding Information Technology Achievement in Government
- ✓ 2013 Best of NIEM Award and induction into the NIEM Hall of Fame
- ✓ 2014 Alliance for Innovation Award for Outstanding Innovation in Local Government

ASAP History

Month Year	Event
Aug 2004	APCO & CSAA kickoff project to create and test a data exchange between an alarm monitoring company and a 911 PSAP; York Co., VA and Vector Security are selected; York Co. uses a copy of Richmond's CAD; Vector Security uses GE
Jan 2005	APCO and CSAA formerly partner to develop an exchange that will be consistently used by CAD providers and alarm monitoring companies for PSAPs to increase efficiency and decrease errors
Jul 2006	The Alarm Interface Exchange 2.0 goes live at York Co. VA; includes only Burglar and Hold-up alarms
Aug 2006	APCO requests the City of Richmond to join the pilot to generate additional volumes of alarm exchanges; City of Richmond's interface goes live within 24 hours of the request
Oct 2006	The alarm exchange pilot is expanded to include Fire and Medical alarms
Sept 2007	The City of Richmond implements new Intergraph CAD System
Jan 2008	The Public Safety Data Interoperability (PSDI) project is launched;
Apr 2008	The PSDI steering committee holds first meeting; among the decisions made is to upgrade the External Alarm Interface Exchange to NIEM 2.0

Jun2008	IJIS issues an RFP to upgrade the alarm exchange IEPD to NIEM 2.0
Jul 2008	IJIS awards IEPD contract to Waterhole Software
Aug 2008	The External Alarm Interface IEPD is completed using NIEM 2.0
Sep 2008	The IEPD is published on www.niem.gov; the External Alarm Interface Exchange is submitted to the APCO ANS process as a proposed ANSI
Jan 2009	APCO publishes APCO/CSAA ANS Standard 2.101.1-2008
Apr 2009	Enhancements implemented: • Bi-directional "update" messages implemented • Automatic address validations initiated by MasterMind
Jan 2010	The CSAA and Nlets sign the short term MOU to conduct proof of concept: allows 2 more alarm monitoring companies & 3 PSAPs
Feb 2010	Nlets assigns ALQ and ALR message keys for alarm exchange traffic
Jun 2010	Nlets inspects Vector Security's facility and performs audit
Jul 2010	Nlets approves Vector Security for connectivity to Nlets message switch
Aug 2010	Vector and the City of Richmond go live using ORIs for routing and the use of Nlets message keys
Apr 2011	Houston goes live with ASAP
May 2011	CSAA becomes a SPO / Message Broker Development Begins
Apr 2012	City of Richmond & Vector Security go-live on new Message Broker
Oct 2012	Washington DC goes live with ASAP
Jan 2010	The CSAA and Nlets sign the short term MOU to conduct proof of concept: allows 2 more alarm monitoring companies & 3 PSAPs
Feb 2010	Nlets assigns ALQ and ALR message keys for alarm exchange traffic
Jun 2010	Nlets inspects Vector Security's facility and performs audit
Jul 2010	Nlets approves Vector Security for connectivity to Nlets message switch
Aug 2010	Vector and the City of Richmond go live using ORIs for routing and the use of Nlets message keys
Apr 2011	Houston goes live with ASAP
May 2011	CSAA becomes a SPO / Message Broker Development Begins
Apr 2012	City of Richmond & Vector Security go-live on new Message Broker
Oct 2012	Washington DC goes live with ASAP
Dec 2012	James City County VA goes live with ASAP
Jan 2013	Tempe AZ Police Communications goes live with ASAP
Jul 2014	Twelve alarm monitoring companies are in production with ASAP
Aug 2014	Morgan County AL goes live with ASAP
Nov 2014	Henrico County VA goes live with ASAP
Mar 2015	Denton County TX, Chandler AZ, & Cary NC go live with ASAP
Aug 2015	ADT goes live with ASAP
Dec 2015	Boca Raton FL goes live with ASAP
Jan 2016	Guilford County – Greensboro NC goes live with ASAP
Mar 2016	Grand Prairie TX goes live with ASAP
May 2016	Durham City – Durham County NC goes live with ASAP
May 2016	Kernersville NC goes live with ASAP
Jul 2016	Delaware County OH goes live with ASAP
Nov 2016	Johnston County NC goes live with ASAP
Nov 2016	High Point NC goes live with ASAP

Jan 2017	Williamson County TX goes live with ASAP
Jan 2017	Bucks County PA goes live with ASAP
Apr 2017	Highland Park TX goes live with ASAP
Apr 2017	Rochester/Monroe County NY goes live with ASAP
Jun 2017	Wilson County NC goes live with ASAP
Jun 2017	Manatee County FL goes live with ASAP
Jul 2017	Dane County WI goes live with ASAP
Aug 2017	Newport News VA goes live with ASAP
Sep 2017	Union County NC goes live with ASAP
Oct 2017	Loudoun County VA goes live with ASAP

REFERENCES

https://www.niem.gov/about-niem/news/city-richmond-wins-twice-november-best-niem-and-2013-gcn-award

http://augustafreepress.com/mcdonnell-announces-2013-governors-technology-award-winners/

https://gcn.com/articles/2013/10/09/gcn-award-richmond-asap.aspx?m=1

http://cwhonors.org/case_studies/2013Finalists/Safety%20and%20Security/1301_CityofRichmondVA2013.pdf

http://transformgov.org/en/blogs/blogpost/2360/Announcing_the_TLG2014_Innovation_Award_Winners

https://www.youtube.com/watch?v=31Zme94Urq8&index=3&list=PLcrTnX9941X3Qzlwp_o1TbPbxgZHi_Fyn

http://americancityandcounty.com/pubsafe/richmond-york-alarm-interface-cc-200912

http://www.prnewswire.com/news-releases/city-of-richmond-va-and-intergraphr-honored-with-ijis-institute-innovation-award-for-advancement-of-public-safety-62247727.html

http://www.wfmynews2.com/news/guilford-metro-911-homeowners-could-see-faster-response-times/51911611

http://www.twcnews.com/nc/triad/news/2016/01/26/new-technology-helps-first-responders-get-to-emergencies-faster.html

http://psc.apcointl.org/2012/03/29/asap-to-psap-what-will-your-agencys-return-on-investment-be/

ABOUT THE IJIS INSTITUTE

The IJIS Institute unites the private and public sectors to improve mission-critical information sharing and safeguarding for those who protect and serve our communities. The IJIS Institute provides training, technical assistance, national scope issue management, and program management services to help government fully realize the power of information sharing.

Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus in Ashburn, Virginia, the IJIS Institute has grown to nearly 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the IJIS Public Safety Technology Standards Committee for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in the commitment to improving justice, public safety, and homeland security information sharing.

For more information on the IJIS Institute:

- Visit the website at: http://www.ijis.org/,
- Follow the IJIS Institute on Twitter: @ijisinstitute,
- Read the IJIS Factor Blog, and
- Join us on LinkedIn at: Justice and Public Safety Information Sharing.

About the IJIS Public Safety Technology Standards Committee (IPSTSC)

The purpose of the IJIS Public Safety Technology Standards Committee is to promote and contribute to the development of technical and functional standards for public safety IT components, to provide industry input and policy review on technical matters faced by the public safety community, and to oversee IJIS Institute projects assigned to the committee.