Shooter Detection Systems™

AN ALARM.COM COMPANY

Reducing Response Time to Active Shooter Incidents with Gunshot Detection

WHITEPAPER

North Providence, RI police respond to shot detections during a Shooter Detection Systems indoor gunshot detection demonstration at the North Providence High School in 2017.

Some of the greatest challenges to facility security include the monitoring of multiple spaces and gathering areas, coupled with tracking the frequent comings and goings of staff, visitors, and vendors to your facility or campus. These challenges increase even more when managing a site with multiple buildings or satellite facilities that are being monitored from one security operations center. When you add an active shooter incident into the mix, knowing exactly where the incident is happening in real time is critical, so first responders can rapidly mitigate the threat and building occupants can quickly get to safety.

While this concept is well understood, putting it into practice is another story. If a person is in Building C while an active shooter starts firing in Building A, how do they know? When do they know? Who notifies 911 and how long does it take? How does that information get to first responders? Just as important, is it accurate?

At Virginia Tech in 2007 an active shooter managed to go undetected for two and a half hours after his first two shots were fired in a dormitory. He later shot 47 people that he locked inside an academic hall.[1] After this incident the implementation of more robust mass notification systems became commonplace. Emergency kiosks, panic buttons, and "blue light boxes" became more widely deployed. These types of systems have helped people feel safer and have improved emergency communications, however they still require some form of human action to set them off, such as a person who presses a panic button or a security dispatcher who must compose and send the mass notification message, which can cause errors and delays.

RUN-HIDE-FIGHT IS A "VICTIM INITIATED MITIGATION SYSTEM"

With these systems in place, where does this leave 911? One of the earliest and most comprehensive studies on active shooter incidents was a 2012 Naval postgraduate school study which found that relying on 911 notification is an inadequate strategy to reduce response time in an active shooting incident, and that instead, a "Victim Initiated Mitigation System" is the most effective means of reducing casualties.[2] The Department of Homeland Security adopted this bystander model in their How to Respond active shooter booklets and what became the training commonly referred to as "Run, Hide, Fight".[3] What they and other authorities are admitting to is that civilian bystanders are by default the most reliable "first responders" on the scene fast enough to stop an active shooter, and should be trained to react accordingly. This would be a terrifying prospect for most civilians, and where we can—and should—leverage technology solutions.

While 911 and mass notification systems remain well-established, viable solutions alongside video and access control, the addition of gunshot detection supplements these systems by filling in critical missing gaps and improving the flow of information during an active shooter incident. The premise behind gunshot detection is that it will alert first responders faster than any current method. Providing vital location information, including where in the building the incident is happening, cuts through typical alert delays so a more immediate response is initiated. To maximize effectiveness a gunshot detection system should be capable of automating the delivery of real-time incident data and updates to 911 operators.

A system should also integrate with mass notification, video, public address systems and other alarms simultaneous. This includes security personnel, staff, and visitors, so appropriate response actions can be instantly initiated, without dependence on human intervention in the earliest seconds of an active shooter incident.

A MILITARY APPROACH TO THE ACTIVE SHOOTER

It is important to note gunshot detection technology's roots in history, long before it was developed for commercial applications. As a capability gunshot detection first originated in a United States Government initiative in 1995 and was sponsored by a research arm of the Department of Defense called the Defense Advanced Research Projects Agency (DARPA). The initiative was to develop prototype systems that paired acoustic muzzle blast and ballistic shockwave signatures to predict the location of gunfire events and associated shooter locations. Six different systems were developed and tested, but it wasn't until the Iraq War in 2003 that the need for these systems became critical. At this time, U.S. troops were battling against an aggressive insurgency while traversing some of the roughest terrain on earth in noisy Humvees, and they often did not know they were being shot at until a fellow soldier was hit. Knowing they were being shot at and being able to identify where the shots were coming from would give them a lifesaving and tactical advantage.

DARPA selected the company that had produced the most successful technology from their trials, BBN Technologies out of Cambridge, Massachusetts, and challenged them to rapidly develop vehicle gunshot detection systems that could not only localize a shooter to plus or minus 15-degree accuracy, but it also had to report within one second of a shot and do so on vehicles traveling up to 60 miles per hour on rough terrain and in harsh environments. That system, called Boomerang,[4] was quickly deployed and is still in use today, credited with saving the lives of soldiers in military conflicts across the globe.

THE ACTIVE SHOOTER THREAT TO THE PUBLIC

In the 1990's and 2000's the U.S. witnessed a rising and disturbing trend of mass shooting incidents happening in schools, workplaces, movie theaters and other everyday environments. This created an influx of active shooter solutions to the market including ballistic glass, door locks and panic buttons. While they might be useful, these solutions still do not address the lack of critical information flow as a shooting incident unfolds—the what, when and where questions still must be answered, and quickly. To address these problems, Shooter Detection Systems began adapting the core technology from the Boomerang system for indoor environments, and brought the SDS Indoor Gunshot Detection System to the commercial market in 2014.

TRANSITIONING TO INDOOR DETECTION

Accurately detecting a gunshot signature indoors is not easy given factors such as signal deflection, refraction and the short distances between signal and sensor. SDS engineers translated their experience from Boomerang outdoor detection and created a new approach for indoor application consisting of a two-factor verification based on infrared and acoustic signal analysis. This approach, now enhanced with machine learning and advanced sensor components, has set the standard for high detection and accuracy rates and low false alerts rates.

Two U.S. soldiers return to their Humvee equipped with the Boomerang Shooter Detection System. SDS founders bought the IP for the Boomerang system to create their indoor gunshot detection system.

ALL GUNSHOT DETECTION SYSTEMS ARE NOT CREATED EQUAL

In the process of educating yourself on what gunshot detection system is right for your building or campus, it is easy to get lost in technical and marketing jargon along the way. Before you get too far down the rabbit hole, remember the key questions: How do you know it is a gunshot? How is the information getting to you and others in danger? How long does that take? Is the information accurate?

At their core, all indoor gunshot detection systems are comprised of one or more sensors strategically positioned within facilities that transmit gunshot alerts through a communications platform. When evaluating sensor types, it is important to understand how the sensor functions. It is not technically difficult to place a microphone on a wall and calibrate it to detect an acoustic signature that meets a certain criteria. This approach leads to a high number of false alerts, which will lead to panic—or the inverse—users who ignore a detection alarm due to multiple false alerts. Some manufacturers claim that they use two or even three types of detection technologies in their sensors, but there are key differences in these approaches. Since every gunshot creates both an acoustic signature (bang) and an infrared signal (flash), a sensor that requires both of these signals to declare a shot detection will be most effective. If a manufacturer claims to detect a gunshot through a physical barrier (like a wall), it is likely they are not using the infrared signal to validate the event. Some manufacturers rely on a catalog of sounds to compare a possible shot against sound files to provide a confidence level. The concern here is how reliable and up to date that catalog is, and if it requires a human to verify the shot detection. If so, valuable time will be lost in the verification process. Some sensors require calibration to a specific environment, for example a manufacturing plant or an airport concourse. Sensors that require manual calibration can be problematic in that they require close monitoring and analysis for a time before they are fine-tuned to sounds in the environment. Also, in many cases systems that are not utilizing infrared signal detection as a validation tool require external evaluation of gunshots before issuing an alert—usually by a human monitoring the signals, which causes more delay in an already fast-moving incident.

SHOCKWAVE, PERCUSSION, AND CONCUSSIVE FORCE

True two-factor authentication is the most reliable approach for reliability and speed of alerting. SDS Gunshot detection devices use sensors to detect a change in the compression of air molecules when a bullet is discharged. Some manufacturers try to differentiate themselves by saying that they use a unique type of sensor such as a pressure sensor, concussive force sensor, or shockwave sensor. Don't be fooled by terminology, as these devices are all measuring the same thing in the same way. Just as the membrane in your ear can sense pressure, shock and sound, all manufacturers use a microphone to detect gunshots, so in this respect, all gunshot detection sensors on the market detect percussion, concussive force, and the shockwave of a bullet, including SDS. In fact, beware of manufacturers that claim to only detect shockwaves. Technically a shockwave travels in a specific direction and this would mean that the sensor would only be effective if it happened to be near the path of a bullet. In other words, these terms are not unique detection parameters, they are all acoustic properties. The only thing that will set a sensor apart is the use of infrared across the entire detection range of the sensor. Furthermore, the quality of the infrared sensors used matters and therefore should be highly rated and will be the most delicate component of a gunshot sensor. For this reason, SDS' infrared sensors offer up to 10 times greater sensitivity, leading to better flash detection accuracy than typical infrared devices on the market.

SDS' gunshot detection sensors rely on both acoustic and infrared flash detection to declare a shot, resulting in a 99.9% accuracy rate and producing less than 1 false alert per 5 million hours of use.

SDS' technology captures the infrared muzzle flash as well as the acoustic properties of the gunshot muzzle blast, including the pressure wave (percussion, shockwave, concussive force) of the projectile.

EXTERNAL VALIDATION

Systems that rely on acoustics alone can potentially produce false alerts due to loud noises in the environment, so external validation measures are put into place to verify a gunshot before an alert is sent to authorities. Some systems send audio files to human analysts at a monitoring station to verify "possible" shot events or stream audio to the cloud. Audio clips sent outside of a local server may open organizations up to privacy concerns or violate privacy laws in hospitals and other settings. Sensors that rely on any type of external validation will have delays in alerting speed, can create privacy violations, and run the risk of producing false alerts.

MULTI-MODE SENSORS AND SIGNALS PROCESSING

SDS has validated, through DHS testing, competitive trials against other manufacturers, and national lab third party testing, to be the recognized leader in the two-factor acoustic and infrared approach. Sensors that require both the signature of a gunshot (acoustic sensor) and the flash of a weapon (infrared sensor) to validate a gunshot signal will be most accurate in filtering out false alerts. When evaluating a gunshot sensor's capabilities, understanding how the signal detection mode(s) are utilized to output shot alerts is critical. Are both or all detection modes advertised required to validate a gunshot, or are they 'nice to have' features that help with post-event analysis? Put the onus on the manufacturer to provide detailed information about the usage requirement and reliability of multiple detection modes. More importantly, ask for third party testing results or if the sensor has been evaluated and accepted by government agencies.

POWER, NETWORKING AND ENCRYPTION

After detection accuracy, communication and networking are also important considerations. Power-over-Ethernet (PoE) has advantages and involves wire pulls and minor infrastructure work. DC power requirements could be problematic and subject to easy tampering. Wireless systems may be the most flexible to install, however, end users should ask about sensor uptime and self-testing features and how they impact battery life, and if the communications system is secured with encryption.

BENEFITS OF AUTOMATION

To put the benefit of reducing response time with gunshot detection into perspective, the average length of an active shooter incident is around five minutes[5] with an average of one death occurring every 5 to 15 seconds[6] while active shooting is taking place. Ultimately a security end user needs to be able to rely on the gunshot detection system to automate the alerting process as early as possible and with the highest level of accuracy to justify the investment. After the dormitory shooting at Virginia Tech, the perpetrator fled the building undetected and returned hours later to complete his mission. Thirty-two people lost their lives when it was finally over. If gunshot detection technology were in place to detect the initial shot, the response may have been drastically different. How many lives could have been saved?

Ask for third-party testing results to validate manufacturer claims about performance.

ACTIVE SHOOTER TRAINING

An additional benefit of gunshot detection that might get overlooked is the impact it can have on active shooter drills and training. Over 20 years of realistic active shooter drills being conducted in schools and other environments have shown that these drills are potentially more traumatizing than they are beneficial.[7] Some gunshot detection systems have simulation and training modes that will activate the sequence of information flow, including integrated actions within video, mass notification, access control, etc., without needing to present a weapon into the environment. Similar to fire alarm drills, a simulated active shooter drill can help organizations initiate a calmer, more organized, less traumatic training experience.

THIRD-PARTY VALIDATION

For all the benefits gunshot detection can bring to an organization, one of the difficulties with system selection is that there is no one governing body that regulates the industry or monitors marketing claims.

A product bearing a green or blue SAFETY Act mark will have only a Developmental Testing and Evaluation Designation (DT&E), indicating that the technology is still in the development and testing phase. An important resource any security end user should look for is the U.S. Department of Homeland Security's SAFETY Act program. Technologies that have been SAFETY Act Certified bear the red Department of Homeland Security (DHS) seal of approval. This indicates that the technology is listed on the DHS Approved Products List for Homeland Security and has been vetted by the DHS Science and Technology Directorate (S&T), a DHS arm that monitors emerging threats and encourages private industry to create technology solutions to abate them.

There are also international authorities like the U.K.'s National Protective Service Authority and Australia's Security Construction and Equipment Committee that provide similar certifications to tested anti-terrorism technologies. Beyond looking for a system's third-party validations, end users should include their integrator and security advisors early in the process and ask for customer references.

QUESTIONS TO ASK MANUFACTURERS

- Does the sensor alert automatically, or does it require external validation to alert?
- How does it filter out false alerts?
- What is the false alert rate?
- What is the reliability rate of detection?
- What is the alerting speed?
- Do the sensors require calibration?
- How are the sensors powered?
- Does the sensor have a built-in-self-test (BIST)?
- Does battery power reduce sensor uptime?
- Is the software hosted on-premises or is it cloud-based?
- Can you share independent third-party test reports?
- Do you have customer references in my industry?

THE BOTTOM LINE

Security professionals today need to understand a wide rage of technologies and how they can be effectively deployed without breaking the budget. Manufacturers that cannot clearly describe how their technology works, rely on downplaying competitor technologies, or do not embrace the added work of third-party verification are only creating more confusion about what solutions will deliver the best results. During the selection process organizations should focus on finding a system that has a high rate of detection accuracy, fast alerting speed, flexible integration capabilities including 911 alerting, and devices that use secure communications and are safe to use on your network. Equally important is a system that can be integrated seamlessly with an organization's video and emergency notification systems, and one that enhances active shooter training. This is where true automation happens and where gunshot detection can have the most impact on reducing the loss of life during active shooter incidents.

ABOUT SHOOTER DETECTION SYSTEMS

SDS, an Alarm.com company, is a leading provider of patented gunshot detection solutions for schools, government buildings, transportation hubs, entertainment facilities and businesses of all sizes. The company's Indoor Gunshot System is SAFETY Act Certified by the U.S. Department of Homeland Security included in the Catalogue of Security Equipment of the Centre for the Protection of National Infrastructure (CPNI), and SL4 Certified by the Australian Government. For more information visit ShooterDetectionSystems.com.

Reference Sources:
1 Virginia Tech Review Panel Report, 2007, Virginia Tech University, Blacksburg, VA
2 Defeating the Active Shooter, 2012, Ergenbright & Hubbard, Naval Postgraduate School, Monterey, CA
3 Active Shooter: How to Respond, 2008, U.S. Department of Homeland Security, Washington, D.C.
4 Shooter-detection 'Boomerangs' Helping in Iraq, 2009, United States Army, army.mil online
5 A Study of Active Shooter Incidents in the United States Between 2000 and 2013, 2013, U.S. Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C.
6 ALICE active shooter training: Learning how to thwart violence intruders, 2017, Rapid City Journal, Rapid City, SD
7 The Impact of Active Shooter Drills in Schools, 2020, Everytown for Gun Safety Fund, New York, NY

Contact SDS today to learn how we can help you protect your buildings and people with reliable, proven gunshot detection solutions.

300 Newburyport Turnpike

Rowley, MA 01969

Email: sales@shooterdetectionsystems.com

Phone: 1-844-SHOT911

www.ShooterDetectionSystems.com

Shooter Detection Systems™

AN ALARM.COM COMPANY

230525