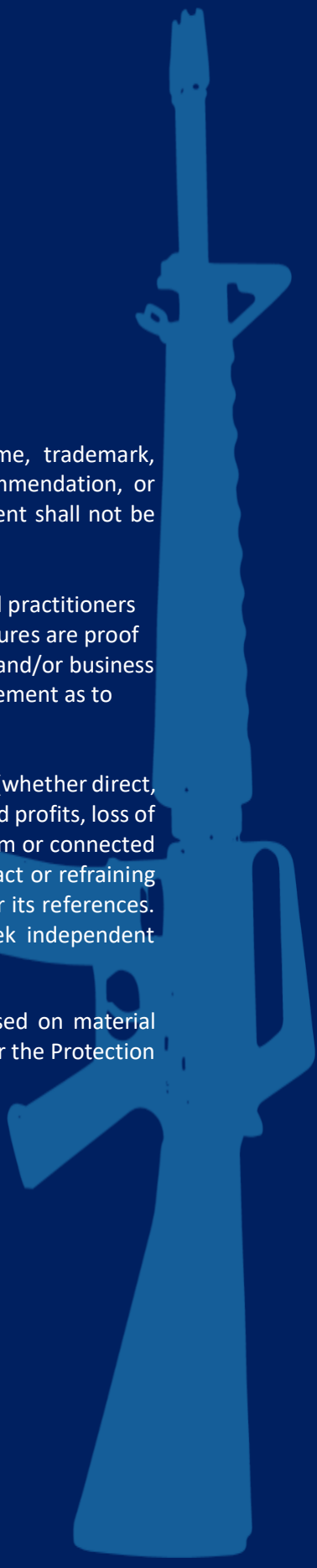
CPNI

Centre for the Protection of National Infrastructure

Technical Guidance to Gunshot Detection Systems (GDS)

October 2020



Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

This guide has been prepared by CPNI and is intended to assist security managers and practitioners working for the UK Government and critical national infrastructure. No security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business and compliance with any applicable law and regulations and must use your own judgement as to whether and how to implement our recommendations.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Introduction

This document presents an overview of technical aspects of a GDS including verification methods and factors that may affect its operational performance. Technical understanding is provided around user interfaces and a GDS's ability to integrate with other physical security systems.

This document does not cover Military or Police use of GDS.

This document is primarily focussed on indoor GDS's as part of CPNI's wider Marauding Terrorist Attack programme of work.

This document should be considered in conjunction with CPNI's guidance on Marauding Terrorist Attacks.

Concepts of Deployment

CPNI has only undertaken research and testing on the **indoor** deployment of GDS. It has been seen that indoor GDS deployments are able to suitably balance a high level of detection with a very low false alarm rate. This does not mean that there are not technologies available that might suit a specific need in either a **covered** or **outdoor** area, but these are significantly harder problems.

In an indoor environment there are 2 main physical deployment methodologies.

1. **Wide area coverage** – multiple sensors can be deployed to cover all of the building footprint e.g. cover all ingress/egress points and the entire building floor plate.

2. **Vulnerable point coverage** – single sensors can be deployed at key locations within the building which have been identified as likely points for a firearm attack e.g. ingress/egress points or an area where an attacker would be more likely to fire the weapon e.g. a reception with a security guard or where there is likely to be a crowd of people.

Both deployment approaches have factors for consideration and the options chosen should be guided by undertaking an OR.

Wide area coverage

- Pros
  - A GDS should detect a firearm attack anywhere in the building.
  - The wider area coverage can be helpful in following the location of subsequent shots as an attacker moves. This can aid with tracking an attacker if sensor location and a visual tracking interface is available.
- Cons
  - Cost will increase proportionally with the size of the building/area to be covered.
  - Overload control room response due to multiple sensor alerts being presented.

Vulnerable Point Coverage

- Pros
  - The cost of installation will be lower than covering the entire building with sensors
  - A less complicated situational awareness picture is presented to security staff as there are fewer sensors to monitor.
- Cons
  - It is reliant on a gunshot being discharged at designated critical points. If the weapon is discharged outside of sensor covered area, then GDS detection will not occur.
  - The time between detections will be greater and attacker location information will be more be out of date.

Verification Methods

GDS use a number of different methods of verifying gunfire. These include:

Automated System Analysis (**full automation**) – Sound and/or light emitted when a gunshot is fired is analysed and processed within the system, based on specific criteria. A detection is confirmed if they fall within set thresholds associated with that particular gunshot type. Most GDS perform some form of mathematical analysis on detection to ensure low false alarm rates.

Considerations

⇒ Mathematical analysis is intended to lower the rate of false alarms. **Manufacturers/Suppliers should be able to supply details of testing that has been carried out to determine these.**

⇒ Detection is confirmed almost immediately.

⇒ The analysis may fail to take into account environment specific factors at the time a gunshot occurs affecting the characteristic detail captured.

System Analysis and Human Verification (Human in the loop) – Initial capture of a gunshot characteristic is performed, mathematical analysis is applied and then the information is relayed to a human analyst who will perform additional analysis to confirm if a gunshot has been fired. This is typically seen in outdoor acoustic only setups where high levels of ambient noise could lead to a higher level of false alarms. Human verification should not be confused with a security officer in a sites Security Control Room, this human is part of the GDS company.

Considerations

⇒ May add additional level of confirmation leading to lower false alarm rates (depending on the skill of the human verifier). Manufacturers/Suppliers should supply details of detection rates – this should have been carried out in a scientific "statistically significant" testing environment and should not be anecdotal evidence, conjecture or hearsay

⇒ Additional time will be added to confirm detection – details should be sought from the manufacturer on how long this takes

⇒ Is the audio data required to leave the sensor and or site for analysis and if so, are there any privacy/data sharing concerns that need to be mitigated?

User Interface

Like many other physical security detection systems, a GDS manufacturer will commonly provide a Graphical User Interface (GUI) to display information to aid situational awareness. Each manufacturers GUI will be different in terms of look and feel but is likely to include some key information.

Generally, a GDS will provide similar alert detail to any other detection system;

1) a location for the detector
2) a time stamp

The GDS GUI may also provide a map that can be utilised as a base layer for alerts to displayed on – this may be in the form of an aerial map, or a more bespoke option for a site and/or building. This may benefit SCR operators at larger sites as the location of the alert is easily visualised and no mental translation of an alert description into a specific location would be required.

Should a map interface be used it should be specifically designed for the purpose, accurate and up to date. For more information, see CPNI control rooms guidance on “maps” and “visual warnings”

It may be useful to prioritise GDS alerts as a high priority. If multiple GDS sensors are being activated, other alarms, for example Perimeter Intrusion Detection System alarms may be of little or no interest

Standalone or Integrated SMS

As with most detection systems, a GDS can either be a standalone system or integrated with other security systems such as CCTV systems, AACS, public address systems or active delay systems as part of a Security Management System (SMS).

Standalone GDS

⇒ Pros
- Simpler to understand user interface
- Dedicated interface that may add additional functionality i.e. activated sensors may fade or change colour over time to show an attacker's route

⇒ Cons
- More difficult to implement cause and effect i.e. a GDS activation automatically triggers a CCTV camera and locks a door
- Users will be operating the system infrequently and will be unfamiliar with the system/layout and its functions.

An Integrated GDS

⇒ Pros
- Integrates all systems into one place
- Adds more options for integration of other systems
- Operator familiarity as they use the same system every day
- Ease and speed of correlation between GDS and other systems e.g. CCTV
- Can reduce cognitive load on SCR staff in the initial confusing stages of an incident
- Can speed up response during initial stages of an incident if automation of notification (and action) is implemented correctly

⇒ Cons
- Single point of failure
- Screens may become confusing with more technologies added (CCTV, AACS, PIDS, GDS)
- Most systems not designed for GDS integration.

If a GDS is integrated with as SMS, the SMS display should be as uncluttered and as simple to understand as possible.

If the flow of actions and events is not carefully planned or tested thoroughly then unintended consequences could follow. It is advised a full mapping process is undertaken as part of the operational requirement and technical specification process. It is also useful to exercise this capability as part of wider scenario testing.

Example System Integrations

Integration	Action on gunshot notification
Access Control	Lock/Unlock predetermined access points
Video Management	Record/Display closest CCTV footage for (e.g.) 5 seconds before GDS notification and 5 seconds after GDS notification
Messaging Systems	Send SMS/Email to nominated personnel or group of people
Public Announcement	Make pre-recorded announcement to staff in building
Security Management Systems	Change the layout of the SMS GUI to a simplified "MTA response" layout
Active Delay Systems	Deploy fog or strobe technology to disorientate attackers

Factors Influencing Performance

When a GDS is commissioned it is expected that it will perform as designed. However, there are various factors that may influence its performance. These can be divided into environmental and operational factors.

Environmental

- ⇒ Light or noise characteristics – locations prone to the below issues could affect false alarm or detection rates adversely
  - ⇒ areas with high ambient noise – this may "drown out" gunshots
  - ⇒ areas with potential for loud sudden noises – this may increase the chances of a false alarm (for acoustic technologies)
  - ⇒ areas where flashing light sources may occur - this may increase the chances of a false alarm (for optical technologies), especially where these are high intensity, such as arc welding, or trains arcing

- ⇒ Building fabric – what a building is constructed of has to be considered when locating gunshot sensors as:
  - ⇒ sound deadening fabrics (doors/walls) may reduce clarity and therefore range
  - ⇒ depending on age and manufacturer, glass in windows and doors will potentially have different IR refractivity, some will allow IR light to pass, others will block IR completely
  - ⇒ Note that GDS sensors are not "line of sight" – the sensor does not necessarily need to "see" the firearm itself i.e. a sensor in one room may be activated by a gunshot fired in another (depending on sensor range)

Operational

- ⇒ Maintenance – Ensure sensors are free from obstruction and dirt. Often sensors come with built in test or maintenance functionality. It is recommended these are used as per the manufacturer's guidance.

- ⇒ Tampering – Tampering of sensors is a possibility but is considered an unlikely vector of attack. Sensors should have the capability to notify staff if physically disturbed. It is recommended CCTV coverage and physical checks by personnel should include sensor locations to ensure physical tampering has not occurred

- ⇒ Alert flooding and granularity – In the case of a marauding firearms attack it is likely multiple shots will be fired. Consideration should be made as to the frequency of alerting from each individual sensor. During CPNI trials, each sensor would issue alerts a maximum of one alert every 5 seconds, this was seen to allow the security officers time to assess and act on each alert.

- ⇒ Weapon/Ammunition – Whilst all GDS will advertise a given range of detection, the type of weapon and ammunition used will influence performance. A higher calibre of ammunition will show a higher level of "flash" or "bang" and therefore is more likely to be detect at the outer limit of range (and possibly further) that is advertised. Conversely detection levels associated with smaller calibre of ammunition is likely to decrease at the extremities of range claimed.

- ⇒ Heartbeat – A sensor should have the ability to send a "heartbeat" signal to its central system to prove it is online and operational

Pre-Installation, Installation and Commissioning

Sites should utilise a GDS that has been tested by CPNI and is in the Catalogue of Security Equipment

Pre-Installation & Installation

It is essential that manufacturers/approved installers undertake the necessary installation work. They will understand the technical considerations to ensure the system performs as required.

Each GDS is likely to have different nuances affecting installation which, will be affected by the building layout and materials i.e. its operational environment. Every site/location will have a different configuration and is likely to be constructed of different materials. Sound and light will travel and react differently based on the construction of the building and therefore sensor layout is key to ensuring the required coverage is achieved and the system operates as advertised.

At a minimum, manufacturers should supply the following prior to installation:

⇒ Details of which environments the GDS has been designed to operate in and formal performance measurements where available.

⇒ Procedures and requirements for installation, commissioning and maintenance plus a typical maintenance schedule, including a list of approved installers and maintainers.

⇒ Method statement detailing how the GDS should be installed. Details of health and safety issues associated with the installation, running or maintenance of the system, including information on toxic or dangerous materials in the product which may be released during an attack.

⇒ Physical sensor configuration, positioning, optimum installations and system settings based on the defined attack styles, plus any details on tamper detection capabilities of the GDS.

Commissioning

Due to the unique nature of a GDS, commissioning a system is of the utmost importance to ensure that a sites Operational Requirement is met. It is difficult, but not impossible, for live/blank fire testing to be conducted post installation so a method of replicating a gunshot and the physics of it is required to ensure a system is working as expected.

A manufacturer or approved installer should

a) Prove the system is functionally working (with live/blank ammunition tests) prior to (and after) installation

b) Provide commissioning tools that replicates gunfire to the system (optical and/or acoustic), to demonstrate that the installed system is functional, prior to the system "going live".

Live/blank ammunition tests and/or commissioning tools should be used within a set maintenance schedule to ensure the system continues to operate as expected.

A physical device should be utilised for commissioning. While it is possible for the system to "self-check" the integrity of any connection back to the main control unit, it is not possible for a device to test that the actual sensing components are functional.