INTERNATIONAL AMMUNITION TECHNICAL GUIDELINES

IATG 09.10

Third edition
March 2021

Security principles and systems

UN SaferGuard
Securing ammunition, protecting lives

IATG 09.10:2021[E]

Warning

The International Ammunition Technical Guidelines (IATG) are subject to regular review and revision. This document is current with effect from the date shown on the cover page. To verify its status, users should consult www.un.org/disarmament/ammunition

Copyright notice

United Nations Office for Disarmament Affairs (UNODA)
United Nations Headquarters, New York, NY 10017, USA

conventionalarms-unoda@un.org

Contents

Foreword

Ageing, unstable and excess conventional ammunition stockpiles pose the dual risks of **accidental explosions at munition sites** and **diversion to illicit markets**.

The humanitarian impact of ammunition-storage-area explosions, particularly in populated areas, has resulted in death, injury, environmental damage, displacement and disruption of livelihoods in over 100 countries. Accidental ammunition warehouse detonations count among the heaviest explosions ever recorded.

Diversion from ammunition stockpiles has fuelled armed conflict, terrorism, organized crime and violence, and contributes to the manufacture of improvised explosive devices. Much of the ammunition circulating among armed non-State actors has been illicitly diverted from government forces.[1] In recognition of these dual threats of explosion and diversion, the General Assembly requested the United Nations to develop **guidelines for adequate ammunition management**.[2] Finalized in 2011, the International Ammunition Technical Guidelines (IATG) provide voluntary, practical, modular guidance to support national authorities (and other stakeholders) in safely and securely managing conventional ammunition stockpiles. The UN SaferGuard Programme was simultaneously established as the corresponding knowledge-management platform to oversee and disseminate the IATG.

The IATG also ensure that the United Nations entities consistently deliver high-quality advice and support – from mine action to counter-terrorism, from child protection to disarmament, from crime reduction to development.

The IATG consist of 12 volumes that provide practical guidance for 'through-life management' approach to ammunition management. The IATG can be applied at the guidelines' **basic, intermediate, or advanced levels**, making the IATG relevant for all situations by taking into account the diversity in capacities and resources available. Interested States and other stakeholders can **utilize the IATG for the development of national standards and standing operating procedures**.

The IATG are reviewed and updated at a minimum every five years, to reflect evolving ammunition stockpile-management norms and practices, and to incorporate changes due to changing international regulations and requirements. The review is undertaken by the UN SaferGuard Technical Review Board composed of national technical experts with the support of a corresponding Strategic Coordination Group comprised of expert organizations applying the IATG in practice.

The latest version of each IATG module can be found at www.un.org/disarmament/ammunition.

[1] S/2008/258.

[2] See also the urgent need to address poorly-maintained stockpiles as formulated by the United Nations Secretary-General in his Agenda for Disarmament, *Securing Our Common Future* (2018).

Introduction

Effective and efficient security is an essential element of any conventional ammunition stockpile management programme, as it reduces and/or mitigates the risks of sabotage, loss, theft, leakage and proliferation (collectively these are generally known as diversion). It can be used to identify future procurement requirements or surpluses. The systematic control of ammunition stockpiles is in keeping with a philosophy of 'due care' and therefore States should take a pro-active, rather than re-active, stance in ensuring that ammunition is accounted[3] for and secured to the highest standards.

This module provides guidance for practical conventional ammunition stockpile management. It sets out sensible and practicable measures that will assist in preventing the theft, leakage and proliferation of conventional ammunition stockpiles. These measures are reasonable and achievable and will enhance any conventional ammunition stockpile management programme.

[3] Inventory management is covered in IATG 03.10 *Inventory Management.*

Security principles and systems

1 Scope

This IATG module establishes the guiding principles, defines procedures and introduces technical security systems for the effective and efficient security of ammunition storage areas in support of a conventional ammunition stockpile management programme.[4]

This module should be read in conjunction with IATG 03.10 *Inventory Management*, which contains the actions to be taken on discovery of a loss or theft of ammunition or explosives.

2 Normative references

A list of normative references is given in Annex A. These documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

A further list of informative references is given in Annex B in the form of a bibliography, which lists documents that contain additional information related to the contents of this IATG module.

3 Terms and definitions

For the purposes of this module the following terms and definitions, as well as the more comprehensive list given in IATG 01.40 *Glossary of terms, definitions and abbreviations,* shall apply.

The term ‘diversion’ refers to *the shifting of weapons, ammunition or explosives from the legal market or owner to an illegal market or owner as a result of losses, theft, leakage or proliferation from a stockpile or other source*.

The term ‘security’ refers to *the result of measures taken to prevent the theft of explosive ordnance, entry by unauthorised persons into explosive storage areas, and acts of malfeasance, such as sabotage*.

In all modules of the International Ammunition Technical Guidelines, the words 'shall', 'should', 'may' and 'can' are used to express provisions in accordance with their usage in ISO standards.

a) **'shall' indicates a requirement**: It is used to indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

b) **'should' indicates a recommendation**: It is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form, 'should not') a certain possibility or course of action is deprecated but not prohibited.

c) **'may' indicates permission**: It is used to indicate a course of action permissible within the limits of the document.

d) **‘can’ indicates possibility and capability**: It is used for statements of possibility and capability, whether material, physical or casual.

[4] These principles and techniques are very similar to those for the security of weapons contained within MOSAIC 05.20 *Stockpile management: Weapons* from which much of this IATG is derived.

4 International instruments

Article 11 of the UN Firearms Protocol[5] requires that *States **shall** take appropriate measures, ... to require the security of firearms, their parts and components and ammunition at the time of manufacture, import, export and transit through its territory*. These requirements, already agreed by many states, are a core component of this IATG.

5 General

To be most effective, it is important that the technical systems required for effective security are included during the resource allocation process of conventional ammunition stockpile management. The financial costs of security are minimal, when compared to the potential value of the ammunition stockpile, yet they have the potential for high impact on preventing the theft and illicit proliferation of conventional ammunition. Costs should be measured against the potential impact of poor security, (i.e. political impact, reputational consequences and overall financial costs), not just on simple financial loss accounting.

6 Principles and aim of conventional ammunition stockpile security **(LEVEL 1)**

6.1 Principles of stockpile security

The following principles of physical security should be applied to ammunition storage and processing areas:

A) there shall be an effective accounting system for all ammunition stocks held in all APBs and ESH at all ASA and a system of regular stock checks;

B) physical security systems should be derived from an effective risk assessment process;

C) physical security should be built into new storage facilities at the design stage;

D) an effective perimeter security infrastructure shall be in place;

E) access shall be controlled at all times;

F) access shall be restricted to authorised personnel only;

G) only trusted individuals, who have been security cleared, shall be nominated as authorised personnel to work within the facility; and

H) temporary personnel shall be accompanied at all times.

6.2 Aim of stockpile security

Absolute security is theoretically impossible as no secured facility can ever be 100% impervious to a determined attack or to theft/diversion from within. The aim of stockpile physical security should therefore be to:

A) deter and reduce any attempted incursions or internal thefts;

B) thwart any attempted security breach;

C) immediately detect a security breach or threat;

D) assess the scale of any security breach or threat;

[5] United Nations General Assembly Resolution A/RES/55/255. *Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition supplementing the United Nations Convention against Transnational Organized Crime*. 08 June 2001. 'The Firearms Protocol'. (Entered into Force on 03 July 2005).

E) delay the time necessary for the illegal removal of ammunition and explosives from storage areas; and

F) allow security personnel to respond and take appropriate action.

7 Stockpile risk assessment[6] (LEVEL 1)

A risk assessment should examine conventional ammunition stockpile security systems to determine:

a) the financial value of the facility and contents within it;

A) active hazards to conventional ammunition security and their frequency, (i.e. the probability of stockpile leakages through espionage, theft or diversion, or stockpile damage/destruction due to sabotage or other forms of attack);

B) passive hazards and their frequency, (i.e. natural catastrophes such as floods, earthquakes, fires etc);

C) attractiveness indicators for active hazards to conventional ammunition security (based upon the content of a given facility and its susceptibility to direct or surreptitious attack);

D) vulnerability to espionage, theft or diversion; and

E) vulnerability to sabotage or terrorist attack.

This information, when used properly, will allow the responsible authority to establish management priorities in the most cost-effective and secure manner. Residual risk of loss, theft or diversion should then be kept to a minimum.

The risk assessment should also formally identify those ammunition items that may be classified as being attractive to criminals and terrorist organisations (ACTO). Although arguably all ammunition items may be of some use to criminals and terrorists, ACTO classified ammunition is usually that ammunition that would significantly increase terrorist capability. Table 1 lists those items that should be classified as ACTO, and that should be subject to more stringent security than other ammunition items. States may wish to add items to the basic ACTO list:

ACTO Item	Potential Terrorist Use
MANPADS	▪ Attacks on civil aviation.
Detonators	▪ Initiation of Improvised Explosive Devices (IED). ▪ Usually strictly controlled on civilian explosives market.
Bulk Explosive	▪ Used as main charge for IEDs. ▪ More powerful than home-made or commercial explosives.
Man-portable Anti-Tank Missiles	▪ Attacks on VIP vehicles.
Hand Grenades	▪ Concealable weapon that can be used in confined spaces.
Small arms ammunition	▪ Close Quarter Assassinations.

Table 1: ACTO ammunition items

[6] One risk assessment methodology can be found in UFC 04-020-01, *DoD Security Engineering Facilities Planning Manual,* Chapter 3. 11 September 2008.

8 Physical security of conventional ammunition stockpiles

8.1 Development of physical security systems (LEVEL 1)

There are no international standards for the implementation of physical protective security systems. There are, however, a range of European Standards (EN) and national guidelines[7] that form international good practice for security equipment that can be utilised for the protection of ammunition storage areas and facilities. They are used as informative standards within this IATG.

The security requirements for each location should be determined by the assessment of criteria that shall include:

A) the type of assets to be protected and the role of the unit or users;

B) the value of assets (whether monetary or in terms of utility to illicit users) to be protected;

C) the threats to those assets, (see Clause 7);

D) the protection level desired against such threats, which may include cost benefit analysis; and

E) any design constraints imposed by the organisation storing the conventional ammunition.

The following components should be examined and considered during the development of a physical security system:

A) b) security regulations and standard operating procedures (SOP);

B) security plan;

C) staff selection and vetting;

D) access control;

E) physical security of buildings and structures; and

F) physical security of perimeter.

8.2 Security regulations (LEVEL 1)

Comprehensive security regulations[8] shall be compiled which should include the requirements of this module if compliance is to be met. Such regulations should be:

A) published as a legal authority;

B) available to all appropriate personnel;

C) clear and consistent with no legal or operational contradictions;

D) applicable to all ammunition stockpiles within a state; and

E) regularly reviewed.

Security regulations, which are a legislative and regulatory issue, should be supported by effective standing operating procedures (SOP) that lay down clear operational activities and responsibilities. SOPs should contain the following information as a minimum:

A) outline the scope of the instructions;

[7] A comprehensive national standard that may be of use is the*DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AAE). 17 April 2012.*

[8] This could take the form of legislation, regulatory or statutory instruments.

B) nominate the individual in charge of security at the location (appointment, location and telephone number). This will usually be the Security Officer;

C) outline any generic and known security threats;

D) list all those at the location with security responsibilities (security officers, safety officers, armaments officers, transport officers, stores officers, accounting officers etc);

E) individual terms of reference for those with security responsibilities, written in simple unambiguous language;

F) explain the access control policy;

G) rules for the control of security keys;

H) inventory and accounting procedures;

I) detailed security procedures to be followed in the different areas of the ammunition storage facility;

J) action on discovery of incursion, thefts, losses or accounting surpluses; and

K) action in response to alarms.

8.3 Security plan (LEVEL 1)

The security plan is the foundation to effective stockpile management of conventional ammunition and shall be based on the requirements of the security regulations. A written security plan shall be developed for each stockpile location.

Security plans can differ dependent on local requirements, local security organisation etc, although there should be common essential elements in each plan. Annex C contains a model plan that may be adopted by stockpile management organisations.

The security plan should be updated regularly to reflect any factors that may change. It should be a flexible document easily adaptable to changing circumstances and requirements. Security classification of the plan shall be the responsibility of the designated security officer at the conventional ammunition storage facility.

8.4 Staff selection and vetting systems (LEVEL 2)

Physical security and ammunition inventory management systems are all vulnerable to failure should staff not accept their responsibilities, fail to follow SOPs or become subverted. This means that organisations shall make every effort to ensure that staff are;

A) selected who do not have criminal convictions and are unlikely to possess criminal tendencies;

B) trained effectively; and

C) likely to remain loyal, well motivated and appropriately rewarded.

Conversely, poorly paid, inadequately trained and under-motivated staff are more likely to be involved in malfeasance (including laxity in carrying out duties, being susceptible to bribery, failure to follow procedures or even active involvement in conventional ammunition theft and sale).

Stockpile management organisations should ensure that appropriate procedures are developed and followed for the security vetting[9] of staff prior to employment in ammunition storage areas and that they are security vetted at regular intervals throughout their employment. It should also be a

[9] Security vetting is a process used to perform background checks on an individual's suitability for a particular appointment. It normally consists of: 1) confirming an individual's identity; 2) looking at associations that may cause a conflict of interest; and 3) determining vulnerabilities in an individual's life through which improper pressure could be applied.

condition of their contracts that they shall report any relevant changes in personal circumstances to security vetting staff. A history of gender-based or intimate partner violence, even if not classified as a criminal matter in some jurisdictions, should also be considered a disqualifying factor.

It should be noted that the 'human factor' plays a crucial role in safe and secure ammunition management and hence constitutes one of the weakest links in any physical security system. Only adequately paid and trained personnel who receive organizational recognition for their work and are provided with prospects for personal and professional development will develop a high degree of resilience against subversion. Therefore, early and adequate investments in the selection, training and well-being of staff should be considered at least as important as improvements to the physical infrastructure.

8.5 Access control

8.5.1 Keys (LEVEL 1)

Keys to ammunition storage areas, buildings, containers and intruder detection systems (IDS) shall be stored separately to other keys and shall not be left unsecured or unattended at any time. They shall be accessible only to those individuals whose duties require them to have access to the conventional ammunition storage areas. A roster of authorised personnel (custodians) should be kept by the authority responsible for ammunition security.

A record shall be kept each time an individual removes keys from the secure key cabinet.

The number of keys shall be kept to an absolute minimum, and master keys shall be prohibited.

8.5.2 Combination locks (LEVEL 2)

The main advantage of combination locks is that they can be easily re-coded, while key and lock systems must be entirely replaced in case one of the keys is lost. Conversely, there is no physical way of controlling and limiting the access (such as counting or retaining keys) to a facility. Hence, the use of combination locks is often limited to applications where it is undesirable for management personnel to leave the premises with keys (e.g. centralized key safe-boxes or access doors).

The combinations to locks shall be dealt with in the same manner as keys. Mechanical combination locks must not remain in open position, as the combination may be visible for unauthorized personnel.

Combinations should be changed at regular intervals and must be changed immediately when individuals change or move appointments and if it is suspected that unauthorized personnel gained knowledge of a combination.

Records of combinations should be held in sealed envelopes by the security officer even if they are logged onto secure computer systems.

Every combination lock guarded facility or container must have a record of access by individual, date and time prominently displayed on its door.

8.5.3 Entry to ammunition storage areas (LEVEL 1)

Strict personnel and vehicle access control shall be established for all areas storing conventional ammunition. Entry to ammunition storage areas should be authorised in writing by the authority responsible for ammunition security.

Vehicles and individuals should be subject to random inspection and search upon entry to and exit from ammunition storage areas.

8.6 Physical security infrastructure for buildings and structures

8.6.1 Doors and gates (LEVEL 2)

Access doors and gates shall be sufficiently robust and comply with national security standards. As a minimum, the doors should be made of solid hardwood with steel on the outside face. Door frames should be rigidly anchored to prevent disengagement of the lock bolt by prying or jacking of the door frame. Door and gate hinges should be located on the inside and should be of the fixed pin security type or equivalent. More detailed information on the construction of doors to achieve various levels of security may be found in LPS 1175 *Specification for testing and classifying the burglary resistance of building components, strong-points and security enclosures*.[10]

Access doors and gates shall be secured with high security padlocks (Clause 8.6.3).

8.6.2 Windows (LEVEL 1)

Windows and other openings to ammunition storage buildings shall be kept to a minimum and provided with appropriate locks and security bars or grilles. For new ESH no windows is preferred.

8.6.3 Locks and padlocks (LEVEL 2)

Padlocks for the gates and explosive storehouses should be compliant with European Standard EN 12320:2012, *Building hardware – Padlocks and padlock fittings – Requirements and test methods*.

8.6.4 Intrusion detection systems[11, 12] (LEVEL 3)

Buildings and structures used for the storage of conventional ammunition should be fitted with appropriate intrusion detection systems (IDS). IDS should be fitted to all doors, windows and other openings. Interior motion or vibration detection systems may also be fitted.

All alarm signals from such systems should be received at a central control or monitoring system from which a response force can be dispatched. The response force should respond to activated IDS (to include system tampering or compromise) as soon as possible, but the response shall be no later than 15 minutes after receipt of the alarm signal.

If IDS line security is unavailable, two independent means of alarm signal transmission from the alarm area to the monitoring station should be provided and any visible lines must be inspected weekly. Where possible, one of the two independent means of alarm signal transmission should be a secure wireless link. The dual transmission equipment shall continuously monitor the integrity of communications links.

IDS transmission lines should have electronically monitored line supervision in order to detect evidence of tampering or attempted compromise.

A daily record should be maintained of all alarm signals received which should be reviewed to identify and correct IDS reliability problems. The log should reflect the following:

A) nature of the alarm, (nuisance, system failure or illegal entry);

B) date, time and location of alarm; and

---

[10] Loss Prevention Standard (LPS) 1175 *Specification for testing and classifying the burglary resistance of building components, strong-points and security enclosures.* Issue 6. Building Research Establishment (BRE) Global. 24 May 2007.

[11] Also referred to as alarms.

[12] DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AAE).* 17 April 2012.

C) action taken in response to the alarm.

IDS should be tested weekly to ensure the proper functioning of the alarm sensors. Any visible lines must be inspected monthly and the inspection documented by the owner or user, except as noted above when IDS line security does not exist, for which inspections of visible lines are conducted weekly.

IDS should have a protected independent backup power source.

8.7 Physical security infrastructure for the perimeter

8.7.1 Perimeter security fencing

8.7.1.1 General

A fence or wall forms a useful barrier and also delineates the boundary of a protected or restricted area. The level of protection offered by a fence will depend on its height, construction, the material used to increase its performance or effectiveness such as topping, perimeter intrusion detection systems (PIDS), lighting or close-circuit television (CCTV).

The type of fence used should reflect the type of threat i.e. terrorist, criminal, vandals or armed attack. Fences are graded according to the level of protection they offer, Class 4 offering the highest security and Class 1 the lowest.

The effectiveness of any security barrier will depend to a large extent on the level of security at the points of entry. Gates shall be constructed to the same security standard as the fence and control of entry shall be maintained, otherwise the security of the fence will be negated. The perimeter fence shall have a minimum number of pedestrian and vehicular access gates, consistent with operational requirements.

Signs should be prominently displayed on all approaches to the perimeter to indicate to civilians that they are approaching a restricted area to which access is not permissible. If appropriate, such signs should also indicate the presence of armed guards and dogs.

8.7.1.2 Class 1 security fencing (LEVEL 1)

A fence designed with no particular security requirements and is at least 1.5m high. Such a fence is only intended to mark a boundary and to offer a minimum of deterrence or resistance to anyone other than a determined intruder. There will be occasions when the use of other perimeter security systems may be appropriate.

Picture 1: Class 1 fencing

Picture 1 shows a standard BS 1722 Part 10[13] chain link fence, approximately 2.9m high constructed with chain link fabric and a barbed wired topping. Supporting posts can be either reinforced concrete or tubular steel.

Chain link fences offer limited delay to attack and should be considered as a basic perimeter fence measure to delineate a boundary. Chain link does not host alarm systems well due to the nature of its construction.

[13] BS 1722-10:2006, *Fences. Specification for anti-intruder fences in chain link and welded mesh*. November 2006. www.bsi-global.com. This has been included as it is a good example of best practice in security fencing, and all fences are tested prior to classification within the standard.

8.7.1.3 Class 2 security fencing (LEVEL 1)

Picture 2: Class 2 security fencing

An anti-intruder fence that offers a degree of resistance to climbing and breaching by an opportunist intruder not having particular skills and only using material and breaching items that are readily to hand. A Class 2 fence should be supported by other perimeter security systems.

Picture 2 shows a standard BS 1722 Part 10 Anti-Intruder fence, 2.9m high constructed with welded mesh fabric and a barbed wire topping.

8.7.1.4 Class 3 security fencing (LEVEL 2)

Picture 3: Class 3 security fencing

An intermediate security barrier designed to deter and delay a resourceful attacker who has access to a limited range of hand tools. The design and construction will offer resistance to attempts at climbing and breaching. A Class 3 fence should normally be supported by other perimeter security systems.

Picture 3 shows an Intermediate Security Welded Mesh Fence. This fence complies with BS 1722 Part 14. The fence is 4m high, including barbed tape concertina topping. It is constructed using narrow aperture welded mesh to resist climbing and cutting.

An intermediate security fence offers a good balance of delay to attack versus cost.

8.7.1.5 Class 4 security fencing (LEVEL 3)

Picture 4: Class 4 security fencing

A high-security barrier designed to offer the maximum deterrence and delay to a skilled and determined intruder who is well equipped and resourced. It should be designed and constructed to offer a high degree of resistance to a climbing or breaching attack. A Class 4 fence shall be supported by other perimeter security systems.

Picture 4 shows a High Security Welded Mesh Fence. This fence is based on BS 1722 Part 14 but is 4.8m high including barbed taped concertina topping. It is constructed using narrow aperture welded mesh with an additional layer up to 3m.

High security fences provide the highest level of delay to attack; however, they are expensive to construct. Class 4 security fences should always be used in conjunction with CCTV and an intruder detection system.

8.7.1.6 Clear zones (LEVEL 2)

Zones clear of vegetation should be established and maintained for a minimum of 4m within a security fence and 10m outside the security fence (real estate permitting).

8.7.1.7 Drainage (LEVEL 1)

Drainage structures and water passages that penetrate the fence having a cross-sectional area of greater than 0.25m^2 should not be permitted or shall have bars and grilles preventing access at each end. Access to any existing structures and passages should be prevented.

8.7.2 Perimeter illumination (LEVEL 2)

Exterior and internal perimeter illumination shall be of sufficient intensity to allow detection of unauthorised activity by the guard force. All access points to a storage area should have direct illumination above all entry points. Switches shall be installed in such a manner that they are only accessible to authorised personnel.

An automatic backup generator and power system is essential on high risk and high value sites.

All perimeter illumination systems of the facility should radiate slightly outwards in order to facilitate night vision of the guard force and restrict that of those looking into the inner perimeter. The perimeter lighting should be placed inside the compound where it will be difficult to sabotage or destroy.

8.7.3 Perimeter intrusion detection systems (PIDS) (LEVEL 3)

8.7.3.1 General

Perimeter Intrusion Detection Systems, (PIDS), is a generic term which covers a wide range of technologies designed to provide advance warning of an intruder gaining access to a secure area.

All detection systems demand a compromise between detection capability and unwanted or nuisance alarm[14] rates. By their nature PIDS are designed to operate in a less favourable environment than internal intruder detection systems.

Perimeter fences around structures and buildings used for the storage of conventional ammunition should be fitted with appropriate PIDS. All alarm signals from such systems should be received at a central control or monitoring system from which a response force can be dispatched. The response force should respond to an activated PIDS as soon as possible, but the response shall be no later than 15 minutes after receipt of the alarm signal.

The performance of any PIDS will depend not only on the intrinsic characteristics of the technology employed but also on the specific site conditions under which it is deployed. *For this reason, it is strongly recommended that specialist technical advice is sought before any system is procured.*

Installation of a PIDS shall not be taken in isolation. To be effective it should operate as part of an integrated security system. This may include physical measures such as fences and barriers, providing both detection and delay together with visual surveillance systems and perimeter illumination providing alarm verification. Not least will be the integration with site security procedures and the guard force.

The specific type of PIDS employed should depend upon the site conditions, operational requirement and other constraints that will be placed on its operation.

8.7.3.2 PIDS types

There are a range of PIDS types, which may be considered for deployment, including:

A) buried detection systems;

B) fence mounted systems;

C) electric fence systems;

D) field effect systems;

E) continuity monitoring systems;

[14] Caused, for examples, by animals or weather.

F) free standing systems;

G) taut wire systems; and

H) rapid deploy systems.

The range of systems and factors involved in deployment means that it is not realistic to provide a cost estimate until the system requirements have been refined further.

8.7.3.3 PIDS records and tests

A daily record should be maintained of all alarm signals received, which should be reviewed to identify and correct PIDS reliability problems. The log should reflect the following:

A) nature of the alarm, (nuisance, system failure or illegal entry);

B) date, time and location of alarm;

C) personnel involved; and

D) action taken in response to the alarm.

PIDS should be tested quarterly to ensure the proper functioning of the alarm sensors.

8.7.4 Visual surveillance systems (LEVEL 3)

Visual surveillance may be used to increase the effective range and area of ground covered by the individuals of the security staff, thereby minimising staff requirements. Technology is available that can provide day, low-light and night coverage, but such technology should not be used to replace an appropriate level of physical presence by security staff.

Visual surveillance systems, usually CCTV or motion-initiated systems, may be used to:

A) cover all gates, doors, perimeters and interiors of conventional ammunition storage facilities;

B) provide constant, real time monitoring; and

C) record activity for review in the event of loss or theft.

D) Available camera systems technology, which can be supported by a range of data transmission technologies, includes:

E) normal visible light range;

F) low light capable; and

G) infra-red.

The requirements of Clause 8.7.3.3 for records and tests should also apply to visual surveillance systems.

8.7.5 Patrols and dogs (LEVEL 1)

A guard and response force[15] should check the security integrity of ammunition storage areas during non-duty hours at both prescribed and random occasions. These checks should be recorded, with these records maintained for a minimum of 90 days.

[15] This may include military personnel, police or civilian security personnel.

Staff should be properly trained and equipped to perform their duties in accordance with the appropriate SOP. Trained working dogs may be used as a complementary measure to the guard and response force.

Irregular spot checks and unannounced test call outs of guard force and back up personnel by night and by day are essential to check and practice both individuals and procedures.

9 Aspects of diversion[16]

9.1 background to diversion

The product for the clandestine arms market is overwhelmingly small arms and light weapons (SALW), but, in order to be of any effect, weapons require ammunition. Significant quantities of ammunition may be necessary to ensure the sustainability of violence.

The aim of an effective security system should be to reduce the risks of diversion due to loss, theft, leakage or proliferation to an absolute minimum. There can be no such thing as 100% absolute security because of human factors, but security levels should be as close to 100% as possible.

[16] Information in this Clause is from *Guns, Planes and Ships: Identification and Disruption of Clandestine Arms Deliveries*. Griffiths H and Wilkinson A E A. (ISBN 978 66 7728 069 7). SEESAC. August 2007.

Annex A
(normative)
References

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this module. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this module are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO maintain registers of currently valid ISO or EN:

a) BS 1722-10:2006 *Fences. Specification for anti-intruder fences in chain link and welded mesh*. November 2006. (www.bsi-global.com);

b) EN 12320:2012 *Building hardware – Padlocks and padlock fittings – Requirements and test methods*;

c) IATG 01.40 *Glossary of terms, definitions and abbreviations*. UNODA;

d) IATG 03.10 *Inventory Management*. UNODA;

e) Loss Prevention Standard (LPS) 1175 *Specification for testing and classifying the burglary resistance of building components, strong-points and security enclosures.* Issue 6. Building Research Establishment (BRE) Global. 24 May 2007;

f) United Nations General Assembly Resolution A/RES/55/255. *Protocol against the illicit manufacturing of and trafficking in, their parts and components and ammunition supplementing the United Nations Convention against Transnational Organized Crime*. 08 June 2001. 'The Firearms Protocol'. (Entered into Force on 03 July 2005).

The latest version/edition of these references should be used. The UN Office for Disarmament Affairs (UNODA) holds copies of all references[17] used in this guideline and these can be found at: www.un.org/disarmament/un-saferguard/references. A register of the latest version/edition of the International Ammunition Technical Guidelines is maintained by UNODA, and can be read on the IATG website: www.un.org/disarmament/ammunition. National authorities, employers and other interested bodies and organisations should obtain copies before commencing conventional ammunition stockpile management programmes.

[17] Where copyright permits.

Annex B
(informative)
References

The following informative documents contain provisions, which should also be consulted to provide further background information to the contents of this guideline:

a) *Guns, Planes and Ships: Identification and Disruption of Clandestine Arms Deliveries*. Griffiths H and Wilkinson A E A. (ISBN 978 66 7728 069 7). SEESAC. August 2007;

b) *Handbook of Best Practices on Conventional Ammunition*, Chapter 3. Decision 6/08. OSCE. 2008. www.osce.org/fsc/33371;

c) DoD 5100.76-M *Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AAE)*. US Department of Defense. 12 April 2012. http://dtic.mil/whs/directives/corres/pdf/510076m.pdf; and

d) UFC 04-020-01 *Security Engineering Facilities Planning Manual*. US Department of Defense. 11 September 2008. http://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-020-01

The latest version/edition of these references should be used. The UN Office for Disarmament Affairs (UNODA) holds copies of all references[18] used in this guideline and can be found at: www.un.org/disarmament/un-saferguard/references. A register of the latest version/edition of the International Ammunition Technical Guidelines is maintained by UNODA, and can be read on the IATG website: www.un.org/disarmament/ammunition. National authorities, employers and other interested bodies and organisations should obtain copies before commencing conventional ammunition stockpile management programmes.

[18] Where copyright permits.

Annex C
(informative)
Model for a security plan[19] (LEVEL 1)

C.1 Name, location and telephone number of the establishment security officer.

C.2 Scope of the plan.

C.3 Content and value of the stocks.

C.4 The generic security threats.

C.5 Detailed geographic map of the site location and its surroundings.

C.6 Detailed diagrams of the layout of the site, including all its buildings, entry and exit points, and of the location of all features such as electricity generators/substations; water and gas main points; road and rail tracks; wooded areas; hard and soft-standing areas etc.

C.7 Outline of physical security measures for the site, including but not limited to details of:

A) fences, doors and windows;
B) lighting;
C) Intruder Detection System (IDS);
D) Perimeter Intrusion Detection System (PIDS);
E) automated access control systems;
F) guards;
G) guard dogs;
H) locks and containers;
I) control of entry and exit of persons;
J) control of entry and exit of goods and material;
K) secure rooms;
L) hardened buildings; and
M) CCTV.

C.8 Security responsibilities (including but not limited to the following personnel, as applicable):

A) security officer;
B) safety officer;
C) armament officer;
D) production manager;
E) transport officer;
F) heads of department;
G) stores/supply officers;

[19] Quoted from Best Practice Guide on National Procedures for Stockpile Management and Security. FSC.GAL/14/03 Rev 2. OSCE. 19 September 2003.

H) foreman in charge of operations/accounting/movement;

I) workers; and

J) all personnel authorised to have access to the site.

C.9 Security procedures to be followed in production/process areas; storage areas; servicing; processing; trials; quality assurance; climatic and other tests as well as further activities in respect of weapon stockpile management.

C.10 Control of access to storage and processing rooms, buildings, structures and areas.

C.11 Procedures for handling and transport of conventional ammunition.

C.12 Control of security keys – those in use and their duplicates.

C.13 Accounting – audits and stock checks.

C.14 Security education and briefing of staff.

C.15 Action on discovery of loss/surplus.

C.16 Details of response force arrangements (e.g. size, response time, orders, activation and deployment).

C.17 Action to be taken in response to activation of alarms.

C.18 Action to be taken in response to emergency situations (e.g. fire, flood, raid etc).

Amendment record

Management of IATG amendments

The IATG are subject to formal review on a five-yearly basis. This does not preclude amendments being made within these five-year periods for reasons of operational safety, efficacy and efficiency or for editorial purposes.

As amendments are made to this IATG module they will be given a number, and the date and general details of the amendment will be shown in the table below. The amendment will also be shown on the cover page of the IATG by the inclusion of the amendment number and date.

As the formal reviews of each the IATG module is completed, new editions will be issued. Amendments will be incorporated into the new edition and the amendment record table cleared. Recording of amendments will then start again until a further review is carried out.

The most recently amended, and thus extant, IATG module is posted on www.un.org/disarmament/ammunition

Number	Date	Amendment Details
0	01 Feb 15	Release of Edition 2 of IATG.
1	31 March 21	Release of Edition 3 of IATG.