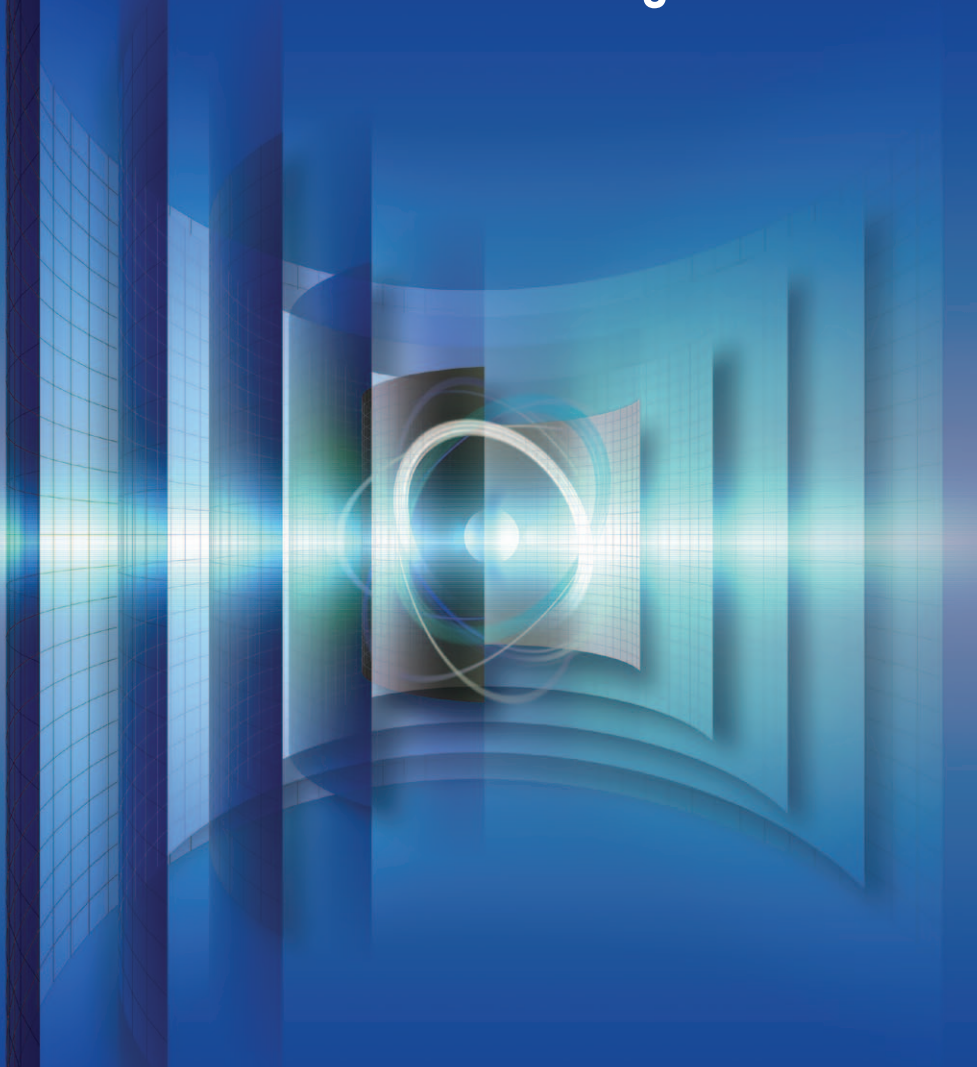
IAEA Nuclear Security Series No. 10

Implementing Guide

Development, Use and Maintenance of the Design Basis Threat



IAEA
International Atomic Energy Agency

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 10

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

COPYRIGHT NOTICE

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
May 2009
STI/PUB/1386

IAEA Library Cataloguing in Publication Data

Development, use and maintenance of the design basis threat : implementing guide. Vienna : International Atomic Energy Agency, 2009.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 10)
STI/PUB/1386
ISBN 978–92–0–102509–8
Includes bibliographical references.

1. Nuclear facilities — Security measures. 2. Radioactive substances — Security measures. 3. Nuclear terrorism — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL 09–00572

FOREWORD

In response to a resolution by the IAEA General Conference in September 2002, the IAEA adopted an integrated approach to protection against nuclear terrorism. This approach coordinates IAEA activities concerned with physical protection of nuclear material and nuclear installations, nuclear material accountancy, detection of and response to trafficking in nuclear and other radioactive material, the security of radioactive sources, security in the transport of nuclear and other radioactive material, emergency response and emergency preparedness in Member States and at the IAEA, and promotion of adherence by States to relevant international instruments. The IAEA also helps to identify threats and vulnerability related to the security of nuclear and other radioactive material. However, it is the responsibility of the States to provide for the physical protection of nuclear and other radioactive material and associated facilities, to ensure the security of such material in transport, and to combat illicit trafficking and the inadvertent movement of radioactive material.

Physical protection systems are intended to prevent unacceptable consequences arising from malicious activities. The more serious the consequences, the more important it is to have a high degree of confidence that physical protection will be effective as planned.

The need for a high level of confidence in the effectiveness of physical protection has long been recognized by those concerned about nuclear material and nuclear facilities. Nuclear material and facilities have the potential for a variety of unacceptable radiological and proliferation consequences if subjected to a malicious act. The highest level of confidence in physical protection demands a close correlation between protective measures and the threat. This approach is firmly grounded in the fundamental principle that physical protection of nuclear assets under the jurisdiction of a State should be based on the State's evaluation of the threat to those assets. As described in this publication, an understanding of the threat can lead to a detailed description of potential adversaries (the design basis threat), which, in turn, is the basis of an appropriately designed physical protection system. This direct link gives confidence that protection would be effective against an adversary attack.

International experience in using a design basis threat to protect assets of high consequence is largely based on the protection of nuclear material and facilities. Furthermore, the nuclear security documents defining and recommending that physical protection be based upon the threat — The Physical Protection Objectives and Fundamental Principles (GOV/2001/41/Attachment), the Recommendations on the Physical Protection of Nuclear Facilities and Nuclear Material (INFCIRC/225/Rev. 4 (corrected)), and the

Convention on Physical Protection of Nuclear Facilities and Nuclear Material as Amended (INFCIRC/274) (adopted on 8 July 2005; (GOV/2005/57)) — do so exclusively for the protection of nuclear material and facilities. Given the historical background, and its continuing contemporary relevance, it has been necessary to draw on that nuclear protection experience in developing this publication. However, the general approach can also be applied to protecting other assets that require a high degree of confidence in the effectiveness of their protection, such as high-activity radioactive material.

Specialists from France, Germany, Japan, the Russian Federation, Spain, the United Kingdom, and the United States of America assisted the IAEA in preparing this publication. A draft was presented to an open-ended technical meeting in December 2006, and subsequently circulated for comment to all Member States. This publication is consistent with The Physical Protection Objectives and Fundamental Principles; the Convention on Physical Protection of Nuclear Facilities and Nuclear Material as Amended; and the Recommendations on the Physical Protection of Nuclear Facilities and Nuclear Material.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Rev. 4 (Corrected) [1] describes the design basis threat (DBT) tool and recommends development of a notional DBT. Recognizing the importance assigned to the DBT tool in INFCIRC/225, a number of IAEA Member States requested that workshops be developed and conducted to present a methodology for developing, maintaining, and using a DBT. As an adjunct to the workshops, a draft was developed and circulated for comment.

The draft was intended to implement the recommendations in INFCIRC/225/Rev. 4 (Corrected), which was issued in 1999. Since then, further developments have occurred to strengthen the international regime for the physical protection of nuclear material and radioactive material and associated facilities, including endorsement of The Physical Protection Objectives and Fundamental Principles (GOV/2001/41/Attachment) [2] by the IAEA Board of Governors in September 2001, and endorsement of the revised Code of Conduct on the Safety and Security of Radioactive Sources by the Board of Governors in 2004. These objectives and principles were then incorporated into the 8 July 2005 Amendment to the Convention on the Physical Protection of Nuclear Material [3]. This Implementing Guide represents an update of the original draft guidance reflecting further developments.

1.2. OBJECTIVE

A DBT is a comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. Such definitions permit security planning on the basis of risk management. A DBT is derived from credible intelligence information and other data concerning threats, but is not intended to be a statement about actual, prevailing threats. Historically, States have used DBTs in their regulatory system to achieve appropriate allocations of resources to the protection of nuclear material and nuclear facilities against malicious acts by potential adversaries that could result in high consequences, particularly radiological consequences or consequences of proliferation; however, a DBT can also be used to protect any asset with associated high potential consequences (e.g. other radioactive material of high activity).

This publication provides guidance on how to develop, use and maintain a DBT. It is intended for decision makers from organizations with roles and responsibilities for the development, use and maintenance of the DBT.

1.3. SCOPE

This Implementing Guide:

- Describes a DBT, including what it is and why and under what circumstances it is used;
- Identifies and recommends the roles and responsibilities of organizations that should be involved in the development, use and maintenance of a DBT;
- Describes how to conduct a national threat assessment as a precursor to a DBT;
- Explains how a DBT can be developed, including:
  - the information required to develop a DBT;
  - the decision making processes for the development of a DBT;
- Explains how a DBT is incorporated into a State's nuclear security regime[1];
- Explains the conditions for a review of the DBT, and how the review and update are conducted

This publication does not include recommendations for physical protection measures, nor does it include guidance on the design and evaluation of physical protection systems.

[1] The nuclear security regime includes all nuclear security activities in a State for the protection of nuclear and radioactive material and facilities (including transport), and the prevention of illicit trafficking. It encompasses the legislative and regulatory framework, the designation of competent authorities, the definition of responsibilities between the State and operator with regard to nuclear security, the administrative measures and technical features at a facility, transport, or transport checkpoint to prevent the unauthorized removal and illicit trafficking of nuclear and radioactive material, and the radiological sabotage of nuclear and radiological facilities. It also includes the measures taken to facilitate the mitigation of the consequences of such a malicious act were it to occur, including recovery of stolen material.

1.4. STRUCTURE

Following the background discussion in Section 1, Section 2 provides a description of a DBT. Section 3 presents the purpose and value of a DBT in a State's nuclear security regime. Section 4 describes the roles and responsibilities in the development, use and maintenance of a DBT. Section 5 outlines the approach to conduct a threat assessment as a precursor to DBT development. Section 6 describes the process of taking the output of a threat assessment and developing a DBT. Section 7 provides an overview of how a DBT is used in a State's nuclear security regime. Section 8 discusses how a DBT is maintained.

SPECIAL NOTE

This publication recommends the use of national intelligence and other sensitive information, and the involvement of national intelligence agencies in the development of a threat assessment and a DBT. Some of this information and many of its sources require protection. This normally involves using a national system of information classification and associated protection measures. The DBT itself, because of its use in the design and evaluation of physical protection systems, would also be of value to an adversary wishing to carry out a malicious act. It is essential that it be appropriately protected. Those with access to a DBT will usually need proper authorization, in accordance with national laws and regulations, and the physical means to store and protect it.

2. DESCRIPTION OF A DESIGN BASIS THREAT

A fundamental principle of physical protection is that it should be based on the State's current evaluation of a threat [2]. This evaluation is formalized through a threat assessment process. A DBT is derived from this threat assessment to facilitate the development of physical protection on the basis of a State's evaluation of the threat. To define the DBT, the set of threats described in the State's threat assessment are modified to take account of other factors, such as technical, economic and political issues, and the particular requirements of planning for the design of the physical protection system. To

make the transformation from threat assessment to DBT, rigorous analysis and decision making are essential.

A DBT is a description of the attributes and characteristics of potential insider and outsider adversaries who might attempt a malicious act, such as unauthorized removal or sabotage against which a physical protection system for nuclear or other radioactive material or associated facilities is designed and evaluated [1]. This section explains this description and introduces the relationship between the responsibilities of the State and the operator[2] and the relationship between the actual threat and the DBT.

The definition of a DBT is derived on the basis of four important themes. These are:

— *Insider/outsider adversaries.* A potential adversary is any individual or group of individuals, including both outsider adversaries and insiders, deemed to have the intent/capabilities to commit a malicious act.
— *Relationship between malicious acts and unacceptable consequences.* Some malicious acts[3], such as unauthorized removal of material or radiological sabotage, can lead to unacceptable consequences and therefore must be prevented.
— *Attributes and characteristics* The relevant attributes and characteristics of potential adversaries describe their motivation, intention and capability to commit a malicious act. Motivation could be economic, political, or ideological. Intentions may include unauthorized possession of material, radiological sabotage and public embarrassment. The capabilities of adversaries are determined by their composition, including their numbers, grouping, their possible inclusion of insiders, and insider collusion, and their organization; as well as their abilities and assets, including tactics, weapons, explosives, tools, transportation, level of access, and skills of the adversary.
— *Design and evaluation.* A DBT, which is defined at the State level, is a tool used to help establish performance requirements for the design and evaluation of physical protection systems. The capabilities of adversaries in this area help operators and State authorities to determine the criteria

[2] An operator is any entity or person authorized to use, store, or transport nuclear material or radioactive material. An operator would normally hold a license or have another form of authorization from a competent authority or would be a contractor of such a licensee or other authorized entity.

[3] Malicious acts could also include gaining control of equipment or facilities for blackmail

for detection, delay and response for the design and evaluation of an effective physical protection system.

The DBT contains that set of adversary characteristics against which the operators and State organizations have the responsibility for protection and accountability. The division of these responsibilities may vary from State to State. The responsibilities that are assigned to the operator to protect against the DBT should be defined in accordance with the missions, capabilities, resources, and authority of the operator.

It is quite possible that some threats defined in the threat assessment will not be included in the DBT, and that protection against these threats will remain the responsibility of the State. Nevertheless, although the State will develop measures to counter these threats, the operator may still have a role in assisting the State either to protect against these threats or to mitigate their consequences.

A State may decide to have more than one DBT to reflect different needs for protection, such as:

— Different target material (e.g. nuclear material and radioactive material);
— Different types of facilities (e.g. nuclear power plants, research reactors and transports);
— Different adversary objectives (e.g. theft, radiological sabotage, economic disruption).

These distinctions highlight the importance of clarifying the planned use of a DBT prior to developing it.

Figure 1 shows the relationship between the potential threats in the threat assessment and the DBT. It shows the range of all threats, from a condition of low threat capabilities (at the bottom of the chart), to high threat capabilities (at the top of the chart). This range represents the known, actual and prevailing threats that are evaluated in the threat assessment. Through the process to develop the DBT, these threats will be assessed to determine whether they would be appropriate as a basis for design requirements for physical protection. Some will be screened out for reasons described in Section 6, while others will be refined and further developed. The result of the screening and refinement process will be the definition of the maximum threat capabilities against which protection will be reasonably ensured. This definition contains the capabilities for all potential threats against which the State has decided to develop specific protection measures (see the dashed horizontal line). The level of threat labelled in the figure as DBT is that subset of these threat capabilities which is used as a basis to regulate physical protection. The DBT can

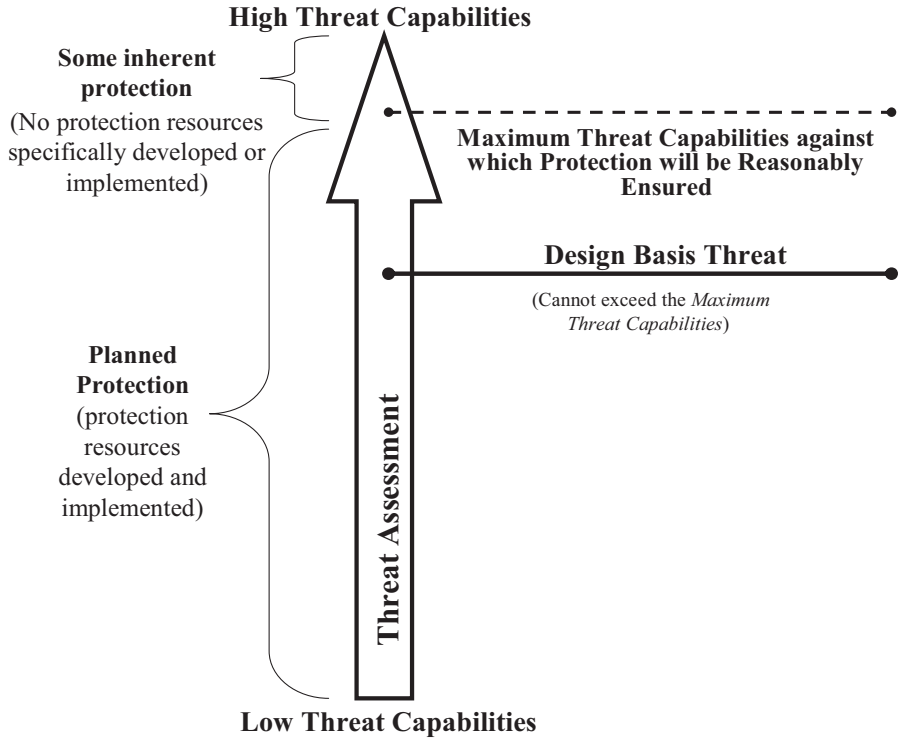


FIG. 1. Relationship between threats included in the DBT and those considered in a threat assessment.

encompass all the threats in the maximum threat capabilities against which protection will be reasonably ensured provided that all these threats are appropriate for a DBT. It should be noted that neither the maximum threat capabilities against which protection will be reasonably ensured nor the DBT describe a single identifiable or named adversary. They are representative descriptions drawn from all credible threats of concern.

Figure 2 depicts the relationship between State and operator responsibilities for implementing effective physical protection against threats. As is shown, the State will ensure that protection resources will be applied to all threats included under the *maximum threat capabilities against which protection will be reasonably ensured.* The State and operator will share the responsibility for this protection, with the operator having the primary responsibility for those threat capabilities within the DBT, and the State having primary responsibility for those threats between the DBT and the maximum threat capabilities against which protection will be reasonably ensured.

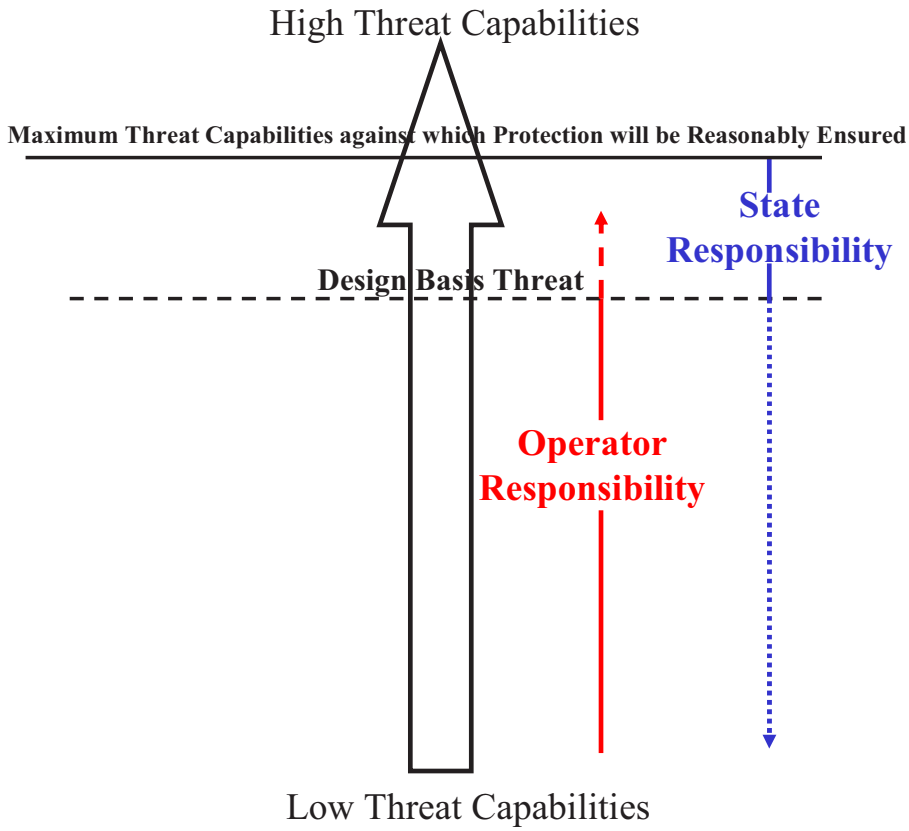


FIG. 2. Roles and responsibilities for protecting against threats.

Protection resources will be neither developed nor assigned to protect against threat capabilities that exceed the threshold of maximum threat capabilities against which protection will be reasonably ensured; however, existing protection and mitigation measures are expected to provide some inherent protection against these threat capabilities.

3. PURPOSE OF A DESIGN BASIS THREAT

A DBT is a tool that provides a common basis for planning for physical protection by the operator and approval of its physical protection plan by the competent authority for nuclear security. This section discusses the concerns

that give rise to the need for a DBT and the value of a DBT to the State and the operator.

3.1. NEED FOR A DESIGN BASIS THREAT

A physical protection system is designed to prevent adversaries from successfully committing a malicious act. To ensure that this objective is met, the designer for physical protection should understand the conditions under which the protection system must perform. A clear description of these threats defines these conditions and is therefore an essential prerequisite for reasonably assured and effective physical protection. Ideally, intelligence and other sources of information related to threats would provide sufficient information for the specification of requirements for the design and for the performance of a physical protection system to help ensure that this objective is met. However, intelligence is often limited, and threats are inherently dynamic. A physical protection system designed only for the current threat may not be effective against tomorrow's threat.

In the absence of a sufficiently detailed and specific description of the threat, it is difficult to precisely determine the level of protection that would be appropriate and effective for a given facility or activity. Given the potentially severe consequences of some malicious acts and the high costs of providing protection, uncertainties concerning the level of protection that is necessary are unlikely to be acceptable to a State's responsible authorities. A well specified description of the threat is necessary for a confident determination that protection is adequate and sufficient.

To address the need for a well specified description of the threat, the concept of a DBT was introduced. A DBT[4] is the State's description of a representative set of attributes and characteristics of adversaries, based upon (but not necessarily limited to) a threat assessment, which the State has decided to use as a basis for the design and evaluation of a physical protection system.

3.2. VALUE OF A DESIGN BASIS THREAT

The DBT provides a detailed and precise technical basis for design and evaluation criteria for physical protection, and can therefore provide greater

[4] As mentioned earlier, a State may choose to have more than one DBT (see Section 2).

assurance that the level of protection is sufficient. The use of the DBT to develop a physical protection system should lead to an efficient allocation of resources for protection by reducing the arbitrariness that might otherwise exist in establishing requirements for physical protection. The DBT not only enables a flexible approach to regulation that permits customization of the design of the physical protection system to address unique features of the material or facilities, but also sets a baseline against which the need for changes in physical protection can be evaluated, and provides a clear basis for defining the physical protection responsibilities of the operator.

A DBT is not an end in itself but rather a tool for achieving a set of objectives. Developing a DBT is only of value to the State if it is used for designing and evaluating a physical protection system. To accomplish this, the DBT needs to be incorporated into the regulatory framework and used to:

— Establish performance objectives and requirements for physical protection systems;
— Specify design criteria for physical protection systems;
— Establish criteria for evaluation of physical protection systems;
— Distinguish between the responsibilities of the State and those of the operator.

At the level of the operator, methods of detection, measures for delay, and the composition of the response to malicious acts should be developed and evaluated to address the attributes and characteristics of the adversaries as described in the DBT.

4. ROLES AND RESPONSIBILITIES

Overall responsibility for the development, use, and maintenance of a DBT rests with the State. The manner in which this is accomplished within a State depends on the State's own arrangements for developing policy, legislation, and regulation. There may be flexibility in having different competent authorities involved in the DBT process: one for development and maintenance of the DBT, and other(s) for use of the DBT. It is recommended that all these activities be assigned to the single competent authority responsible for the use of a DBT (e.g. the competent authority for oversight of the security of nuclear and radioactive material and facilities) owing to its

insight into the physical protection that a DBT will influence; however, the decision on who will be the competent authority for DBT development and maintenance remains with the State. If the State decides to have separate authorities for these two roles, an important element of coordination is to ensure that DBTs are developed that fit into the regulatory scheme. In particular, close coordination is needed between these two authorities to identify the types of facilities/licensees for which DBTs are needed (based on the regulatory framework) and to ensure that the development of these DBTs take into account the potential consequences related to the theft and radiological sabotage of nuclear and other radioactive material for each type of facility and licensee.

Recommendations for roles and responsibilities are outlined below. Some responsibilities are defined for high levels of government, and are therefore organized under the heading of 'State'. Other responsibilities are associated with specific organizations within the State under the appropriate headings.

4.1. STATE

The State should ensure that:

— The legal framework enables the incorporation of a DBT, either through a legally binding instrument or by an administrative act;
— The competent authority for development of the DBT has the skills and authority necessary to initiate the development of the DBT, to gain access to the appropriate information and to obtain the assistance of other State bodies to develop and maintain the DBT;
— Appropriate State organizations participate in the threat assessment process;
— The organizations involved in the DBT are identified and their roles are specified;
— There is effective integration between the operator and the many organizations in a State contributing to protection against the DBT.

4.2. COMPETENT AUTHORITY(IES) FOR DEVELOPMENT, USE AND MAINTENANCE OF A DESIGN BASIS THREAT

The responsibilities for DBT development, use and maintenance may reside with a single authority, or may be divided among several authorities. In either case, the following responsibilities need to be clearly assigned.

For the development and maintenance of the DBT, the competent authority:

— Coordinates the process to determine whether a DBT is the appropriate mechanism for implementing a threat based approach to protection to provide reasonable assurance of an adequate level of protection.[5]
— Initiates the processes for developing a threat assessment document for the DBT.
— Coordinates the process for development of the DBT and documents the assumptions and decisions.
— Ensures that the DBT's conclusions are consistent with other legal, legislative, or regulatory requirements.
— Verifies whether the existing regulatory framework is adequate for empowering relevant State bodies, to the extent needed, to provide their complementary part in protection and mitigation. If not, it initiates the necessary steps for improving the regulatory framework.
— Gains consent for the DBT from all relevant State organizations.
— Disseminates the DBT, or aspects of it, to those responsible for providing physical protection, and to those involved in the DBT's development and review.
— Determines how the DBT should be reviewed and properly maintained.
— Decides when it is appropriate to initiate a formal update of the DBT.
— Promulgates, applies and verifies the appropriate security measures and confidentiality rules to protect the information provided for, and contained in, the DBT.

For incorporation of the DBT within the regulatory security system and using it to develop appropriate protection measures, the competent authority:

— Clarifies the planned use of the DBT to help define what type of DBT is needed;
— Verifies that the existing regulatory framework is adequate for ensuring the use of the DBT by operators;
— Incorporates the DBT into the regulatory framework;
— Decides how the DBT will be used, and what regulatory requirements should apply;

[5] If the rigour associated with a DBT is not deemed appropriate, the competent authority needs to identify an alternative threat based approach to provide adequate assurance of appropriate protection.

— Ensures that the requirements for physical protection arising from the DBT are consistent with legal or regulatory requirements.

4.3. INTELLIGENCE ORGANIZATIONS

The involvement of the organizations responsible for the gathering and assessment of intelligence is essential for developing a credible threat as a basis for evaluating physical protection measures. Intelligence expertise may exist in several organizations, such as the ministry of foreign affairs, law enforcement bodies and military bodies. Such organizations are familiar with the processes of gathering and assessing intelligence information and are skilled in making the necessary judgments. They may have access to sources of information, including information from international liaisons that may otherwise be unavailable to the competent authority developing the DBT. The responsibilities of the intelligence organizations specifically include:

— Gathering and providing information on potential threats to high consequence or high value targets;
— Leading analysis of the available data to ensure that the resulting threat assessment document and DBT are founded on credible data.

4.4. OPERATORS

A physical protection system, and the specific measures that support it, are either developed by the operator (and validated by the regulatory body) or directly defined by the regulatory body. In either case, the operator has the prime responsibility for implementing protection measures. The operator's knowledge of the financial, operational and safety impact of specific measures may influence the division of responsibility for security measures between the operator and other entities. Because of this, the operator's input, either formal or informal, should be taken into consideration in developing the DBT. The operator should:

— Provide feedback to the competent authority developing the DBT, as requested, concerning the financial, operational, and safety impact of potential decisions relating to the DBT;
— Provide supporting information regarding any concerns about insider threats and any incidents that may have had a malicious origin;

— Develop and implement the necessary protective measures against the DBT, including those relating to security systems, nuclear material control, emergency preparedness, law enforcement and transportation.

4.5. OTHER ORGANIZATIONS

A variety of agencies and authorities (for example, the national and local police authorities, armed forces, border control authorities and customs authorities) play a part in protection, either on their own or in conjunction with others, and should also be involved or consulted in the process to develop a DBT. These organizations may have similar responsibilities to those of the operator to:

— Develop the required protection measures under their purview as determined to protect against the DBT;
— Provide feedback to the competent authority developing the DBT concerning the financial and operational impact of potential decisions on the DBT. [6]

5. PERFORMING A THREAT ASSESSMENT

Two main stages are undertaken in the development of a threat basis for the design of physical protection: the first is threat assessment; the second is the evaluation and decision making process that results in a DBT.[7] This section describes in detail the first of these stages: the steps and processes that constitute performing a threat assessment. The second of these stages is addressed in Section 6.

[6] This feedback would make sure that the competent authority developing the DBT had taken into account the impact of decisions concerning the DBT. For example, the impact of including capabilities for an aircraft crash in the DBT.

[7] There are situations where a DBT may not be the appropriate tool to implement threat based protection. In these cases, an alternative threat statement should be developed as a basis for security. This is discussed at the end of Section 5.

As the threat assessment and the DBT development are team efforts, the competent authority will need to assemble appropriate experts from relevant disciplines, as mentioned in Section 4, prior to initiating the threat assessment.

5.1. CONDUCTING A THREAT ASSESSMENT

A threat assessment is a formal process of gathering, organizing and assessing information about existing or potential threats that could result in or lead to a malicious act. For a threat assessment to be used effectively as a foundation for threat based protection, several organizations with different areas of expertise need to work closely together. These include organizations with responsibilities and experience in the collection and analysis of intelligence data, but which may have limited experience with the types of facilities and material that are to be protected; and organizations — such as the regulatory authority — that are familiar with the operational conditions and protection strategies, but which may be inexperienced in the process of threat assessment. Close working relationships between all of the relevant organizations is essential to produce an effective threat assessment document.

Where possible, the regulatory authority should establish agreements and the requisite authorization to participate directly in the threat assessment. In this way, their insight can be integrated into the assessment to better adapt the assessment to the issues of concern.

The threat assessment process can be described in terms of information input, analysis and output (see Fig. 3).

5.1.1. Input

The input to the threat assessment should consist of a comprehensive compilation of information about all potential adversaries and their motivation, intentions and capabilities. All reliable national and international sources of information should be considered. Sources of information should include intelligence and law enforcement agencies, official government reporting, other sources of classified or unclassified material, incident reporting by operators, and corroborated reporting in the media. In addition to threat information related to specific material or facilities of concern, relevant information regarding adversary characteristics for analogous high value, high consequence industries should be considered.

This information gathering process would include, for example, details of historical events and planned events, and information acquired on the basis of evidence that may indicate a possible intent to attack high value or hardened

assets and facilities, such as evidence of training. Factors that the threat assessment should address, but may not be limited to, are:

— Gobal and domestic threats;
— Credible capabilities, even if not yet demonstrated;
— Insider threat issues.

Evaluation of the credibility of the information used in performing the threat assessment is critical. Information provided by law enforcement and intelligence agencies should be accompanied by a judgement on how much confidence can be attached to it. To be most credible, information should be derived from sources that are known to have access to the originator of the information, and are judged to be transmitting it accurately and reliably. Open source information (i.e. media) should be used only when it is judged to be accurate and factual. The degree of confidence in any information, e.g. whether or not the source of information has first hand knowledge and is known to be reliable, has to be taken into account when deciding how that information will be used later.

5.1.2. Process of analysis

Once the information has been collected, the data are analysed to identify and document the credible motives, intentions and capabilities of the potential threats. Collection and analysis are continuous activities as analysis will often demonstrate the need for more information. The analysis should pay particular attention to potential threats that may be relevant to nuclear and other radioactive material, and associated facilities and transport. The process involves evaluating what is known and making a judgment about how adversary groups or individuals might behave in the future. The capabilities of the intelligence community to gather the data comprehensively and assess the data accurately will affect the confidence placed in the final DBT, and should therefore be considered.

The aim is to provide a credible assessment of potential threats, including their composition, motivation, intentions and capabilities. It is not intended to define specific scenarios or the tactics that the adversary may use.

The competent authority and the other participants in the threat assessment process should consider at least the following attributes and characteristics for each identified internal and external threat, although there may not be data available for all the listed attributes and characteristics for each threat:

— *Motivation:* political, financial, ideological, personal;
— Willingness to put one's own life at risk;
— *Intentions:* radiological sabotage of material or of a facility, theft, causing public panic and social disruption, instigating political instability, causing mass injuries and casualties;
— *Group size:* attack force, coordination personnel, support personnel;
— *Weapons:* types, numbers, availability;
— *Explosives:* type, quantity, availability, triggering sophistication, acquired or improvised;
— *Tools:* mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment;
— *Modes of transportation:* public, private, land, sea, air, type, number, availability;
— *Technical skills:* engineering, use of explosives, chemicals, paramilitary experience, communications skills;
— *'Cyber' skills:* skills in using computer and automated control systems in direct support of physical attacks, for intelligence gathering, for computer based attacks, for money gathering, etc.
— *Knowledge:* targets, site plans and procedures, security measures, safety measures and radiation protection procedures, operations, potential use of nuclear or other radioactive material;
— *Funding:* source, amount and availability;
— Insider threat issues: collusion, passive or active involvement, violent or non-violent engagement, number of insider adversaries;
— *Support structure:* presence or absence of local sympathizers, support organization, logistical support;
— *Tactics:* use of stealth, deception, or force.

In addition to addressing the attributes listed, the threat assessment should attempt to address the compilation and aggregation of the attributes.

All threats are analysed at this stage unless it is clear that credibility of the information about them is suspect.

5.1.3. Output

The output of this first stage is a threat assessment document describing the overall threat environment and all known credible threats that need to be taken into consideration by the State. The supporting analytical narrative should provide as much detail as possible about these threats and the credibility of the information. This threat assessment document is used in developing the adversary attributes and characteristics that make up the DBT.

Both the threat assessments and the details of intelligence sources are typically sensitive and protected information.

5.2. DECISION TO USE A DESIGN BASIS THREAT OR ANOTHER THREAT BASED APPROACH

A threat based approach to physical protection should be taken to achieve reasonable assurance that an appropriate level of protection is provided. In accordance with a graded approach,[8] a formal DBT may not be needed in all situations to provide reasonable assurance. Therefore, the competent authority for developing the DBT should lead the effort to decide — primarily on the basis of the potential consequences of malicious acts — whether a DBT should be used, or whether another, alternative, threat-based approach should be taken.

Making the decision on whether or not a DBT is the appropriate tool for implementing threat based protection requires balancing the benefits of a DBT approach with the costs of its use and as compared with an alternative approach. The DBT provides a more detailed and precise technical basis for design and evaluation criteria and can, therefore, provide greater assurance that the protection is sufficient; however, it requires greater resources and competences on the part of the regulatory authority and the operator. Whether the greater assurance is required and appropriate, and whether the benefit outweighs the cost, is a decision for the State. Nevertheless, the following decision criteria are recommended:

— Development of a DBT is recommended if the State has determined that the potential consequences of a malicious act would be severe[9];
— Development of a DBT should still be considered for protection of assets with associated lesser consequences if:

---

[8] A graded approach is an approach to the establishment and imposition of physical protection requirements that takes into account the relative attractiveness and nature of the nuclear/radioactive material, the potential consequences associated with the unauthorized removal of nuclear/radioactive material and the potential consequence of radiological sabotage against nuclear/radioactive material or associated facilities.

[9] The designation *severe* consequences will vary from State to State. It is used here to denote consequences that are deemed by the State to be severe enough to require a high assurance of successfully preventing malicious acts that would result in those consequences

- the threat assessment indicates the existence of a threat with known intent to commit a malicious act affecting the asset under consideration,
- the threat assessment indicates a highly capable threat for which intent is unknown;
- there is too much uncertainty in the threat assessment owing to a limited amount of data or a low level of confidence in the sources of the data.

The decision to pursue a DBT may be influenced by the limited availability of the necessary capabilities and resources at both the competent authority level for defining and at the operator level for utilizing a DBT in developing security measures. However, limited capability and limited resources should not constitute a reason for forgoing the use of a DBT. If the considerations mentioned above suggest that it is necessary to have the level of assurance associated with a DBT approach, the State may need to make the necessary resources and capabilities available.

Regardless of whether a DBT approach or another threat based approach to security is used, the competent authority should ensure that there is a threat related basis for the resulting protection. The competent authority should document the basis for its decision to use the DBT or another approach.

6. DEVELOPING A DESIGN BASIS THREAT

The methodology for developing a DBT involves using the threat assessment document and, through a process of screening and decision making, defining the DBT. This section describes in detail the process for developing a DBT.

6.1. INPUT TO THE DESIGN BASIS THREAT

The main input for the DBT is the threat assessment document. This document helps ensure that the resulting DBT will be realistic and credible. The consequences deemed by the State to be unacceptable need to be understood by the competent authority developing the DBT.

6.2. PROCESS

The process for the development of the DBT include further analysis and, most importantly, decision making. The analysis and decision making process has three major phases:

(1) Screening the threat assessment output for those threats with motivation, intention, and/or capability to commit a malicious act;
(2) Translating the resulting screened list into a statement of representative attributes and characteristics of the postulated adversary;
(3) Modifying the statement of representative threat attributes and characteristics on the basis of relevant policy considerations.

6.2.1. Phase 1: Screening the threat assessment

In this phase, the competent authority considers the possible targets of potential malicious actions that could lead to unacceptable consequences, and then compares these to the attributes and characteristics of the postulated adversaries as described in the threat assessment document.

There are two steps to Phase 1:

- *Step A: Review of capabilities.* The threats described in the threat assessment document are reviewed to determine whether or not they possess the capabilities necessary to commit a malicious act that could lead to unacceptable consequences. If the capabilities of the threat are not sufficient to cause these unacceptable consequences, then that threat is discarded from further consideration for the DBT. However, considerable caution needs to be exercised. A threat should not be excluded from further consideration on the basis that the existing physical protection is sufficient. The impact of any existing physical protection measures on the threat should be ignored.[10] Only threats of the lowest capabilities are likely to be excluded at this step of decision making. The remaining threats will be screened further in Step B.
- *Step B: Review of motivation and intentions.* The threats from Step A are considered with regard to their motivation and intentions. If the threat, in addition to having sufficient capabilities, is also believed to have sufficient

[10] This is because these measures might later be removed by an operator if the DBT does not include threat characteristics against which they would be effective and needed.

motivation (or actual intention) to commit the malicious act, then this threat is retained for further consideration in Phase 2 of the process. If neither motivation nor intent is present, the threat is a candidate for exclusion; however, care must be exercised when excluding a highly capable threat on the basis of perceived lack of motivation or actual intent. The competent authority should make this decision on the basis of whether or not the threat's perceived motivation is completely inconsistent with the consequences of concern, and also whether the degree of confidence in the data used to assess the threat's motivation and intent is sufficient to be able to exclude the threat.

Given the significance of the decision that will be made, it is important that the reasons for any exclusion are well documented.[11] The output from this phase is a modified threat assessment document that includes the range of credible threats that is capable and may be motivated or may have the intention to commit a malicious act leading to unacceptable consequences. Those threats removed as a result of the screening should still be considered for future review if new information is acquired at a later time.

6.2.2. Phase 2: Translating data on specific threats into representative adversary attributes and characteristics

The threats in the modified threat assessment document from Phase 1 should be reviewed with regard to their motivation, intentions, and capabilities. The threat descriptions from Phase 1 should be translated into a set of representative adversary characteristics that are representative of the specific ones. All the threat characteristics (i.e. motivation, intentions, and all the detailed capabilities including the number of adversaries) identified in the threat assessment process should be addressed.

The representative adversary characteristics should not simply represent a combination of the worst characteristics of each threat in the threat assessment as this may result in an unrealistic definition of adversaries. In fact, some of these threat characteristics may even be mutually incompatible. Instead, a measured approach should be taken, in which one or more credible adversary descriptions are developed that represent the range of characteristics from the threat assessment.

[11] Information on threats that are excluded may be sensitive, and should be properly protected.

The output of this effort is a concise but comprehensive definition of representative attributes and characteristics of the adversaries on the basis of which a protection system could be designed and evaluated.

6.2.3. Phase 3: Modifying representative adversary attributes and characteristics on the basis of policy factors

The representative adversary characteristics from Phase 2 should be assessed with regard to relevant policy factors that have been identified by the competent authority in conjunction with other State authorities. This may result in adjustments to the representative adversary characteristics developed from Phase 2 to enable levels of security to be made more sustainable. Furthermore, the benefits to society of continued operation of facilities should be balanced against the costs of protection and the risks of the consequences of a potential malicious act. The competent authority should consider policy factors while endeavouring to maintain a technical basis for the DBT as provided by the threat assessment.

In assessing the results of Phase 2, the following policy factors should be considered in the decision making process. They may lead to further modifications of the representative adversary characteristics, as follows:

- Degree of conservatism of the DBT:
  - Compensating for uncertainty and different interpretations in the data used in the baseline threat assessment;
  - Creating a robust DBT to permit physical protection that remains credible as the threat evolves with time;
  - Including characteristics of potential threats about which there is no current intelligence because it is prudent to do so;
- Cost–benefit–consequence tradeoffs:
  - Balancing the benefit to society of the asset, the consequences for society of successful malicious acts against the asset, and the costs to society of reducing the risks of such acts;
  - Implementing appropriate physical protection comparable with that for other assets and infrastructure of similar consequence severity, such as protection for explosives, chemicals, and biological agents;
- Political factors:
  - Impact of the decisions on public confidence;
  - Relative contribution to public welfare of the assets;
  - Confidence of neighbouring States in the protection;
  - Threat situations in neighbouring States.

When applied to the representative adversary attributes and characteristics, these factors could influence a change in the level of adversary capabilities. The impact of the degree of conservatism and political factors would likely result in an increase in these capabilities, whereas the cost–benefit tradeoffs would likely decrease them.

The resource implications of decisions for the DBT should be considered by the competent authority. Although concern about costs should not be allowed to result in an understatement of the threat, such considerations may have an impact on whether and how a particular threat is countered by the State or by the operators. It may require unsustainable resources to counter a DBT that includes an unrealistically high level of threat capabilities. For new facilities, a State may wish to consider the possible long term advantages of designing protection against a more conservative threat than the DBT, given the cost implications of upgrades added after the facility is in operation.

The competent authority, working with other State authorities, needs to decide what level of risk is acceptable and what level of threat it will protect against, given the availability of protection resources, the benefit of the asset to society, and other priorities. Risk, in this sense, is a combination of the severity of the consequences of a potential malicious act, and the likelihood that the malicious act will be successfully committed.

Prior to finalizing and using a DBT, the competent authority should coordinate its content with other relevant State authorities. The competent authority should seek comments from other affected parties but the final decision on the content of a DBT, and the responsibility for this content, should rest with the competent authority.

6.3. OUTPUT

The process of defining the DBT has two outcomes. The primary result is the DBT document.[12] The DBT is that set of attributes and characteristics of threats for which the State organizations and the operators have protection responsibilities and accountability. However, the second result will identify those threats that are not appropriate for inclusion in a DBT but against which the State requires that protection should be reasonably ensured. Such threats would be primarily countered by the State.

[12] A State may have more than one DBT, reflecting a graded approach or varying threats (see Section 2).

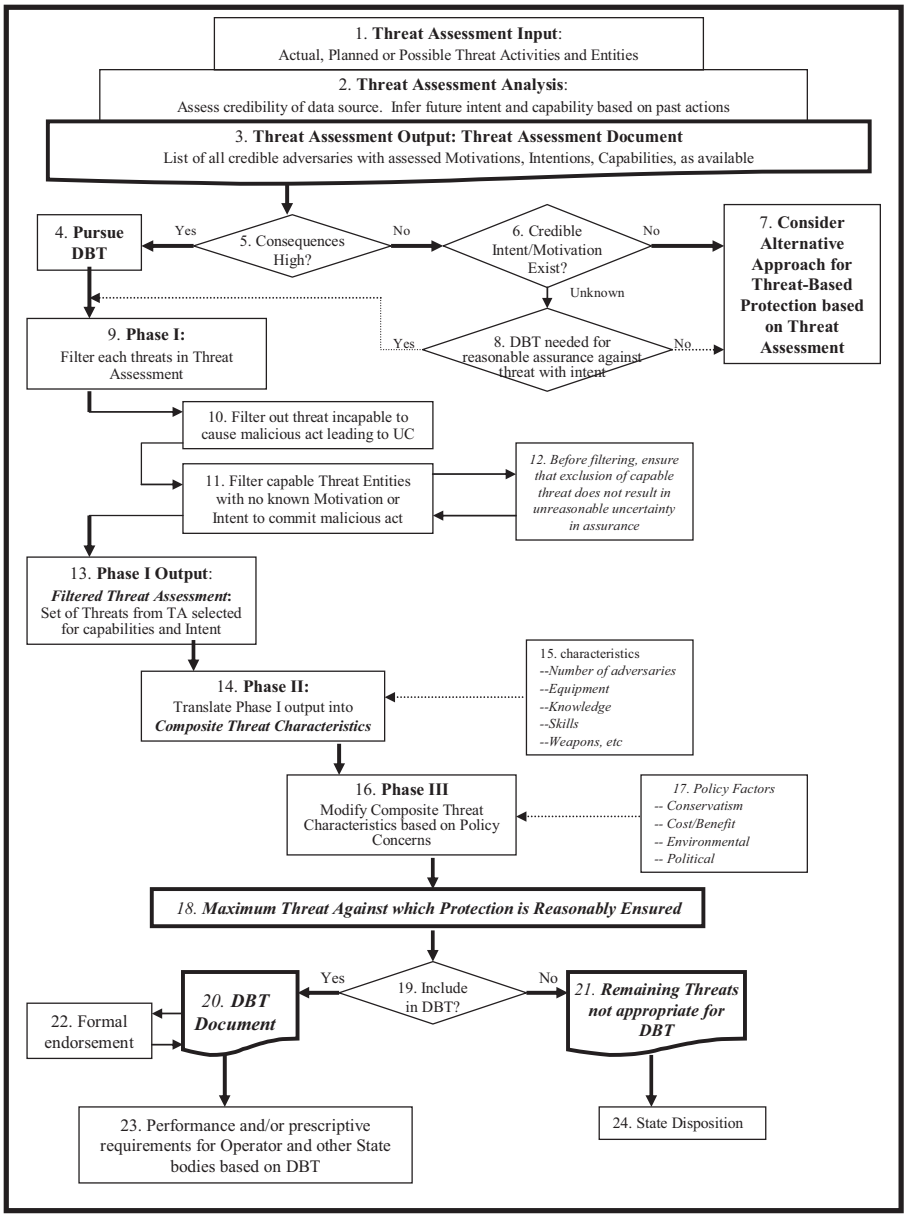


FIG. 3. Development of a DBT.

The flow chart in Fig. 3 represents the threat assessment process and development of the DBT as outlined in Sections 5 and 6.

6.4. DEVELOPING AN ALTERNATIVE THREAT STATEMENT

The alternative threat based approach considers many of the factors described in Sections 6.1–6.3 of this Implementing Guide, but in a less rigorous manner, and perhaps involving fewer organizations. Nevertheless, a formal process for developing an alternative threat based protection should be undertaken. It should:

— Identify the threats from the assessment which have motivations, intentions or capabilities that correspond to the assets to be protected.
— Assess the influence of the policy factors (Section 6) on the identified threat capabilities.
— Document these threat capabilities in a threat statement that will be used by the regulatory authority to define requirements for the design and evaluation of the physical protection system. These requirements for the operator are commonly prescriptive in nature.

These requirements should be developed with consideration of the capabilities of the threats in the threat statement, and with sufficient conservatism to achieve the desired assurance. This threat statement and the resulting protection requirements should be periodically reviewed to ensure that they continue to result in reasonable assurance of adequate protection. If it becomes clear that reasonable assurance cannot be achieved through this approach, the DBT approach should be reconsidered.

7. USING THE DESIGN BASIS THREAT

The use of the DBT by the regulatory authority should take into account the authorities and responsibilities of all the organizations involved, as established by the State's nuclear security regime. The division of responsibilities for physical protection between the regulatory authority, the operators and other State organizations varies from State to State, and use of the DBT will reflect this. In using the DBT the regulatory authority, in coordination with other State authorities, should consider relevant factors, including:

— Legal and regulatory constraints established by the national constitution, and/or laws on weapons, penal codes, or public order and security;

— Security responsibilities and competencies of other government entities, for example, military forces, police authorities, and other regulators;
— Operator competencies and resources, and the technical, cultural, and financial constraints on the operators' activities.

Using this knowledge the regulatory authority, in discussion with other national State authorities, should identify the responsibilities of the operators, and should ensure that all national authorities involved understand their roles, functions and responsibilities with regard to physical protection against the DBT.

The State ensures that sharing responsibilities for protection among different entities does not compromise the comprehensiveness of the protection and that the respective contributions to protection are effectively integrated. The regulatory authority could assist the State in this.

The DBT, or some parts of it, should be distributed to those who need it, and who are authorized to receive it. The need for the information contained in the DBT needs to be balanced with the need to protect sensitive intelligence information, and the conclusions drawn from it. To help achieve this balance, the competent authority responsible for dissemination of the DBT should consider distributing the DBT to those groups that:

— Need to know the DBT (either the entire DBT, or some part thereof) in order to fulfil their responsibilities with regard to physical protection. This will include operators, State responders, and public security authorities.
— Have participated in the DBT development process in order to advise on necessary updates but are not themselves charged with providing protection.

It may be helpful to develop a version of the DBT that is less sensitive in terms of classified information so that it can be more readily distributed to, and used by, entities that would not normally be required to protect classified information. Any dissemination of the DBT should be made in accordance with the State's constitutional, legislative, regulatory and organizational framework.

A State's regulatory framework is likely to determine whether a DBT is: (1) incorporated into a legally binding instrument; or (2) put into effect through an administrative act, such as a directive or an instruction. If a DBT is explicitly part of the regulatory framework, and if thereby it has a legal status, the regulatory authority should ensure that the DBT document and the physical protection requirements that derive from it are consistent with other legal requirements.

A State could use several different approaches to formalizing the use of a DBT by the operator(s), including the following:

(a) The regulatory authority provides the DBT to the operator together with a general requirement to protect against specified characteristics of the adversary; the operator is required to interpret the DBT and to design and implement an effective physical protection system.
(b) The regulatory authority establishes performance requirements for physical protection systems that are effective against the DBT; the operator is required to design and implement a physical protection system that satisfies these performance requirements.
(c) The regulatory authority specifies prescriptive protection measures based on the DBT; the operator is required to comply with those prescriptive requirements.

The criteria for the selection of a performance based approach ((a) and (b)) or a prescriptive approach (c) will depend on the State's legislative framework and organizational structure and several other factors such as:

— The competence of the operator to interpret performance requirements and to design, implement, and evaluate an effective physical protection system;
— The number of facilities and operators that will be governed by the regulation, and the extent to which prescriptive requirements limit the flexibility of the operator to develop appropriate protective measures;
— The severity of the potential consequences of the malicious acts that are to be prevented.

The incorporation of a DBT into the regulatory framework will permit management of the risks of a malicious act by developing appropriate security measures and systems. It should be followed by an evaluation of the existing physical protection systems by the regulatory authority to ensure that they are effective against the DBT. To make such an assessment, a DBT is used as the basis for:

— Developing potential adversary scenarios for committing malicious acts;
— Conducting performance analyses of the physical protection system to determine its effectiveness and to assess its possible degradation against the potential adversary;
— Identifying any vulnerabilities of the physical protection system;

— Improving the system (if necessary), analysing and prioritizing upgrade options for effectiveness and assessing the associated cost–benefit tradeoffs.

The design and evaluation of physical protection is outside the scope of this Implementing Guide. However, the use of threat based design criteria such as the DBT encourages a strategic approach to physical protection. It is important that the regulatory authority adopt well documented, systematic methods for evaluating the operator proposals for physical protection and emergency preparedness and response plans and for any proposed changes. Such methods are likely to include assessing the operator's efforts to develop detailed adversary scenarios on the basis of the DBT, to identify vital areas, develop strategies for physical protection, and to create a security culture.

8. MAINTAINING THE DESIGN BASIS THREAT

8.1. INPUT

A formal review process should be established to maintain the validity of a DBT. The review process should include a continuing assessment of the existing threat environment. The process should also include an assessment of quickly evolving threats that have to be dealt with urgently. In such circumstances, it may be necessary to take additional security measures before the DBT has been formally reviewed. The manner in which emerging threats are addressed will vary from State to State.

While organizing a DBT review is primarily the responsibility of the competent authority, the process should be undertaken in conjunction with other State authorities. The competent authority should decide what period of time is appropriate for regular, formal reviews of the DBT. This period will depend on factors such as the State's legislation and regulation with regard to physical protection, the stability of the threat environment, the conservatism built into the DBT, and the available resources. A review will not necessarily result in a revision of the DBT.

A number of events may trigger consideration for a review of the DBT that are outside the periodic review process. The competent authority should decide what trigger conditions or events are appropriate. These trigger events may include:

— An event or act, internal or external to the State, that significantly changes the perception of, or the actual level of, the threat.
— Significant changes in government policy, law, or international arrangements that affect the responsibility of the State authorities or the operator. Examples include changes involving the use of deadly force, response arrangements, or organizational responsibilities.
— Changes in activities related to nuclear material that introduce new potential consequences. Examples include construction of a different type of facility, use of material of higher enrichment, or a new type of operation.
— A proposal for review by an interested party.

8.2. PROCESS

When the competent authority has determined that a review (and possibly a revision) of the DBT is necessary, it should undertake the same process as that used to define the original DBT, starting with the threat assessment. The competent authority would be responsible for leading and coordinating the review and revision process.

The same organizations that were involved in the development of the DBT need to be involved by the competent authority in the review process and also any other organizations identified as having relevant information or being likely to be affected.

8.3. OUTPUT

The review will decide whether or not it is necessary to revise the existing DBT and reissue it. If an update is required, the analysis and decision making process will be the same as the process used in the development of the DBT. However, the competent authority will also take into consideration lessons learned in relation to the use of the DBT, specifically with regard to integration between different organizations.

The update of the DBT should be followed by an assessment of the adequacy of the existing physical protection system with regard to the new DBT and appropriate measures should be taken as required.

REFERENCES

[1] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev. 4 (corrected), IAEA, Vienna (1999).

[2] The Physical Protection Objectives and Fundamental Principles (GOV/2001/41/Attachment), IAEA, Vienna (2001).

[3] Convention on the Physical Protection of Nuclear Material, INFCIRC/274, and the Amendment of 2005 thereto, IAEA, Vienna (2005).

GLOSSARY

operator. Any organization or person applying for authorization or authorized and/or responsible for nuclear, radiation, radioactive waste or transport security when undertaking activities or in relation to any nuclear facilities or sources of ionizing radiation. This includes, inter alia, private individuals, governmental bodies, consignors or carriers, licensees, hospitals, self-employed persons, etc. (see the IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection — 2007 Edition).

sabotage. Any deliberate act directed against a nuclear or radiological facility or nuclear or radioactive material in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances (Convention on the Physical Protection of Nuclear Material and Nuclear Facilities).

threat. An entity with motivation, intention and capability to commit a malicious act (developed after extensive consultation in Member States[13]).

threat assessment. An evaluation of the existing threats, usually including intelligence assessments, which describe the motivation, intentions, and capabilities of these threats to commit malicious acts (developed after extensive consultation in Member States[14]).

threat statement. A document that summarizes the threat assessment and has been modified to account for policy considerations. The DBT is an example of a threat statement (developed after extensive consultation in Member States[15]).

unacceptable consequence. A threshold of consequence that a State decides is so severe as to justify that resources be expended to prevent its occurrence. The resources are expended by those organizations responsible for providing the protection (developed after extensive consultation in Member States[16]).

---

[13] Needed for clarity as this is a security term.
[14] Needed for clarity as this is a security term.
[15] Needed for clarity as this is a security term.
[16] Needed for clarity to differentiate from quantified criteria.

This publication provides guidance on how to develop, use and maintain a design basis threat (DBT). It is intended for decision makers with roles and responsibilities for the development, use and maintenance of the DBT. This guide describes a DBT; identifies and recommends the roles and responsibilities of organizations that should be involved in the development, use and maintenance of a DBT; describes how to conduct a national threat assessment as a precursor to a DBT; explains how a DBT can be developed; explains how a DBT is incorporated into a State's nuclear security regime; and explains the conditions for a review of the DBT, and how the review and update are conducted.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102509–8
ISSN 1816–9317