International Journal of Nuclear Security

Volume 9
Number 2 *ICEP 2022 Conference Papers*

Article 6

5-2024

Threat Modeling Based on a Design Basis Threat for Nuclear Security

Abu Zafor Mohammad Salahuddin
Military Institute of Science and Technology, Bangladesh

Altab Hossain
Bangladesh Military Academy

Mohammad Shawkat Akbar
Nuclear Power Plant Company Bangladesh Limited

Recommended Citation

Salahuddin, Abu Zafor Mohammad; Hossain, Altab; and Akbar, Mohammad Shawkat (2024) "Threat Modeling Based on a Design Basis Threat for Nuclear Security," *International Journal of Nuclear Security*: Vol. 9: No. 2, Article 6.
http://doi.org/10.7290/ijns09449466
Available at: https://trace.tennessee.edu/ijns/vol9/iss2/6

International Journal of Nuclear Security, Vol. 9, No. 2, 2024—ICEP 2022 Conference Papers

Threat Modeling Based on a Design Basis Threat for Nuclear Security

Abu Zafor Mohammad Salahuddin,[1] Altab Hossain,[2,*] and Mohammad Shawkat Akbar[3]

[1]Department of Nuclear Science and Engineering, Military Institute of Science and Technology, Dhaka-1216, Bangladesh
[2]Department of Mechanical Engineering, Engineering Faculty, Bangladesh Military Academy, Chattogram-4315, Bangladesh
[3]Nuclear Power Plant Company Bangladesh Limited, Bangladesh
[*]Corresponding author email: altab76@gmail.com; altab@nse.mist.ac.bd

Abstract

Identification of the design basis threat (DBT) of a nuclear facility is an important factor of overall safety, for which the operator is mainly responsible per the guidelines of the International Atomic Energy Agency. As threat levels increase especially threats beyond the DBT-the responsibility of the state also increases. In recent years, only a few studies on nuclear security and DBTs have comprehensively detailed the full spectrum of nuclear facilities in a nation. Thus, this paper presents the correlation between an actual threat and the DBT. The objectives of the study are to assist in establishing physical protection system (PPS) standards that present risks to a nuclear facility, and to determine the level of protection. According to current threat patterns, 34 types of possible and perceivable threat events were identified for DBT in this study. A threat matrix was developed after compiling the assessed threat grades, and this matrix can be a design basis for developing a PPS for any nuclear facility and its security. The DBT study revealed that based on threat variables, each threat in the matrix has a translated representation of threat grades of high, medium, or low. To achieve precision using the deterministic approach, a new seven-step sliding scale for nuclear security events was created, ranging from 0 to 100. The identified threat levels are very low (1–10), low (11–30), moderate (31–50), high (51–60), very high (61–70), severe (71–90), and extreme (91–100). In conclusion, this study revealed that rigorous analysis and decision-making are essential to transforming the threat assessment for the DBT.

DOI:

Keywords: Design basis threat; nuclear security; threat matrix; risks; threat assessment

1. Introduction

Nuclear material (NM) is widely used in many industries, including medicine, agriculture, and scientific research. However, NM is also extremely volatile and has the capacity to be exploited by malicious individuals to trigger nuclear catastrophe and other antistate objectives. Because of this threat, NM is a highly controlled substance, secured by the International Atomic Energy Agency (IAEA) through a structured framework of nuclear security and structured procedures such as the physical protection system (PPS). The PPS is established by the design basis threat (DBT) of the nuclear installation (NI) handling the NM. The DBT is the appreciated *threat basis* for the NM and NI, and it provides comprehensive threat models.

Practically, the threat to an NI varies based on multiple factors that are associated with geopolitical, technical, economic, and cultural conditions specific to the region of the NI. Because all security events are not equally applicable to any nuclear installation in terms of effects, the DBTs and threat models of each installation differ widely. Identifying the applicable threats to an NI is considered a prerequisite for threat modeling through the DBT. Most operators develop the PPS for the NI based on a single DBT to fulfil the compliance requirements of the IAEA. As an international regulatory body, the IAEA recommends having more than one DBT for PPS development [1].

Limited research has been conducted on the development process of a DBT and threat modeling to an NI. Thus, the purpose of this study was to investigate the applicable threat models through DBT development that would serve as a standard for the PPS development of NI. MATLAB software was used for three assessment templates based on three different perspectives: threat, vulnerability, and consequence.

2. Threats to Nuclear Security

a. Current Risk Configuration

An NI poses adverse conditions for extremism on a global scale [2–3], rendering terrorists increasingly vulnerable. In the twenty-first century, the September 11, 2001, attack at the World Trade Center, and related terrorist acts have highlighted the imbalance in existing threat assessments. These dynamic threats require sophisticated skills pertinent to both nonstate military and nonstate violent actors.

b. Threat Identification

In the process of identifying nuclear threats, it is important for the state to collect information from as many credible sources as possible, including national intelligence and state, regional, and local sources. The PPS should be based on a regularly updated evaluation of the credible threat to nonstate military and nonstate violent actors, reflecting the capabilities and intentions of potential adversaries. This basis is commonly known as the *threat assessment*. For designing a PPS, two types of threats need to be considered: military and nonmilitary threats. Military threats are posed by the trained military during a conventional war environment and are treated as *beyond DBT* events, requiring a separate threat assessment and force structure. Nonmilitary threats are posed by mainly adversaries, terrorists, lone-offenders, or related actors in the peacetime environment for malicious activities and are included in the DBT. The lists of applicable threats considered by different countries in the DBT for any NI [4–5] are presented in Table 1.

Table 1. List of applicable threats for an NI.

Ser	Threat	Ser	Threat	Ser	Threat
1	Aircraft as a weapon	13	CBR release—water supply	25	Subsurface threat
2	Aerial reconnaissance	14	Civil disturbance	26	Release of on-site hazardous materials
3	Arson (deliberate fire)	15	Coordinated or sequential attack	27	Robbery
4	Assault	16	Disruption of building and security system	28	Theft
5	Ballistic attack—active shooter	17	Explosive device—mailed or delivered	29	Unauthorized entry—forced
6	Ballistic attack—small arms	18	Explosive device—man-portable external	30	Unauthorized entry—surreptitious
7	Ballistic attack—standoff weapons	19	Explosive device—man-portable internal	31	Unmanned aerial vehicle
8	Breach of access control point—covert	20	Explosive device—suicide/ homicide bomber	32	Vandalism
9	Breach of access control point—overt	21	Explosive device—VBIED	33	Vehicle ramming
10	CBR release—external	22	Hostile surveillance	34	Workplace violence
11	CBR release—internal	23	Insider threat (smuggling/information sharing)	35	Reserved for military threats
12	CBR release—mailed or delivered	24	Kidnapping	36	Reserved for military threats
CBR: chemical, biological, and radiological; VBIED: Vehicle-borne improvised explosive devices					

3. DBT and Threat Modeling

a. IAEA Guidelines and Correlation of the DBT

The DBT refers to an adversary's profile, encompassing their type, composition, capabilities, motivations, and methods (i.e., tactics, techniques, and procedures) further forming the basis for the security and operations of a facility. It describes the attributes and characteristics of potential insider and outsider adversaries who might attempt a malicious act—unauthorized removal or sabotage against which the PPS for the NM and NI is designed and evaluated [5–6]. DBT has strong correlations with the following:

- Threat: Intention and capability of an adversary to initiate an undesirable event
- Vulnerability: A weakness in the design or operation of a facility

- Consequence: The level, duration, and nature of the loss resulting from an event
- Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence

The DBT should be in accordance with the state's ongoing threat assessment, which derives from the threat assessment process. Defining the DBT involves adjusting the threats outlined in the state's threat assessment to reflect current technical, economic, and political issues, as well as PPS requirements. Transforming the threat assessment into a DBT requires comprehensive analysis and decision-making. However, the main objective of the DBT is to ensure that the developed PPS is suitable and effective for any NI [1]. Thus, it has three intents:

- To assist in establishing PPS standards
- To support the calculation of the threat, vulnerability, and consequence of the facility when calculating risk to said facility and determining necessary levels of protection
- To determine performance standards and countermeasures necessary to overcome specific adversary characteristics

b. Responsibility of DBT

Following IAEA guidelines and practices of different states, the operator is responsible for determining threats for the DBT. As threat levels increase, the state's responsibility also increases. Threats beyond the DBT are the responsibility of the state. The threat assessment conducted by the state leads to a DBT, which determines the performance needed from the PPS of the NI and provides a basis to assess changes in threat levels. The elements of threat are motivation, intention, number, and the capacity of adversaries in terms of equipment, weapons, method of attack, knowledge of facilities, insider cooperation, training, funding, and more.

c. DBT Development Methodology

A comprehensive threat assessment can be used to determine the potential threat level of an event by examining various threat factors of actual security incidents. These variable threat factors include the datum-level threat, target merit, and threat merit. Once a threat assessment is compiled, the report evaluates threat grades of threat variables for all 34 types of threat events, further yielding a threat matrix that can operate as a standard design basis in developing the PPS for an NI. The DBT delivers a basis for system design and a reliable standard for evaluating the suitability of the PPS. In the DBT report, individual threat analysis is used for developing PPS criteria, establishing an outline of type, composition, and capabilities of adversaries.

d. Threat Modeling through DBT

Threat Assessment Technique: DBT Perspective

When performing a threat assessment, it is essential to analyze each undesirable event by considering parameters such as threat definition, threat scenario, datum-level threat,

threat analytics, target merit, and threat merit. Threat definition is used for mutual understanding of the threat, whereas the threat scenario provides specific characteristics of the threat event, such as numbers of adversaries, sizes, speeds, tactics, and more. Similarly, a datum-level threat is an estimate of the relative threat posed to national facilities such as nuclear power plants. The analytical basis of the threat scenario, datum-level threat, target merit, and threat merit are normally predicated based on examples of threat events. Target merit describes the appeal of a target in terms of the likelihood of a threat event, and it is a more accurate and facility-specific threat determination that may modify the datum-level threat.

Threat merit evaluates potential future threat levels that may differ from the current threat rating. To compensate for this information, threat merit is used in the threat assessment report. Because datum-level threat, target merit, and threat merit are variable, the respective ratings may be noted as VL (very low), L (low), M (medium), H (high), or VH (very high), used according to the severity and impact of the actual safety incident [6–7]. Outlined in Table 2, a comprehensive threat assessment has been formulated.

Table 2. Threat assessment template.

Threat Event	<Name of threat>				
Threat Definition	<Mention common understanding of threat>				
Threat Nos.	<Number the threat>	Original Assessment	<Date of assessment >	Revision	<Mention last revision nos.>
Threat Scenario					
<Mention specific characteristics of threat event, such as numbers of adversaries, sizes, speeds, tactics, etc.>					
Datum-Level Threat					Threat Grade
<Mention estimate of baseline or relative threat posed to NIs such as nuclear power plants. Ratings may include VL, L, M, H, or VH.>					<Assessed Grade>
Threat Analytics					
<Mention examples of threat event from national and international sources, intelligence report, criminal history record>					
Target Merit					Threat Grade
<Mention attractiveness of an *NI* as a target for likelihood of threat event under assessment>					<Mention assessed threat grade>
Threat Merit					Threat Grade
<Assess threat level in future that might be changed from present threat rating based on datum-level threat, threat analytics, and target merit through wisdom and prediction>					<Mention assessed threat grade>
References					
<Mention references of undesirable/threat events>					

DBT Development from Threat Assessment

A threat assessment is a facility-based threat evaluation used to determine the threat merit of every threat event based on the facility value or merit indicating a reasonably appreciated threat level to an NI in terms of a threat grade. Such a threat grade is dependent on two variable threat factors—the datum-level threat, which describes the baseline threat of the threat event, and target merit, which describes the attractiveness of the target such as an NI for a specific threat event. As presented in Table 3, a threat matrix can be developed after compiling the assessed threat grades of two threat variables. The threat matrix can be a good design basis for a DBT and developing the PPS for an NI.

Table 3. DBT for NI from threat perspective.

Ser	Undesirable Events	Datum-Level Threat	Target Merit	Threat Merit (DBT)
1	Aircraft as weapon	Very low	Very low	Low
2	Aerial reconnaissance	High	High	High
…	…	…	…	…
…	…	…	…	…
33	Vehicle ramming	Low	Low	Low
34	Workplace violence	Low	Low	Moderate

Vulnerability Assessment Technique

The vulnerability assessment technique considers four major factors—motivation, intention, capabilities, and policy—with each factor using its own attribute to reflect the level of vulnerability cumulatively. The level of vulnerability can be assessed on a sliding scale, which can be conducted from either an internal or external perspective, comprising global and domestic threat sources. As displayed in Table 4, a new vulnerability assessment, which includes the boundary conditions, factors, and attributes, has been created.

Table 4. Vulnerability assessment template.

Threat Event	Aircraft as Weapon		Threat Grade		Low
Source Type	Outsider		Insider		Attribute Level
	Global	Domestic	Global	Domestic	
Motivations					
Intentions					
Capabilities					
Policy Factor/Likelihood					

DBT Development from Vulnerability Assessment

The vulnerability assessment is a capability-based threat evaluation. Its purpose is to determine the threat merit of every threat event based on overall capability of the self and adversary, indicating a reasonably appreciated threat level to an NI in terms of the threat grade. Table 5 depicts how a vulnerability matrix can be developed through compiling the assessed vulnerability grades of threat attributes. This vulnerability matrix is a good DBT for developing the PPS for an NI.

Table 5. DBT for NI from the vulnerability perspective.

Ser	Undesirable Events	Motivation	Intention	Capability	Policy	DBT
1	Aircraft as weapon	Very low	Very low	Low	Low	Low
2	Aerial reconnaissance	High	High	High	High	High
…	…	…	…	…	…	…
…	…	…	…	…	…	…
33	Vehicle ramming	Low	Low	Low	Low	Low
34	Workplace violence	Low	Low	Moderate	Moderate	Moderate

Consequence Assessment Technique

The consequence assessment technique takes nine major factors and considers asset damage, loss of life, injury, loss of primary service, loss of core process, loss of core function, loss of secondary service, loss of subsidiary process, and loss of subsidiary function. Each factor has its own attribute to reflect the level of consequence and effect cumulatively [8–9]. The level of consequence and effect can be assessed on a sliding scale. Similar to the vulnerability assessment technique, this consequence assessment can be conducted from both an internal and external perspective.

DBT Development from Consequence Assessment

The consequence assessment involves evaluating threats based on their effects. Its objective is to determine the significance of each threat event by assessing overall effects, indicating a reasonably perceived level of consequence to an NI in the form of a consequence grade. Thus, a consequence matrix (Table 6) can be developed by consolidating the evaluated consequence grades of the attributes. This consequence matrix can be a good design basis or DBT for developing the PPS for an NI.

Table 6. DBT for NI from the consequence perspective.

Ser	Undesirable Events	Asset Damage	Life Loss	Injured	Primary Service Loss	Core Process Loss	Core Fun Loss	Secy Service Loss	Sub Process Loss	Sub Fun Loss	DBT
1	Aircraft as weapon	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
2	Aerial reconnaissance	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
33	Vehicle ramming	L	L	L	L	L	L	L	L	L	L
34	Workplace violence	VL	M	M	M	M	M	M	M	M	M

4. Quantified Threat Modeling

The threat grade is reasonably enumerated in terms of competence, commitment, and objectives regarding the facilities [10–11]. Quantified threat modeling serves as an efficient interface between threats and security measures, which can be integrated into the final phase of developing another PPS validation program to assess its efficacy. The effectiveness of the PPS can also be reaffirmed through the use of alternative physical methods, including conducting real-time or tabletop exercises, along with other approaches that are employed to ensure its continuous validation.

a. Quantification Scale

The threat, vulnerability, and consequence assessments are dependent on variable factors. All attributes and factors have their own individual merit that collectively reflects the true level of threat, vulnerability, and consequence of each factor. Moreover, given the absence of historical data on security events, the degree of consequence, vulnerability, and threat associated with these security events can be quantified on a five-step sliding scale out of 100 points. The following steps are very low (1–20), low (21–30), medium (31–60), high (61–80), and very high (81–100). To attain accuracy using the deterministic approach, a new seven-step sliding scale can be quantified ranging from 0 to 100. All factors of the threat, vulnerability assessment, and DBT may be rated using this measurement scale, reflecting the quantified level of severity, effect, and consequence as appropriate to variables.

DOI:

b. Quantified Risk from Quantified DBT

From the assessment techniques outlined in this paper, three quantified DBTs (Q-DBTs) have been examined from three different perspectives—threat, vulnerability, and consequence. All Q-DBTs are based on expert opinion and dependent on historic data, credible sources, and experience through threadbare analysis. The Q-DBT from threat is more generic, whereas the Q-DBTs from vulnerability and consequence are more precise because of the analysis of adversary and target specifics. Quantified risk (Q-Risk) can be obtained by mathematical manipulation of the Q-DBT**.** Here, Q-Risk is an aggregated average of factors such as capability, likelihood, and effect, where the likelihood is a summarized average of motivation and intention of the adversary as well as policy. Factors of the NI represent regulatory strength and weakness [12–13].

5. Conclusion

An NI is classified as a *special infrastructure* that requires a special threat assessment technique to identify the possible and perceivable threats. Because of this classification, a comprehensive threat assessment template was developed. Drawing from the current threat pattern, a comprehensive analysis using the new assessment template has led to the identification and consolidation of plausible threats. After compiling the assessed threat grades of threat variables, the DBT was developed from the threat perspective, which is the threat model for a particular NI. Similarly, the vulnerability of the NI was assessed by considering four major factors and attributes—motivation, intention, capabilities, and policy factors. Considering these factors, a new vulnerability assessment template was developed. Using this template, the DBT was established through consolidating the assessed vulnerability grades of attributes to form a specific threat model to the NI from a vulnerability perspective. The consequence assessment of the NI was accomplished by considering nine major factors and attributes—asset damage, loss of life, injury, loss of primary service, loss of core process, loss of core function, loss of secondary service, loss of subsidiary process, and loss of subsidiary function. Thus, a new consequence assessment template was devised. According to the template, the DBT was formulated after consolidating the evaluated consequence grades of attributes, representing another threat model that is specific to the NI from a consequence perspective.

For quantification purposes, a deterministic approach was adopted, eschewing the probabilistic approach. All the variables and factors of the threat, vulnerability assessment, and DBT may be rated in this type of measurement scale, reflecting the quantified level of severity, effect, and consequence as appropriate to the type of variables.

6. References

1. International Atomic Energy Agency. *Development Use and Maintenance of the Design Basis Threat*; Nuclear Security Series No. 10; International Atomic Energy Agency: Vienna, 2009. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf (accessed 2024-02-11).
2. International Atomic Energy Agency. *Preventive and Protective Measures against Insider Threats*; Nuclear Security Series No. 8; International Atomic

Energy Agency: Vienna, 2008. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1359_web.pdf (accessed 2024-02-11).

3. Salahuddin, A. Z. M.; Hossain, A.; Akbar, M. S. An Analysis on Threat Security Interfacing and National Preparedness on Effective Security System for Nuclear Materials and Nuclear Facilities in Bangladesh. *International Journal of Applied Security Research*, **2018**, *13* (2), 199–208. DOI: 10.1080/19361610.2018.1422363.
4. US Department of Homeland Security. *The Design Basis Threat*; US Department of Homeland Security: Washington, DC, April 2010; pp. 7–7.31.3. https://info.publicintelligence.net/DHS-DesignBasisThreat.pdf
5. Säteilyturvakeskus Strålsäkerhetscentralen Radiation and Nuclear Safety Authority. *Design Basis Threat for Use of Nuclear Energy and Use of Radiation*; 1/Y42217/2020; Nuclear Safety Authority: Finland, 2020. https://www.stuklex.fi/en/DBT_2020en.pdf (accessed 2024-02-11).
6. Salahuddin, A. Z. M.; Hossain, A.; Akbar, M. S. Threat Modeling on Nuclear and Radioactive Materials Based on Intelligent Approach. *International Journal of Nuclear Energy Science and Technology*, **2018**, *12* (1), 199–207. DOI: 10.1504/IJNEST.2018.10013860.
7. International Atomic Energy Agency. *Nuclear Security Glossary;* Nuclear Security Series No. 1; International Atomic Energy Agency: Vienna, 2015. https://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf (accessed 2024-02-11).
8. Norman, T. L. *Risk Analysis and Security Countermeasure Selection*; CRC Press: New York, 2013, 101–160.
9. Biringer, B. E.; Matalucci, R. V.; O'Connor, S. L. *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*, 1st ed.; John Wiley and Sons, Inc.: New Jersey, 2007, 75–81.
10. US Department of Homeland Security. *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*; Cybersecurity and Infrastructure Security Agency: Washington, DC, 2010. https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf (accessed 2024-02-11).
11. Baker, A. B.; et al. *A Scalable Systems Approach for Critical Infrastructure Security*; SAN2002-087; Sandia National Laboratories: Albuquerque, New Mexico, April 2002; 12–43.
12. Kang, Y. *Development of Physical Protection Vulnerability Assessment Tool TESS*; International Conference on Physical Protection of Nuclear Material and Nuclear Facilities; CN 254 92; International Atomic Energy Agency: Vienna, 2017, 661–671.
13. Jang, S. S.; Kwan, S. W.; Yoo, H. S.; Kim, J. S.; Yoon, W. K. The Vulnerability Assessment Code of a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE). *Journal of Nuclear Engineering and Technology*, **2009**, *41* (5), 747–752. DOI: 10.5516/NET.2009.41.5.747.