A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

2023 Electricity Sector Design Basis Threat

Physical Security Advisory Group

Rev. August 2023

TLP:GREEN

RELIABILITY | RESILIENCE | SECURITY




1401 H Street NW
Suite 410
Washington, DC 20005
202-790-6000 | www.eisac.com

Table of Contents

Design Basis Threat

The Electricity Information Sharing and Analysis Center's (E-ISAC) Physical Security Advisory Group (PSAG) developed this reference document to provide instruction on using a design basis threat (DBT) for the protection of the physical infrastructure of the bulk power system (BPS) to prevent instability, uncontrolled separation, or cascading within an interconnection.

This document's intended use is assessing physical electrical infrastructure based on current reasonable and credible threat considerations. It is not intended to cover all facility-specific threats and assets for consideration (e.g. safety of personnel, workplace violence, and exposure to dangerous chemicals, etc.). Owners/operators of individual facilities may need to apply protection measures separate or beyond those contained in this DBT to cover all the hazards and threats identified in asset owner/operator assessments.

The PSAG will continue to monitor and address threats as necessary in the annual review of the DBT. To assist Asset Owners and Operators in using the DBT to mitigate vulnerabilities to their facilities, the PSAG requested the U.S. Department of Energy (DOE), Office of Infrastructure Security and Energy Reliability to develop an implementation guide. As part of their commitment and support to the PSAG, DOE's Pacific Northwest National Laboratory (PNNL) created a guide that provides one possible approach for companies or utilities to use in assessing vulnerabilities of their physical protection systems (PPS) and their response to threats at their facilities. The guide uses the Vulnerability of Integrated Security Analysis (VISA) process to show vulnerability assessment practitioners how to implement a DBT. The VISA methodology looks at the functions of detection, assessment, delay, and response against a given threat, to determine the overall system effectiveness of a physical security system and to evaluate cost-effective upgrades. The VISA Implementation Guide can be found on the E-ISAC Portal. In addition, the E-ISAC and the PSAG provide no-charge, train-the-trainer workshops to utilities that want to host training at their sites. These workshops teach participants how to apply the DBT and VISA to real-world facilities. For more information contact physicalsecurity@eisac.com.

Notice of Modifications

This document is the August 2023 revision of the *Electricity Sector Design Basis Threat*, published by the E-ISAC in coordination with the PSAG as an update to the original DBT published on February 25, 2016. The 2023 update includes additional resource information on the Vulnerability of Integrated Security Analysis Implementation Guide, additional clarification of insider threat definitions, guidance for determining asset protection levels and how to use them with the DBT, as well as providing some additional style revisions. The August revision reflects an updated reference under Chapter 2 related to explosives, which was modified from the May 2023 version.

Chapter 1: Definitions

1.1 Design Basis Threat (DBT)

The threat against which an asset must be protected and upon which the protection system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT includes the tactics that aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics.[1] Furthermore, 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.[2]

1.2 Asset Protection Level (APL)

Owner/operators will determine the appropriate threat and protection level for their BPS assets through their own system analysis. After a thorough system analysis, owner/operators should assign each site with an Asset Protection Level (APL) corresponding to the facility's operational criticality to the grid. In the context of this DBT, APL 1 (High) sites would be critical to the operation of the BPS, APL 2 (Medium) sites would be important to the operation of the BPS, and APL 3 (Low) sites would be the least important to the operation of the BPS. One way of doing this analysis would be to assess the maximum tolerable downtime for the site if it were destroyed or taken out of service for an extended period.

When customizing a DBT for their own use, an Owner/operator may choose whatever criticality criteria they wish for each protection level.

Once the downtime analysis is complete and APLs assigned, those levels are linked to the corresponding threat levels outlined in Chapter 2. As described in the VISA Implementation Guide, "the [analysis] team must only use the level of threat that applies to the corresponding APL. Once the team designates the level of the threat, the [analysis] team must stay within that threat." For sites designated APL 1 (High), the High Threat description described in 2.1 should be used. For sites designated APL 2 (Medium), the Moderate Threat described in 2.2 should be used. For sites designated APL 3 (Low), the Low Threat described in 2.3 should be used. Once the APL and the threat level are aligned the physical security system can be evaluated based on scenarios derived from the threat described in the appropriate section. A key concept is that the analysis team can only use the capabilities within that specific threat statement when developing scenarios and determine system effectiveness, nothing more. This allows for reasonable and credible assessment of security systems and upgrades while bounding the upper limits of a realistic threat.

1.2 Outsider

The term "outsider" refers to a person who does not have unescorted access to a facility. An outsider may have the intent to engage in theft, damage, or destruction of critical equipment or infrastructure with or without general industry knowledge. Other actions to be considered are kidnapping, threats and/or violence against personnel, a standoff attack against a facility, and cyber-enabled attacks.

1.3 Insider

The term "insider" refers to a current or former employee, contractor, or business partner who has or has had authorized access to an organization's network, system, data, or facilities. An insider may circumvent or abuse authorized access in a manner that negatively affects the confidentiality, integrity, or availability of an organization's information or its information systems, the operation of the BPS, the safety of employees or the security of assets. Insiders are often privy to information that would be difficult or impossible for an outsider to

[1] JP 1-02. SOURCE: JP 3-07.2 *Department of Defense Dictionary of Military and Associated Terms*

[2] International Atomic Energy Agency DBT Terminology

obtain. This can include custom implementations of security or operating systems, idiosyncrasies in personnel or procedures, pattern of life information, equipment malfunctions, or other uncorrected vulnerabilities.

An insider may circumvent or use access in a manner that negatively affects the confidentiality, integrity, or availability of an organization's information or information systems, the operation of the BPS, the safety of employees, or the security of assets.

- Passive Insider: A passive insider may pass information to an outside adversary group to assist in accomplishing its goal, whether through malicious intent or unintentionally. This information can come in the form of intellectual property, blueprints, operational knowledge, documents, security procedures, and physical protection system knowledge. The passive insider does not participate in any other way.
- Active Nonviolent Insider: An active nonviolent insider can act either alone or together with outside adversaries. This insider can provide information like the passive insider and also use authorized access and authority, in addition to stealth and deceit. Active nonviolent insiders may also conduct disruptive actions, such as IT sabotage (e.g. manipulating security networks and other control systems), insider fraud and/or espionage. Nonviolent disruptive actions may also include limited physical damage (such as damaging computer equipment or cutting fiber optic cables).
- Active Violent Insider: The active violent insider will use their specialized knowledge and skillset to penetrate and maximize physical damage against an organizations security, systems, and critical assets. They are willing to risk death and/or use deadly force, and possibly weapons, against personnel or critical components in an attempt to complete their mission.

1.4 Unacceptable Consequences

The term "unacceptable consequences" refers to a threshold, or consequence, that an owner / operator decides is so severe as to justify expending resources to prevent its occurrence. These thresholds are addressed in detail in Chapter 3.

Chapter 2: Threat Levels

2.1 High Threat

- Numbers: Up to three outsiders and up to one active nonviolent insider
- Motivation: Highly motivated and willing to put their own lives or the lives of others at risk
- Intention: Damage, destruction, or adverse impact to the BPS
- Weapons, Tools, and Equipment: Pistols, rifles, and shotguns (the entity would consider caliber or gauge based on past history and intelligence information). Up to 50 pounds[3] of man-portable explosives, incendiary devices, ladders, hand and power tools, flashlights or other signaling devices, night vision and thermal optics, chains and cables, vehicles (ATVs, automobiles, trucks, boats, and/or aircraft) brought onsite by the actor, on-site heavy equipment[4], and a small Unmanned Aircraft System (UAS) (the entity would consider type based on past experience or intelligence) used for surveillance or sabotage
- Communications Tools: Voice/data over cell phones or other mobile devices, two-way radios, and social media
- Modes of transportation: Generally, any and all common modes of transportation are available, including bicycles, electric bicycles, ATVs, automobiles, trucks, boats, and walking as a transport mode
- Technical skills: Electrical engineering knowledge, operational knowledge, ability to determine critical facilities and critical components, knowledge of physical security systems, cyber skills, explosive demolitions, and explosive breaching (does not include tactical breaching)
- Knowledge: Detailed understanding of sites, people, equipment, procedures, and knowledge of critical components
- Tactics: Explosive breaching, explosive demolitions, standoff ballistic attack, arson, surveillance, cyber-enabled physical attacks, physical-enabled cyber attacks, and use of stealth, deception, or violence, removing bolts from transmission towers or cutting down wooden transmission poles

2.2 Moderate Threat

- Numbers: Up to two outsiders and up to one passive OR active nonviolent insider
- Motivation: Personally, ideologically, or financially motivated, not willing to intentionally risk their lives but willing to risk the lives of others to accomplish their goal
- Intention: Sabotage, damage, destruction, or vandalism to the BPS or its components
- Weapons, Tools, and Equipment: Pistols, rifles, and shotguns (the entity would consider caliber or gauge based on past history and intelligence information). Up to 15 pounds of man-portable low explosives, incendiary devices, ladders, hand and power tools, flashlights or other signaling devices, night vision and thermal optics, chains and cables, vehicles (ATVs, automobiles, trucks, boats, and/or aircraft) brought onsite by the actor, on-site heavy equipment, and a small UAS (the entity would consider type based on past experience or intelligence) used for surveillance
- Communications Tool: Voice/data over cell phones or other mobile devices, two-way radios, and social media

[3] Asset owners and operators are encouraged to work with local law enforcement or security professions to best determine the type of explosives to reference when assessing a high threat.

[4] Heavy equipment includes "heavy duty motor equipment" as defined by Table 2-1 in the U.S. Fish and Wildlife Service's *Heavy Equipment Utilization and Replacement Handbook (2015);* https://www.fws.gov/policy/HeavyEquipHB.pdf, and "heavy duty motor vehicles" as defined in (ibis.) Section 2.2 as having a GVWR of 35,001 lbs. and greater.

- Modes of transportation: Generally, any and all common modes of transportation are available, including bicycles, electric bicycles, ATVs, automobiles, trucks, boats, and walking as a transport mode
- Technical skills: Use of publicly available information to determine target facilities and components, explosive demolitions
- Knowledge: Understanding of the site, people, equipment, and procedures: Personal observation and publicly available information on site targets
- Tactics: Explosive demolitions, arson, standoff ballistic attack, surveillance, and less sophisticated use of stealth, deception, or violence

2.3 Low Threat

- Numbers: Up to two outsiders
- Motivation: Personally or financially motivated, not willing to risk their own lives or the lives of others
- Intention: Theft, vandalism, and harassment to facility and system components
- Weapons, Tools, and Equipment: Firearms (the entity would consider the details based on past history and intelligence information), fireworks, ladders, hand and power tools, flashlights or other signaling devices, chains and cables, vehicles and heavy equipment, and a small UAS (the entity would consider type based on past experience or intelligence) used for surveillance
- Communications Tools: Voice/data over cell phones or other mobile devices, two-way radios, and social media
- Modes of transportation: Generally, any and all common modes of transportation are available, including bicycles, electric bicycles, ATVs, automobiles, trucks, boats, and walking as a transport mode
- Technical skills: Use of publicly available information to determine target facilities and components
- Knowledge: Personal observation or publicly available information on targeted sites
- Tactics: Surveillance and use of available cover and concealment

Chapter 3: Unacceptable Consequences of a Physical Attack

3.1 Unacceptable Consequences (General)

Across regions, ownership, asset types, regulatory boundaries, and geographical borders, owners/operators will experience wide variation in the applicable types of unacceptable consequences. These can vary among many categories, including reputation, financial, material, or technical, and can go into specifics of losses of particular components, capabilities, or anything else that is critically important to the owner/operator. Additionally, different asset categories (transmission, distribution, and controls) have varying unacceptable consequences with regards to contributing to the instability, uncontrolled separation, or cascading failure within an interconnection. Section 3.1.1 addresses unacceptable consequences of an attack on the Bulk Power System (BPS), Section 3.1.2 addresses control centers, and Section 3.1.3 provides a general template for distribution assets.

3.1.1 Unacceptable Consequences of a Physical Attack on the Bulk Power System

- Instability, uncontrolled separation, or cascading within an interconnection caused by:
    - Loss or degradation of critical security systems or components
    - Catastrophic loss of critical components
    - Unauthorized physical access to a control center or cyber system
    - Loss of primary or backup BPS control center and its ability to control the grid
- Loss or compromise of proprietary critical node information (includes Critical Energy Infrastructure Information)
- Loss of a primary black-start unit or path

3.1.2 Unacceptable Consequences of a Physical Attack on Controls and/or Control Centers

- Compromising control systems through unauthorized physical access, through an attack on operators or directly operating systems in such a manner as would adversely affect reliable operation or damage equipment
- Compromising the center's ability to control the energy distribution network, including adverse measures to stop the control center from performing its function

3.1.3 Unacceptable Consequences of a Physical Attack on the Distribution Network

- An outage of x size for more than n hours; in which the operating utility determines x and n based on their specific requirements
- Loss of critical difficult-to-replace substation components

Chapter 4: Physical Security Advisory Group

The following is the 2022-2023 roster of the Physical Security Advisory Group.

Physical Security Advisory Group Roster: 2022-2023	
Name	**Organization**
Barry Childs	Duke Energy, PSAG Co-Chair
Barry Page	C4S2Global
Carlos Ross	Ameren
Dave Foster	Puget Sound Energy
David Godfrey	Garland Power and Light
David Grubbs	Garland Power and Light
Jeff Murray	U.S. Department of Homeland Security
Jeffrey Imsdahl	Xcel Energy
Jim McGlone	Federal Energy Regulatory Commission
Jim Spracklen	Pacific Northwest National Laboratory
John Greaves	Southern Company
Larry Mallory	New York Power Authority
Luc Landry	Hydro-Québec
Norma Browne	Ameren
Patrick Stier	SERC Reliability Corporation
Randall White	Southern California Edison
Rob Siefken	Safeguards3
Ross Johnson	Bridgehead Security, PSAG Co-Chair
Sam Queeno	American Electric Power
Scott Yost	Capital Power
Thomas Chadwick	Dominion Energy
Travis Moran	SERC Reliability Corporation

Appendix A: Design Basis Threat Acronyms

AOO	Asset Owners and Operators
APL	Asset Protection Level
ATV	All-terrain vehicles
BPS	Bulk Power System
DBT	Design Basis Threat
DOE	U.S. Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
HME	Homemade Explosives
IED	Improvised Explosive Device
PNNL	Pacific Northwest National Laboratory
PPS	Physical Protection System
PSAG	Physical Security Advisory Group
TLP	Traffic Light Protocol
UAS	Unmanned Aircraft System
VISA	Vulnerability of Integrated Security Analysis