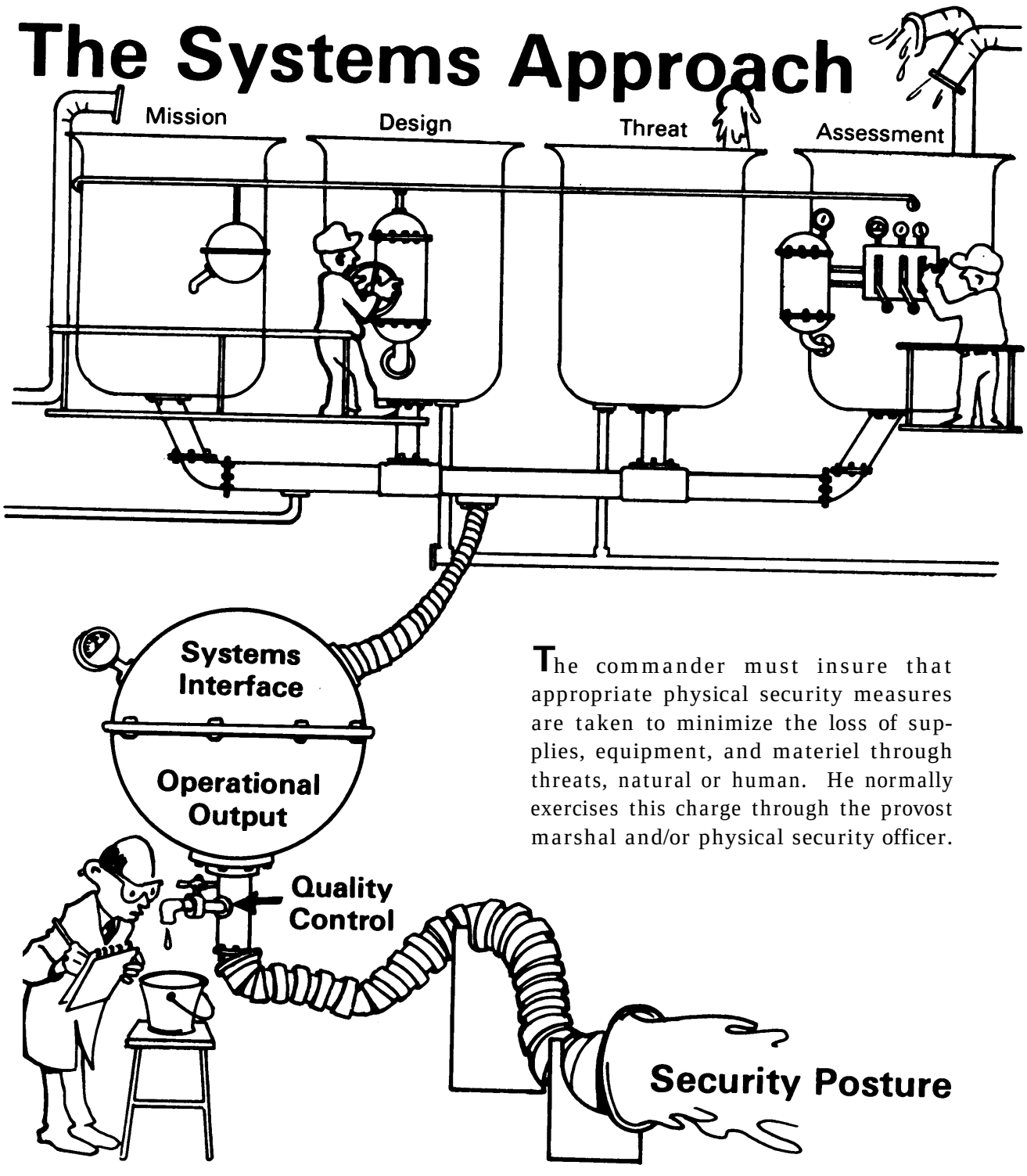
Chapter 1



The commander must insure that appropriate physical security measures are taken to minimize the loss of supplies, equipment, and materiel through threats, natural or human. He normally exercises this charge through the provost marshal and/or physical security officer.

Formulating

Section I

1-1 System Design

You should formulate and implement your basic physical security design from a total system approach. It should be organized in depth and contain mutually supporting elements and be coordinated to prevent gap or overlap in responsibilities and performance.

a. Total system approach is based on:

(1) Thoughtful and continuing analysis of existing protective measures.

(2) Determination of the possibility of interference with the operational capabilities of the installation or facility from any or all sources.

(3) Careful evaluation of the measures necessary and practicable that maintain security at a desired level.

(4) Tailored to the needs and local conditions of each installation or activity.

b. Mutually supporting elements include:

(1) Physical perimeter barrier(s).

(2) Clear zones.

(3) Protective lighting.

(4) Entry control facilities.

(5) Detection, including the use of sensors and assessment systems.

(6) Warning systems.

(7) Perimeter defensive positions, if appropriate.

Note: Selection and use of **means beyond minimum requirements:**

- Established by command directives.
- Coordination and cooperation between physical security officers and facilities engineers is a necessity.
- Wherever threat indicates need for increased security.

1-2 Design Considerations

a. Available resources must be used in the most efficient manner to achieve adequate protection for an entire installation.

b. Emphasis goes to the **operational requirements** of the installation in determining the type and extent of physical protection. The physical security manager should consider the following pertinent factors in the indicated sequence.

(1) Mission assignment— importance of the installation or unit to the mission of the Army.

(2) The area to be protected, including the nature and arrangement of the activity; classification of information, data, activities; the number of personnel involved; monetary and/or strategic value of materiel located therein; or other important features inherent to the problem, such as existing threats, either natural or human.

(3) Criticality and vulnerability of information, materiel and personnel.

(4) Integration of operating, maintenance, and other requirements.

(5) Environment, such as political and economical aspects, legal considerations, terrain, weather, climate, etc.

(6) Feasibility, effectiveness, and desirability of various possible methods of providing adequate protection.

(7) Costs of materiel and equipment to be installed as well as availability of finds to provide at least minimum protection for all critical areas and activities This minimum may be less than the desirable degree of physical protection; therefore, the program must be flexible so that refinements can be added as additional resources become available.

(8) Possible changes in operation, such as expansion, relocation and retrenchment. Coordination must be maintained with appropriate staff offices so that changes may be projected as far in advance as possible, and necessary supplemental personnel and/or funds can be requested.

c. Changes in mission and activities of an installation or activity may also require adjustments in security. **Physical security planning and programing must be a continuing process** if security managers are to provide the best protection possible.

d. All security measures should be employed so that they complement and supplement each other. Lack of integration of security measures may result in a waste of money, equipment, and manpower. But more important, the security of an installation may be placed in jeopardy. By the considerations outlined, a sound physical security program should evolve.

e. The **formulating procedure** is sound whether it is applied to changes on existing installation or the construction of a new facility.

1-3 Assessment Of Security Posture

The degree of protection desired on any installation is predicated upon an analysis of two factors-criticality and vulnerability.

a. Resource Criticality

(1) Determination

(a) Importance to the national defense structure.
(b) Effect of its partial or complete loss.

(2) Evaluation

(a) Installation. High criticality-great effect on national defense structure.
(b) Command/activity. High criticality—partial or complete loss—immediate and serious impact to perform its mission for a considerable period of time.

b. Resource Vulnerability

(1) Determination

(a) Susceptibility to threats that result in damage, loss, destruction or disruption.
(b) Type Of installation or activity involved, industrial or other processes performed, physical layout and construction.

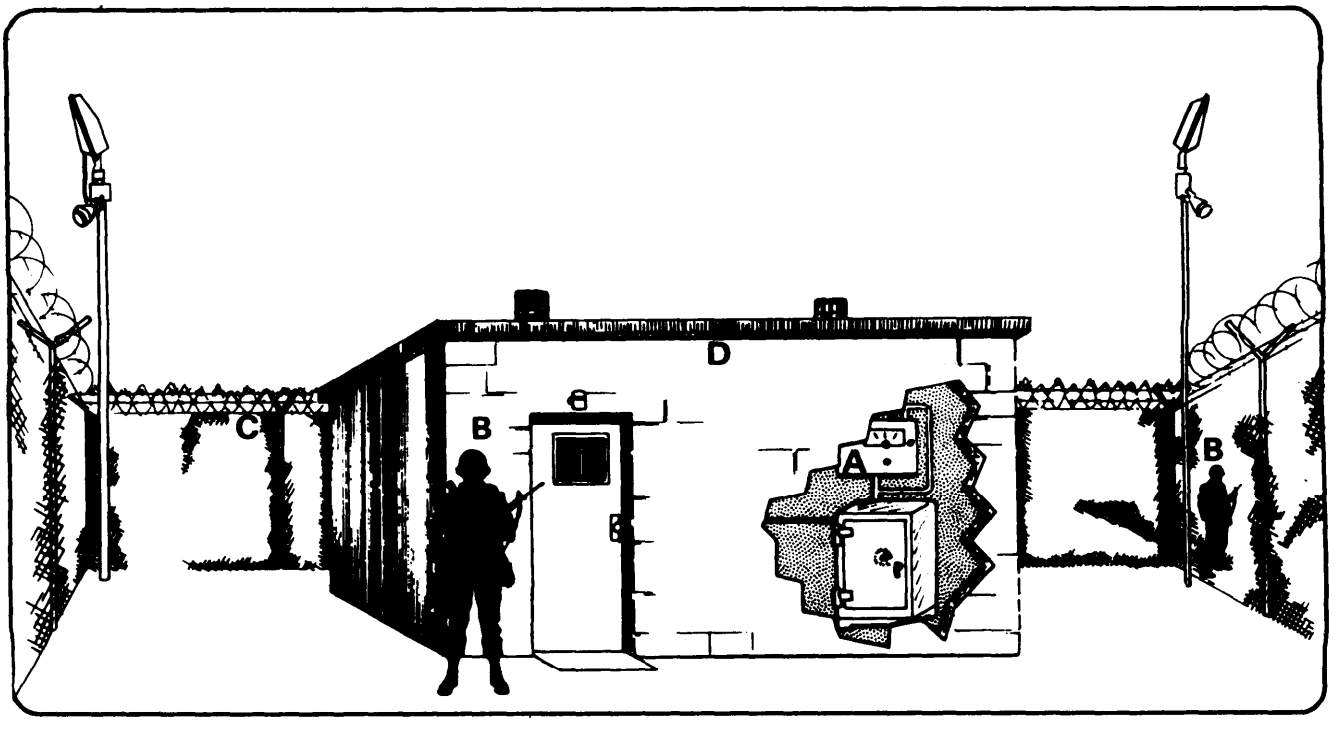
(2) Evaluation

(a) High vulnerability—one or more threats easily causing sufficient loss, damage, or destruction to affect the mission of the whole installation or its subordinate commands/activities.
(b) Decreased vulnerability—existing threats not likely to cause interference with the mission.
(c) It should be noted that cost of

protective measures in terms of equip ment and manpower may not allow for optimum security for the entire installation. Also, determination of security priority based on criticality and vulnerability is essential to proper allocation of resources.

c. Security in depth (guards, physical barriers, and systems) is always the goal of those individuals responsible for the security of an installation or activity. No object is so well protected that it cannot be stolen, damaged, destroyed, or compromised. Therefore, access must be made so difficult that an intruder will be deterred from committing a criminal act or will be detected and apprehended before he can successfully complete the criminal act. **Accumulated delay time for the intruder must be built into a system for protection in depth.** This protection results from the security in-depth ring (see figure 1).

d. Physical security is only part of the overall defense plan of an installation. It does not include dispersion of facilities, continuity of operations, civil defense structures, construction specifications, or plans formulated to cope with natural or human threats that happen. The formulating process must allow for the integration of all these measures.



LEGEND

A IDS
B Guards
C Barrier
D Building (barrier)

Figure 1—Security in-depth ring.

Security Threats

Section II

Security threats are acts or conditions that may result in the compromise of information; loss of life; damage, loss, or destruction of property; or disruption of the mission of the installation or facility. Before the physical security manager can develop an effective security program, he must determine the possibility of interference with the operational capabilities of the installation or facility from any and all sources. Recognition of all risks is mandatory if he is to make recommendations for physical security measures to control or eliminate them. The severit y of security threats depends on such variables as the type of installation or facility involved, mission or processes performed, physical layout, and construction. The geographical location, the enemy situation, and the existing state of law and order are most important factors.

1-4 Definition

a. Security threats are acts or conditions, which include human threats, that may result in:

(1) Disruption of the installation or facility.

(2) Damage, loss or destruction of property.

(3) Personal injury or loss of life.

(4) Compromise of defense information.

b. Threat severity depends on such variables as:

(1) Type of installation or facility.

(2) Mission or processes performed.

(3) Physical layout and construction.

(4) Geographical location.

(5) Stability of the situation.

(6) Existing state of law and order.

(7) Protection measures in effect.

1-5 Categories

Security threats are classified as either natural or human.

a. Natural Threats

(1) Usually the consequence of natural phenomena.

(2) Normally not preventable by physical security measures.

(3) May greatly affect security operations in one or more of these ways.

(a) Require an increase in protective measures.

(b) May reduce the effectiveness of existing security measures by such occurrences as:

- Collapsed perimeter fences.
- Inoperable protective lighting.
- Damaged patrol vehicles.
- Poor visibility.

Examples of natural threats are:

Floods— flooding of the installation with resulting property damage, destruction of perimeter barriers and short circuiting of intrusion detection systems. Heavy rains or snowfalls, even though they do not result in floods, may cause some of the same damages.

Storms— high winds or rain causing nuisance alarms and short circuiting in IDS, and limiting visibility of security personnel.

Earthquakes— causing nuisance alarms, possible fires from broken gas mains, buildings weakening and falling down.

Winds— disrupting power lines, setting off nuisance alarms, causing safety hazards with flying debris.

Snow and Ice— blocking patrol roads, increasing response time to alarms, and freezing of locks and alarm mechanisms.

Fires— damage/destruction of perimeter barriers or buildings.

Fog— causing reduced visibility for security forces and increased response time to alarms and may require additional security personnel.

b. Human Threats

These threats are the result of a state of mind, attitude, weakness, or character trait on the part of one or more persons. They include acts of commission or omission—overt and covert—which could disrupt or destroy the operation or mission of an installation or facility.

Examples of human threats are:

- ❑ Pilferage (appendix A).
- ❑ Sabotage (appendix B).
- ❑ Espionage (appendix C).
- ❑ Bombing (appendix D).
- ❑ Pilferage in Consumer Outlets (appendix A).
- ❑ Attacks on Key Persons (chapter 14).
- ❑ Carelessness and accidents in performance of official duties.
- ❑ Disaffection and disloyalty of employees.
- ❑ Safety hazards from equipment malfunction.
- ❑ Human Intelligence Threat (HUMINT).

1-6 Risk Analysis

This process is invaluable to the security manager in establishing priorities of protection of assets. Basically, it consists of

a. Identifying items and functions in terms of:

(1) Total replacement

(2) Temporary replacement

(3) Unrecoverable costs

(4) Allied and related costs.

b. Conducting a hazards and vulnerability study of personnel, facilities, items, and functions.

c. Conducting a probability of occurrence assessment through indicators, such as:

(1) Documented records

(2) Insurance claims or adjustments

(3) Weather, etc.

d. Establishing a range of losses based on experience involving specific items (minimum to maximum in terms of dollar value), and assessing the losses over a 3-5 year period.

e. Correlating the degree of loss experienced with the ranges of losses or functions.

f. Comparing the low against high elements of ranges for all items and functions; then averaging weight against risk value in terms of criticality (Defense Industrial Security Institute, DSA).

1-7 Evaluation of Risks

The actual degree of risk involved depends on two factors:

- ■ Probability of adverse effects occurring as a direct result of the threat(s).

■ Extent to which the installation or activity will be affected by the threat(s).

Security threats significantly impact on a physical security program by requiring the incorporation of the following considerations:

❑ All determinable threats.
❑ Continuing activity beginning in peacetime and expanding to meet the particularities of formal hostilities.
❑ Coordination and integration with other protective programs, such as crime prevention and safety.