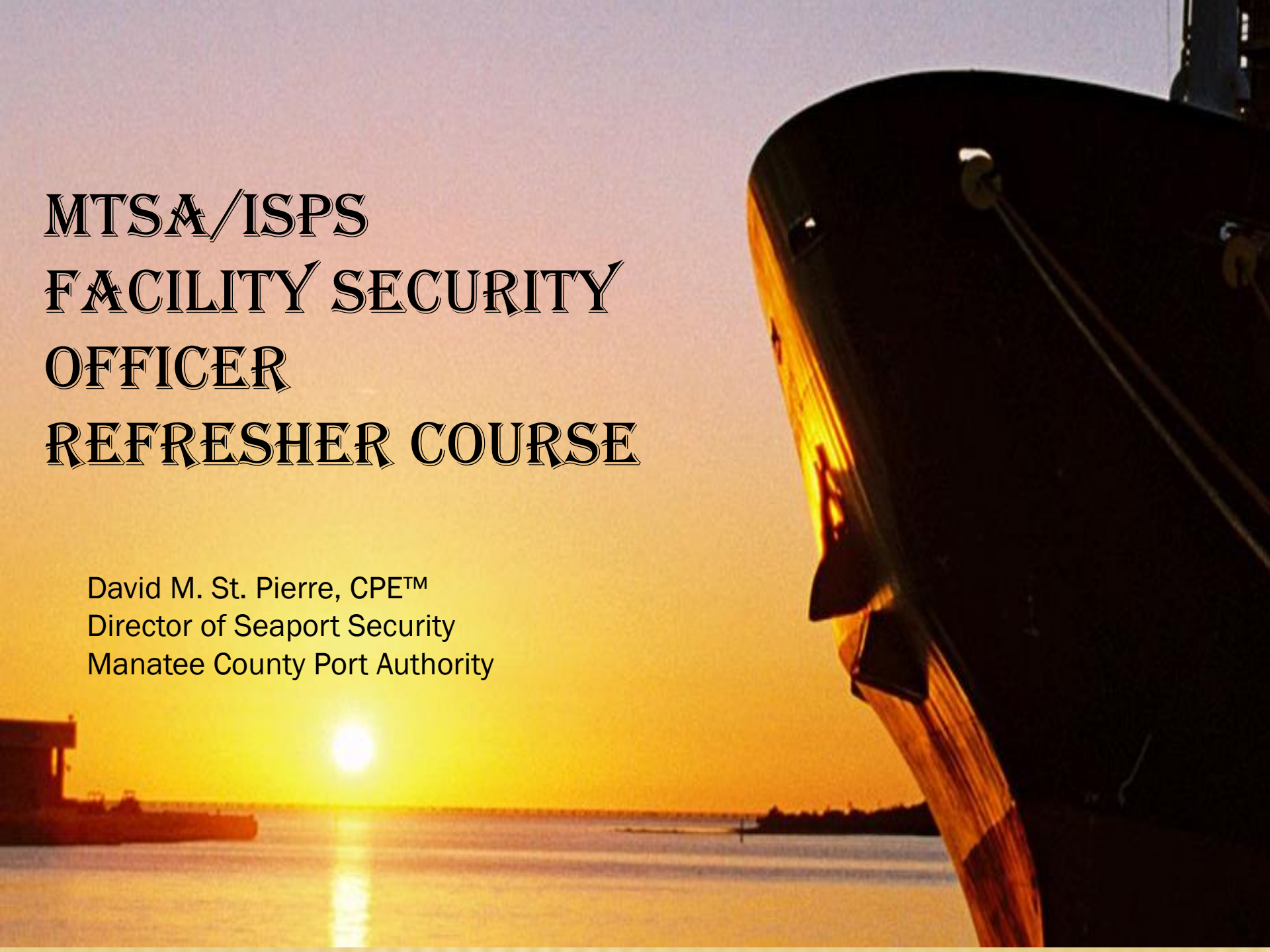


MTSA/ISPS FACILITY SECURITY OFFICER REFRESHER COURSE

David M. St. Pierre, CPE™
Director of Seaport Security
Manatee County Port Authority

SEPTEMBER 11, 2001

"All the News That's Fit to Print"

The New York Times

Late Edition

VOL. CL . . . No. 51,874 NEW YORK, WEDNESDAY, SEPTEMBER 12, 2001 75 CENTS

U.S. ATTACKED

HIJACKED JETS DESTROY TWIN TOWERS AND HIT PENTAGON IN DAY OF TERROR

A CREEPING HORROR

Buildings Burn and Fall as Onlookers Search for Elusive Safety

President Vows to Exact Punishment for 'Evil'

- Following the tragic events of September 11, 2001 the twenty-second session of the International Maritime Organization met and unanimously agreed to the development of new measures relating to the security of ships and port facilities

THE RESULTS

- **IMO Diplomatic Conference on Maritime Security amends SOLAS.**
  - **The ISPS Code is created**

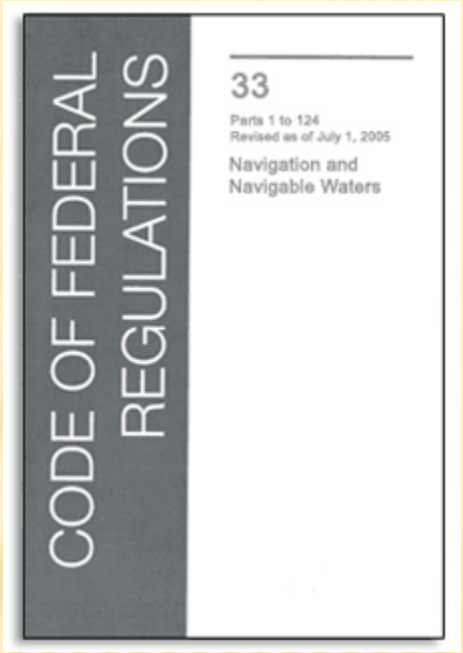
THE RESULTS

- **The U.S. Congress passes the Maritime Transportation Security Act of 2002 (MTSA)**
  - **The law requires the U.S. Coast Guard draft implementation regulations.**
  - **The Coast Guard published the regulations under Title 33 of the Code of Federal Regulations Parts 101-106. (33 CFR 101-106)**

WHAT IS THE ISPS CODE?

- The ISPS Code is the method of ensuring that the provisions of the SOLAS 74 Convention, as amended, regarding security are implemented

WHAT ARE 33 CFR PARTS 101 THRU 106?



- These are the regulations drafted by the U.S. Coast Guard to implement the provisions of the Maritime Transportation Security Act.

SAFE PORT ACT PROVISIONS

- Creation of the Transportation Worker Identification Credential
- Establishment of interagency operational centers for port security
- Extended the Port Security Grant Program
- Container Security Initiative (CSI)
- Foreign port assessments
- Customs-Trade Partnership against Terrorism (C-TPAT)

TRANSPORTATION WORKERS IDENTIFICATION CREDENTIAL (TWIC)

HISTORY

- Nov 2001, Post 9-11 Report
- Nov 2002, Maritime Transportation Security Act
- Aug 2004, Homeland Security Presidential Directive 12
- Nov 2004 – Oct 2005 first prototype tests
- Dec 2004, USCG, Merchant Mariners Documentation
- Spring 2006, NMSAC
- MAY 2006, NPRM
- July 2006, increased political pressures at the national level
- Oct 2006, available to Federal Government
- Dec 2006, NMSAC Working Group
- Jan 26, 2007, NPRM, Published
- Field Test (LA/LB/ 3 other Port Authorities), tied to Round 6/7 Grants

TRANSPORTATION WORKERS IDENTIFICATION CREDENTIAL (TWIC)

Goals

- Positively identify authorized individuals who require unescorted access to secure areas of the nation's maritime transportation system;
- Determine the eligibility of an individual to be authorized unescorted access to secure areas of the maritime transportation system;
- Enhance security by ensuring that unauthorized individuals are denied unescorted access to secure areas of the nation's maritime transportation system; and,
- Identify individuals who fail to maintain their eligibility qualifications after being permitted unescorted access to secure areas of the nation's maritime transportation system and revoke the individual's permissions.

CONTAINER SECURITY INITIATIVE

- The **Container Security Initiative** (**CSI**) was launched in 2002 by the U.S. Bureau of Customs and Border Protection (CBP), an agency of the Department of Homeland Security. Its purpose was to increase security for container cargo shipped to the United States.
- As the CBP puts it, the intent is to "extend [the] zone of security outward so that American borders are the last line of defense, not the first."

CONTAINER SECURITY INITIATIVE

- Containerized shipping is a critical component of international trade. According to the CBP:
  - About 90% of the world's trade is transported in cargo containers.
  - Almost half of incoming U.S. trade (by value) arrives by containers onboard ships.
  - Nearly seven million cargo containers arrive on ships and are offloaded at U.S. seaports each year.

CONTAINER SECURITY INITIATIVE

- CSI consists of four core elements:
  - Using intelligence and automated information to identify and target containers that pose a risk for terrorism.
  - Pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports.
  - Using detection technology to quickly pre-screen containers that pose a risk
  - Using smarter, tamper-evident containers.

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- C-TPAT is a voluntary supply chain security program led by U.S. Customs and Border Protection (CBP) and focused on improving the security of private companies' supply chains with respect to terrorism.

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- Types of participants in C-TPAT include:
  - U.S. importers of record
  - U.S./Canada and U.S./Mexico highway carriers
  - Rail, sea, and air carriers
  - U.S. marine port authority and terminal operators
  - U.S. air freight consolidators, ocean transportation intermediaries and non-vessel operating common carriers
  - Mexican manufacturers
  - Certain invited foreign manufacturers
  - Licensed U.S. customs brokers

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- According to U.S. Customs and Border Protection, the benefits of participating in C-TPAT could include:
  - Playing an active role in the war against terrorism
  - A reduced number of CBP inspections.
  - Priority processing for CBP inspections.
  - Eligibility to attend C-TPAT training seminars.

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- U.S. Customs and Border Protection has proposed some benefits to its C-TPAT partners that include:
  - Reduced Customs inspections
  - Reduced border delays
  - Entitlement to a CBP account manager
  - Eligibility for account-based processes
  - Participation in the war against terrorism
  - Need certification to proceed with Importer Self Assessment program (ISA)

MTSA TRAINING REQUIREMENTS

- May 19, 2015 Coast Guard letter to MTSA regulated facilities and security course provideers.
  - MARAD oversight of voluntary MTSA course approvals ended October 1, 2014.
  - Current approved courses remain valid.
  - Future course approvals reviewed by CG using Quality Standard System process.
  - Regardless of claims no courses are approved that are not listed on CG Homeport site.

IRAM RISK MODEL

Scenario: Target + Attack Mode

HOW DO WE CHARACTERIZE THE FACTORS IN THE IRAM RISK MODEL?

- Scenario
  - Application of an attack mode against a target
- Threat
  - Relative likelihood of attack being attempted
- Vulnerability
  - Probability that the attack will be successful given an attempt
- Consequence
  - Consequence points representing the impacts of a successful attack

SCENARIO

- Application of an attack mode against a target
- For each target, one or more attack modes are required to be analyzed

TARGET CLASSES

- Classify each target using a standard list
- There are several specific classes within the six major target types:
  1. Barge
  2. Facility
  3. Infrastructure
  4. Key Asset
  5. Vessel
  6. Other

ATTACK MODES

Land Attacks

-  Terrorist Assault Team
-  Standoff Weapon from Land
-  Truck Bomb
-  Passenger/Passerby
-  Sabotage

Sea Attacks

-  Boat Bomb
-  Boat Bomb (while vessel is present)
-  Multiple Boat Attack
-  Standoff Weapon from
-  Water
-  Swimmer/Diver

DETAILED ATTACK MODE DESCRIPTIONS

For each attack mode, IRAM provides a detailed scenario description to guide you in the consistent analysis of scenario risk

Truck Bomb Attack

Up to two terrorists armed with small arms attack with a vehicle loaded with up to 10,000lbs of TNT equivalent explosives is detonated in proximity to the target focal point. Assume terrorists will attempt to overcome guards and barriers.

HOW DO WE CHARACTERIZE THE FACTORS IN THE IRAM RISK MODEL?

- Scenario
  - Application of an attack mode against a target
- Threat
  - Relative likelihood of attack being attempted
- Vulnerability
  - Probability that the attack will be successful given an attempt
- Consequence
  - Consequence points representing the impacts of a successful attack

THREAT

- Relative likelihood of an attack being attempted on the target
- Scored by choosing one of the categories below:

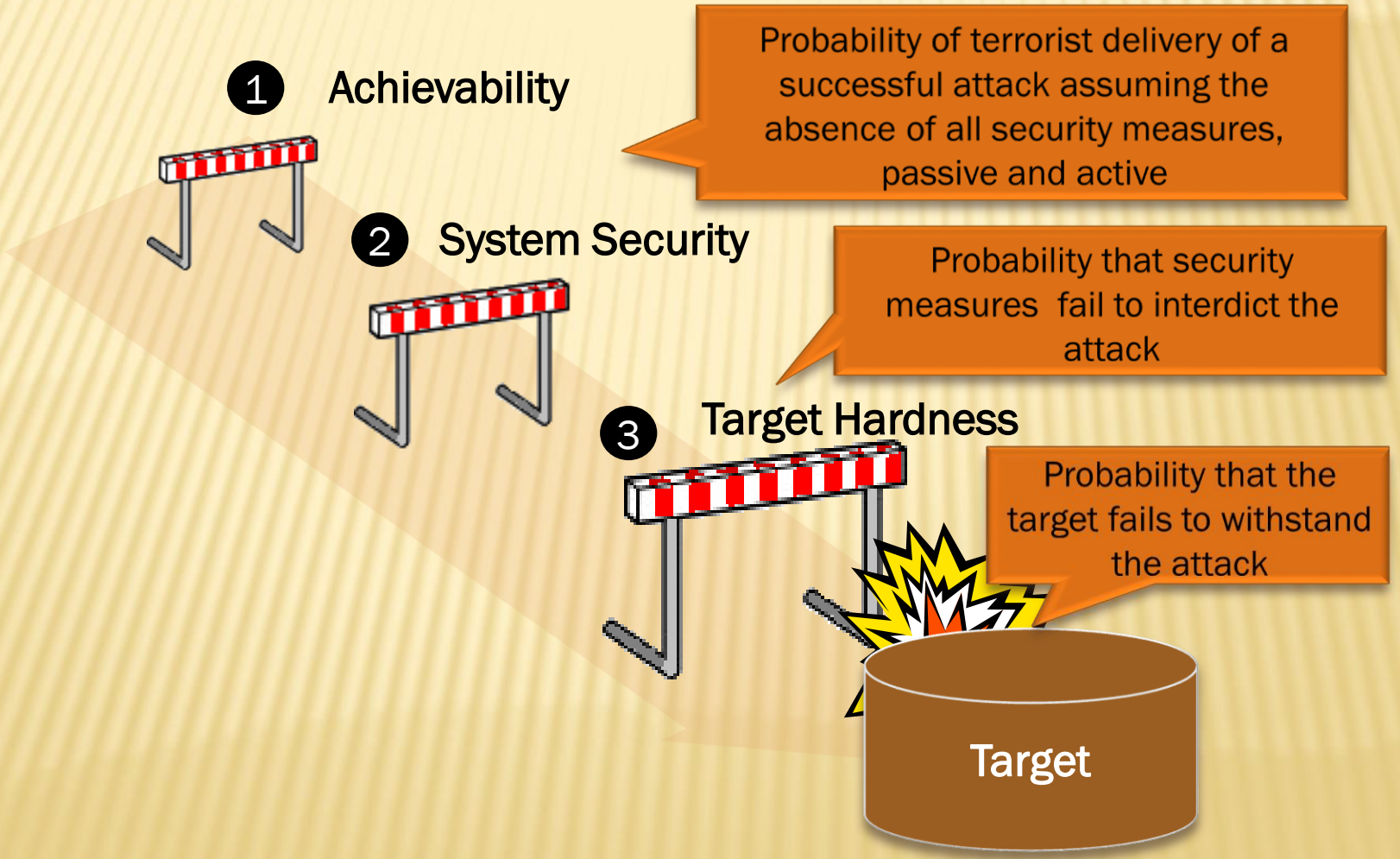
Category	Description	Weight
1	Low Threat	0.1
2	Medium Threat	1
3	High Threat	10

HOW DO WE CHARACTERIZE THE FACTORS IN THE IRAM RISK MODEL?

- Scenario
  - Application of an attack mode against a target
- Threat
  - Relative likelihood of attack being attempted
- Vulnerability
  - Probability that the attack will be successful given an attempt
- Consequence
  - Consequence points representing the impacts of a successful attack

Vulnerability

The vulnerability factors collectively represent the probability that the terrorist is able to successfully execute the attack on the target



ACHIEVABILITY

- Probability of terrorist delivery of a successful attack assuming the absence of all security measures
- Scored by choosing one of the categories below:

Category	Description
1	0% to 5% Achievable
2	5% to 15% Achievable
3	15% to 35% Achievable
4	35% to 65% Achievable
5	65% to 85% Achievable
6	85% to 95% Achievable
7	95% to 100% Achievable

PHYSICAL PROTECTION SYSTEMS DESIGN

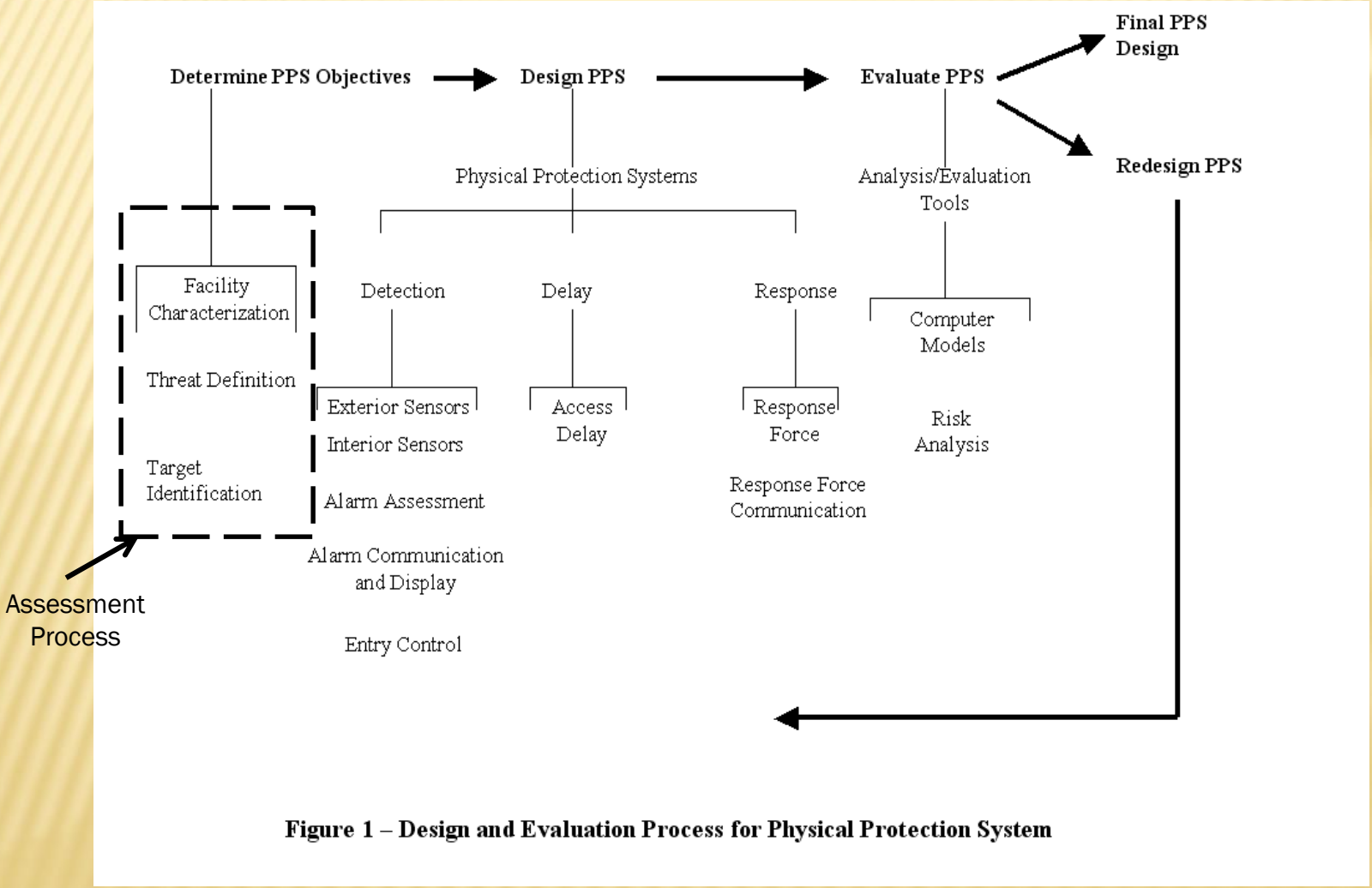


Figure 1 – Design and Evaluation Process for Physical Protection System

PHYSICAL PROTECTION SYSTEMS DESIGN

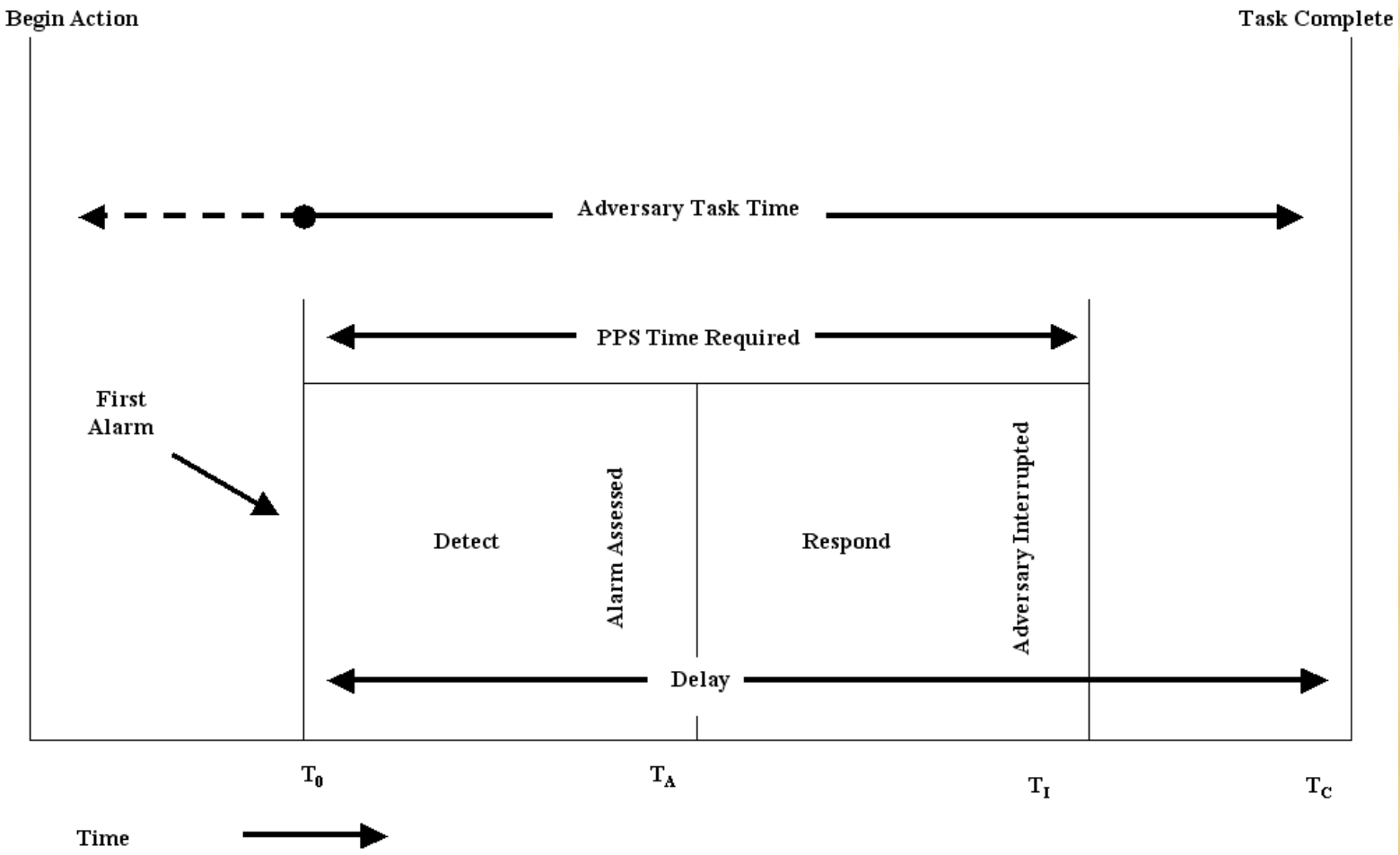


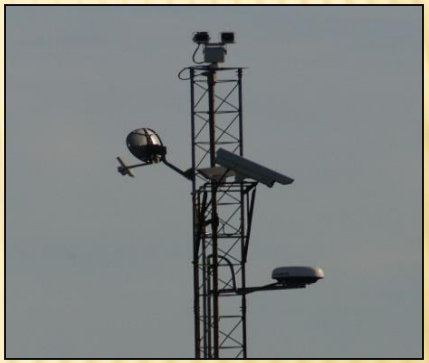
Figure 2 – Adversary Task Time versus PPS Time Requirements

SYSTEM SECURITY

- Probability that security measures provided by the owner/operator fail to interdict the attack
- Scored by individually evaluating four phases of system security:
  - Detect
  - Decide
  - Engage
  - Defeat

DETECT

- The ability to detect an attack in progress
- Components of Detect:
  - Capability and location of sensors/guards
  - Timing of Detection
  - Reliability of Detection System



DECIDE

- Commit to a course of action (COA) to stop the threat and communicate that COA to the necessary parties.
- Three Components of Decide:
  - Situational awareness
  - Use of force/Rules of Engagement
  - Communications

ENGAGE

- Delay the attackers as necessary and bring forces to bear against the attackers
- Three components of Engage:
  - Delay (barriers and access control)
  - Location and readiness
  - Mobility and response times

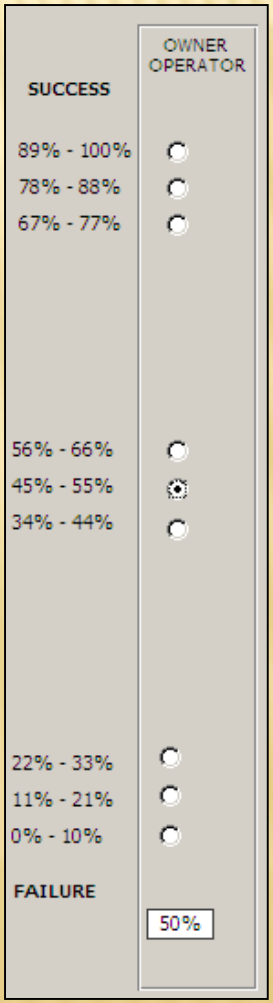
DEFEAT

- Prevent the attackers from damaging or destroying the attack focal point
- Three components of defeat:
  - Organization/force size of security elements
  - Trained/exercised to task
  - Equipped to task

SYSTEM SECURITY CALCULATION

- Each phase of system security is scored separately in a calculator by choosing a category representing probability of success
- Overall system security is calculated a product of all four phases

Detect*Decide*Engage*Defeat



TARGET HARDNESS

- Probability that the target fails to withstand the attack
- Scored by choosing one of the categories below:

Category	Description
1	95% to 100% ability to withstand
2	85% to 95% ability to withstand
3	65% to 85% ability to withstand
4	35% to 65% ability to withstand
5	15% to 35% ability to withstand
6	5% to 15% ability to withstand
7	0% to 5% ability to withstand

HOW DO WE CHARACTERIZE THE FACTORS IN THE IRAM RISK MODEL?

- Scenario
  - Application of an attack mode against a target
- Threat
  - Relative likelihood of attack being attempted
- Vulnerability
  - Probability that the attack will be successful given an attempt
- Consequence
  - Consequence points representing the impacts of a successful attack

CONSEQUENCE

- Choose attack focal point
- Impacts of successful attack are scored considering:
  - Death and injuries
  - Economic impacts
  - Environmental impacts
- Each impact type is monetized to enable a cumulative consequence for each scenario

CONSEQUENCE EXAMPLE COMPARISON

Passenger Vessel

- **Death/Injury:** 5000 pts
- **Economic:** 500 pts
- **Environmental:** 5 pts
- **Total Consequence:** 5505 pts

Oil Tank Ship

- **Death/Injury:** 50 pts
- **Economic:** 500 pts
- **Environmental:** 500 pts
- **Total Consequence:** 1050 pts

Using the IRAM consequence equivalency factors, the passenger vessel has over 5 times the consequence of the oil tank ship