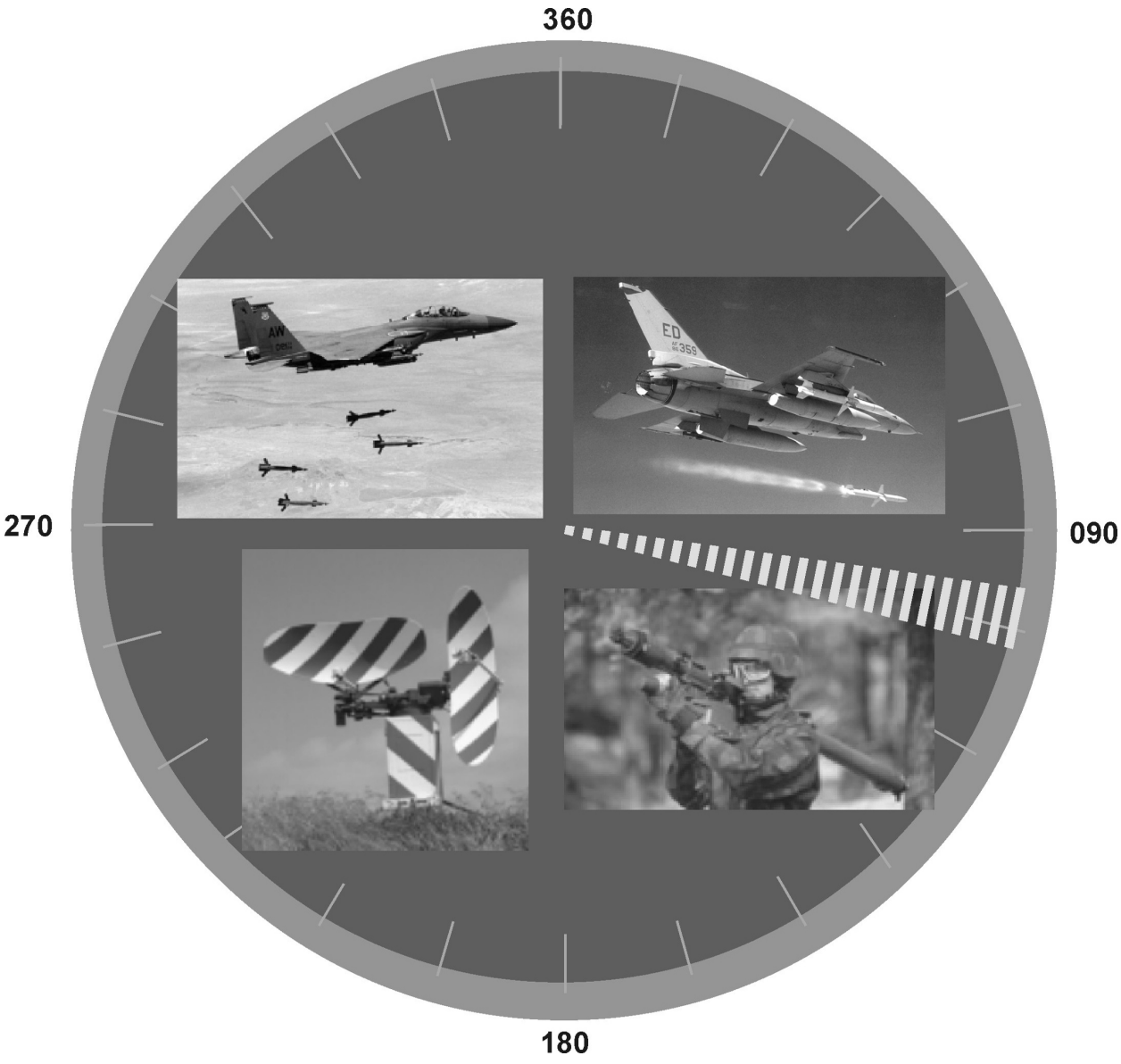
Military Technical College
Radar Department

ERD 402

ELECTRONIC WARFARE FUNDAMENTALS



PREFACE

Electronic Warfare Fundamentals **is a student supplementary text and reference book that provides the foundation for understanding the basic concepts underlying electronic warfare (EW). This text uses a practical building-block approach to facilitate student comprehension of the essential subject matter associated with the combat applications of EW.**

Since radar and infrared (IR) weapons systems present the greatest threat to air operations on today's battlefield, this text emphasizes radar and IR theory and countermeasures. Although command and control (C^2) systems play a vital role in modern warfare, these systems are not a direct threat to the aircrew and hence are not discussed in this book. This text does address the specific types of radar systems most likely to be associated with a modern integrated air defense system (IADS).

To introduce the reader to EW, ***Electronic Warfare Fundamentals*** **begins with a brief history of radar, an overview of radar capabilities, and a brief introduction to the threat systems associated with a typical IADS. The two subsequent chapters introduce the theory and characteristics of radio frequency (RF) energy as it relates to radar operations. These are followed by radar signal characteristics, radar system components, and radar target discrimination capabilities. The book continues with a discussion of antenna types and scans, target tracking, and missile guidance techniques.**

The next step in the building-block approach is a detailed description of countermeasures designed to defeat radar systems. The text presents the theory and employment considerations for both noise and deception jamming techniques and their impact on radar systems. This is followed by a chapter on decoys, both for defeating an IADS as well as for self-protection. Then, the next chapter discusses chaff characteristics, employment, and impact on specific radar systems.

The following two chapters are dedicated to the IR threat. The first covers IR theory, IR target detection and tracking, and advanced IR missile flare rejection techniques. The second chapter presents IR countermeasures to include flare employment, maneuvers, and missile warning equipment.

Electronic Warfare Fundamentals **then addresses an important aspect of EW, specifically electronic protection (EP). This section includes a description of the most common radar EP techniques designed to counter noise jamming, deception jamming, and chaff employment. The book concludes with an overview of the basic components and limitations of a typical radar warning receiver (RWR), current geolocation techniques, and it finally discusses the basic components of a self-protection jamming system.**

TABLE OF CONTENTS

CHAPTER 9. INTRODUCTION TO RADAR JAMMING

1. INTRODUCTION

Radar jamming is the intentional radiation or reradiation of radio frequency (RF) signals to interfere with the operation of a radar by saturating its receiver with false targets or false target information. Radar jamming is one principal component of electronic combat (EC). Specifically, it is the electronic attack (EA) component of electronic warfare (EW). Radar jamming is designed to counter the radar systems that play a vital role in support of an enemy integrated air defense system (IADS). The primary purpose of radar jamming is to create confusion and deny critical information to negate the effectiveness of enemy radar systems. This chapter will introduce the two types of radar jamming, the three radar jamming employment options, and discuss the fundamental principles that determine the effectiveness of radar jamming.

2. RADAR JAMMING TYPES

There are two types of radar jamming: noise and deception.

a. Noise jamming is produced by modulating a RF carrier wave with noise, or random amplitude changes, and transmitting that wave at the victim's radar frequency. It relies on high power levels to saturate the radar receiver and deny range and, occasionally, azimuth and elevation information to the victim radar (Figure 1-1). Noise jamming takes advantage of the extreme sensitivity of the radar receiver and the transmission pattern of the radar antenna to deny critical information to the victim radar.

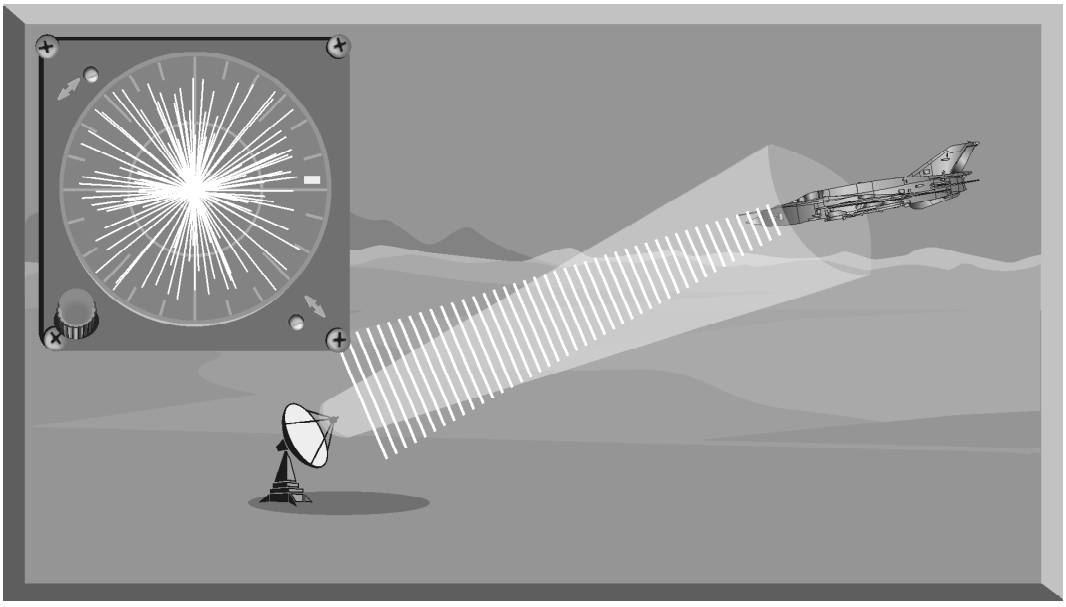


Figure 1-1. Noise Jamming

b. Deception jamming uses complex receiving and transmitting circuits to process and retransmit jamming pulses that appear as a real target to the victim radar. A deception jammer receives the signal from the victim radar and alters the signal to provide false range, azimuth, or velocity information. The altered signal is then retransmitted (Figure 1-2). The victim radar processes this signal, which disrupts the victim radar and confuses the radar operator. To be effective, deception jamming must match not only the victim radar's operating frequency, but all the other operating characteristics, including pulse repetition frequency (PRF), pulse repetition interval (PRI), pulse width, and scan rate.

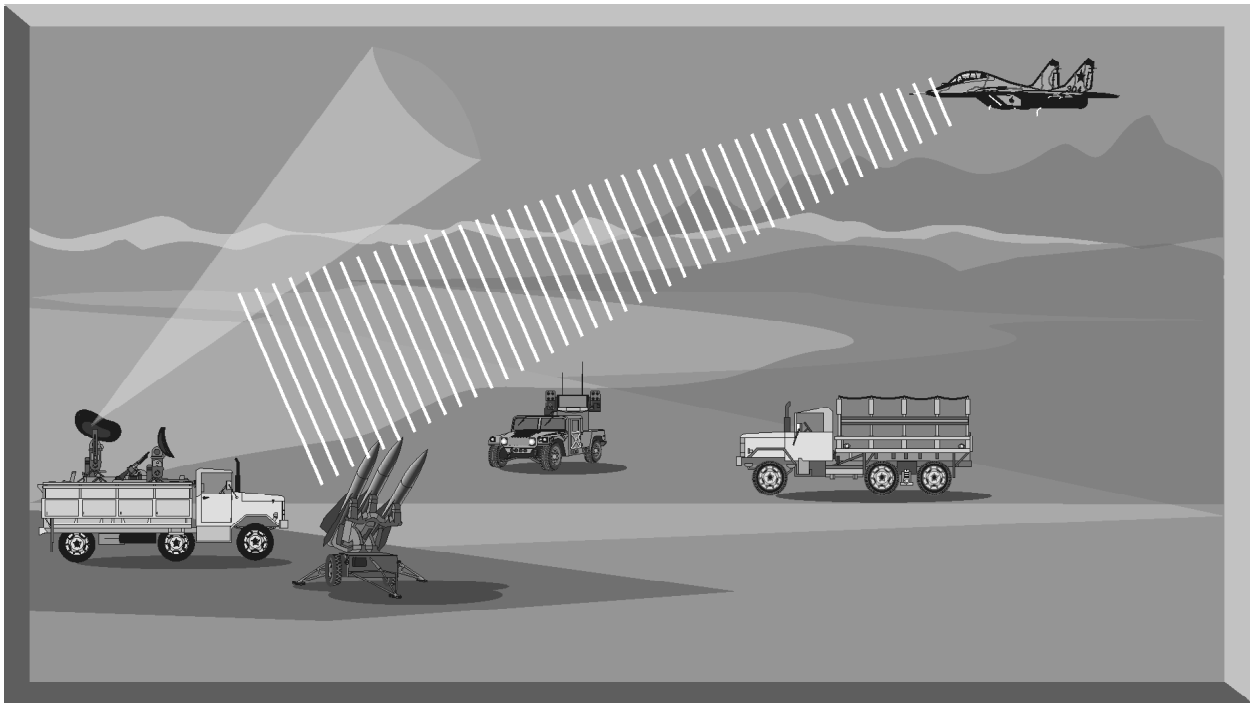


Figure 1-2. Deception Jamming

c. Both noise and deception jamming effectiveness are heavily dependent on another component of EW, specifically, electronic warfare support (ES). ES assets, either airborne or ground-based, provide the threat system specific radar parametric data and update this critical information based on observed threat system operations. This data provides the foundation for developing noise and deception jamming techniques. Intelligence and engineering assessment of this data are used to identify specific threat system weaknesses that can be exploited with the optimum noise, deception, or combination of jamming techniques. This information is then programmed into jamming systems to counter specific threats.

3. RADAR JAMMING EMPLOYMENT OPTIONS

There are currently two primary employment options for both noise and deception jamming techniques. These options are: (1) support jamming, and (2) self-protection jamming. Support jamming can be broken down further into stand-off jamming (SOJ), and escort jamming.

a. To counter early warning, ground control intercept (GCI), and acquisition radars associated with an enemy IADS, noise and deception jamming techniques are employed by specialized support jamming aircraft. The goal of support jamming is to create confusion and delays within the command and control structure of the IADS. Deny, delay or degrade the enemy's ability to engage friendly forces. Support jamming operations can be focused against a national level IADS through the use of a stand-off jamming (SOJ) profile (Figure 1-3) or against a target area threat array using an escort jamming profile.

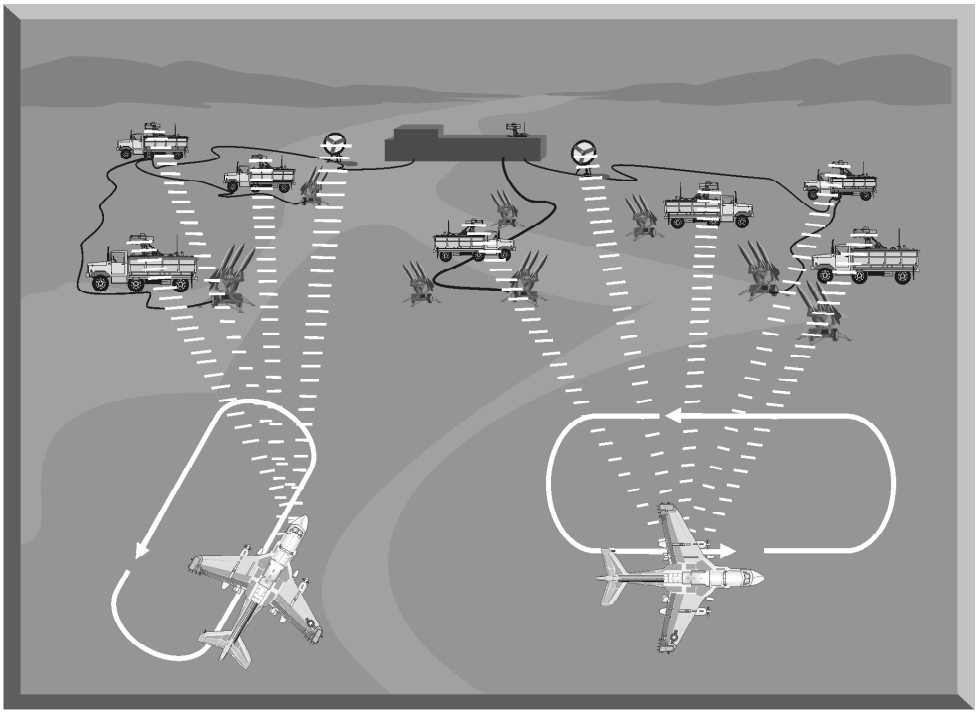


Figure 1-3. Stand-Off Jamming

(1) From an orbit area outside the surface-to-air missile (SAM) engagement zone, SOJ aircraft employ specialized jamming techniques to deny the enemy information about the attack package. SOJ aircraft employ specialized noise jamming techniques to generate jamming strobes on the victim radar display. This effectively denies range and azimuth information on aircraft ingressing and egressing the area covered by the noise jamming strobes. Intensity of the strobes is based on the power in the jamming. The area covered is based on the amount of jamming that can be injected into the main beam and sidelobes of the victim

radar. The effectiveness of SOJ noise jamming is determined by the power the jammer can generate relative to the power the victim radar can generate. This is called the jamming-to-signal (J/S) ratio.

(2) SOJ aircraft can also employ a deception technique to generate false targets to confuse the radar operator and mask the presence of real targets (Figure 9-4). In this specialized technique, the deception jammer must tune to the frequency, PRF, and scan rate of the victim radar. The jammer then transmits multiple jamming pulses that the victim radar receiver processes like real target returns. With enough power, the deception jammer can generate multiple false azimuth targets by injecting jamming pulses into the sidelobes of the victim radar. False moving targets and false range targets are generated by varying the time delay of the jamming pulses based on the PRF and scan rate of the victim radar.

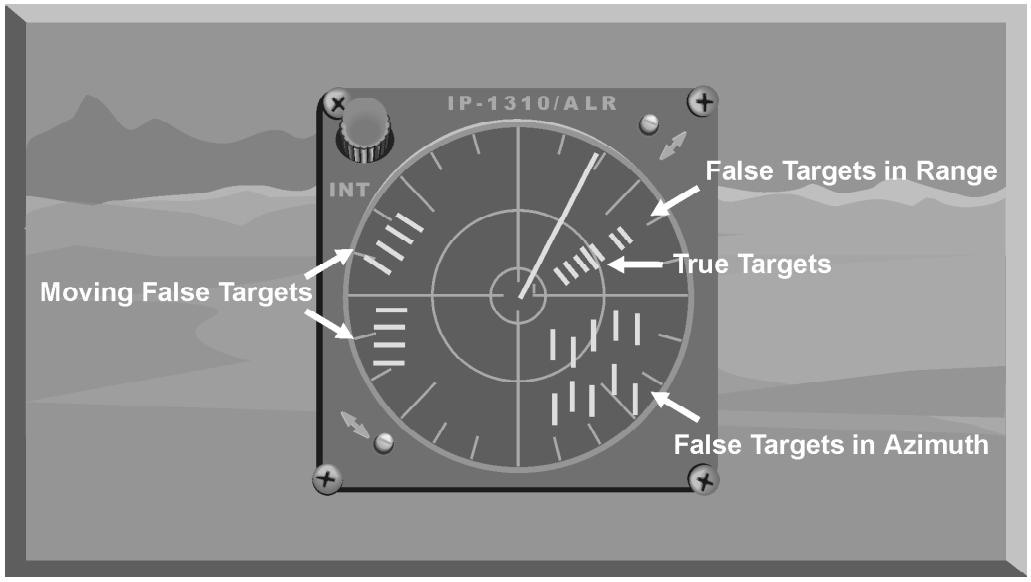


Figure 1-4. False Target Jamming

(3) Escort jamming is a specific tactic used by the EA-6B Prowler. The EA-6B is employed as an integral part of the attack package and is normally positioned behind and above the attack package (Figure 1-5).

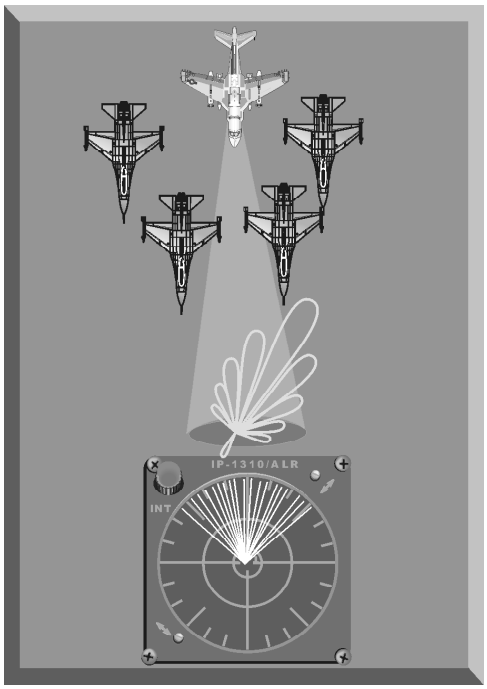


Figure 1-5. Escort Jamming

Using noise jamming, the EA-6B attempts to deny range and azimuth information to the victim radar by injecting high power signals into the main radar beam and sidelobes. To be effective, the EA-6B must be properly positioned in relation to the ingressing or egressing attack package (Figure 1-6).

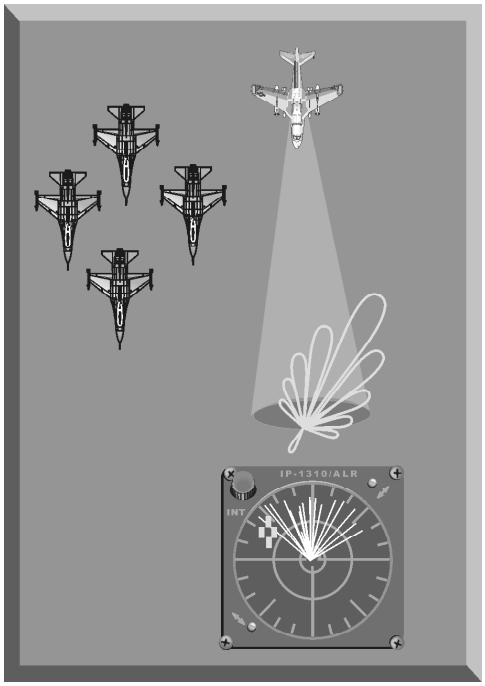


Figure 1-6. Escort Jamming Alignment

b. Self-protection radar jamming targets the radar systems that support jamming cannot negate. Self-protection jamming systems are part of a self-protection suite that includes a self-protection jamming pod, a chaff/flare dispenser, and on some aircraft, a towed decoy system. The overall purpose of these systems is individual aircraft survivability. These systems are designed to counter the individual SAM, AAA, and AI assets associated with the enemy IADS. They employ deception jamming techniques against the target tracking radars (TTRs) associated with these threats. They are designed to break the radar track or generate sufficient tracking errors to cause the missile or bullet to miss the aircraft.

(1) Self-protection radar jamming systems usually employ deception jamming techniques based on several factors. First, effective deception jamming techniques generally require less power than noise jamming techniques. Second, less power means less weight and space, which are very important considerations for modern tactical aircraft. Finally, deception jammers can be designed to jam multiple threats, which is a critical requirement for operations in a dense threat environment (Figure 1-7).

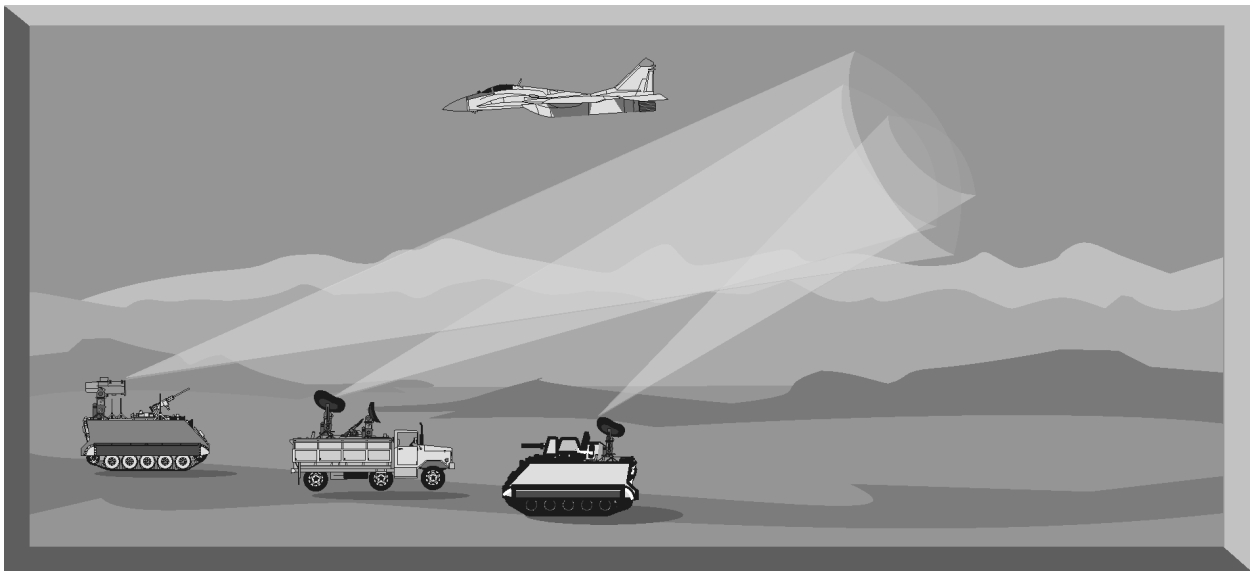


Figure 1-7. Self-Protection Jamming

(2) Despite the advantages of deception jamming techniques for self-protection jamming, there are some limitations that must be considered. First, deception jammers are complex electronic systems that must receive a victim radar's signal, memorize all its characteristics, modify the signal, and retransmit this modified signal at a high power level. Second, to be effective, deception jammers must be programmed with all the signal parameters (frequency, PRF, PRI, pulse width, scan rate, etc.) of the victim radar. Finally, because many deception techniques can be effective against specific threats, selecting optimum techniques to employ against these threats must be based on identified threat

system limitations. Identifying these specific threat systems limitations may be difficult.

4. FUNDAMENTALS OF RADAR JAMMING

There are some fundamental principles that apply to all types of jamming and to all jamming employment options. These principles are based on the characteristics of the jamming system and the characteristics of the victim radar. They include frequency matching, continuous interference, signal-to-noise ratio, jamming-to-signal ratio, and burnthrough range.

a. Based on the data provided by ES systems and intelligence evaluations, radar jamming systems must transmit signals at the frequency of the victim radar This applies to both noise and deception jamming. If a jamming signal does not match the transmitter frequency, the jamming signal is not received and displayed on the scope (Figure 1-8). When a jamming signal matches the transmitter frequency, the jamming signal is received and masks the target display (Figure 1-9).

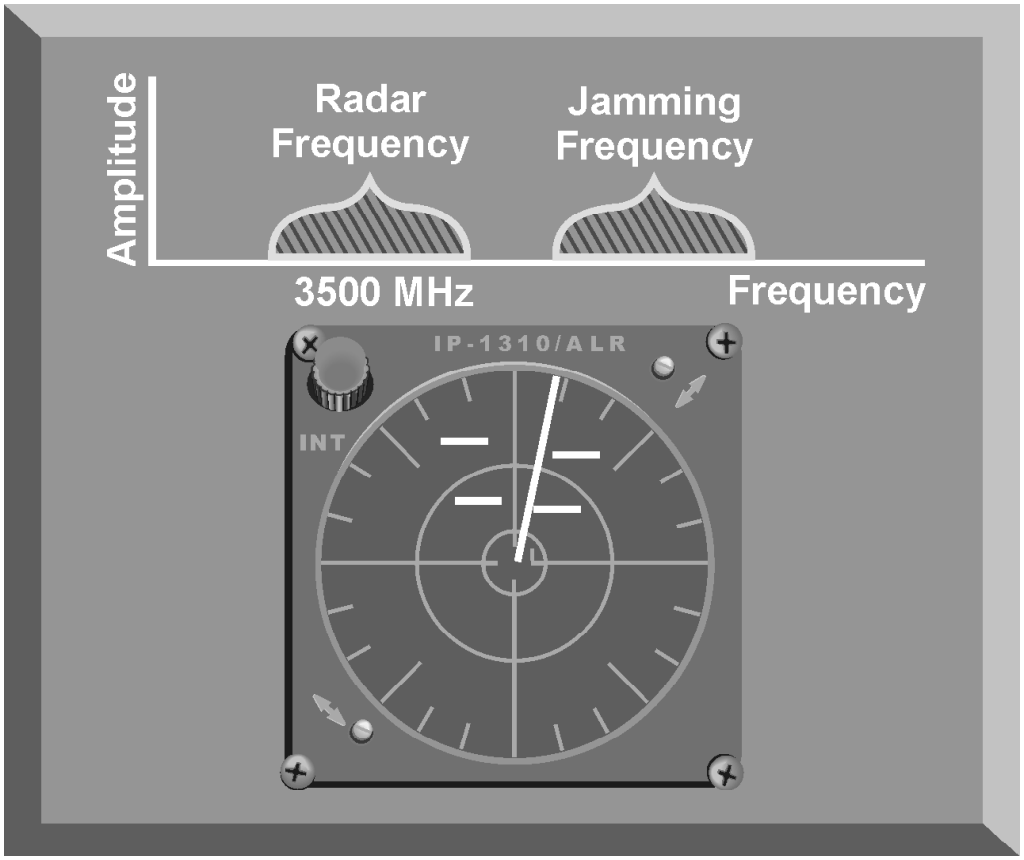


Figure 1-8. Jamming Frequency Error

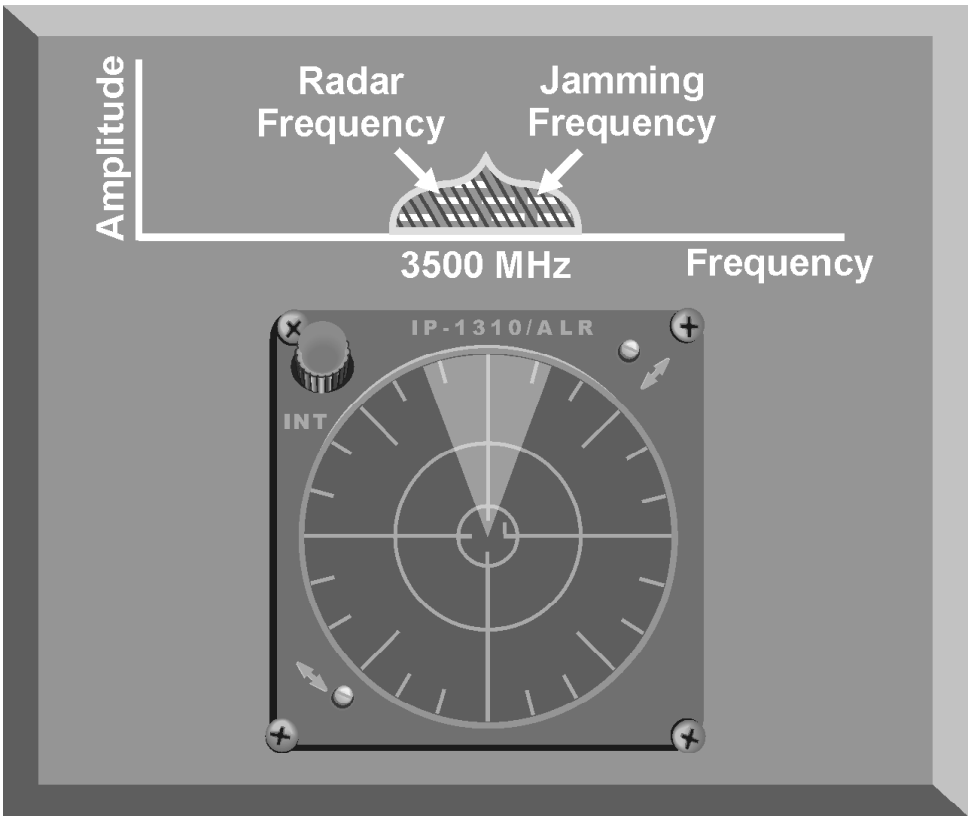


Figure 1-9. Correct Jamming Frequency Matching

b. For maximum effectiveness, a jamming transmitter should produce continuous interference. In much the same way intermittent static on a radio receiver does not completely block out a signal, intermittent jamming on a radar scope may not completely mask the target. An experienced radar operator or advanced automatic tracker can "read through" intermittent jamming and derive sufficient target information to negate jamming effectiveness. While true for noise jamming techniques, continuous interference also applies to deception techniques, especially when target reacquisition is considered.

c. The signal-to-noise (S/N) ratio is a measure of the ability of the victim radar to detect targets. It is also an indication of the vulnerability of the radar to certain jamming techniques, especially noise jamming.

(1) From the discussion of the basic radar equation tought in Radar Theory course before, Eq. 1-1 is the signal power density of a target return at radar receiver. The signal power density of the target return is so weak that it requires very strong amplification before processing and display. Besides the signal power from the target, some level of thermal noise is also generated and amplified along with the target signal. For an "ideal" (no noise) amplifier, Equation 1-2 is used to compute the level of thermal noise generated by the amplifier.

$$\text{Signal Power Density} = \frac{P_T G \sigma A_e}{(4\pi)^2 R^4}$$

P_T = transmitted power
G = antenna gain
σ = target radar cross section (RCS)
A_e = antenna aperture area
R = range to the target

Equation 1-1. Signal Power Density

$$\text{Thermal Noise (N)} = KTBF$$

K = Boltzman's Constant
(1.38 x 10^{-23} watts/Hz degrees K)
T = standard temperature (290° K)
B = radar receiver equivalent bandwidth
F = radar receiver noise figure
(one for "ideal" receiver)

Equation 1-2. Thermal Noise

Note: The instantaneous bandwidth of a receiver is the frequency range over which the receiver can simultaneously amplify two or more signals to within a specified gain.

(2) The radar receiver amplifies both target signal and thermal noise. The output of the radar receiver will contain the target signal and the noise amplified across the bandwidth of the receiver. Separating the desired target signal from the undesired noise signal is one of the major problems confronting radar designers.

(3) Equation 1-3 is derived by dividing Equation 9-1 by Equation 1-2. Many factors in this equation fluctuate and must be estimated using statistical calculations. For example, target RCS fluctuates based on the changing angle of the antenna beam and corresponding changes in the reflected signal. Effective antenna aperture is also a statistical phenomenon based on the fluctuations in target RCS. The thermal noise generated by a receiver is also a fluctuating factor and must be treated statistically. This means that the S/N ratio is a statistical factor associated with a probability of target detection and a probability of a false alarm. A false alarm occurs when the radar operator or automatic tracking circuit designates a fluctuation in noise level as a target. The higher the S/N ratio, the

higher the probability of target detection with a corresponding reduction in the probability of a false alarm.

$$\text{Signal-to-Noise Ratio} = \frac{P_T G \sigma A_e \left(\frac{1}{(4\pi)^2 R^4} \right)}{KTBF}$$

P_T = transmitted power
G = antenna gain
σ = target radar cross section (RCS)
A_e = antenna aperture area
R = range to the target

K = Boltzman's Constant
(1.38 x 10^{-23} watts/Hz degrees K)
T = standard temperature (290° K)
B = radar receiver equivalent bandwidth
F = radar receiver noise figure
(one for "ideal" receiver)

Equation 1-3. Signal-to-Noise Ratio

(4) An analysis of Equation 1-3 suggests that any action that increases the power in the target signal (for example, increasing transmitted power, increasing antenna gain/aperture area, or decreasing target range) will improve the S/N ratio and improve the probability of target detection. It would also appear that decreasing the bandwidth of the radar receiver will increase the S/N ratio and enhance the probability of target detection. However, if the effective bandwidth of the receiver is reduced, this may eliminate a significant portion of the radar signal spectrum and decrease the probability of target detection.

(5) The S/N ratio is also an indication of the range at which a target will be detected. A plot of the receiver output of a typical radar is shown in Figure 1-10. The weak target signal at an extended range is just above the receiver noise level. The target at closer range is easily detected above the noise level. A radar operator or automatic target detector could mistake the very weak target return as a fluctuation in the receiver noise level. This could result in a missed detection. The lack of discrimination between noise and target returns because of a poor S/N ratio can also result in designating fluctuations in the noise level as actual target signals, known as false alarms.

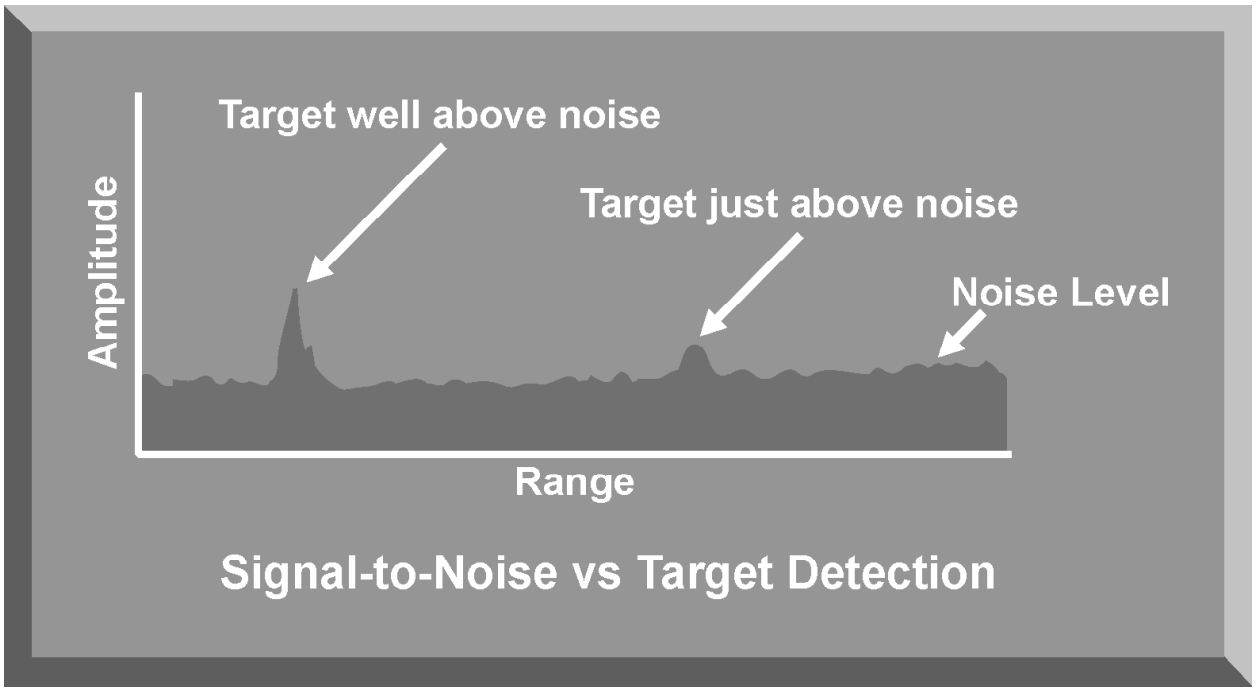


Figure 1-10. S/N Ratio and Target Detection

(6) To preclude, or minimize false alarms, the radar receiver may be equipped with electronic circuits to establish a false alarm threshold. If the signal strength of a radar return is below this threshold level, it will not be detected or displayed (Figure 1-11). This false alarm threshold also influences the probability of target detection. With the threshold set too high, many detected targets will not be displayed. Additionally, if the false alarm threshold is raised automatically in relation to the amplitude of the receiver noise, the radar receiver is more vulnerable to noise jamming.

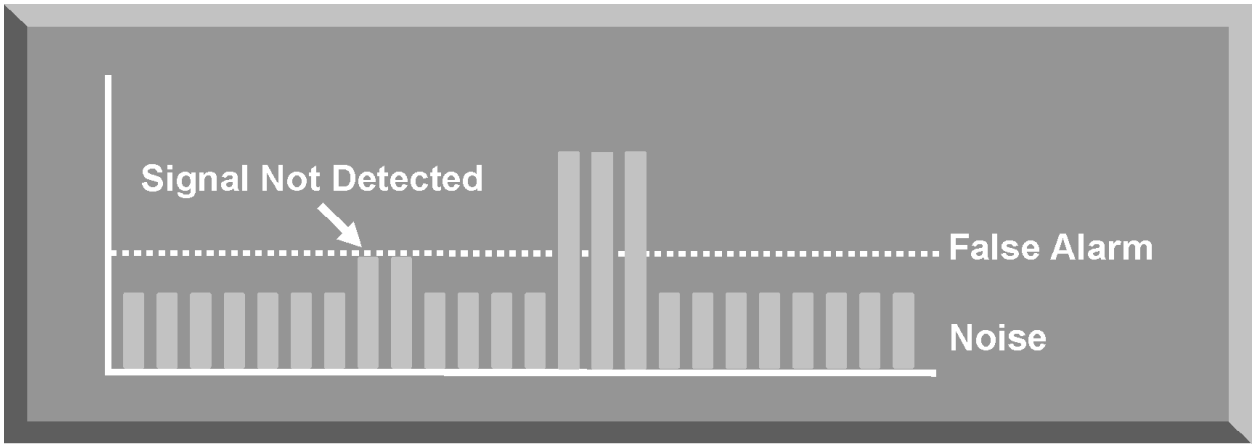


Figure 1-11. Receiver False Alarm Threshold

(7) For any target return to be detected by the radar, the S/N ratio must be greater than one. If the S/N ratio is less than one, the target will not be detected above the receiver noise level. The purpose of noise jamming is to raise the level of noise in the radar receiver to reduce the S/N ratio to less than one. This masks the presence of the true target return. If a false alarm threshold is used, noise jamming raises this threshold to further complicate target detection. Figure 1-12 depicts a S/N ratio greater than one. Figure 1-13 depicts a S/N ratio of less than one due to noise jamming.

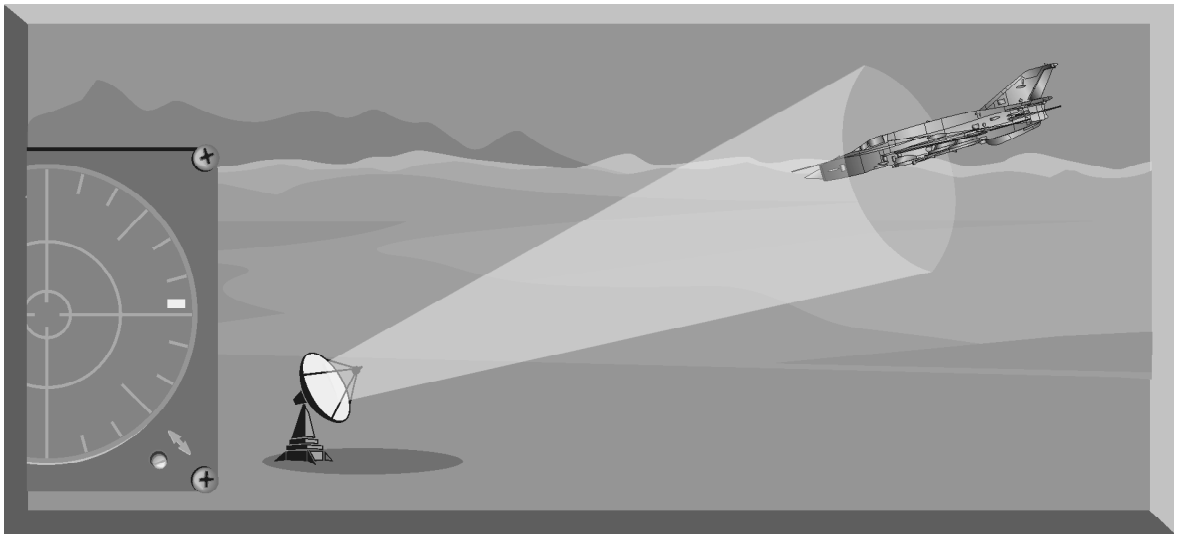


Figure 1-12. S/N Ratio Greater Than One

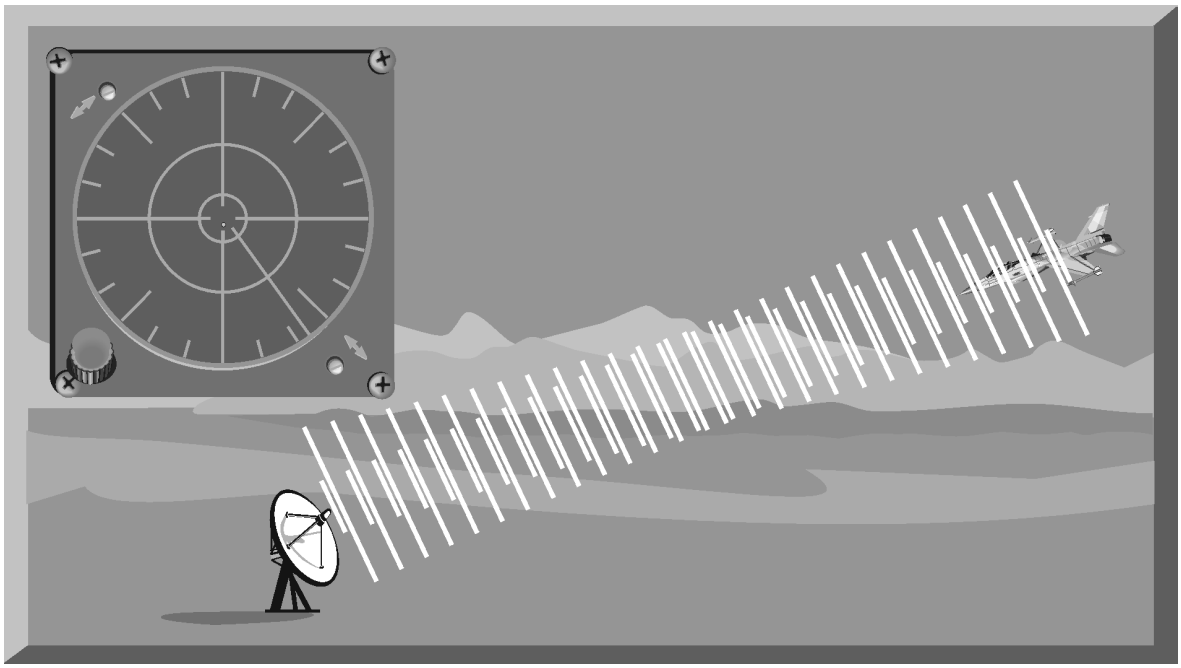


Figure 1-13. S/N Ratio Less Than One

d. The jamming-to-signal (J/S) ratio is a fundamental measure of jamming effectiveness. The J/S ratio compares the power in the jamming signal with the power in the radar return. Equation 1-4 is an expression of the J/S ratio. It is important to note that the J/S ratio should be measured at the output of the radar receiver. This will allow consideration of the receiver signal processing gain applied to the jamming signal.

$$\text{Jamming-to-Signal Ratio} = \frac{P_J G_J}{P_T G_T} \times \frac{4\pi R^2}{\sigma}$$

P_J = jamming power transmitted
G_J = jamming antenna gain
P_T = peak power transmitted by the radar
G_T = radar antenna gain
R = range from jammer to radar
σ = aircraft RCS

Equation 1-4. Jamming-to-Signal Ratio

(1) The most critical factor in both the S/N and the J/S ratios is range. The S/N ratio is calculated based on R to the fourth power. This equates to a signal traveling from the radar to the target, and back to the radar receiver. The J/S ratio is calculated using R to the second power. This factor reflects the "one way" transmission of the jamming pulse from the jammer to the victim radar's receiver.

(2) For a jamming signal to be effective, the J/S ratio must be greater than one. In general, threat radars, especially ground-based radars, transmit much more power than does an airborne jamming system. However, this power must travel twice as far as the airborne jamming signal. At long ranges, a low power jamming system can generate a J/S ratio much greater than one. In Figure 1-14, the jamming pulse completely masks the target return. As the jamming system approaches the target, the distance the radar pulse travels decreases with a corresponding increase of power in the radar return. This reduces the J/S ratio to a value less than one and the radar "sees" the target. This is called the burnthrough range (Figure 1-15).

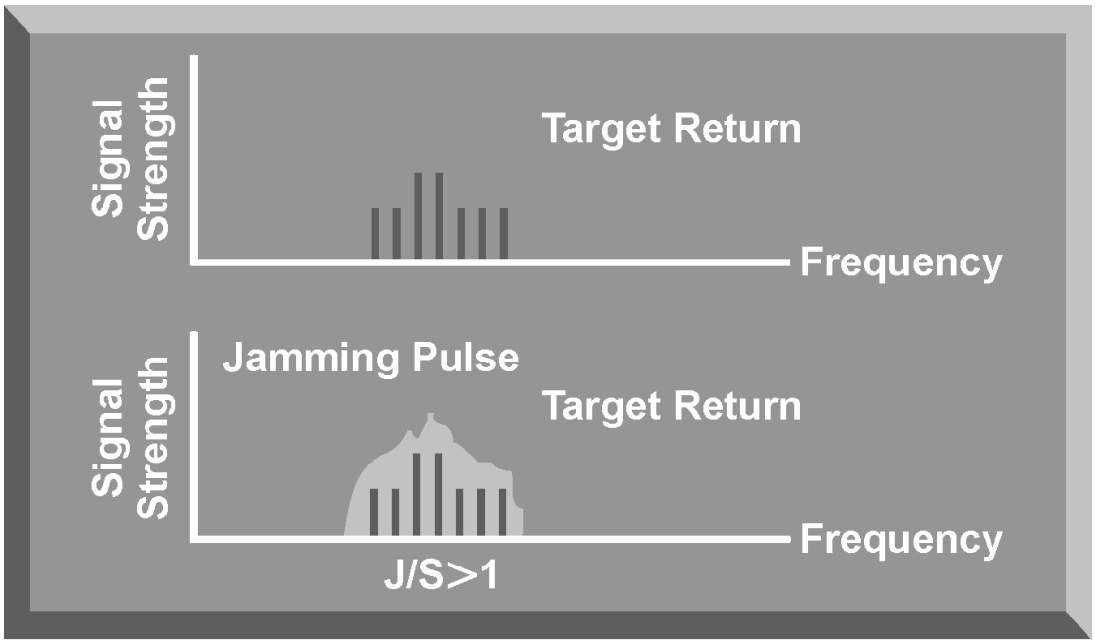


Figure 1-14. J/S Ratio Greater Than One

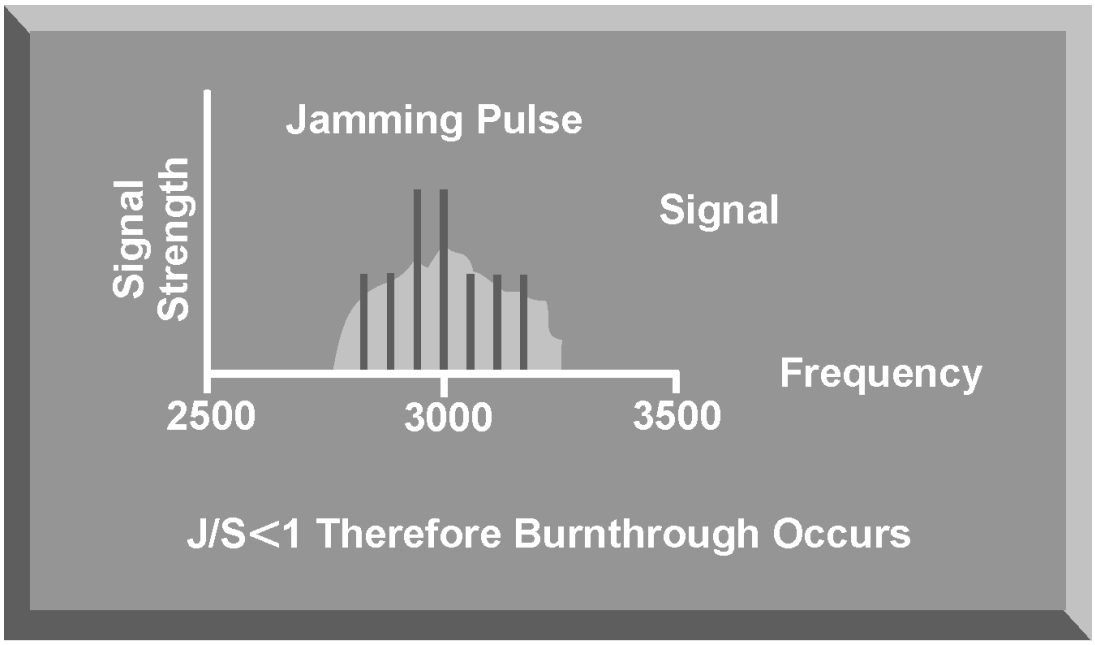


Figure 1-15. J/S Ratio Less Than One

e. Burnthrough occurs when the power in the reflected target signal exceeds the power in the jamming signal. Even when an optimum and continuous jamming technique is transmitting on the exact frequency of the victim radar, the jamming starts to lose effectiveness as it nears the radar. For a particular radar

jamming technique, burnthrough range depends on the detection capability of the victim radar, expressed as the S/N ratio, and the capability of the aircraft's jamming system, expressed as the J/S ratio. The idea of burnthrough range explains why a jamming technique, especially noise jamming, loses its effectiveness as the aircraft approaches the radar. When plotting the jamming and signal power versus range (Figure 1-16), these two values intersect at the point where the J/S ratio is one. At closer ranges, the jamming pulse is no longer masking the aircraft, and the aircraft can be detected. Burnthrough range is the point where the radar can see through the jamming.

Figure 1-16. Burnthrough Range

5. SUMMARY

The purpose of radar jamming is to confuse or deny critical data to the radar systems that play a vital role in supporting the mission of an integrated air defense system. Two types of radar jamming, noise and deception, can be employed in a support-jamming role, or in a self-protection role for individual aircraft. The effectiveness of a jamming technique depends on the ability of the jamming system to generate a jamming signal that replicates the parameters of the victim radar, especially its frequency. The signal-to-noise ratio of the victim radar determines the vulnerability of the radar receiver to jamming while the jamming-to-signal ratio is an indication of the ability of the jamming system to effectively jam the victim radar. These basic radar jamming concepts are fundamental to understanding the impact of specific jamming techniques on radar systems.

CHAPTER 10. RADAR NOISE JAMMING

1. INTRODUCTION

A radar noise jamming system is designed to generate a disturbance in a radar receiver to delay or deny target detection. Since thermal noise is always present in the radar receiver, noise jamming attempts to mask the presence of targets by substantially adding to this noise level. Radar noise jamming can be employed by support jamming assets or as a self-protection jamming technique. Radar noise jamming usually employs high-power jamming signals tuned to the frequency of the victim radar. This chapter will discuss the factors that determine the effectiveness of radar noise jamming, radar noise jamming generation, and the most common noise jamming techniques. These noise jamming techniques include barrage, spot, swept spot, cover pulse, and modulated noise jamming.

2. RADAR NOISE JAMMING EFFECTIVENESS

The effectiveness of radar noise jamming depends on numerous factors. These factors include the jamming-to-signal (J/S) ratio, power density, the quality of the noise signal, and the polarization of the transmitted jamming signal (Figure 10-1).

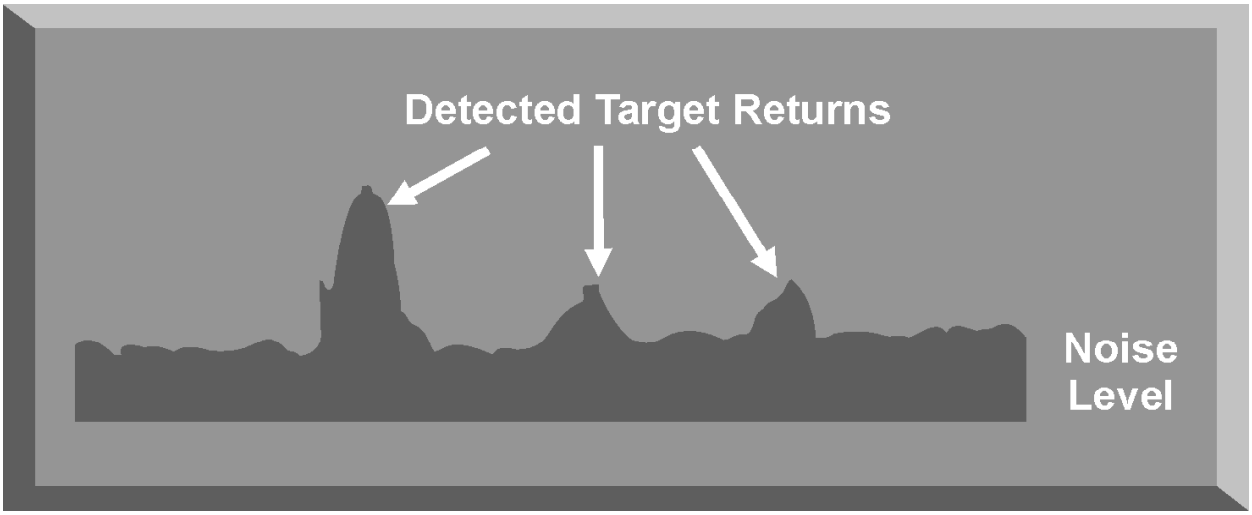


Figure 10-1. Noise Level in a Typical Radar Receiver Output

a. One of the most important factors that impacts the effectiveness of radar noise jamming is the J/S ratio (Figure 10-2). As discussed in Chapter 9, the power output of the noise jammer must be greater than the power in the target return, as measured at the output of the radar receiver. To achieve this level of jamming power, radar noise jammers usually generate high-power jamming signals. These high-power jamming signals can be introduced into the victim radar's main beam

to deny range information and into the victim radar's sidelobes to deny azimuth information.

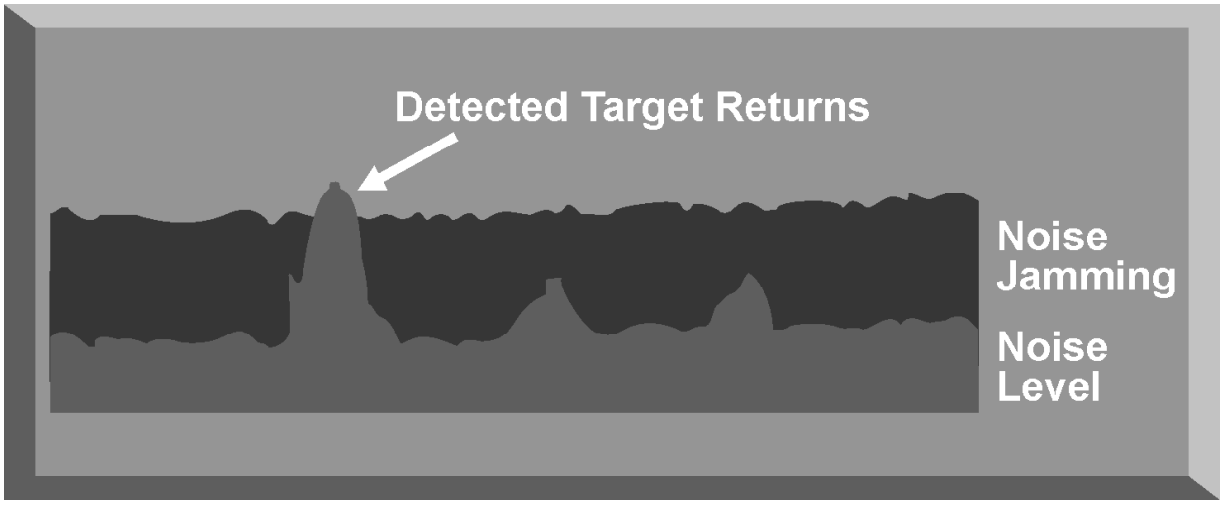


Figure 10-2. Impact of Noise Jamming

b. Another factor which impacts the effectiveness of radar noise jamming is the power density. The power density of the noise jamming signal has a direct relation to the J/S ratio.

(1) If the noise jamming signal is centered on the frequency and bandwidth of the victim radar, the jamming signal has a high power density. The ability of a noise jammer to concentrate the jamming signal depends on the ability of the jammer to identify the exact frequency and bandwidth of the victim radar (Figure 10-3).

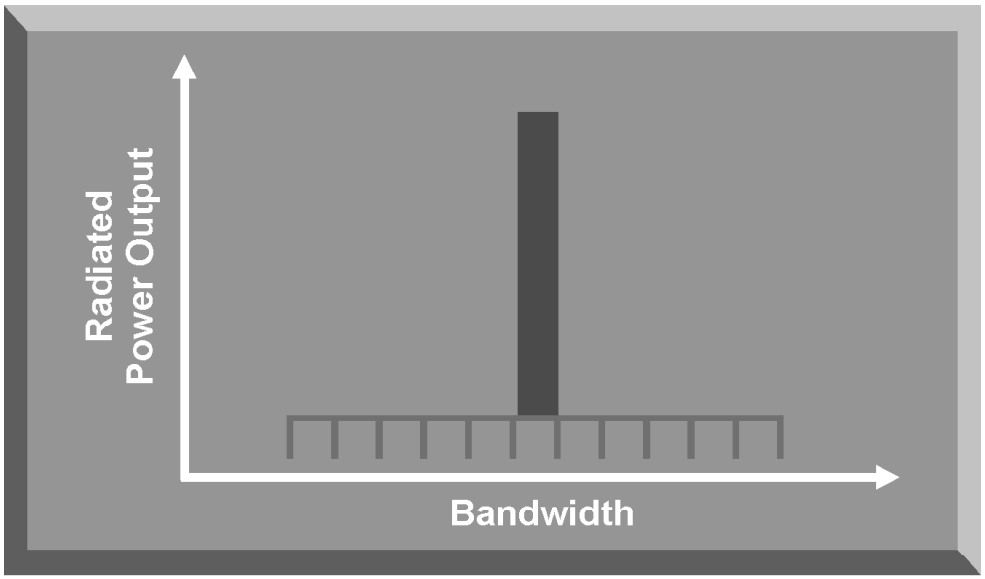


Figure 10-3. Power Density – Narrow Bandwidth

(2) If the generated noise jamming signal has to cover a wide bandwidth or frequency range, the power density at any one frequency is reduced (Figure 10-4). Radar systems that are frequency agile or that employ a wide bandwidth can reduce, or negate, the effectiveness of noise jamming by reducing the power density of the jamming signal.

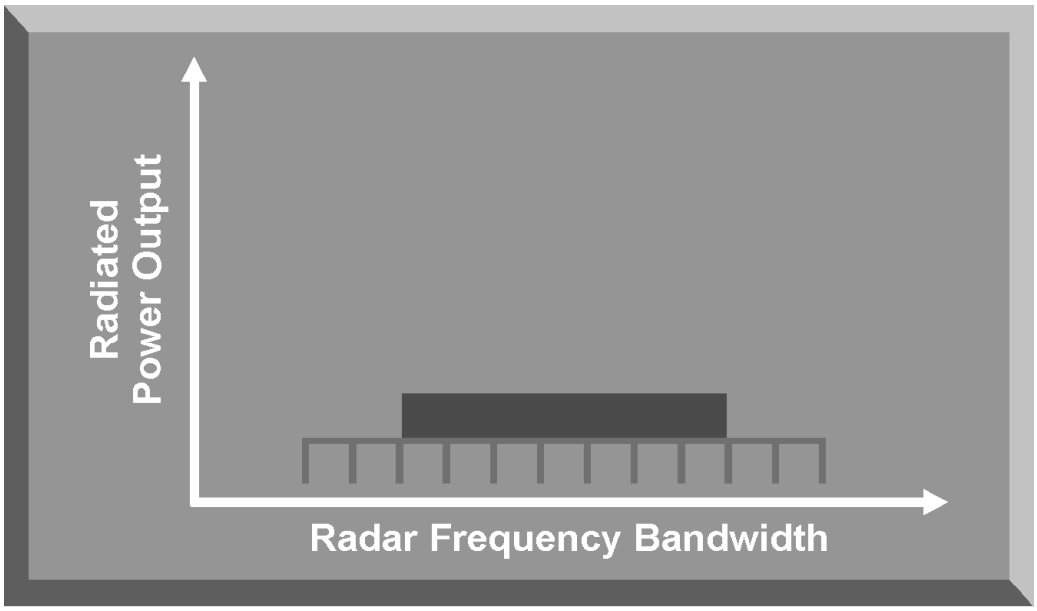


Figure 10-4. Power Density – Wide Bandwidth

c. The quality of the noise jamming also determines its effectiveness. To effectively jam a radar receiver with noise, the jamming signal must emulate the thermal noise generated by the receiver. This ensures that the radar operator or automatic detection circuit cannot distinguish between the noise jamming and normal thermal noise. Thermal noise is referred to as white noise and has a uniform spectrum. All of the frequencies in the bandwidth of the receiver have the same spectrum and an amplitude that varies based on Gaussian distribution. A Gaussian distribution is simply a bell-shaped distribution of amplitudes. In order to be effective, the jamming signal should exactly match the characteristics of the thermal noise signal of the victim radar receiver.

d. Polarization of the noise jamming signal is another significant factor that impacts its effectiveness. As discussed in Chapter 2, if the polarization of the jamming signal does not match the antenna polarization of the victim radar, there is a significant power loss in the jamming signal. Noise jamming systems designed to counter multiple threat radars, with various polarizations, generally use a transmitting antenna with a 45° slant or use circular polarization. Most threat systems are horizontally or vertically polarized. This results in a 50% reduction in effective radiated power (ERP) for most threat systems. A more serious power loss, nearly 100%, in ERP occurs when the jamming antenna is

orthogonally polarized with the victim antenna. The polarization of the noise jamming signal impacts the J/S ratio and the power density.

3. RADAR NOISE JAMMING GENERATION

Noise jamming is produced by modulating an RF carrier wave with random amplitude or frequency changes, called noise, and retransmitting that wave at the victim radar's frequency. Since noise from numerous sources is always present and displayed on a radar scope, noise jamming adds to the problem of target detection. Reflected radar pulses from target aircraft are extremely weak. To detect these pulses, a radar receiver must be very sensitive and be able to amplify the weak target returns. Noise jamming takes advantage of this radar characteristic to delay or deny target detection.

a. The simplest method of generating a high-power Gaussian noise jamming signal is to employ a highly amplified diode to generate a noise signal at the frequency of the victim radar. This signal is filtered and directly amplified to the maximum power that can be generated by the transmitter. This method is called direct noise amplification (DINA). The DINA method of noise generation has a serious limitation. The maximum power available from linear wideband power amplification is extremely limited. Employing any other form of power amplification would alter the Gaussian distribution of the jamming signal. This method of generating radar noise jamming was used extensively during WW II.

b. Modern noise jamming systems generate noise jamming signals by frequency modulating a carrier wave at the frequency of the victim radar. FM noise jammers employ a receiving antenna to intercept the victim's radar signal. The antenna passes the victim radar signal to the receiver for identification. The receiver also tunes the jamming signal generator to the correct frequency. The receiver uses an automatic frequency control (AFC) circuit to tune the voltage-controlled oscillator (VCO) to the frequency of the victim radar. A noise signal is generated by the jamming signal generator and added to the tuning voltage of the VCO to get an FM jamming signal. This signal is sent to a traveling wave tube (TWT) power transmitter. The TWT is normally operated in a saturated mode which produces a high-power jamming signal that covers a wider bandwidth than the victim radar. This reduces the power density of the signal, but the high power levels available from the TWT amplification of an FM signal compensate for this loss. The signal is sent to the transmitting antenna and directed toward the victim radar.

c. Figure 10-5 highlights an important feature of a modern radar noise jamming system: a look-through capability. A look-through mode allows the receiver to periodically sample the signal environment. The objective of the look-through mode is to allow the jammer to update victim radar parameters and change the jamming signal to respond to changes in the signal environment. This greatly enhances the effectiveness of noise jamming systems. One method used to provide a look-through capability is to isolate the transmit and receive

antennas to allow continuous operation of the receiver to update signal parameters. Another method is to switch off the jammer for a brief period to allow the receiver to sample the signal environment. Since this latter look-through method eliminates the jamming signal, the amount of time the jammer is switched off must be kept to a minimum.

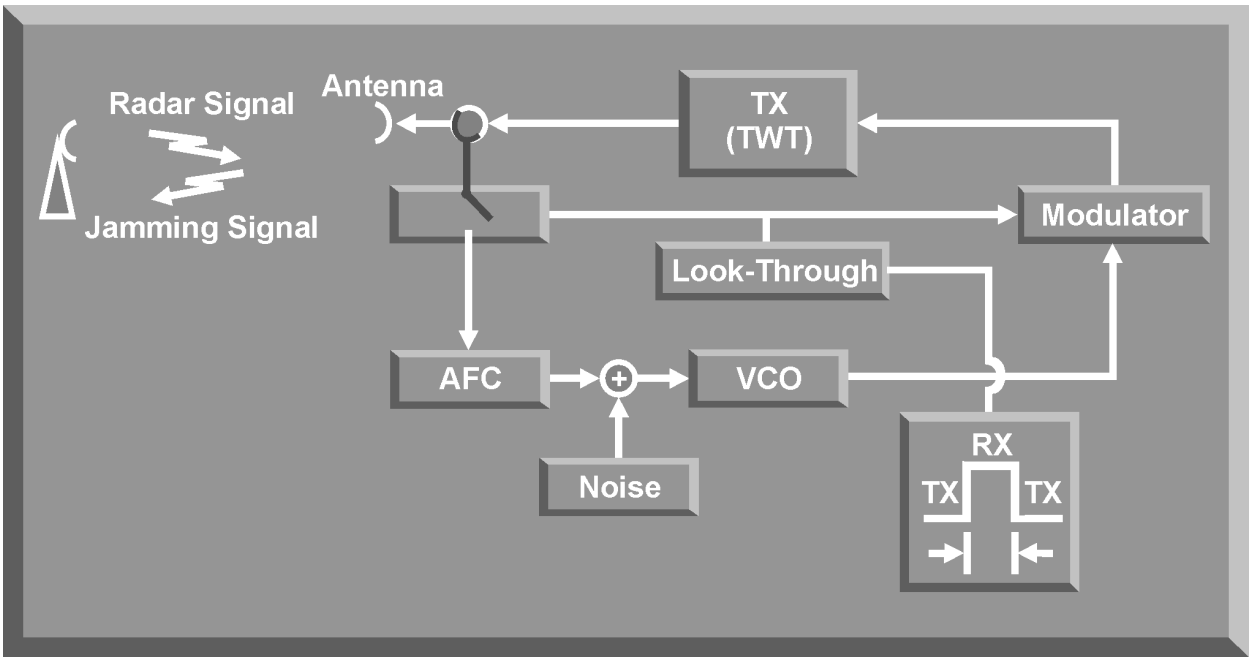


Figure 10-5. Frequency Modulated (FM) Noise Jamming System

4. BARRAGE JAMMING

An important aspect of jamming power is power density. Noise jamming depends on power density for its effectiveness. Power density is a function of the frequency range, or bandwidth, of the jamming signal. If a jammer covers a narrow frequency range, it can concentrate energy in a narrow band. If a jammer covers a wide frequency range, the energy is spread over that entire range. Since the jammer has fixed radiated power, this lowers the effective jamming power at a given frequency. Barrage jamming is a jamming technique where high power is sacrificed for the continuous coverage of several radar frequencies (Figure 10-6). The jamming signal is spread over a wide frequency range, which lowers the ERP at any one frequency. This type of jamming is useful against frequency-agile radars, against a radar system that uses multiple beams, or against multiple radar systems operating in a specific frequency range. By spreading the jamming over a wide frequency range, there is some level of jamming no matter what frequency the radar uses. Barrage jamming was used extensively during World War II. Advantages of barrage jamming are its simplicity and ability to cover a wide portion of the electromagnetic spectrum. The primary disadvantage is the low power density, especially when a high J/S ratio is needed against modern radars.

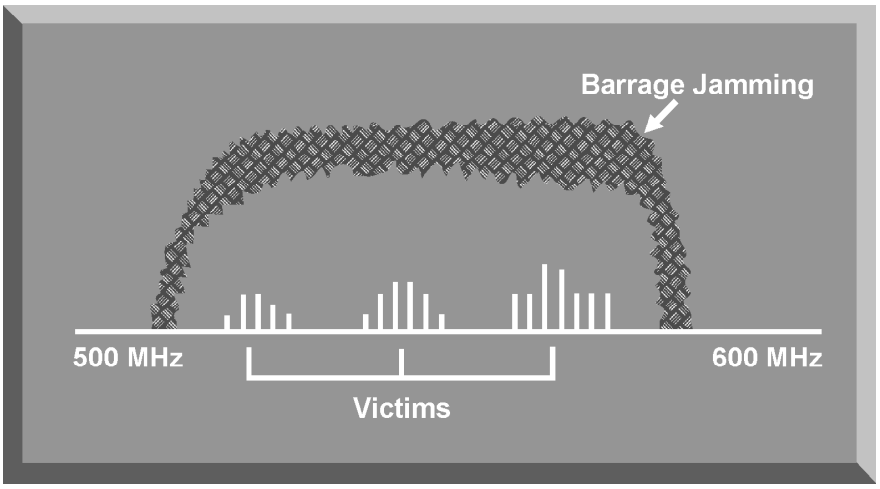


Figure 10-6. Barrage Jamming

5. SPOT JAMMING

One way to take advantage of the noise jammer's simplicity, but raise the jamming signal power, is to use a spot jammer. The earliest spot jammers were very narrow band jammers covering a bandwidth of 10 megahertz or less (Figure 10-7). This narrow band spot jammer was tuned to the anticipated frequency of the target radar. When it is necessary to jam a number of radars at different frequencies, more than one jammer is used. One problem that developed was of carrying the required number of spot jammers to counter a modern IADS. Also, radars that change their operating frequency, or are frequency-agile, defeat the spot jammer. Today, intercept panoramic receivers work with spot jammers to determine the frequency of the victim radar. A look-through capability is included in the system so that the target radar signal can be monitored to assess jamming effectiveness. The jamming signal can be adjusted for any changes in the operating frequency of the radar.

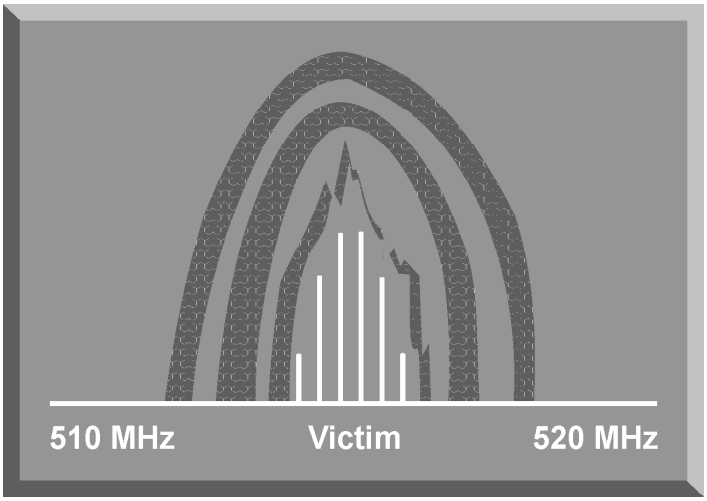


Figure 10-7. Spot Jamming

a. The primary advantage of spot jamming is its power density. Radar or communications receivers can be countered at longer ranges than when using a barrage jammer of equal output power (Figure 10-8).

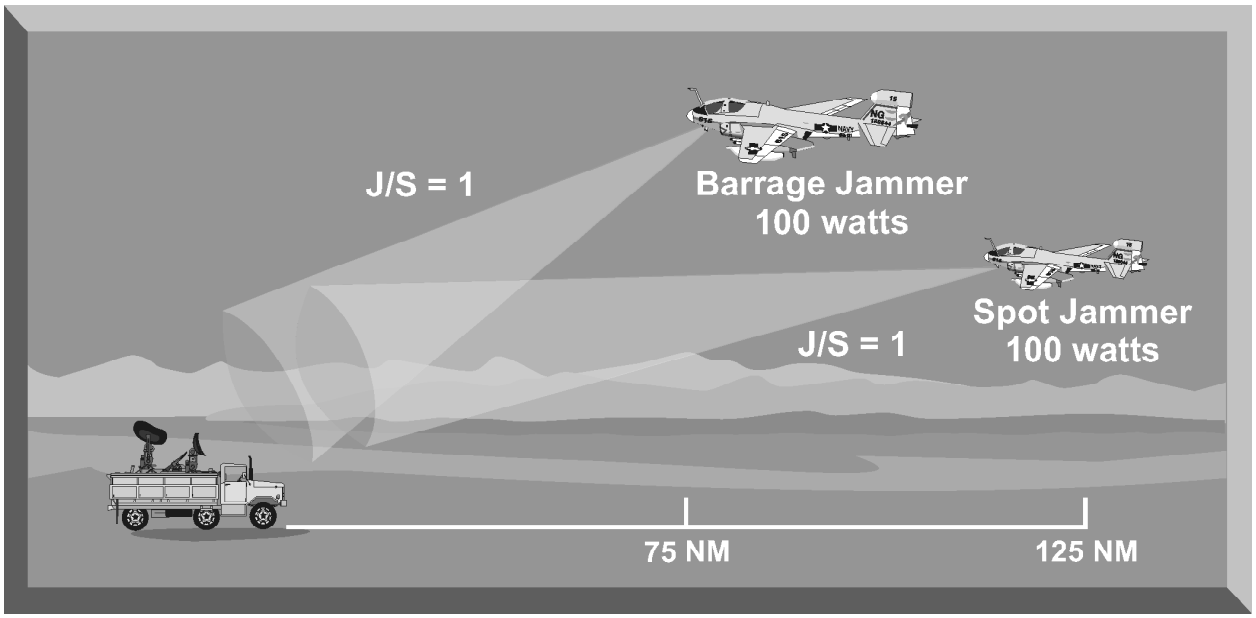


Figure 10-8. Spot Jamming Effectiveness

b. A disadvantage of the spot jammer is its coverage of a narrow band of the frequency spectrum. An operator or computer in the receiver must constantly monitor and tune the jamming signal to the target radar's frequency. The complexity of this process increases when jamming frequency-agile radars that can change frequencies with every pulse.

6. SWEPT-SPOT JAMMING

When high power density is required over a large bandwidth, one solution is to take spot jamming and sweep it across a wide frequency range (Figure 10-9). This preserves the high power density but allows the jamming to cover a large bandwidth. The jamming spot is swept across a broad frequency range at varying speeds. With this technique, a number of radar systems can be covered. Because of their high jamming power, swept-spot jammers are able to cover a number of radars operating in a broad frequency range. However, jamming is not continuous. Fast swept-spot jamming can approximate continuous jamming by causing a phenomenon known as "ringing." Fast sweeping spot noise is like a burst of energy which sets up vibrations within the receiver section. When these vibrations last until the next burst of energy is received, this is known as ringing. Three factors determine swept-spot jamming effectiveness. The first is the power in the spot. The next is the bandwidth, or frequency range, the spot covers. The last is the sweep rate.

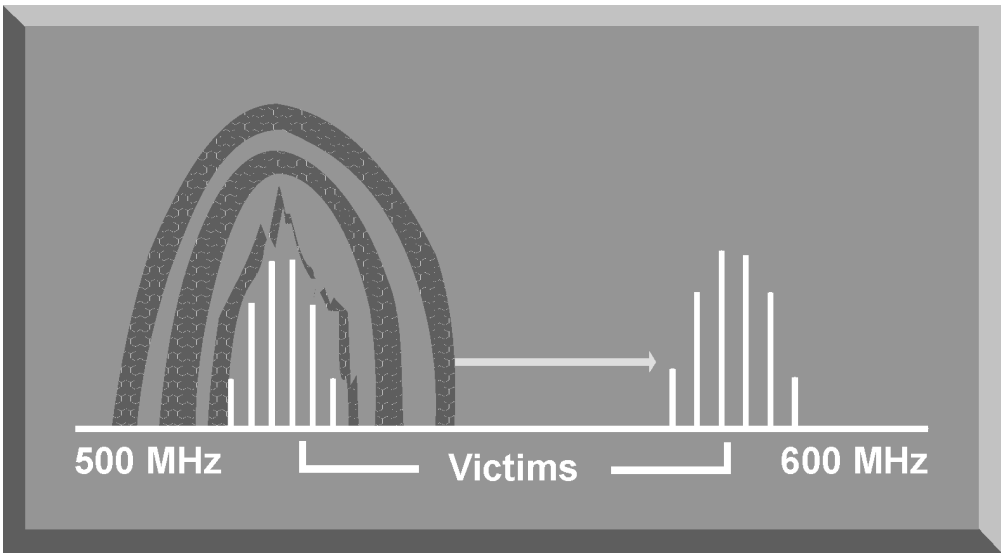


Figure 10-9. Swept-Spot Jamming

7. COVER PULSE JAMMING

Cover pulse jamming is a modification of swept-spot jamming. This is a "smart noise" technique that is responsive for a short period of time (Figure 10-10). A repeater jammer acts as a transponder. It receives several radar pulses and determines the PRF of the victim radar. It then uses this data to predict when the next radar pulse should arrive. Using an oscillator that is gated for a period of time based on predicted pulse arrival time, a noise-modulated signal is amplified and transmitted. This process works against a radar with a steady PRF, and allows a low-powered repeater to respond to a number of threats by time-sharing.

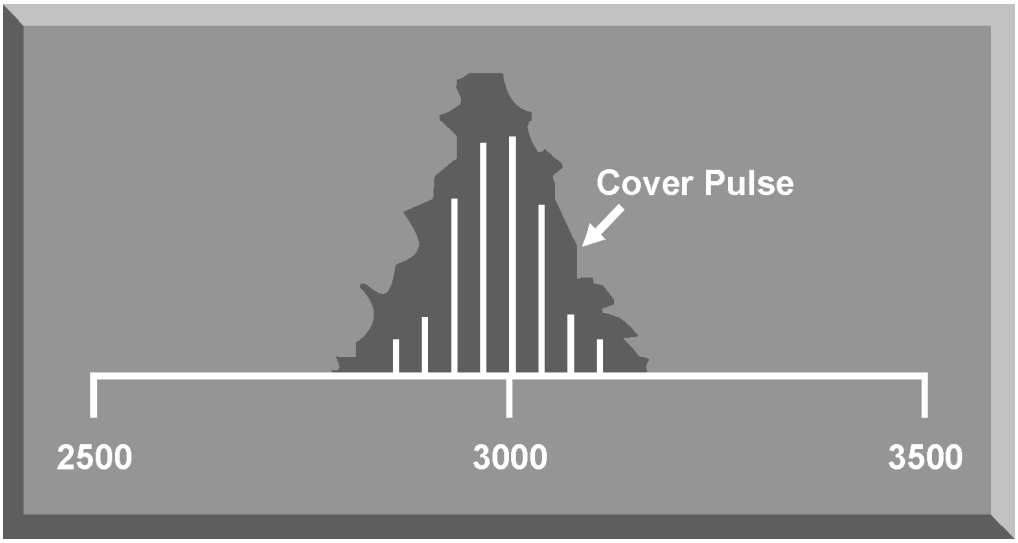


Figure 10-10. Cover Pulse Jamming

a. Cover pulse jamming is used to initiate a range gate pull-off (RGPO) deception jamming technique. The deception jammer transmits a noise jamming signal, or cover pulse, that is much stronger than the target return. The cover pulse raises the automatic gain inside the range gate, and the range tracking loop initiates tracking on the cover pulse. The deception jammer then increases the time delay in the jamming pulse and moves the range tracking gate away from the real target (Figure 10-11).

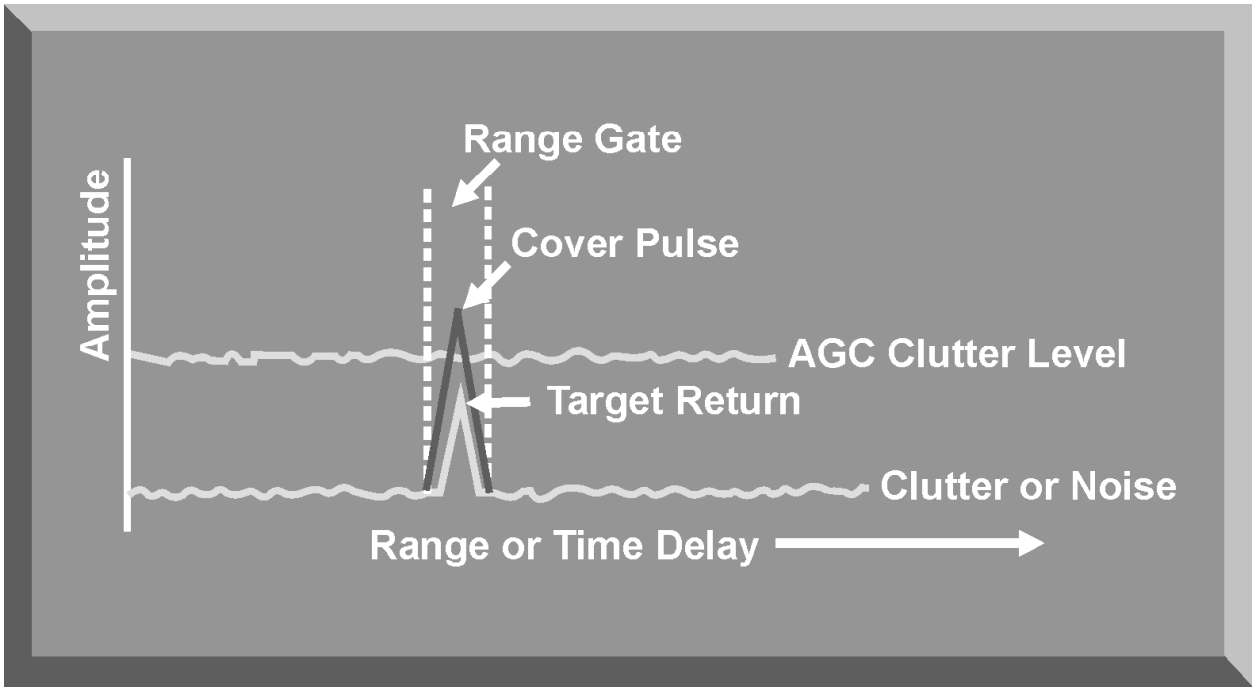


Figure 10-11. Range Gate Pull-Off Cover Pulse

b. A form of cover pulse jamming is also used to initiate a velocity gate pull-off (VGPO) technique against continuous wave and pulse Doppler radars. The cover pulse, in this case, is a strong jamming signal with the same frequency shift as the aircraft return. This cover pulse steals the velocity tracking gate and sets up the velocity tracking loop to steal the velocity tracking gate based on false target Doppler shifts (Figure 10-12).

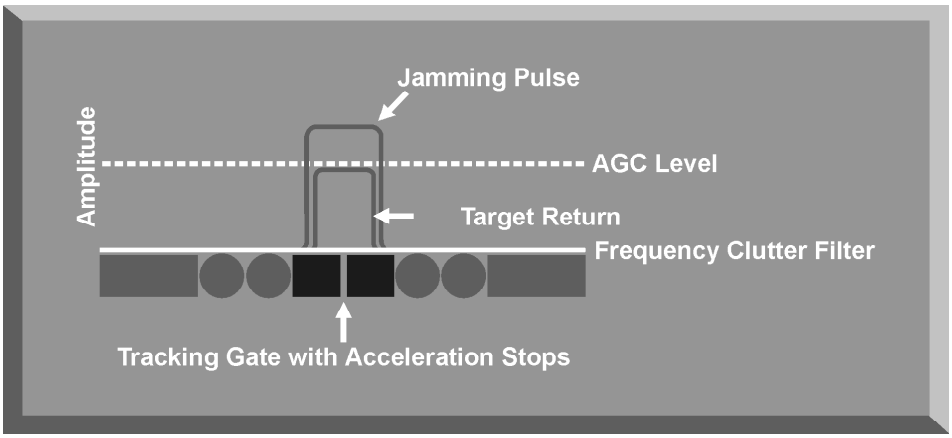


Figure 10-12. Velocity Gate Pull-Off Cover Pulse

8. MODULATED NOISE JAMMING

Modulated jammers are special hybrid jammers which employ noise jamming that is either amplitude or frequency modulated. The purpose of this modulated noise is to defeat target tracking radars (TTRs) rather than deny range information. Modulated noise jamming has proven effective against conical scan and track-while-scan (TWS) TTRs.

a. Modulated jamming alters the noise jamming signal at a frequency that is related to the scan rate of the target radar. If modulated jamming is used against a conical scan radar, a sine wave signal is used (Figure 10-13). The frequency of the sine wave is slightly higher than the scan rate of the victim radar. The amplitude difference results in a constantly varying phase between the radar and the jamming signal. This phase differential produces false targets with a strong signal amplitude everywhere the signals reinforce each other. This causes the conical scan radar to track the false returns and lose the real target return. For this technique to work, the scan rate of the intended victim radar must be known.

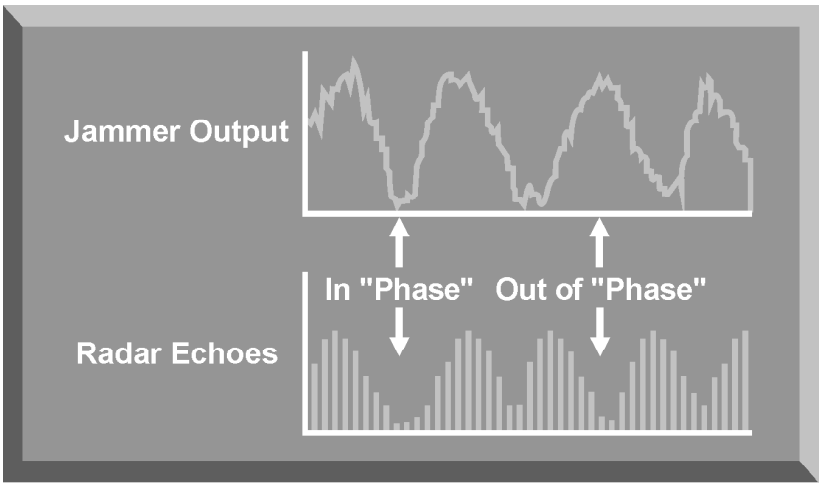


Figure 10-13. Conical Scan Modulated Jamming

b. Against a TWS radar, a rectangular waveform is used to modulate the noise signal. The PRF of the modulation is set at some harmonic of the TWS rate. This synchronization results in a number of jamming strobes on the radar scope. Each jamming strobe is at a different azimuth or elevation depending on which radar beam is being jammed. The number of jamming strobes depends directly on the harmonic used to modulate the signal. In Figure 10-14, a modulating signal frequency that is four times the scan rate of the radar will produce four jamming strobes on the scope. If the jamming is slightly out of tune with the scan rate, the jamming strobes will appear to roll across the radar scope.

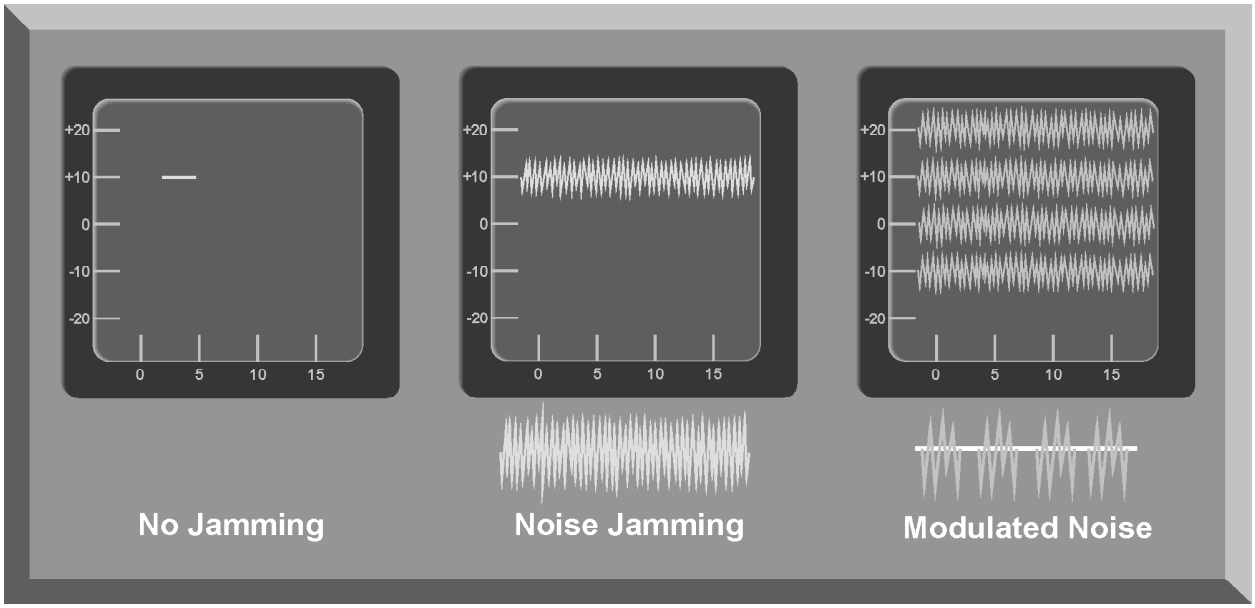


Figure 10-14. TWS Modulated Jamming

9. SUMMARY

Radar noise jamming is employed to deny target acquisition and target tracking data to a victim radar. This is accomplished by injecting amplitude or frequency modulated noise jamming signals into the victim radar's receiver. The radar noise jamming techniques discussed in this chapter included barrage, spot, swept-spot, cover pulse, and modulated jamming. The effectiveness of these noise jamming techniques depends on the power density of the jamming signal compared to the power in the radar return, or the J/S ratio. Radar noise jammers are generally simple, high-power systems which can be effectively employed in a support or self-protection role. Radar noise jamming can be employed in conjunction with deception jamming techniques to maximize the impact of jamming on victim radars.

CHAPTER 11. DECEPTION JAMMING

1. INTRODUCTION

Deception jamming systems are designed to inject false information into a victim radar to deny critical information on target azimuth, range, velocity, or a combination of these parameters. To be effective, a deception jammer receives the victim radar signal, modifies this signal, and retransmits this altered signal back to the victim radar. Because these systems retransmit, or repeat, a replica of the victim's radar signal, deception jammers are known as repeater jammers. The retransmitted signal must match all victim radar signal characteristics including frequency, pulse repetition frequency (PRF), pulse repetition interval (PRI), pulse width, and scan rate. However, the deception jammer does not have to replicate the power of the victim radar system.

a. A deception jammer requires significantly less power than a noise jamming system. The deception jammer gains this advantage by using a waveform that is identical to the waveform the radar's receiver is specifically designed to process. Therefore, the deception jammer can match its operating cycle to the operating cycle of the victim radar instead of using the 100% duty cycle required of a noise jammer. To be effective, a deception jammer's power requirements are dictated by the average power of a radar rather than the peak power required for a noise jammer. In addition, since the jammer waveform looks identical to the radar's waveform, it is processed like a real return. The jamming signal is amplified by the victim radar receiver, which increases its effectiveness. The reduced power required for effective deception jamming is particularly significant when designing and building self-protection jamming systems for tactical aircraft that penetrate a dense threat environment. Deception jamming systems can be smaller, lighter, and can jam more than one threat simultaneously. These characteristics give deception jammers a great advantage over noise jamming systems.

b. Although deception jammers require less power, they are much more complex than noise jammers (Figure 11-1). Memory is the most critical element of any deception jammer. The memory element must store the signal characteristics of the victim radar and pass these parameters to the control circuitry for processing. This must be done almost instantaneously for every signal that will be jammed. Any delay in the memory loop diminishes the effectiveness of the deception technique. Using digital RF memory (DRFM) reduces the time delay and enhances deception jammer effectiveness. Deception jamming employed in a self-protection role is designed to counter lethal radar systems. To be effective, deception jamming systems must be programmed with detailed and exact signal parameters for each lethal threat.

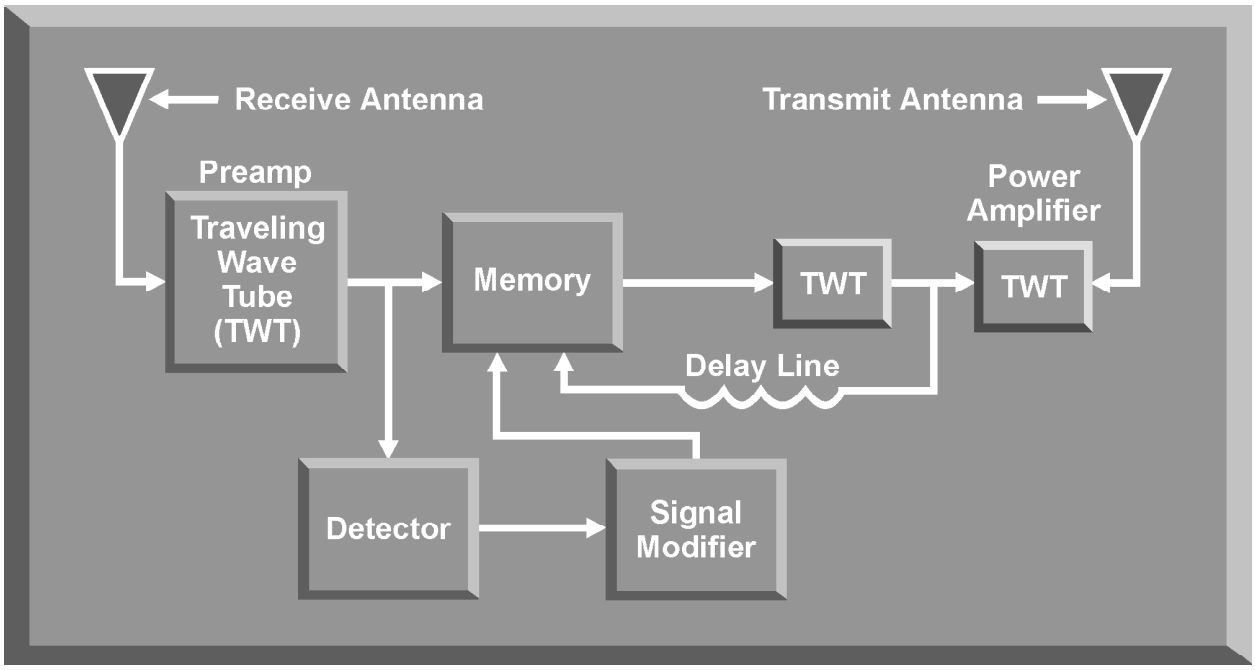


Figure 11-1. Deception Jamming System

c. The requirement for exact signal parameters increases the burden on electronic warfare support (ES) systems to provide and update threat information on operating frequency, PRF, PRI, power pulse width, scan rate, and other unique signal characteristics. An electronic intelligence (ELINT) architecture is required to collect, update, and provide changes to deception jamming systems. In addition, intelligence and engineering information on exactly how a specific threat system acquires, tracks and engages a target is essential in identifying system weaknesses. Once a weakness has been identified, an effective deception jamming technique can be developed and programmed into a deception jammer. For example, if a particular radar system relies primarily on Doppler tracking, a Doppler deception technique will greatly reduce its effectiveness. Threat system exploitation is the best source of detailed information on threat system capabilities and vulnerabilities. Effective deception jamming requires much more intelligence support than does noise jamming.

d. Most self-protection jamming techniques employ some form of deception against a target tracking radar (TTR). The purpose of a TTR is to continuously update target range, azimuth, and velocity. Target parameters are fed to a fire control computer that computes a future impact point for a weapon based on these parameters and the characteristics of the weapon being employed. The fire control computer is constantly updating this predicted impact point based on changes in target parameters. Deception jamming is designed to take advantage of any weaknesses in either target tracking or impact point calculation to maximize the miss distance of the weapon or to prevent automatic tracking. This chapter will discuss the most commonly employed deception jamming

techniques, including false target jamming, range deception jamming, angle deception jamming, velocity deception jamming, and monopulse jamming.

2. FALSE TARGET JAMMING

False target jamming is an effective jamming technique employed against acquisition, early warning, and ground control intercept (GCI) radars. The purpose of this type of jamming is to confuse the enemy radar operator by generating many false target returns on the victim radar scope. When false target deception jamming is successfully employed, the radar operator cannot distinguish between false targets and real targets (Figure 11-2).

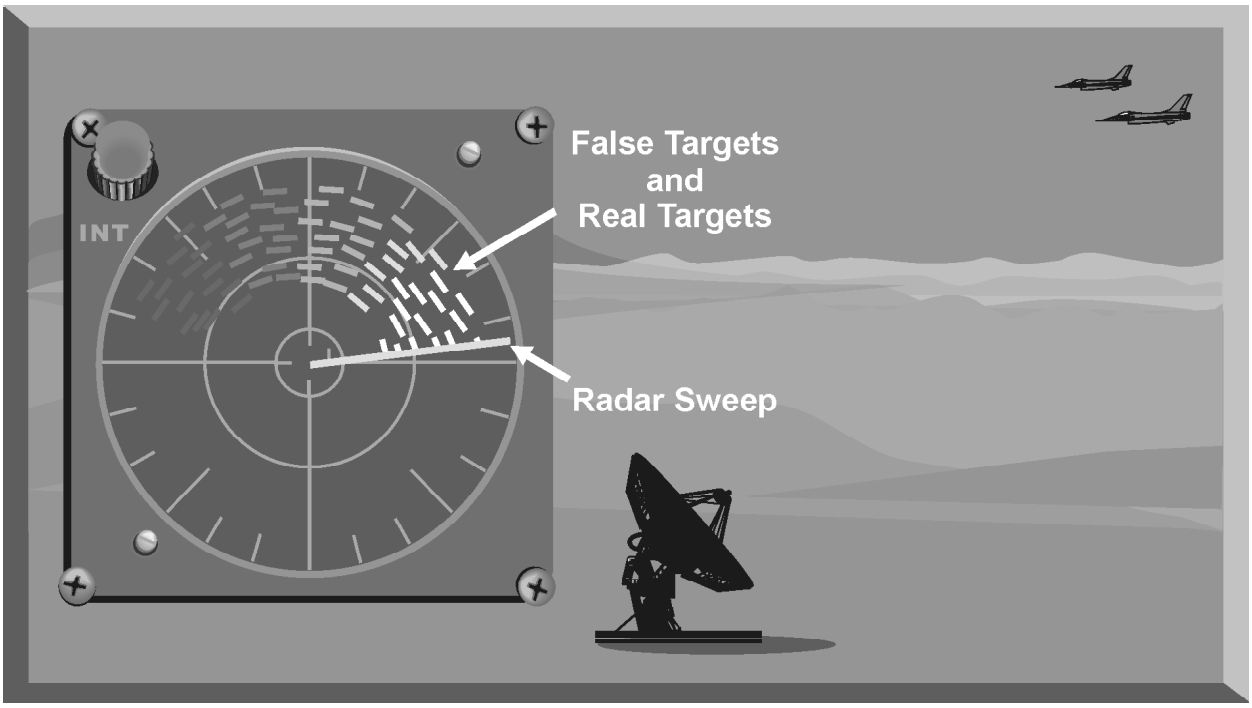


Figure 11-2. False Target Generation

a. To generate false targets, the deception jammer must tune to the frequency, PRF, and scan rate of the victim radar. The jamming pulse must appear on the radar scope exactly like a radar return from an aircraft. Multiple false targets greater in range than the jammer are generated by delaying the transmission of a jamming pulse until after the victim radar pulse has been received. False targets closer in range are generated by anticipating the arrival of a radar pulse and transmitting a jamming pulse before the victim radar pulse hits the aircraft. If the victim radar employs a jittered PRF, only targets greater in range can be generated.

b. To generate different azimuth false targets, the deception jammer synchronizes its transmitted pulse with the victim radar's sidelobes. Due to their

reduced power, when compared to the main beam, sidelobes are difficult to detect and analyze. The receiver in the deception jammer must be sensitive enough to detect these sidelobes and not be saturated by the power in the main radar beam. A false target deception jammer must inject a jamming pulse that looks like a target return into these sidelobes. To penetrate the radar sidelobes requires a lot of power. However, the power must be judiciously used. If a powerful jamming pulse is injected into the main beam, the false targets will be easy to detect. Most false target jammers vary the power in the jamming pulse inversely with the power in the received signal, on a pulse-by-pulse basis. This means the repeater jamming signal is at minimum power when the main beam of the victim radar is on the aircraft and at maximum power when the sidelobes are being jammed. To effectively generate false azimuth targets, the jammer must have a receiver with a wide dynamic range to detect both the main beam and the sidelobes. In addition, the jamming system must be able to generate high power that can be effectively controlled by the receiver.

c. To generate moving false targets, the deception jammer must synchronize with the main beam and the sidelobes in frequency, pulse width and PRF. Amplitude modulated jamming signals, with variable time delays, are transmitted into the sidelobes of the victim radar. The variable time delay provides a false target that changes range, either toward or away from the radar, depending on the time delay. The amplitude modulation provides false azimuth targets that appear to be moving.

d. The effectiveness of false target generation is based on the credibility of the generated false radar returns. If the victim radar can easily distinguish between false returns and target returns, the technique is a failure. The false returns must look identical to an aircraft return. The radar return on the victim radar scope should have the same intensity, depth, and width as a target return.

(1) Power determines the false target intensity when it is displayed on the victim radar scope. Varying jammer output power inversely with received power ensures that each false target has nearly the same intensity as a true target return. The depth, or thickness, of the false target depends on the pulse width of the victim radar. By matching the pulse width of the jamming pulse with the pulse width of the victim radar, the jammer can generate false targets with the same depth as a real target return.

(2) The width of the false target depends on the antenna pattern of the victim radar. This can pose a problem for false-target deception jammers. Because the jamming pulse is transmitted the entire time the radar beam is on the jammer, the width of a false target will tend to be greater than a real target return. Aircraft radar return varies with main beam cross-section. To correct this problem, most false target deception jammers use random modulation in the power of the transmitted pulses. This will vary the width of the false targets and make them look more like the variable returns of actual targets.

3. RANGE DECEPTION JAMMING

Although a specific TTR can track multiple targets and direct multiple weapons, the tracking circuit must select a single target return and track it while ignoring all other returns. Target selection is done by using gate bins. The range gate is used as the primary gate for target selection. A range gate is an electronic switch that is turned on for a period of microseconds based on a certain range or time delay after a pulse is transmitted (Figure 11-3).

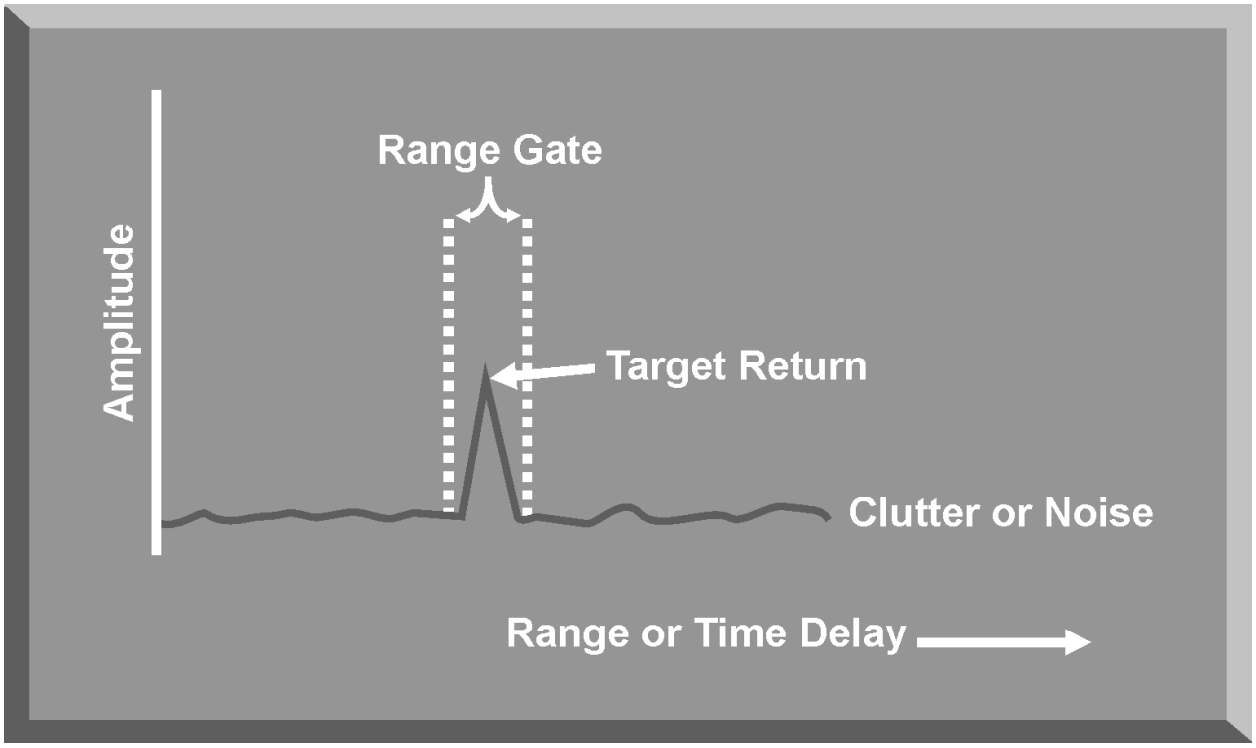


Figure 11-3. Range Gate Tracking

a. Range deception jamming exploits any inherent weakness in a TTR's automatic range gate tracking circuits. When a TTR's range gate locks on to an aircraft, the range deception jammer detects the radar signal. The range deception jammer then amplifies and retransmits a signal much stronger than the radar return. This retransmitted signal, called a cover pulse, is displayed in the range gate with the target signal (Figure 11-4).

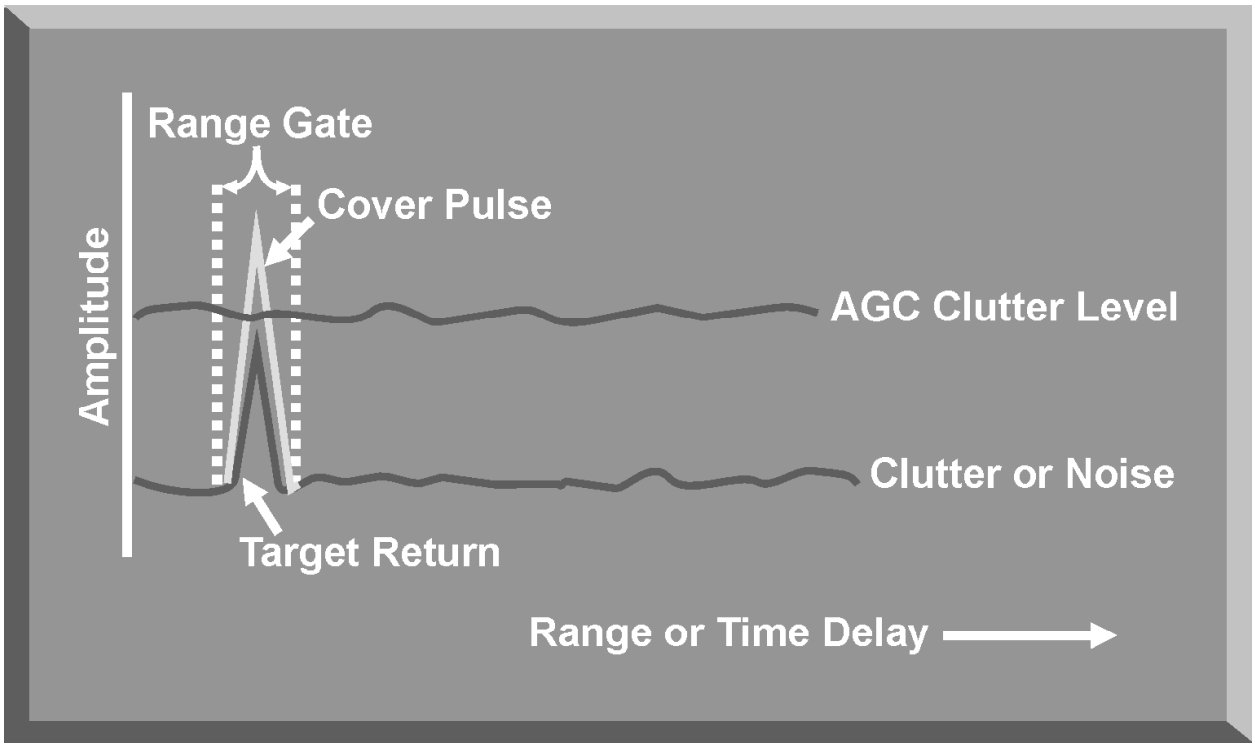


Figure 11-4. Range Gate Jamming Cover Pulse

b. The automatic gain control (AGC) circuit lowers the gain in the range tracking gate to control the amplitude of the cover pulse in the range gate. Reduced gain causes the real target return to be lost, and the range gate only tracks the jamming signal. This is known as range gate capture.

c. Once the range gate is captured by the cover pulse, a technique called range gate pull-off (RGPO) is employed (Figure 11-5). The deception jammer memorizes the radar signal and introduces a series of time delays before retransmitting. By increasing these time delays, the range gate will detect an increase in range and automatically move off to a false range. Once the range gate has moved well away from the real target, the range deception jammer shuts down, and the radar range gate is left with no target to track. The range gate breaks lock and the TTR must again go through the process of search, acquisition, and lock-on to re-engage the target.

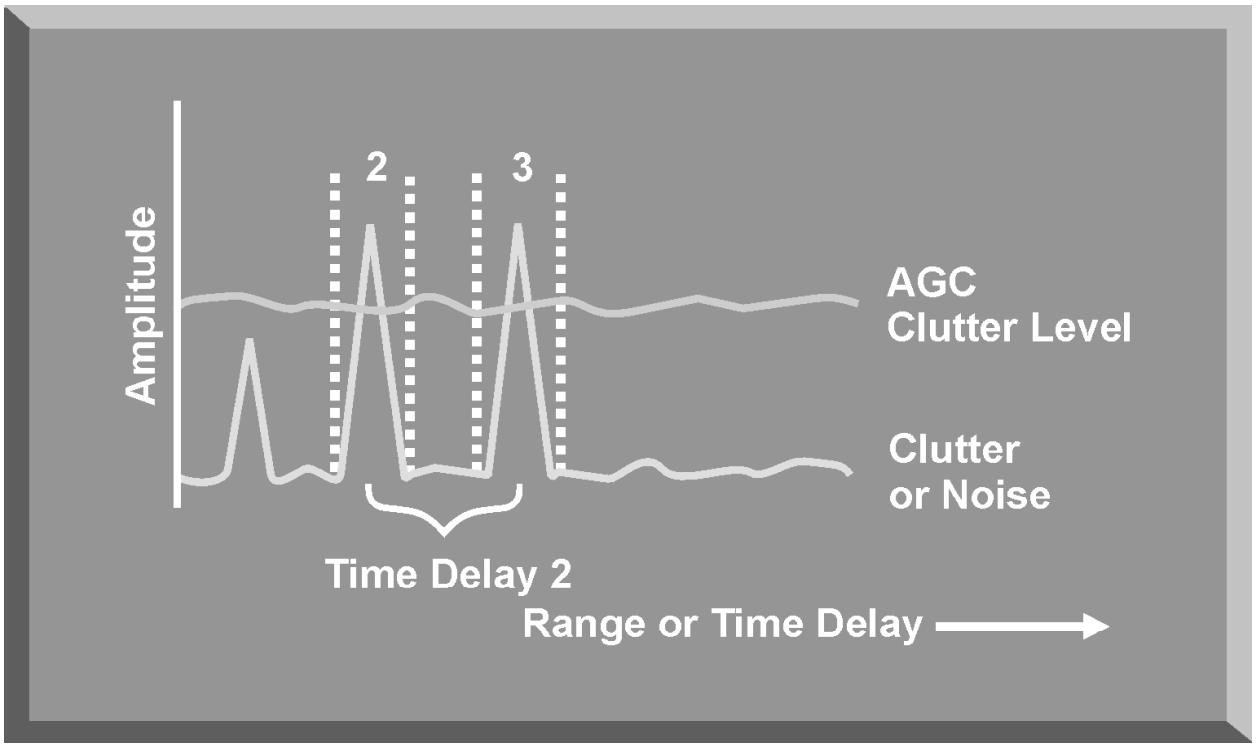


Figure 11-5. Range Gate Pull-Off

d. There are several advantages of range deception jamming, especially when used as a self-protection technique. It can generate sufficient errors to deny range information and is effective against most automatic range tracking systems. This technique does not require a large amount of power, just enough to cover the radar return of the aircraft. If the time delays are not exaggerated, an operator may not detect the loss of range lock-on until after a missile has been fired. The insidious nature of range deception jamming may generate enough miss distance to save the aircraft and pilot.

e. There are disadvantages to using range deception jamming. First, it can be defeated by a trained radar operator. If the operator detects a problem with the automatic range tracking circuit, the system can be switched to manual range tracking mode to defeat RGPO. Also, if the threat system is still able to track the aircraft's azimuth and elevation, range information may not be required to complete target engagement. To maximize range deception jamming effectiveness, it should be employed in conjunction with azimuth and elevation jamming. Finally, this type of range deception jamming is not effective against a leading-edge range tracking system. A leading-edge tracker will not see the delayed cover pulse. As the cover pulse moves off the target, AGC circuits reset the gain to continue tracking the real target. The only way to defeat a leading-edge range tracker is with a deceptive jammer that anticipates the next radar pulse and sends a jamming cover pulse before it reaches the aircraft. This jamming technique can also be defeated by randomly varying the radar PRF.

4. ANGLE DECEPTION JAMMING

Angle deception jamming is designed to exploit weaknesses in the angle tracking loop of the victim radar. The specific technique depends on the tracking method used to derive azimuth and elevation information. Inverse amplitude modulation jamming is the main angle deception technique used against TWS radars. For conical scan radars, scan rate modulation and inverse gain jamming are used. Swept square wave (SSW) jamming is used against LORO tracking radars. Monopulse angle deception jamming will be covered separately.

a. The azimuth and elevation tracking loop for a TWS radar is based on target signal amplitude modulation. The inverse amplitude modulation jammer generates a signal with modulation exactly opposite the expected return. To accomplish this, the angle deception jammer must receive the radar signals from the tracking beams. The jammer responds with a signal of the same frequency, PRF, and scan rate synchronized to the inverse of the radar antenna pattern (Figure 11-6). This induces an error in the angle tracking gate that, over a series of scans, causes the radar to lose target angle tracking.

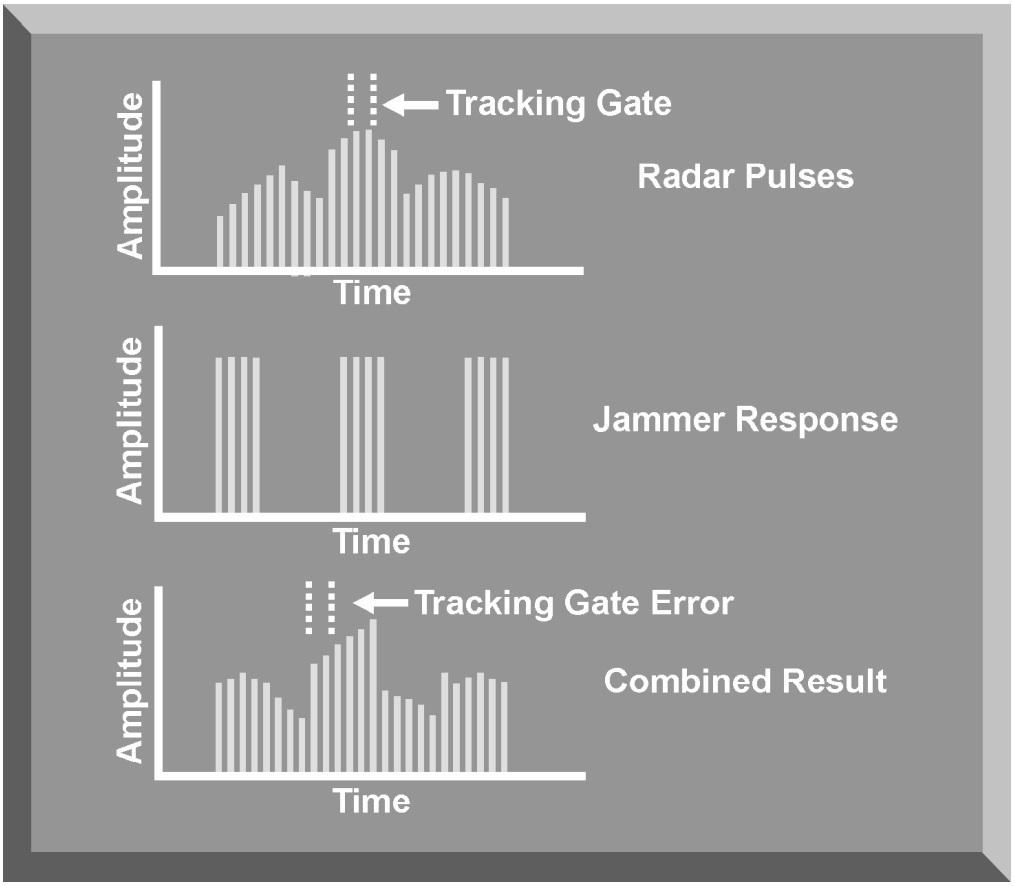


Figure 11-6. Inverse Amplitude Modulation Jamming

b. Inverse gain jamming is also effective against conical scan radars. Since conical scan radars use the phase of the target returns to generate error signals, an inverse gain deception jammer attempts to alter the phase by inducing fake signals into the antennas. In addition, by altering the amplitude of the signal, the jammer induces large errors into the tracking loop. To accomplish this, the jammer must determine the frequency, PRF, and scan rate of the victim radar. It then transmits signals that change the phase and amplitude of the target signal, resulting in a signal 180 degrees out of phase with the actual target (Figure 11-7). This 180-degree error rapidly drives the antenna off the target and causes break-lock.

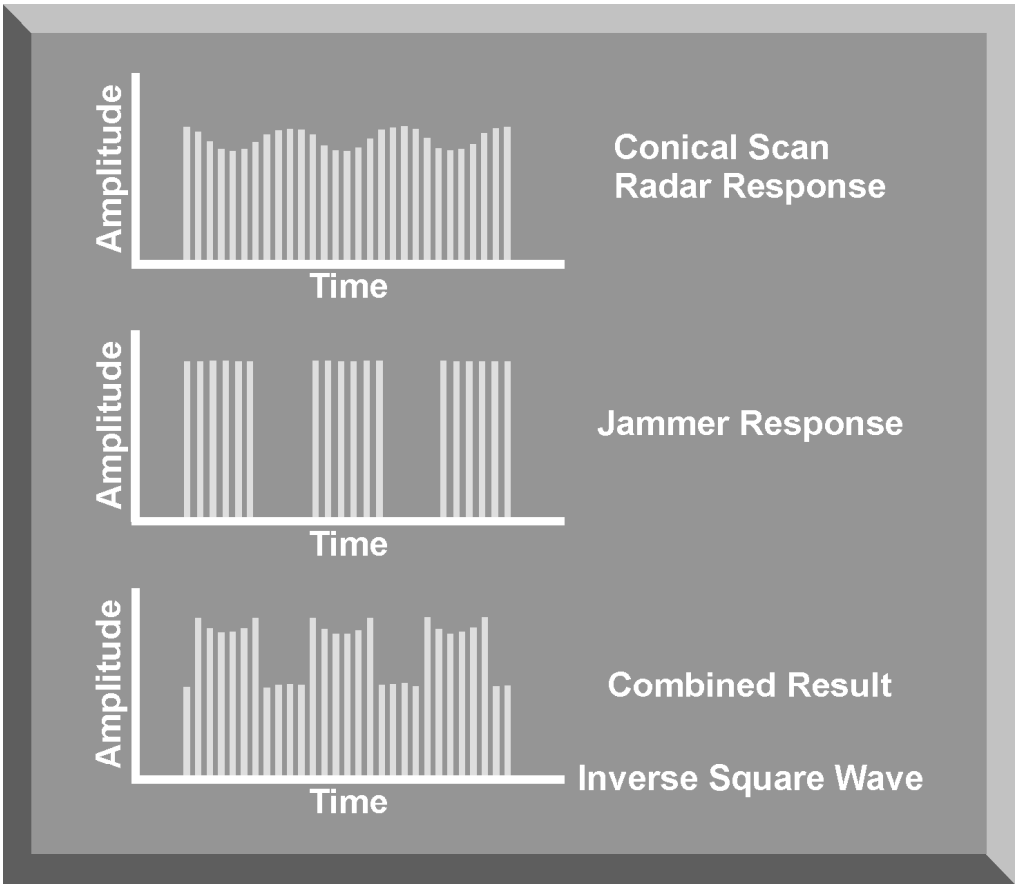


Figure 11-7. Inverse Gain Jamming

c. Scan rate modulation is also used against conical scan radars. This angle deception technique modulates the jamming pulse at or near the victim radar nutation frequency. As the modulation approaches the radar's nutation frequency, large error signals appear in the radar servo tracking loops, producing random gyrations in the antenna system, causing break-lock. This technique is most effective if the modulation jamming is slowly swept in frequency until it matches the nutation rate.

d. Both inverse scan and scan rate modulation jamming require very little power and have proven extremely effective against TWS and conical scan radars. To be effective, however, the angle deception jammer must find the precise scan rate of the victim radar. The jammer must concentrate on one signal at a time, limiting the number of threat systems that can be jammed simultaneously. In a dense threat environment, this can be a severe limitation.

e. The effectiveness of inverse gain and scan rate modulation jamming led radar designers to employ antennas that scan only during the receiving function of the radar system. Generally, this is accomplished by using two antennas. The transmitting antenna illuminates the target. Receiving antennas scan to produce the amplitude modulation of the reflected signal for effective angle tracking. This technique is called Lobe-On-Receive-Only (LORO). Since the transmitting antenna does not nutate, or scan, angle deception jammers cannot detect the modulation required to generate effective inverse gain modulation. Swept square wave (SSW) jamming is the angle deception technique developed to counter LORO angle tracking.

f. SSW jamming continuously varies the frequency of amplitude modulation on the jamming pulse over an expected range of nutation or scanning frequencies. This range is established by either electronic intelligence (ELINT) data on a particular system, or by exploitation. The dotted line in Figure 11-8 shows a threat's nutation or scan frequency. As the frequency of the modulated jamming pulse approaches the threat scan frequency, it induces errors in the angle tracking loop of the victim radar. The longer the SSW jamming stays near the scan frequency, the greater the induced errors. It is important that the sweep rate of the modulating jamming be slow enough to maximize its impact on the victim radar.

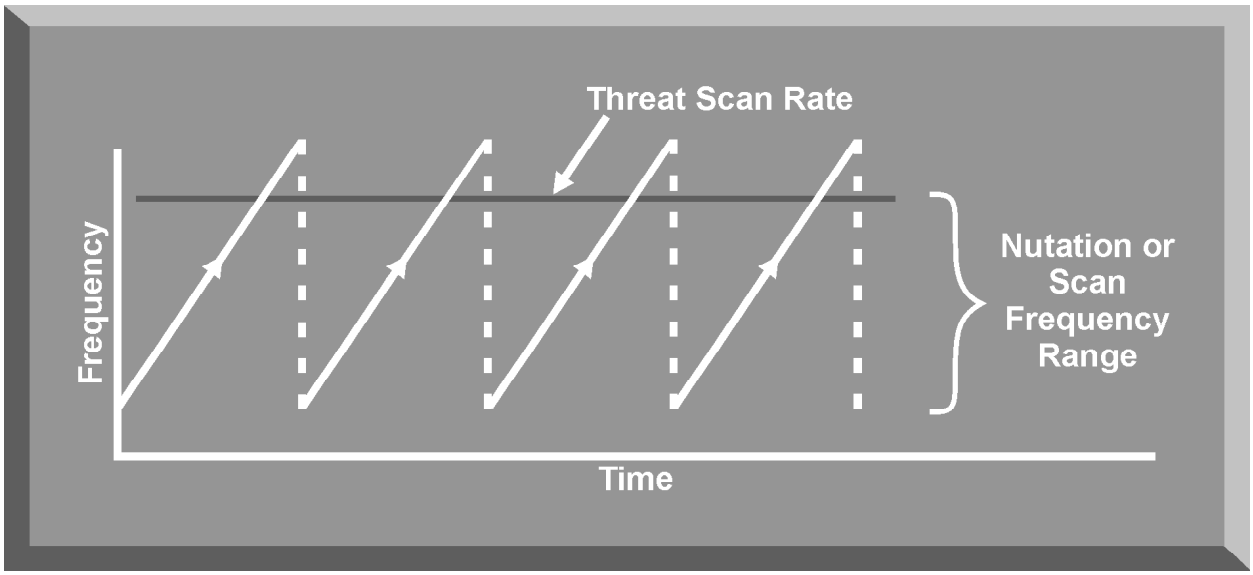


Figure 11-8. Swept Square Wave Jamming

5. VELOCITY DECEPTION JAMMING

Pulse Doppler and continuous wave (CW) radars track targets based on velocity or Doppler-shifted frequency (Figure 11-9). The objective of velocity deception jamming is to deny velocity tracking information and generate false velocity targets. The primary techniques include velocity gate pull-off (VGPO), Doppler noise, narrowband Doppler noise, and Doppler false targets.

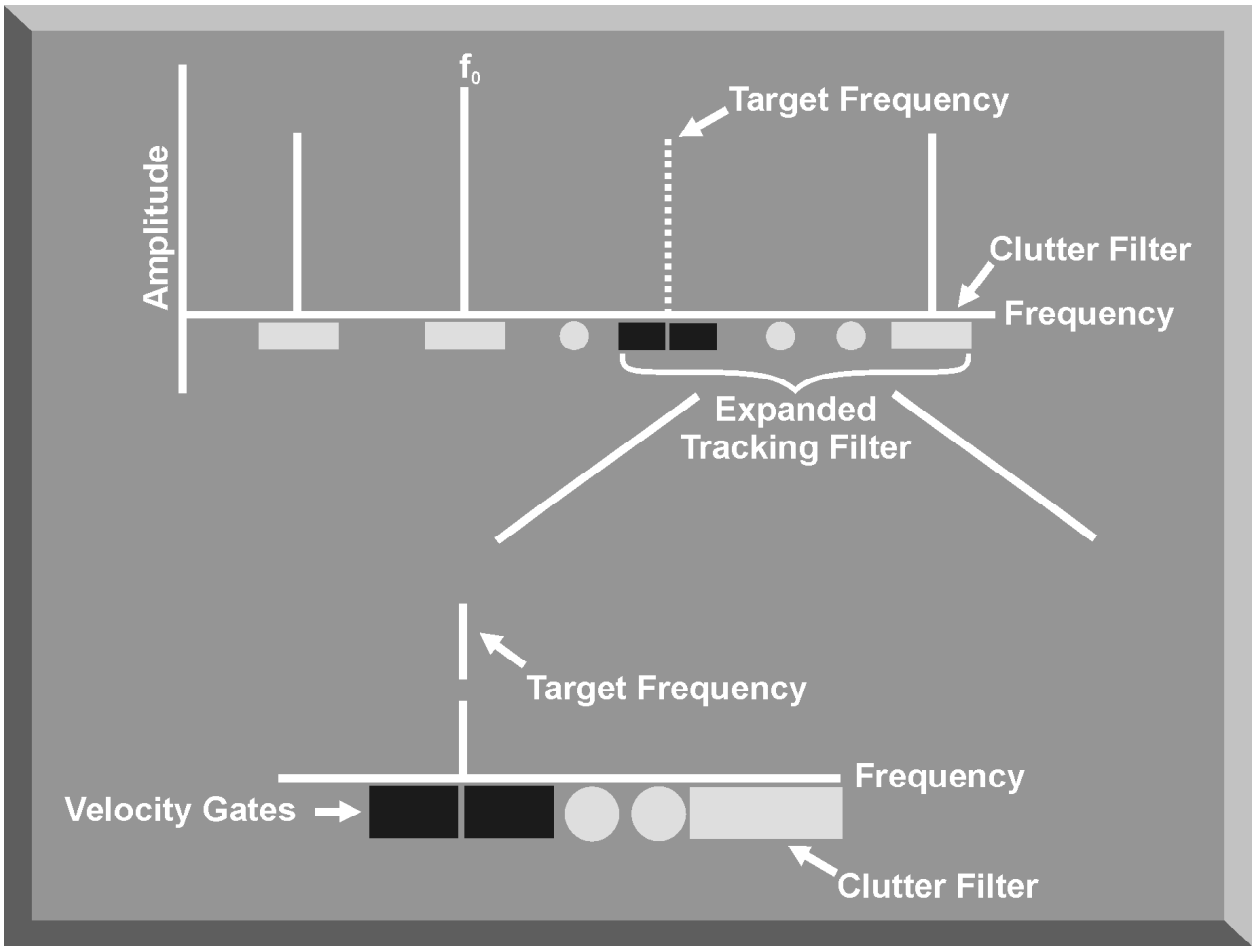


Figure 11-9. Velocity Tracking Gate

a. Velocity gate pull-off counters pulse Doppler or CW radars by stealing the velocity gate of their automatic tracking loop. The objective of VGPO is to capture the Doppler velocity tracking gate by transmitting an intense false Doppler signal. Then the frequency of the false signal is changed to move the tracking gate away from the true target Doppler. This is analogous to the RGPO technique used against the range gate tracking loop.

(1) To accomplish an effective VGPO technique, the jammer receives the CW or pulse Doppler signal. It then retransmits a CW or pulse Doppler signal that is higher in power than the return from the aircraft, but at approximately the same

Doppler frequency (Figure 11-10). It is important that the frequency of this initial jamming pulse appears within the same velocity tracking filters as the target return or the victim radar will disregard it. The frequency band of the Doppler tracking filters is an important piece of intelligence information. The velocity tracking gates are quite narrow, roughly 50 to 250 MHz. Once the jamming pulse appears in the tracking gate, the automatic gain control circuit gains out the target return, and the jamming pulse has captured the velocity gate.

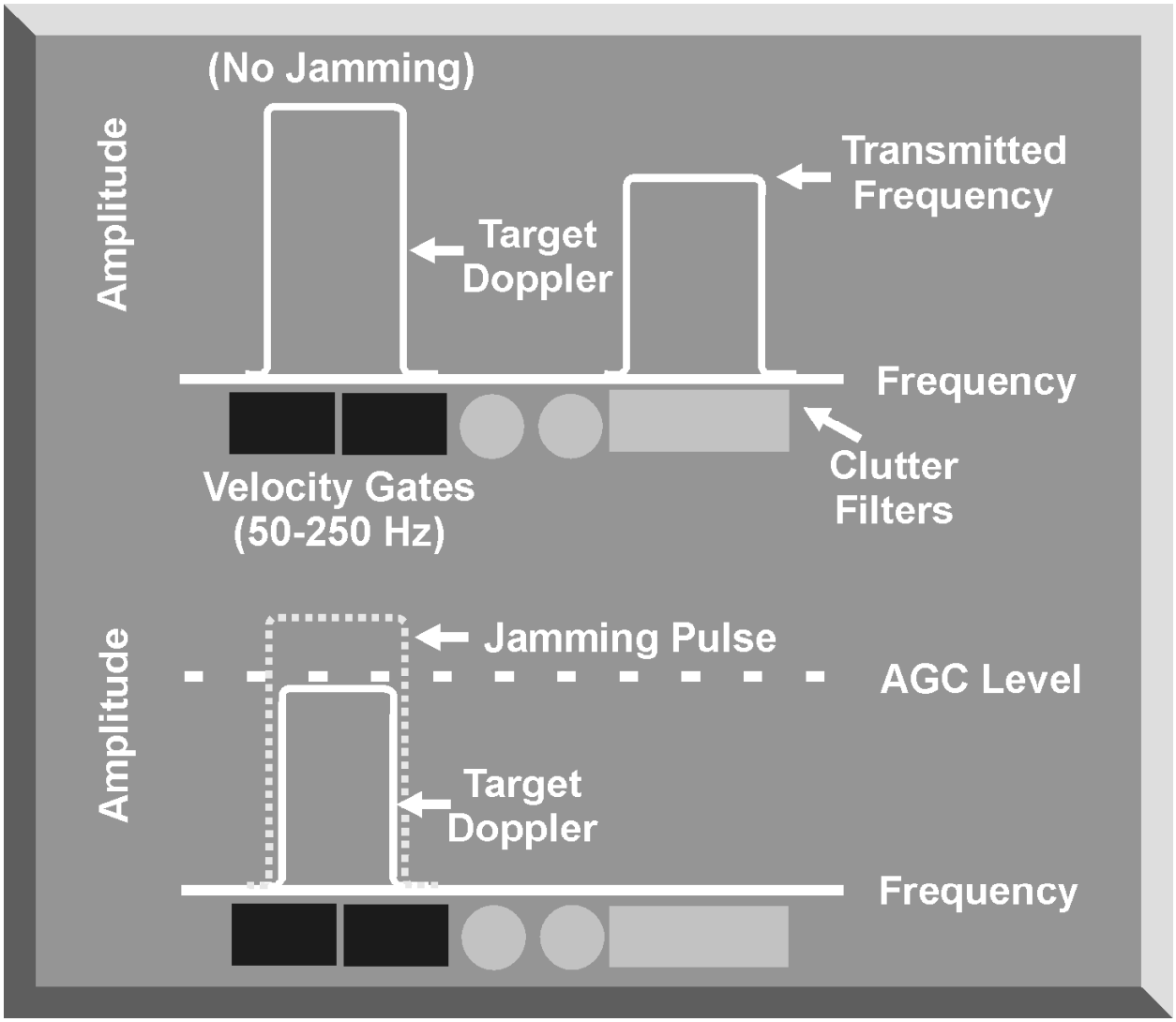


Figure 11-10. Velocity Gate Capture

(2) Once the jamming pulse has captured the tracking gate, the deception jammer slowly changes the Doppler frequency (Figure 11-11). This frequency shift is accomplished by several methods. The most common method uses frequency modulation (FM) within the jammer's traveling wave tube (TWT). By varying the TWT voltage, the Doppler frequency of the jamming pulse is changed

linearly, and the radar tracking gates follow the jamming pulse. By using FM, the jamming pulse can be moved in either a positive or negative direction, depending on the slope of the voltage. By slowly changing the frequency of the modulation, the jamming pulse pulls the tracking gates off the target. When the maximum offset has been achieved, nominally 5 to 50 kHz, the FM is "snapped back" to a minimum value, and the process is repeated to preclude target reacquisition.

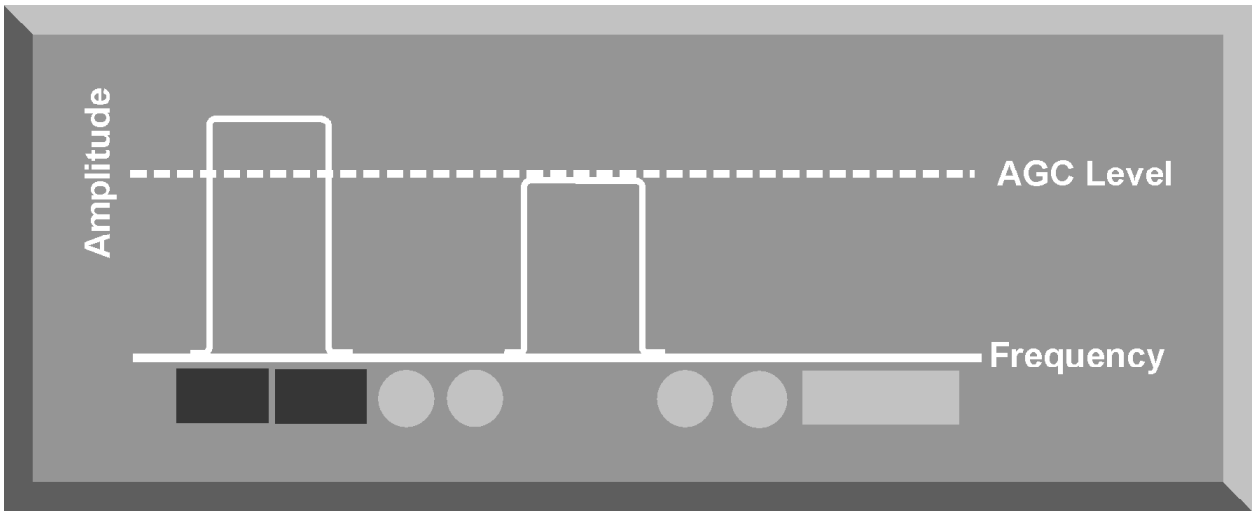


Figure 11-11. Velocity Gate Pull-Off

(3) The rate of change of frequency offset in a VGPO pulse is an extremely critical parameter. Many CW and pulse Doppler radars employ acceleration stops as part of the tracking gates. By differentiating the velocity outputs of the velocity tracking gates with respect to time, the velocity tracker computes target acceleration. Acceleration stops detect and reject unusually large changes in target acceleration. If the VGPO technique changes the frequency of the jamming pulse too rapidly, the tracking loop, with acceleration stops, will reject the jamming pulse and stay on the target. This means that an effective VGPO technique may take from one to ten seconds.

b. Doppler noise differs from most noise techniques in that it is a repeater technique. The jamming system must receive the pulse Doppler radar signal in order to generate an appropriate jamming pulse. Also, noise jamming output is done on a pulse-by-pulse basis and only lasts as long as the pulse duration, or pulse width, of the victim radar signal (Figure 11-12). The Doppler noise jammer receives each pulse and applies a random frequency shift, either positive or negative, to each pulse.

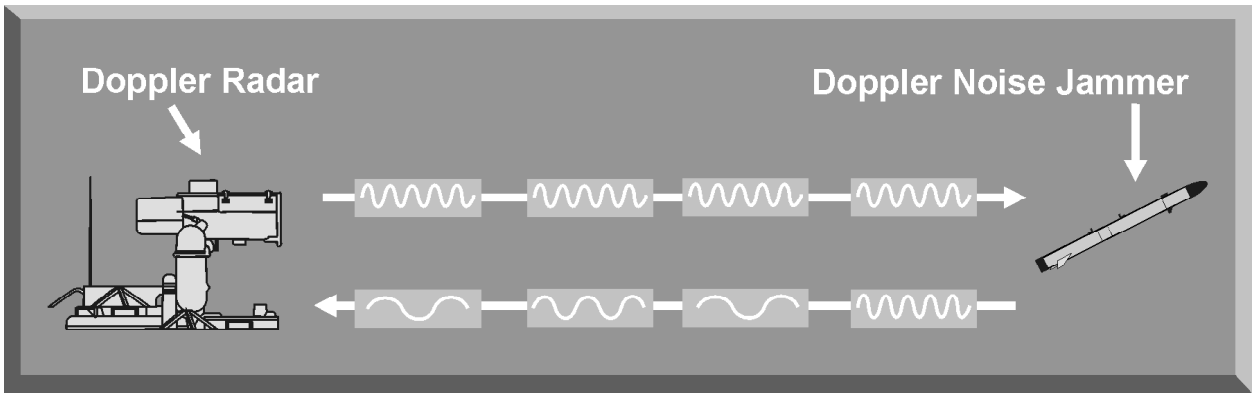


Figure 11-12. Doppler Noise Jamming

(1) When Doppler noise jamming pulses are processed by the signal processor, and the Doppler frequencies are sent to the velocity tracking gate, there are so many different velocities that the tracking gate cannot distinguish the target from the jamming. The random distribution of target velocities effectively masks the true target Doppler velocity. If the velocity tracking loop is not saturated, multiple false targets traveling at different speeds will be displayed.

(2) When a technique called Doppler noise blinking is employed, it interferes with the angle and velocity tracking within most semi-active radar missiles. Doppler noise blinking is accomplished by rapidly transmitting bursts of Doppler noise jamming (Figure 11-13).

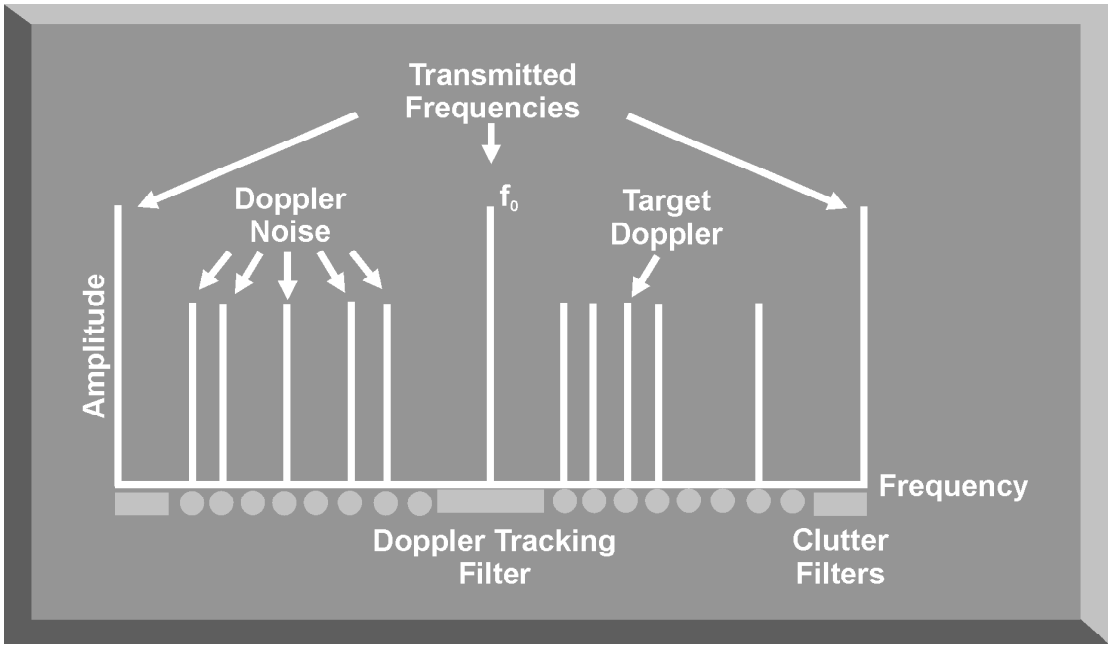


Figure 11-13. Impact of Doppler Noise Jamming

(3) Doppler noise jamming is effective against most pulse Doppler radars and the semi-active missiles employed with these radars. One disadvantage, however, is that it is only effective against the velocity tracking loop. If range tracking is still available to the radar, Doppler noise may highlight the jamming aircraft. Another disadvantage is that Doppler noise requires a sophisticated jammer able to receive the victim radar pulse, generate random positive and negative frequency modulations on this pulse, and retransmit the jamming pulses at the PRF and pulse width of the victim radar. This requires an extremely fast signal processing capability and detailed intelligence information on the victim radar.

c. Narrowband Doppler noise is also a repeater technique. The jamming system receives the pulse Doppler radar signal and generates a noise jamming signal on a pulse-by-pulse basis (Figure 11-14). Narrowband Doppler noise requires detailed information on the frequency coverage of an individual velocity tracking filter, or velocity bin, employed by the victim radar. Once this frequency range is known, the jammer receives each pulse from the victim radar and transmits jamming pulses with a higher and lower frequency shift based on the real target Doppler. These frequency shifts are always within the frequency range of the velocity bin.

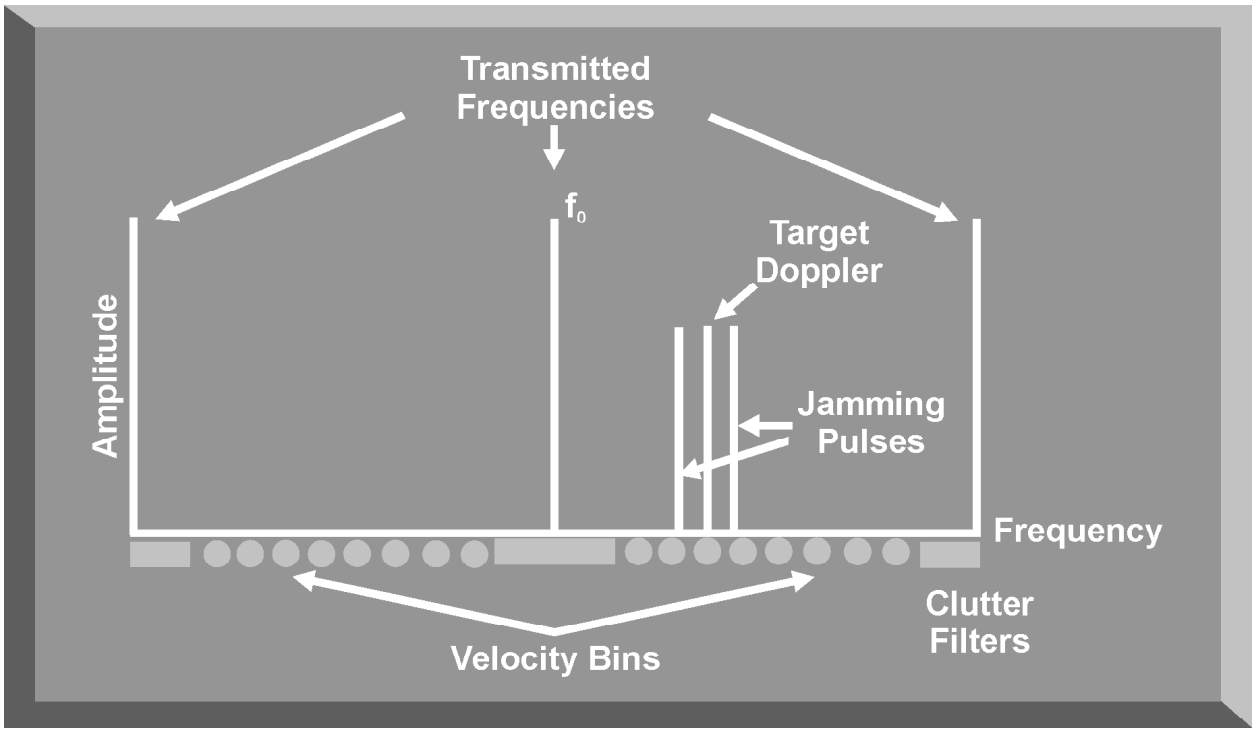


Figure 11-14. Narrowband Doppler Noise

(1) When these pulses are processed by the signal processor and the Doppler signals are sent to the velocity tracking gates, the particular bin that

contains the target Doppler also contains several other targets generated by the jammer. The victim radar signal processor attempts to distinguish the target Doppler from the jamming pulses. It raises the gain in the velocity tracking bins, thinking that the signal with the highest amplitude is the target. But, as the signal gain is increased, the target is "gained out" with the jamming signals and no target is displayed. This is called velocity bin masking and can completely deny target information to a pulse Doppler radar (Figure 11-15).

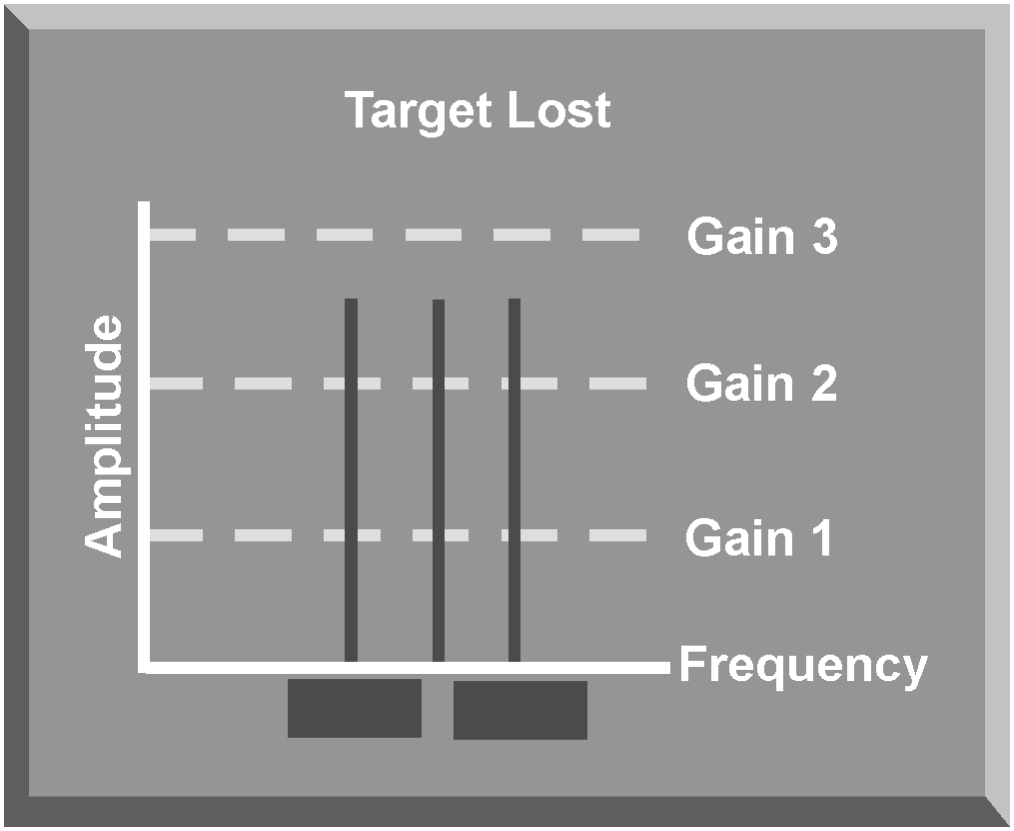


Figure 11-15. Velocity Bin Masking

(2) The advantage of narrowband Doppler noise is that it completely masks an aircraft's velocity from a pulse Doppler radar. The disadvantages include the following: When the victim radar can range-track an aircraft, narrowband Doppler noise highlights the aircraft's presence. To be effective, narrowband Doppler noise requires knowledge of the frequency range of the victim radar's velocity tracking bins, or filters. This detailed information may be available only through threat system exploitation. Finally, sophisticated signal processing and jamming systems are required to receive and transmit in the very narrow frequency band of the velocity bin.

d. Doppler false target jamming is normally used with narrowband Doppler noise or other deception techniques. Its purpose is to initially confuse the radar signal processor with multiple targets and then force the radar signal processor

to raise its gain levels in the velocity tracking loop. The Doppler false target jammer receives each pulse of the victim radar and applies a random frequency shift to a selected number of these pulses (Figure 11-16).

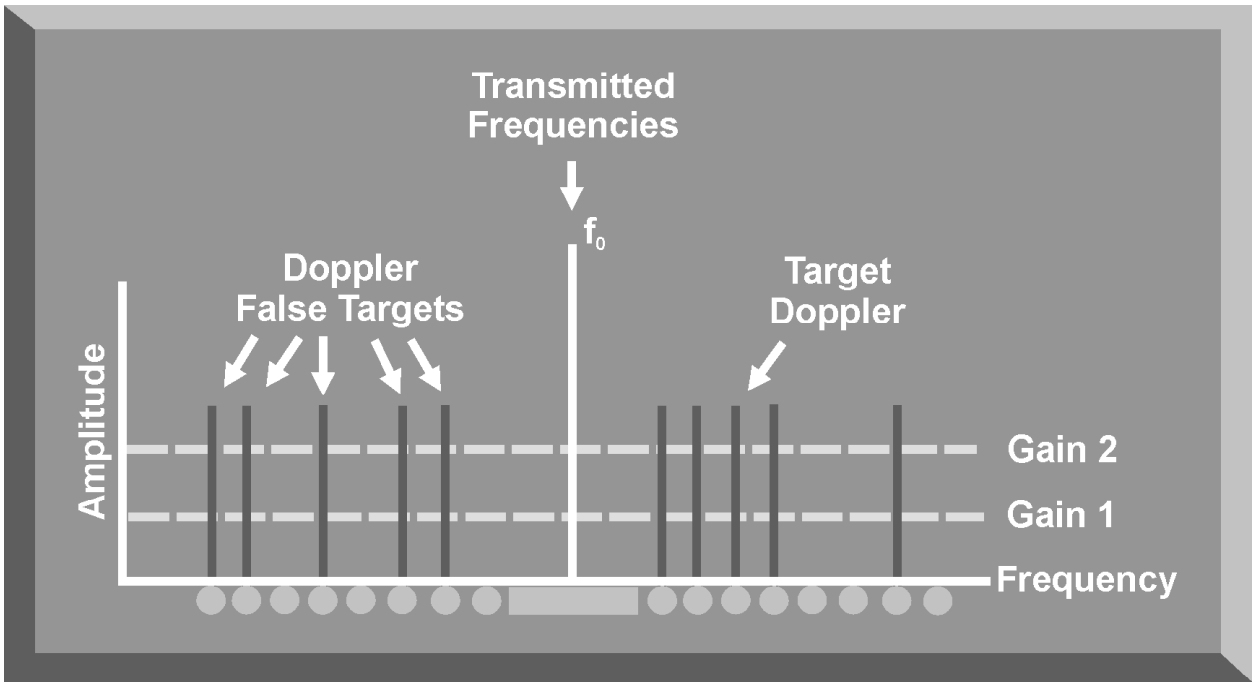


Figure 11-16. Impact of Doppler False Target Jamming

(1) The selected pulses are processed by the signal processor, and multiple Doppler frequencies are sent to the velocity tracking gate. In an attempt to distinguish the target from the jamming pulses, the signal processor increases the gain in each tracking filter, assuming the target Doppler has a higher amplitude than the jamming pulses. This increase in gain sets up the velocity tracking loop for a narrowband Doppler noise technique that will cause the real target to be lost among the generated false targets.

(2) The advantage of Doppler false target jamming is that it can initially confuse the radar signal processor and the radar operator as to the velocity of the real target. It also sets up the radar for narrowband Doppler noise technique and increases its effectiveness. The disadvantage is that the signal processor or the radar operator will eventually be able to distinguish the real target from the false targets based on its velocity. This jamming technique is much more effective when used in conjunction with other Doppler jamming techniques.

6. MONOPULSE DECEPTION JAMMING

The ability of monopulse tracking radars to obtain azimuth, range, and elevation information on a pulse-by-pulse basis make them extremely difficult to jam

(Figure 11-17). Amplitude modulation jamming used against conical scan or TWS radars, such as inverse scan and swept square wave, highlights a target, making monopulse tracking easier. Frequency modulation techniques, such as RGPO and VGPO, are equally ineffective. They serve as a beacon that aids the monopulse radar's target tracking ability. The monopulse radar may be able to track the jammer with more accuracy than tracking actual radar returns because target glint effects are absent from the jamming pulse. Monopulse angle jamming techniques can be divided into two main categories, system-specific and universal. Examples of system-specific jamming techniques include skirt frequency jamming, image jamming, and cross-polarization jamming. These techniques attempt to exploit weaknesses in the design and operation of specific monopulse radars. Cross-eye jamming, a universal technique, attempts to exploit all monopulse radar systems.

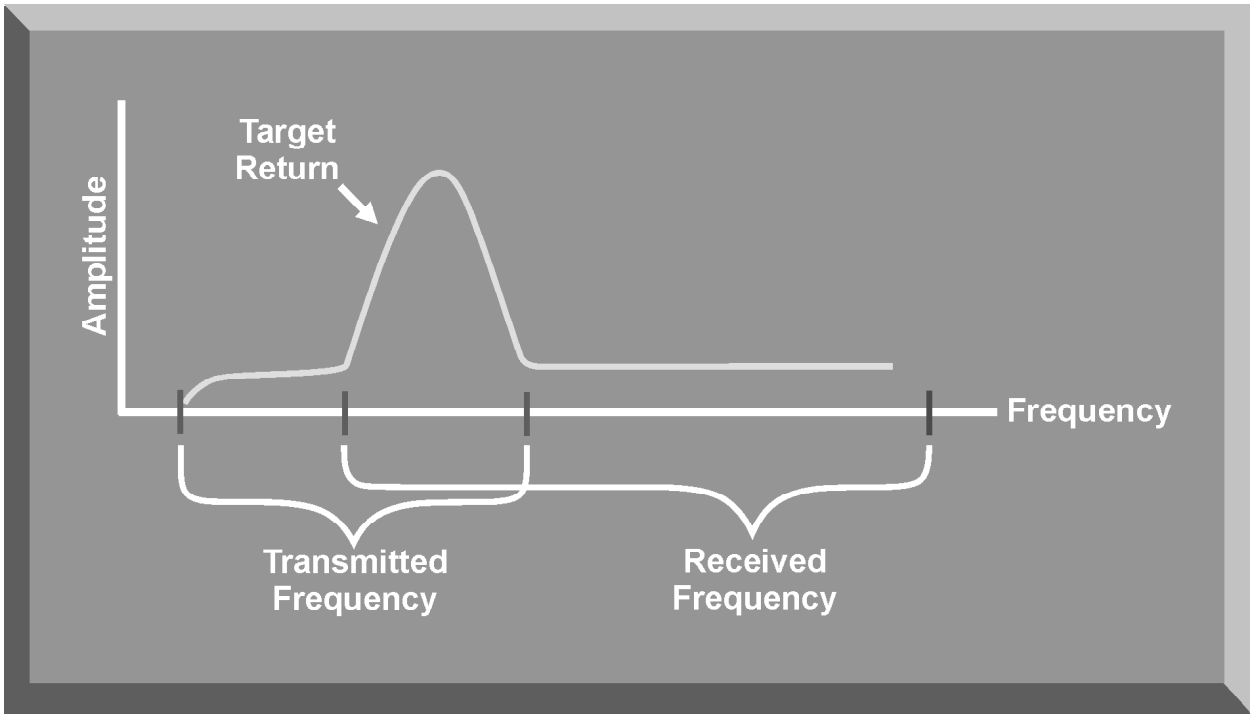


Figure 11-17. Monopulse Radar Receiver

a. Skirt frequency jamming, or filter skirt jamming, is designed to counter the monopulse receiver. Skirt frequency jamming is based on the fact that the intermediate frequency (IF) filter of the monopulse receiver must be correctly tuned to the transmitting frequency of the monopulse radar. It these two components are not exactly tuned, the target signal may be presented on the edge, or skirt, of the receiver IF filter. This offers an opportunity to inject a jamming signal into this skirt (Figure 11-18).

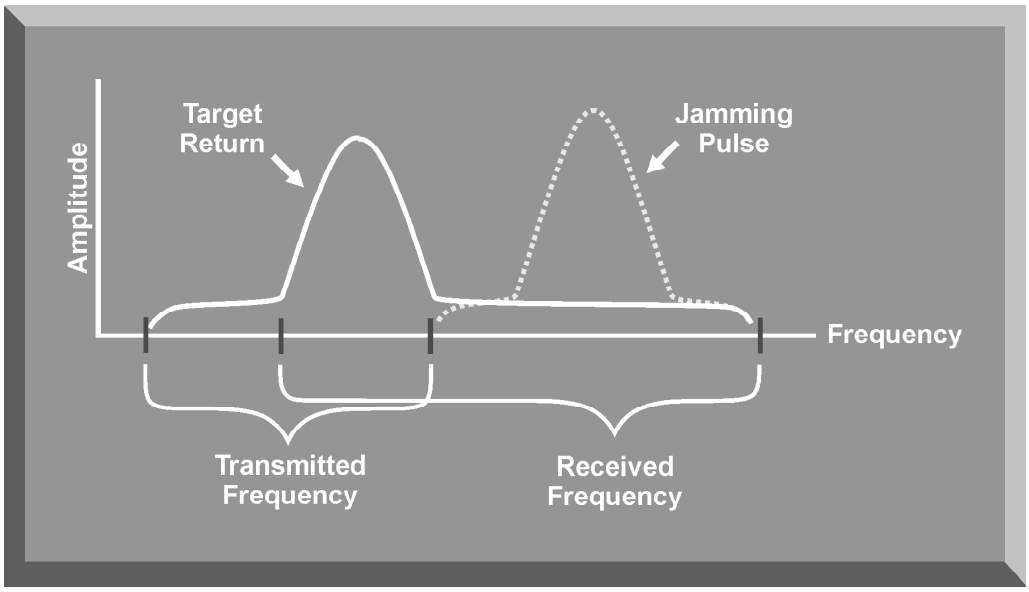


Figure 11-18. Filter Skirt Jamming Pulse

(1) Filter skirt jamming attempts to take advantage of this frequency imbalance by transmitting a jamming pulse tuned slightly off the radar transmitted frequency and in the middle of the receiver IF filter. This jamming pulse will generate a false error signal and drive the antenna away from the true target return.

(2) A well designed and maintained monopulse system does not have a frequency imbalance. The transmitter and IF filter frequencies will be identical. Jamming signals that are even slightly out of this narrow frequency range will not affect the monopulse tracking capability of the radar (Figure 11-19).

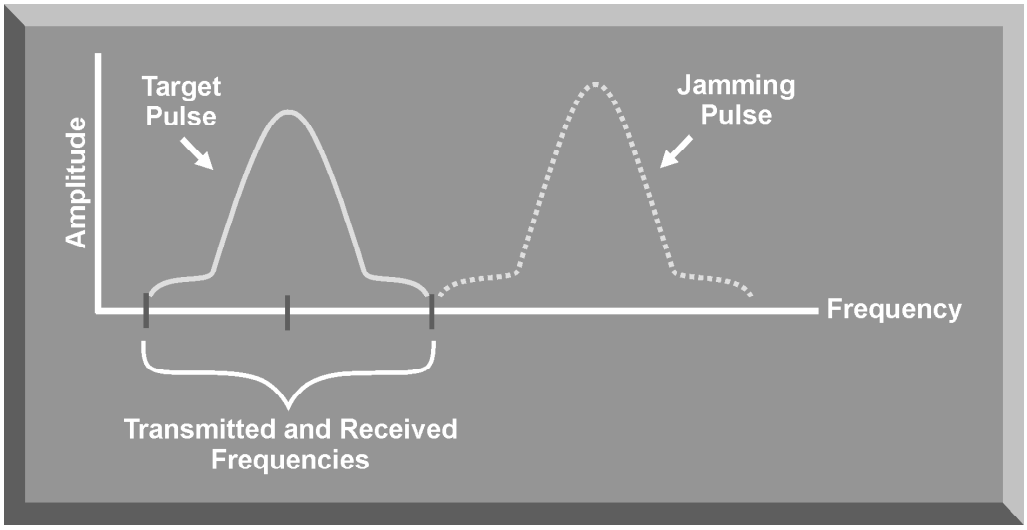


Figure 11-19. Ineffective Filter Skirt Jamming

(3) Effective filter skirt jamming requires extensive knowledge of the internal operation of the IF filter. This information can normally be obtained only by system exploitation. Variances from radar to radar and frequency imbalance exists from one radar IF filter to another. This creates a high degree of uncertainty in the effectiveness of this technique.

b. Image jamming exploits another potential weakness in the monopulse receiver (Figure 11-20). Some monopulse receivers have a wide-open front end with no preselection before the mixer. If the jammer transmits a pulse at the intermediate, or image, frequency, but out of phase with this frequency, the phase of the target tracking signal will be reversed and the antenna will be driven away from the target (Figure 11-21). Effective image jamming requires detailed information on the operation of the monopulse receiver. Of particular importance is the image, or intermediate, frequency and whether the local oscillation frequency is above or below the transmitted frequency. This may require exploitation of the monopulse threat system. In addition, a well-designed monopulse system has preselection in the front end and will reject signals that are out of phase with the transmitted frequencies. This capability renders image jamming ineffective.

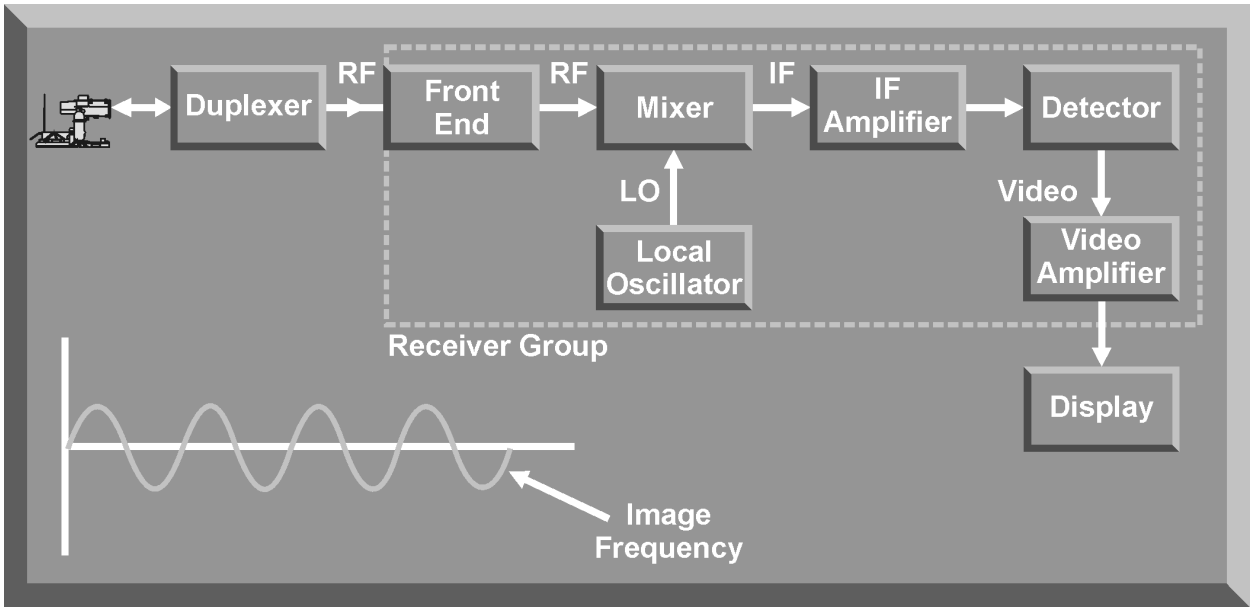


Figure 11-20. Monopulse Image Frequency

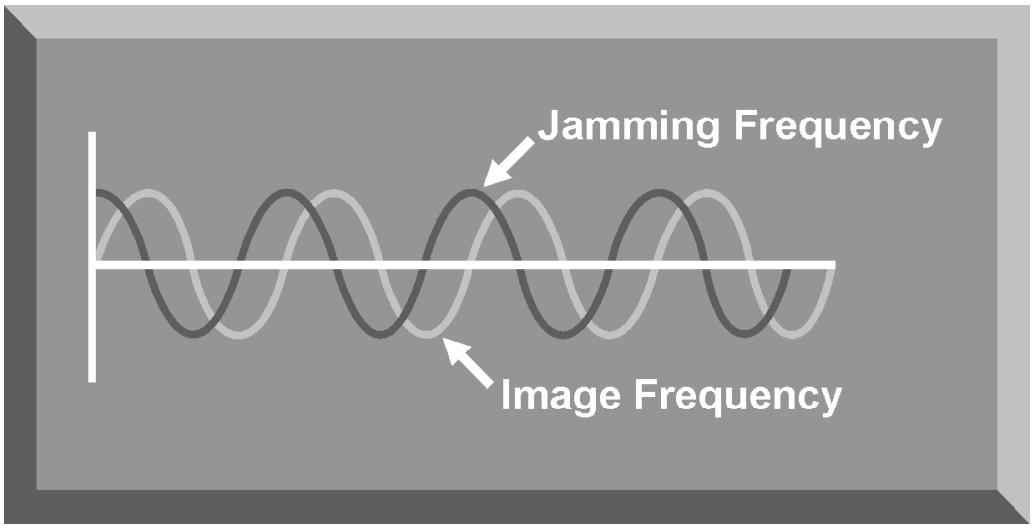


Figure 11-21. Monopulse Image Jamming

c. Cross-polarization jamming exploits the difference in the monopulse antenna pattern for a jamming pulse that is polarized orthogonal to the design polarization. The antenna pattern for a two-channel monopulse radar using sigma and delta beams shows the tracking point to be between the two beams (Figure 11-22). This is true if the radar is using its design polarization. However, the radar antenna also has a receiving pattern for a signal that is cross-polarized with the design frequency. For a cross-polarized signal, the tracking point is shifted one beamwidth to the right. This shift in the tracking point results in a target tracking signal that is 180° out of phase with the real signal. To be effective, a jamming signal polarized orthogonally to the design frequency of the radar would have to be 25 to 30 decibels, or about 1000 times, stronger than the radar signal.

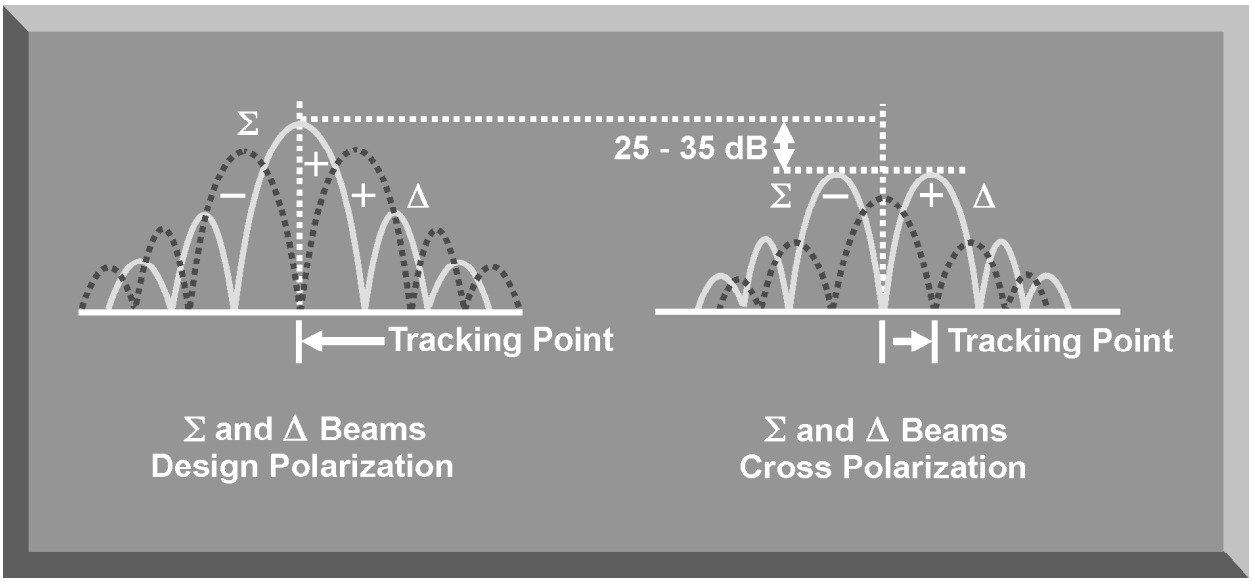


Figure 11-22. Cross-Polarization Antenna Pattern

(1) A cross-polarized jammer must receive and measure the polarization of the victim monopulse radar. The jammer then transmits a very high power jamming signal at the same frequency, but orthogonally polarized, to the victim radar. As a rule, the jamming signal must be 25 to 30 dBs stronger than the target return to exploit the tracking errors in the cross-polarized antenna pattern. Additionally, it must be as purely orthogonal to the design polarization as possible. Any jamming signal component that is not purely orthogonal will highlight the target and require more jamming power to cover the target return.

(2) A cross-polarized jammer must be able to generate a powerful jamming pulse that is polarized orthogonal to the victim radar. A cross-polarized jammer that generates the power and purity of polarization required to defeat monopulse angle tracking poses extreme technological challenges.

d. Cross-eye jamming is a complex technique that attempts to distort the wavefront of the beams in a monopulse radar and induce angle tracking errors. It exploits two basic assumptions of monopulse tracking logic in comparing target returns on a pulse-by-pulse basis. The first assumption is that a target return will always be a normal radar pulse echo. The second assumption is that any shift in amplitude or phase in a target return is due to the tracking antenna not pointing directly at a target. This condition generates an error signal and the antenna tries to null, but the amplitude or phase shifts.

(1) Cross-eye jamming attacks the two assumptions through a process of receiving and transmitting jamming pulses from different antennas separated as far apart as possible. In Figure 11-23, the phase front of a monopulse signal is received by the number 1 receive antenna, amplified by the repeater, and transmitted by the number 2 transmit antenna. The same phase front then hits receive antenna number 2, is shifted 180°, amplified by the repeater, and transmitted by the number 1 transmit antenna. These two out-of-phase signals must be matched in amplitude and must exceed the amplitude of the target return.

(2) When these jamming signals arrive at the victim radar, the tracking loop attempts to null out the amplitude and phase differences. With two widely spaced jamming sources at different phases, the antenna never achieves a null position or tracking solution. The distance between antenna pairs is an important parameter that determines the effectiveness of cross-eye jamming. The wider the spacing between antenna pairs, the more distortion in the victim's wave front near the true radar return. Most fighter aircraft do not provide sufficient spacing between the antennas to maximize effectiveness. Effectiveness is also lost when the aircraft is abeam or going away from the radar. To further complicate matters, when the radar is directly in front of the aircraft, the jamming pulses must have a power at least 20 dBs above the target return. Cross-eye jamming can also be defeated with a leading-edge tracker that rejects jamming signals arriving at the antenna behind the target return.

(3) Countering monopulse angle tracking is the greatest challenge for self-protection jamming systems. Skirt jamming and image jamming have had limited success. Cross-polarization and cross-eye jamming techniques require complex and sophisticated circuitry and much power.

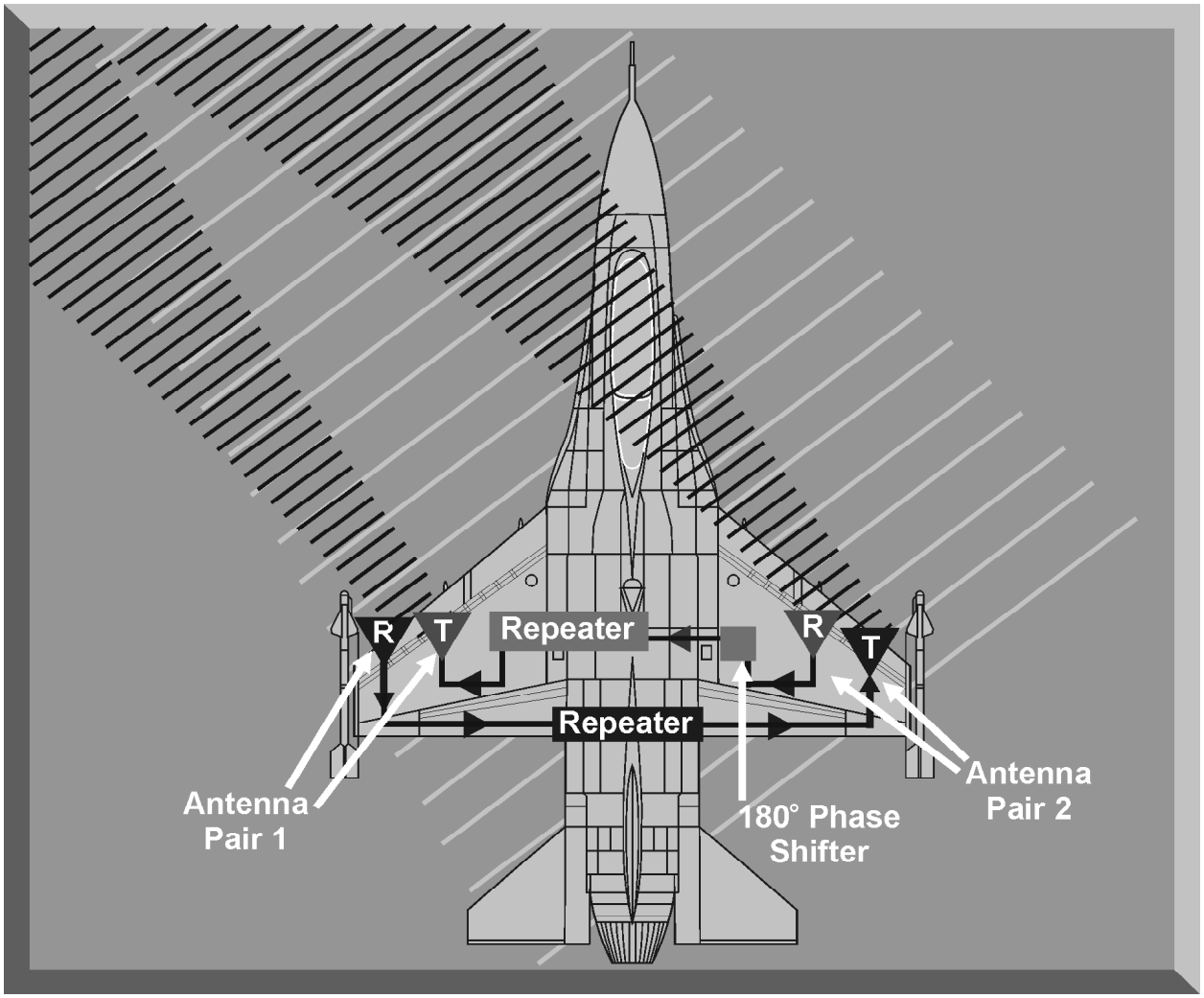


Figure 11-23. Cross-Eye Jamming

7. TERRAIN BOUNCE

Terrain bounce is a jamming technique used primarily at low altitude. It is used to counter semi-active, air-to-air missiles and monopulse tracking radars. The technique involves a repeater jammer that receives the radar or missile guidance signal. The jammer amplifies and directs this signal to illuminate the terrain directly in front of the aircraft. The missile or radar tracks the reflected energy from the spot on the ground instead of the aircraft (Figure 11-24).

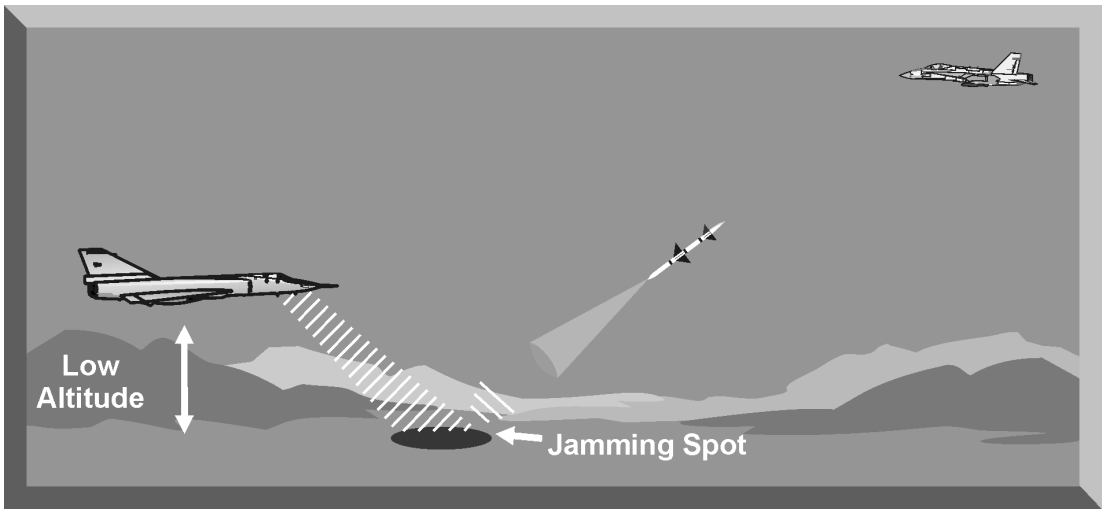


Figure 11-24. Terrain Bounce

a. To be effective, the terrain bounce jamming antennas should have a narrow elevation beamwidth and a broad azimuth beamwidth. This transmission pattern maximizes the energy directed toward the ground and minimizes the energy transmitted toward the missile or radar. To overcome signal losses associated with uncertain terrain propagation, the jamming system should also generate high jamming power. This ensures the energy reflected from the terrain is higher than the energy in the aircraft return. The terrain bounce jamming antennas should have very low sidelobes to preclude activation of any home-on-jam (HOJ) missile capability. For an air-to-air missile, the terrain bounce technique should be activated at long range. This will initially put the aircraft and the jamming spot in the same resolution cell. As the range decreases, the missile will be decoyed by the higher power in the jamming spot.

b. Some problems associated with terrain bounce jamming include the uncertainty of the signal scattering parameters of the various terrain features and the possible changes in signal polarization caused by terrain propagation. In addition, terrain bounce jamming can place maneuvering restrictions and maximum altitude limitations on the aircraft.

8. SUMMARY

There are several deception jamming techniques that can be employed to counter threat radar systems. The effectiveness of these techniques can be enhanced when they are employed in combination. For example, the effectiveness of an RGPO technique is enhanced when an angle deception technique is also employed. Determining the most effective deception technique, or combination of techniques, can present a challenge to intelligence and engineering analysts. However, when employed with maneuvers and chaff, deception techniques can mean the difference between success and failure on the modern battlefield.

CHAPTER 12. DECOYS

1. INTRODUCTION

A decoy is a device designed to look to an enemy radar more like an aircraft than the actual aircraft itself. Decoys do three primary missions: they saturate the enemy's integrated air defense system (IADS), coerce the enemy into exposing his forces prematurely, and defeat tracking by enemy radar. This chapter will discuss saturation decoys, towed decoys, and expendable active decoys. Chaff and flare systems will be discussed in separate chapters.

2. SATURATION DECOYS

A saturation decoy is usually an expendable vehicle designed to emulate a penetrating aircraft. Its mission is to deceive and saturate an enemy's IADS. Employing multiple saturation decoys can force an IADS to devote critical resources to engage these false targets. This depletes enemy assets available to engage penetrating aircraft. In addition, ground or air launched saturation decoys can be used to stimulate the IADS, to collect intelligence data, or to initiate attacks by suppression of enemy air defense (SEAD) assets. The three main characteristics of saturation decoys are their electronic signature, their flight program, and their mission type.

a. Saturation decoys must present an electronic signature, or radar return, that is indistinguishable from the aircraft they are protecting. Decoys can do this by either passive or active measures, or use a combination of both. A passive decoy is essentially a flying radar reflector. The size, shape, and materials used in the decoy are optimized to ensure that the proper amount of radar energy is returned to the enemy radars. Active decoys employ radar repeater systems to receive the enemy radar signal, amplify it and send back a radar return of the proper size to confuse the enemy. Reflecting or transmitting the proper size radar return is critical for both passive and active decoys. A return that is too large or too small will allow the enemy radar operator to differentiate between decoys and aircraft, causing the decoys to be ignored.

b. To continue deceiving an enemy IADS, a decoy must do more than provide the proper-sized radar return. Possessing flight characteristics similar to the aircraft it is protecting increases the probability that the decoy will effectively deceive an IADS for a sustained period of time. Modern decoys can either be powered with rockets, miniature engines, or simply glide for very long distances based upon the altitude and airspeed of the jet that releases them. Additionally, their flight paths can be pre-programmed into an onboard autopilot, allowing the decoy to fly an independent ground track, thus increasing their appearance as attack aircraft worth tracking.

c. Saturation decoys carry out two of the three decoy missions. Launched in significant numbers, they can saturate or overburden an IADS. Meanwhile, their realistic electronic image and preprogrammed flight paths entice the enemy to turn on radars and show his forces.

(1) Saturation decoys launched in coordination with an attacking strike package force the enemy to take time to process meaningless tracks and tie up critical assets. In this role, decoys primarily work against the early warning network of the enemy IADS by presenting the IADS with numerous targets to sort and track. Resources committed to tracking decoys may not be available to track actual aircraft. Additionally, if an enemy knows that decoys are present, he may not commit any resources against targets for fear they are just decoys.

(2) Time of radiation or "emission control" is a critical factor for acquisition and target tracking radars. To be effective and survive on the battlefield, ground threat radars radiate as little as possible; too much time radiating allows ELINT collectors to find their location and either direct aircraft to avoid them or call in an attack upon them. Therefore, when a decoy can get a radar to emit, the radar is now essentially compromised and can be avoided or attacked. Getting the enemy's radars to emit is called "stimulating the IADS," which is generally a precursor to any threat suppression mission.

(3) An extremely successful example of using decoys to stimulate the IADS was carried out in the Bekaa Valley in 1982. The Israelis opened the conflict by launching saturation decoys to successfully simulate an attack. While the Syrians reloaded, Israeli fighters attacked, destroying 17 of 19 Syrian SA-6s in the beginning of the battle. With the ground threat neutralized, the Israeli Air Force went on to destroy 85 Syrian fighters in the pure air-to-air conflict that resulted.

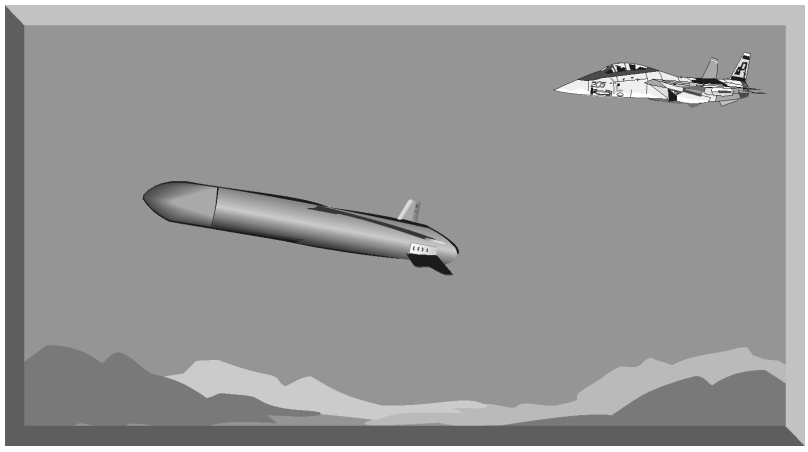


Figure 12-1. Tactical Air Launched Decoy

d. Two examples of saturation decoys are the Navy's Tactical Air Launched Decoy (TALD) in Figure 12-1 and the Air Force's proposed Miniature Air Launched

Decoy (MALD) in Figure 12-2. Both of these decoys can work actively or passively and both have pre-programmable flight paths. The TALD is an unpowered decoy normally launched from an F-14 Tomcat. The Air Force's MALD is a smaller jet-powered decoy also designed to be used by fighter aircraft. The MALD is 90 inches long, 6 inches in diameter, and has 25-inch wings that are foldable–essentially it is the size of an air-to-air missile. Because of its small size, the MALD can be carried into the target area before it is launched. Once launched it uses its speed, independent flight path, and electronically manipulated radar signature to make acquisition radars and target tracking radars mistake it for one of the attacking aircraft.

Figure 12-2. Miniature Air Launched Decoy (MALD)

3. TOWED DECOYS

A towed decoy is a small jammer that is physically attached to the aircraft (Figure 12-3). Unlike the saturation decoys that work against the IADS, the towed decoys are for individual aircraft survival. Towed decoys are designed to defeat enemy missiles in the final stages of an engagement; therefore, towed decoys, as well as other expendables, are known as endgame countermeasures. While towed decoys are primarily designed to provide sufficient miss distance between an attacking semi-active radar missile and the protected aircraft, they may also be effective against pulse Doppler radars and monopulse radars.

a. To be effective, the towed decoy must turn on within the threat radar's resolution cell after the radar is tracking the protected target. To successfully decoy the missile, the towed decoy must return radar signals with sufficient power to simulate a radar cross section (RCS) significantly larger than that of the

protected target. There are currently two generations of towed decoys on the market. Their primary difference lies in the connection each has with the aircraft towing it.

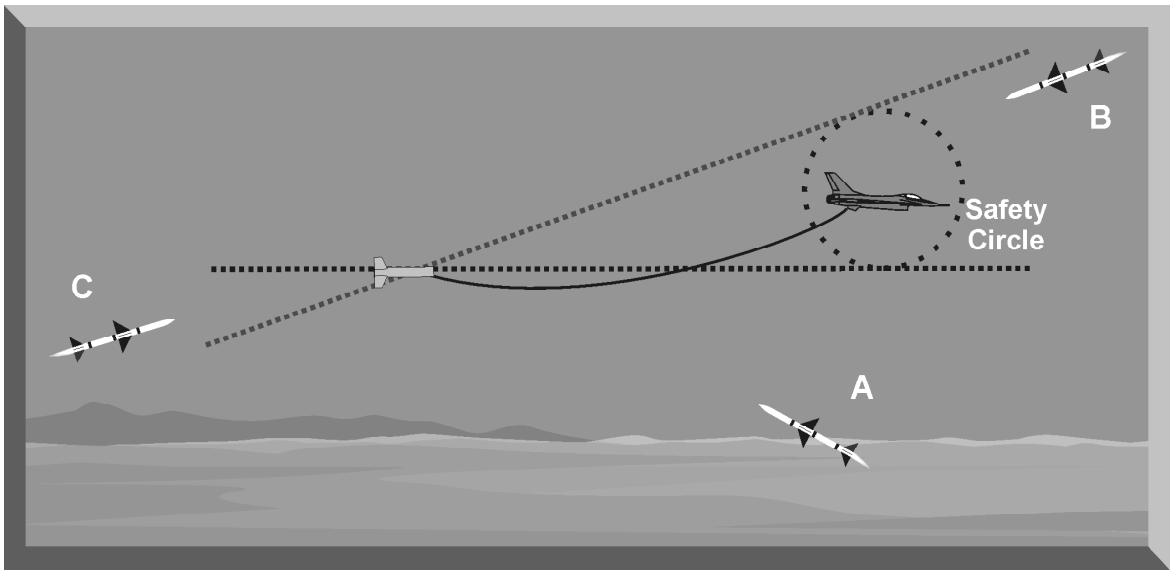


Figure 12-3. Towed Decoy

(1) The first generation of towed decoys contains a simple repeater jammer that enhances any signal it receives in the proper frequency range. The enhanced signal is stronger than the aircraft signal so the missile is lured towards the decoy. These decoys are stand-alone units that contain all the electronics, processors, receivers and transmitters within them. The only tie to the aircraft is for power and status. One of the big advantages of these simple repeater devices is that they do not require the exact frequency of the enemy radar systems to be effective, they will enhance any signal coming at them. An area of concern with the use of towed decoys is possible conflict between the onboard jamming system and the towed decoy. The onboard system could overpower the decoy, causing the attacking missile to ignore the decoy and track the aircraft.

(2) The second generation of decoys is tethered to the aircraft via fiber optic cable. Through this cable travels the different jamming modulations to be used by the decoy. These fiber optic towed decoys (FOTD) only contain the transmitters; the remaining items are in the jet or the pod. This system allows for more complex jamming through the decoy, including cooperative jamming between the aircraft and the decoy.

b. The separation required between the decoy and the aircraft is a primary consideration in developing a towed decoy system. The towed decoy should be positioned far enough behind the aircraft to preclude warhead fragments from missiles guiding on the decoy from also impacting the aircraft. Missile A in Figure

12-3 depicts a situation where the missile will detonate well outside of the aircraft's safety circle. From a pilot perspective, any restrictions on aircraft maneuvering imposed by a towed decoy are very important. The number of decoys that can be carried and the time required for decoy deployment are also important employment considerations.

c. Achieving 360° coverage is a primary limitation of a towed decoy system. When an aircraft equipped with a towed decoy is abeam a threat radar, the radar may be able to discriminate between the aircraft and the decoy. This is a function of the resolution cell of the radar. In addition, missiles approaching from a high-aspect angle, and above the aircraft (Figure 12-3 - Missile B), may fuse on the aircraft while guiding to the decoy. Missiles approaching from a low-aspect angle (Figure 12-3 - Missile C) may not fuse on the decoy and subsequently acquire and fuse on the aircraft. Finally, if the decoy is destroyed or lost, the time required to deploy a replacement decoy is critical, especially if the aircraft is engaged by multiple missiles.

d. An example of a fielded towed decoy system is the AN/ALE-50 (Figure 12-4). This first generation towed decoy system is found on Air Force F-16 and B-1 aircraft, and there is a version that is integrated into the ALQ-184 pod.

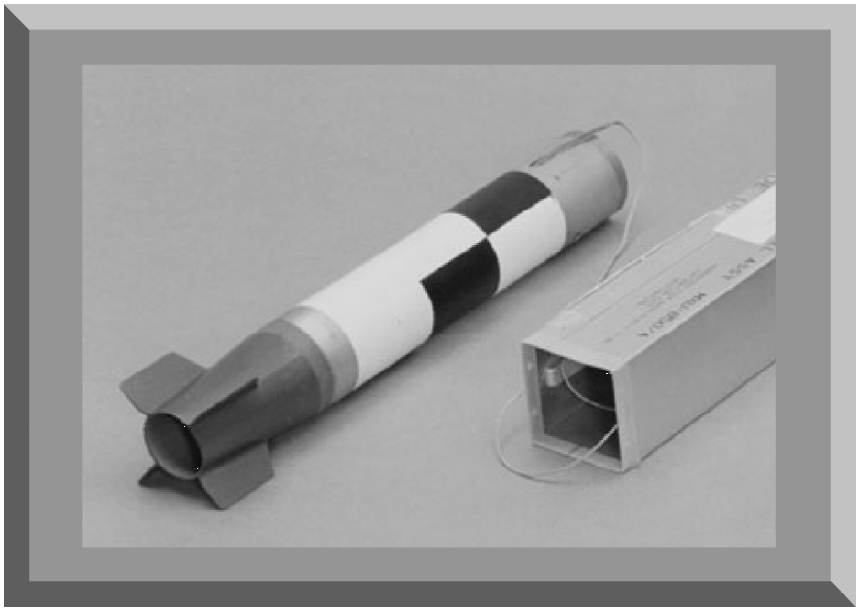


Figure 12-4. AN/ALE-50 System

(1) The system consists of a launch controller subsystem and towed decoys. The launch controller houses the decoy before it is launched, provides power to the decoy, and provides for the monitoring of the electronics. The decoy body is a factory sealed, self-contained unit with everything except for power. Power comes through the tether from the host aircraft; the decoy sends its operating status back through the tether to the aircraft.

(2) ALE-50 decoy use is cleared throughout the flight regime of the F-16 and B-1. Decoys can be deployed without being turned on, but once a decoy has been deployed, it cannot be reeled back in and must be severed before landing. Procedures are in place to reduce the chance that the onboard jamming system will negate the decoy.

(3) The ALE-50 towed decoy is a wideband RF repeater that provides self-protection EA by receiving, electronically amplifying, and retransmitting enemy radar RF signals. Upon receiving a threat radar signal, this simple repeater amplifies the signal and retransmits it. This provides the radar with two signals, one reflected from the aircraft and a stronger one from the decoy. With the signal from the decoy being the more attractive, the radar or missile guides towards the decoy. During combat operations over Kosovo, ALE-50 decoys were credited with saves for both F-16s and B-1s.

4. EXPENDABLE ACTIVE DECOYS

Expendable active decoys are designed to lure the tracking gates of an enemy's radar away from the aircraft. They are endgame countermeasures like towed decoys, but they differ in that expendable decoys free-fall or glide to the ground as opposed to being towed behind the aircraft.

a. Expendable decoys are small, active jamming systems designed to be expended by existing aircraft chaff and flare dispensers, such as the AN/ALE-40 or the AN/ALE-47. Expendable decoys can employ noise or deception jamming with noise jamming being the most common. Deception jamming techniques can be employed to enhance effectiveness against pulse Doppler radars. There are two challenges associated with expendable jammers: the amount of the time the jammer is effective and the packaging (Figure 12-5).

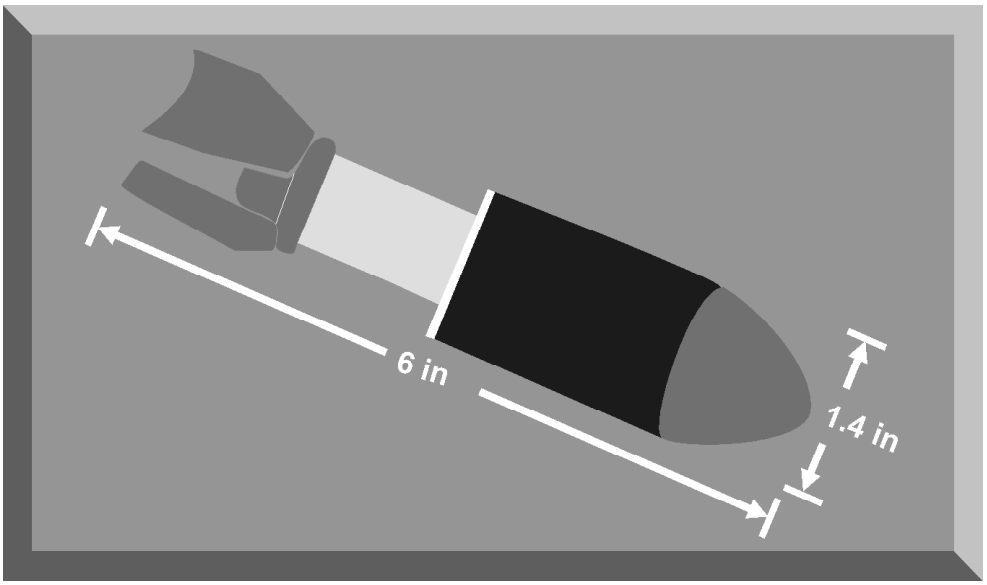


Figure 12-5. Generic Expendable

b. Expendable decoys are designed to provide protection for the dispensing aircraft for a specific period. The dispensing altitude and rate of fall determine this period of effective coverage. Expendable decoys can employ small parachutes of aerodynamic design to slow the rate of fall and increase the time of effective coverage. If the period of coverage is too short, multiple expendable decoys must be employed. This places a premium on timely employment and expendables management.

c. The primary components of an expendable decoy are the transmit and receive antennas, techniques generator, amplifier, and power supply. The transmit and receive antennas should be isolated and capable of high gain, wide bandwidth, and should use compatible polarization with the victim radar. The techniques generator must recognize the victim radar signal and generate the appropriate jamming response. The amplifier must be capable of generating a high power jamming signal over a wide frequency range. To meet these requirements, sophisticated computer and miniaturization techniques are used, and the components packaged to all fit in the aircraft dispenser. These factors impact the cost of expendable decoys and may limit the availability of these assets.

d. The Generic Expendable, RTE-1489, commonly called the GEN-X decoy is a fielded expendable active decoy. The decoy is sized to fit into a 1.4 x 1.4 x 5.8 inch cartridge and take advantage of new microwave/millimeter-wave integrated circuit (MMIC) technology. The GEN-X is programmable and features a broadband antenna and wide frequency coverage. After ejection, the decoy extends three small fins for stability. Its battery ignites to provide power, the receiver locks on to the threat radar signal, and a deception signal is generated and transmitted.

5. SUMMARY

Decoys simply provide the enemy with more targets to process. In the case of saturation decoys, this forces the enemy to commit resources against false targets, or show his defenses. For towed decoys and expendable active decoys, it makes the missile or tracking radar separate a real target from more electronically attractive decoys.

CHAPTER 13. CHAFF EMPLOYMENT

1. INTRODUCTION

Chaff was first used during World War II when the Royal Air Force, under the code name "WINDOW," dropped bales of metallic foil during a night bombing raid in July 1943 (Figure 13-1). The bales of foil were thrown from each bomber as it approached the target. The disruption of German AAA fire control and ground control intercept (GCI) radars rendered these systems almost totally ineffective. Based on this early success, chaff employment became a standard bomber tactic for the rest of the war.

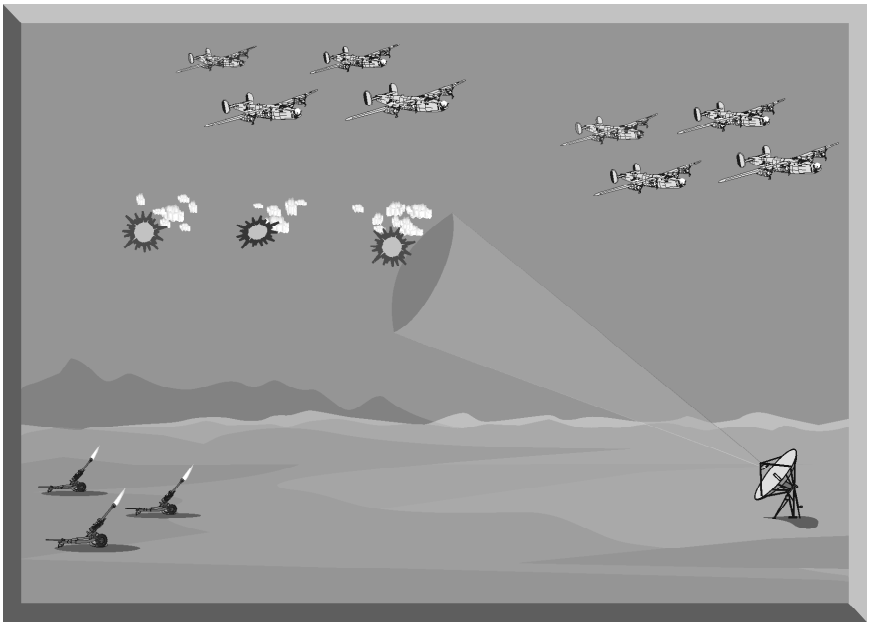


Figure 13-1. "WINDOW" – The First Operational Employment of Chaff

a. Chaff is one of the most widely used and effective expendable electronic attack (EA) devices. It is a form of volumetric radar clutter consisting of multiple metalized radar reflectors designed to interfere with and confuse radar operation. It is dispensed into the atmosphere to deny radar acquisition, generate false targets, and to deny or disrupt radar tracking. Chaff is designed to be dispensed from an aircraft and function for a limited period.

b. Even with the development and deployment of advanced radar threat systems, chaff continues to be an extremely effective EA device. Experience gained during the Vietnam conflict, the 1973 Yom Kippur War, and DESERT STORM clearly shows that chaff effectiveness against radar threats is still a factor with which the enemy must contend. This is especially true when chaff is employed with self-protection jamming and aircraft maneuvers.

c. Chaff screening and self-protection are the two basic chaff employment tactics. Chaff screening tactics, including area saturation and chaff corridor employment, are designed to confuse and deny acquisition information to the early warning, GCI, and acquisition radars supporting surface-to-air missile (SAM) systems. Self-protection tactics are designed to counter acquisition and target tracking radars (TTRs). When used with jamming and maneuvers, chaff can cause TTRs to break lock or generate survivable miss distances if a SAM is fired at the aircraft.

2. CHAFF CHARACTERISTICS

To understand how chaff affects radar systems, it is important to understand its characteristics. The most important chaff characteristics are radar cross section (RCS), frequency coverage, bloom rate, Doppler content, polarization, and persistence.

a. RCS is a measure of the net reradiated energy from a target to the illuminating radar. The RCS of an aircraft varies based on the size, shape, type of skin surface, configuration, and aspect to the illuminating radar. Figure 13-2 shows the effect of aspect on aircraft RCS. The RCS is greatest when the aircraft aspect is 90°, or abeam the radar. The lowest RCS occurs near the 30-70° and 110-150° of aspect. Since the aircraft RCS also varies based on frequency, the victim radar's frequency is a key factor. To be effective, chaff must be dispensed in large enough quantities to create an RCS greater than the aircraft RCS.

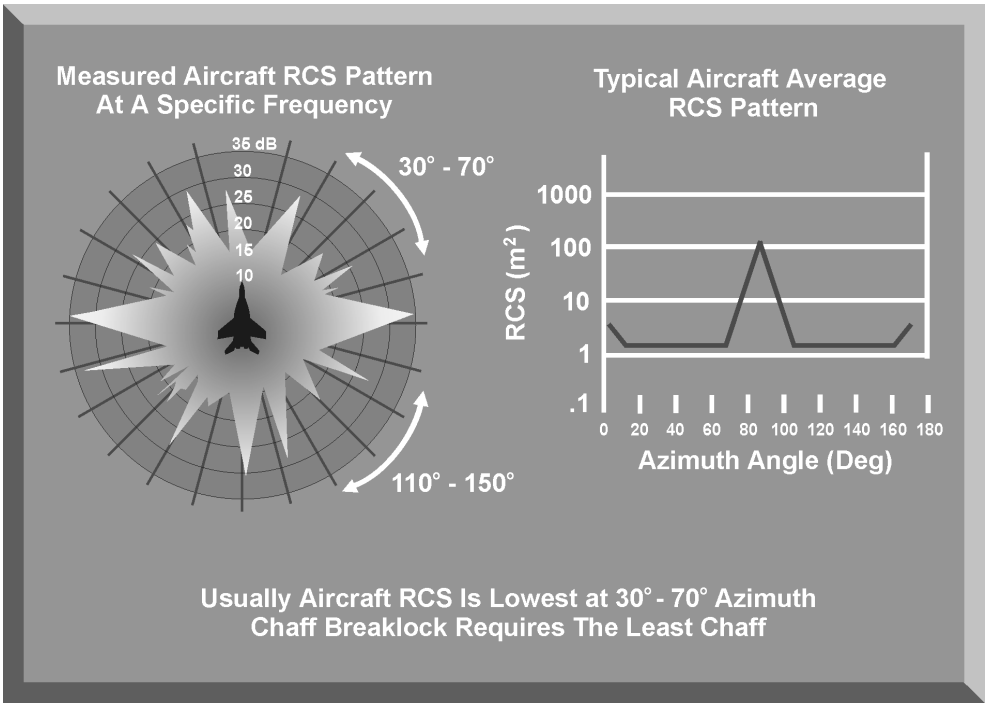


Figure 13-2. Aircraft Radar Cross Section (RCS)

(1) The RCS of a chaff bundle depends on the frequency of the victim radar and the dispensing aircraft's relative position, or aspect. Figure 13-3 shows the RCS of a single RR-170 chaff cartridge based on frequency. It shows that the largest RCS occurs at about 3 GHz. However, for the spectrum between 2-18 GHz, which includes most SAM TTRs, the RCS of the RR-170 cartridge is over 50 square meters. Since the typical fighter aircraft RCS varies between 1 and 10 square meters, depending upon frequency and aspect, the RR-170 chaff cartridge should provide a sufficient RCS to mask the aircraft RCS.

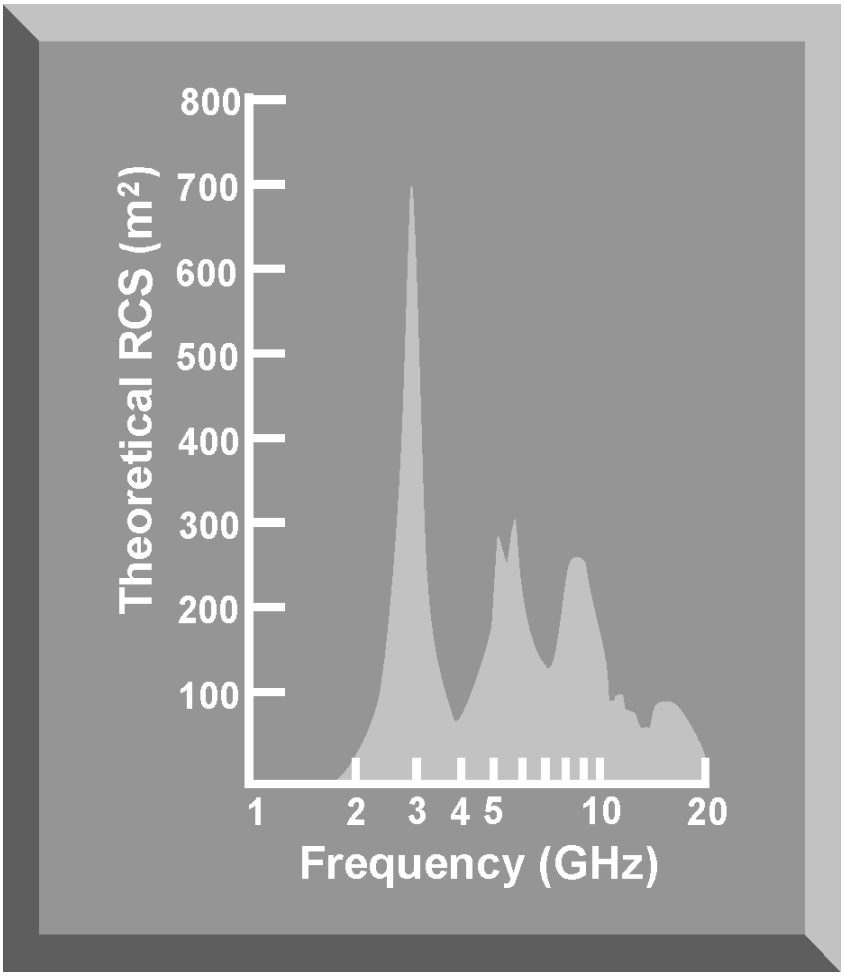


Figure 13-3. RR-170 Chaff Cartridge RCS

(2) The angular relationship, or aspect, between the aircraft and chaff bundle affects the chaff RCS presented to the victim radar. Chaff RCS is greatest when the chaff bundle and the aircraft are abeam the threat radar. It is smallest when the threat radar is off the nose or tail of the aircraft. Aspect is important when developing self-protection maneuvering and chaff dispensing tactics against threat radars (Figure 13-4).

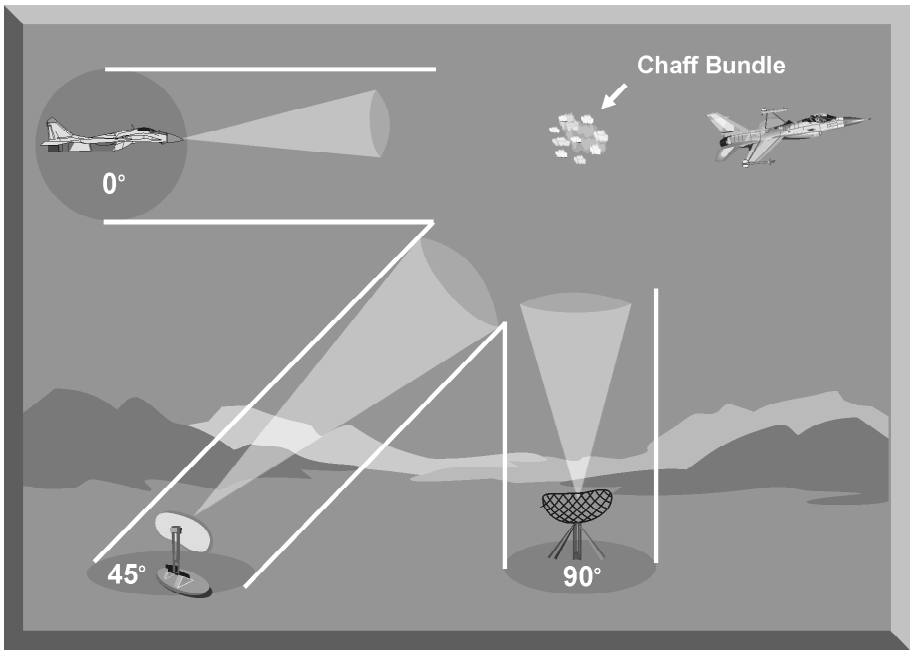


Figure 13-4. Threat Radar Aspect and Chaff RCS

(3) Dispensing multiple chaff bundles simultaneously does not necessarily increase chaff RCS. Multiple bundles increase the density of the chaff but do not directly enhance self-protection capabilities (Figure 13-5). This is an important consideration when developing chaff dispenser rates to counter threats.

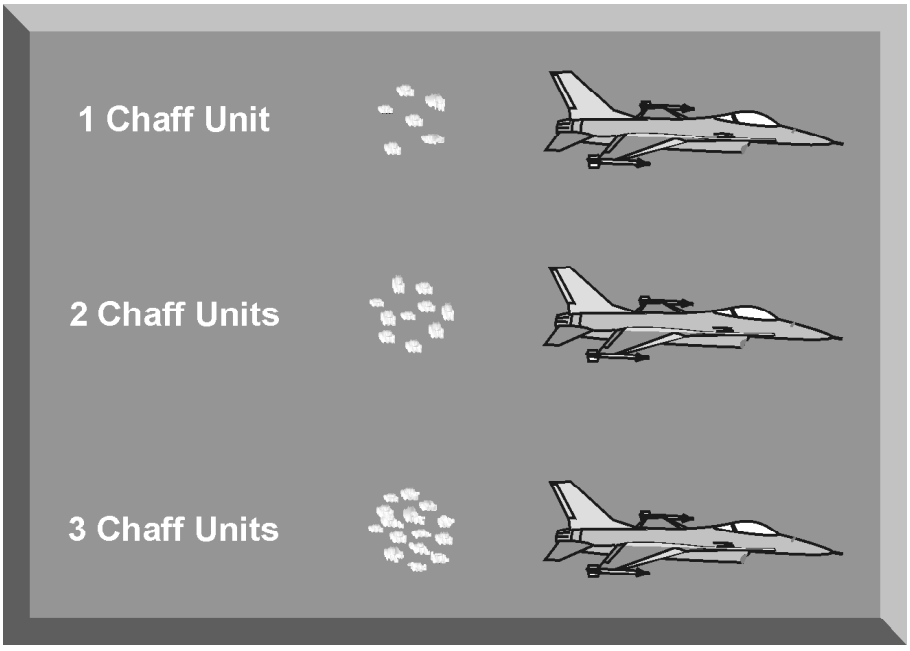


Figure 13-5. Impact of Multiple Chaff Cartridge Employment on Chaff RCS

b. Each strip of chaff is a dipole reflector that reradiates the electromagnetic energy received from an emitting radar and creates a radar echo. The optimum size is cut to about one-half the wavelength of the victim radar's RF. Since a single cut length is restricted in effectiveness to a narrow range of frequencies, different lengths are normally packaged together to provide coverage over a wide range of frequencies (Figure 13-6).

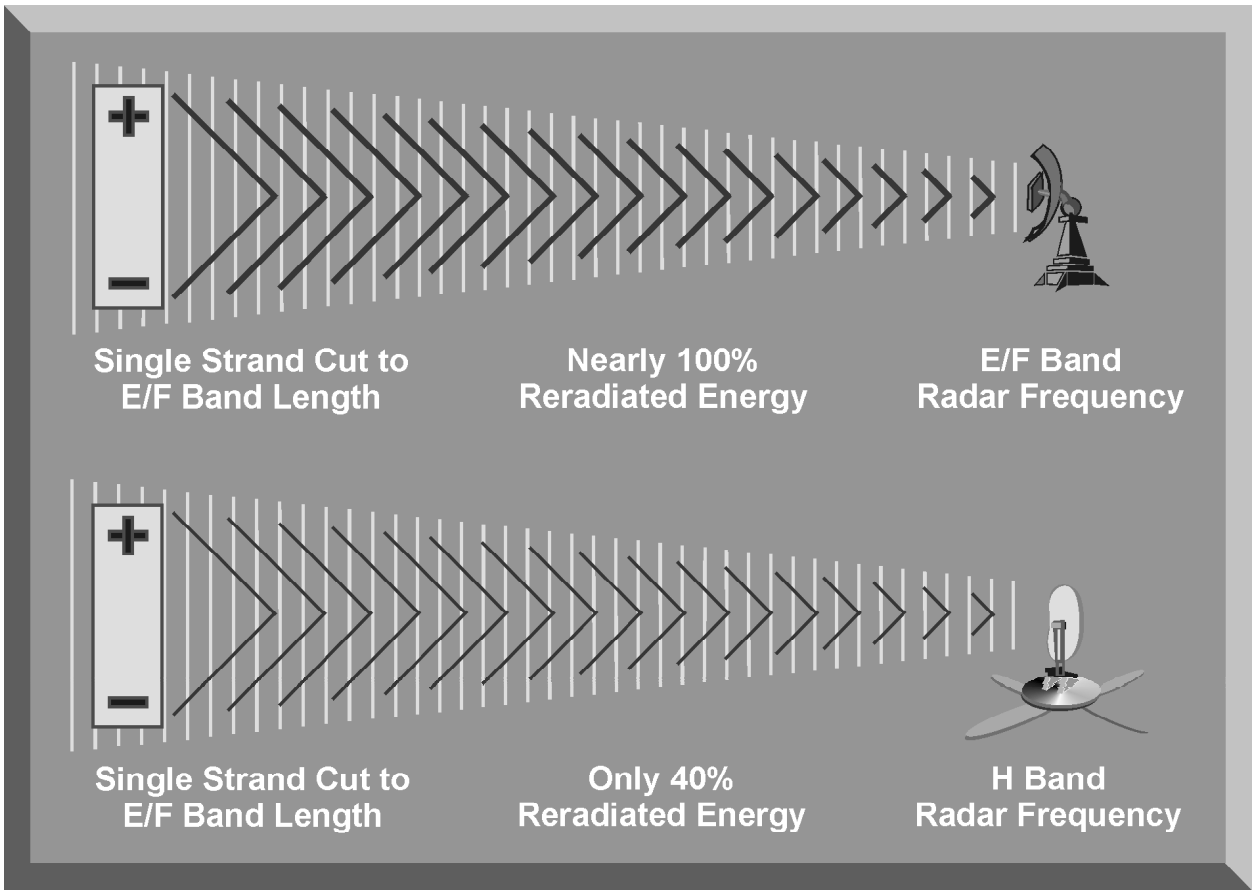


Figure 13-6. Chaff Length and Frequency Coverage

(1) Considerable research and development has reduced the size and increased the effectiveness of self-protection chaff. There are various chaff sizes, shapes, and materials. Most chaff carried on fighter aircraft are made of small aluminum strips, coated strips of nylon, or fiberglass. These strips are cut to various lengths and compressed into bundles that are small and light enough to allow the aircraft to carry and dispense multiple chaff bundles. These cuts of chaff are packaged into chaff cartridges and inserted into a dispenser on the aircraft. An explosive squib assembly ejects the cartridges from the dispenser and disperses the chaff (Figure 13-7).

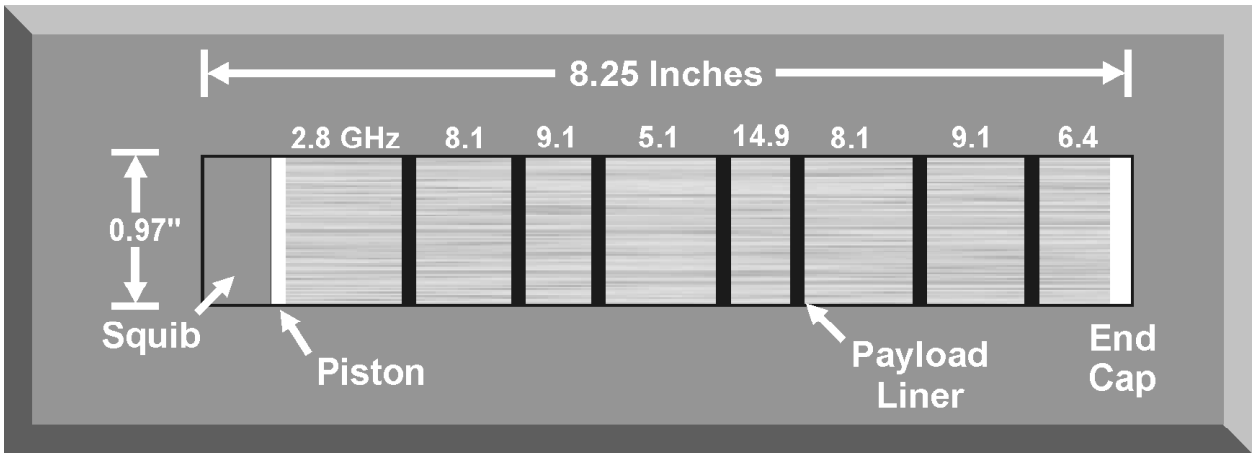


Figure 13-7. RR-170 Chaff Cartridge

(2) To provide as many dipoles as possible and present the maximum radar cross section, each chaff bundle has numerous chaff cuts to match a predetermined range of frequencies. Each chaff cartridge contains almost 3 million dipoles packaged in an eight inch by one-inch cartridge. The dipole frequencies cover the frequency range where most SAM TTRs and air-to-air radars operate (2 - 18 GHZ).

c. Bloom rate, the rate at which chaff will scatter, is also a very important characteristic of self-protection chaff. Self-protection chaff effectiveness is based on the relationship of bloom rate, chaff RCS, aircraft RCS, and the resolution cell of the threat radar system. The ability of chaff to effectively defeat a target tracking radar is directly related to the chaff dispense rate, which determines the chaff RCS, which should be larger than the aircraft's RCS. The chaff bundles must also bloom within the resolution cell of the radar.

(1) Chaff bloom rate is dependent on aerodynamic factors associated with the chaff type, the location of the dispenser on the aircraft, and the aircraft wake or turbulence. Heavy or dense chaff falls faster and blooms slower than lighter and less dense chaff. The location of the chaff dispenser on the aircraft affects the airflow in which the chaff will be dispensed. The ideal position for the dispenser is in the area where there is the most turbulence from the aircraft. Turbulence behind the aircraft is probably the most important factor affecting bloom rate. The more turbulent the airflow, the greater the bloom rate (Figure 13-8). Maneuvering the aircraft while dispensing chaff also enhances the chaff bloom rate.

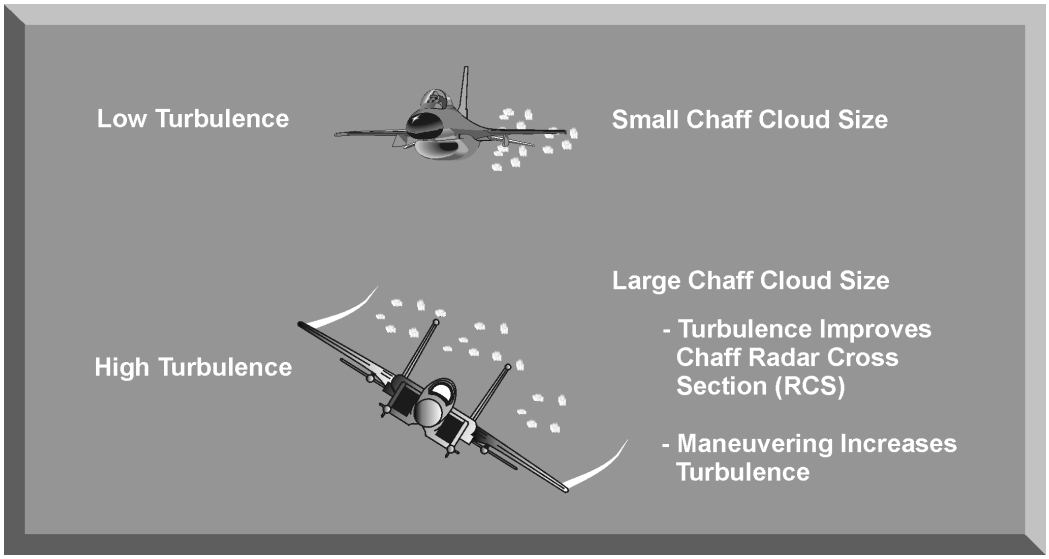


Figure 13-8. Impact of Turbulence and Chaff Bloom Rate

(2) To ensure that the victim radar is decoyed or that it transfers automatic tracking to the chaff, the chaff must bloom within the radar resolution cell. This resolution cell is a three-dimensional spheroid with dimensions based on the pulse width, horizontal beamwidth, vertical beamwidth, and the range of the aircraft (Figure 13-9). There are some rules of thumb that can be used when considering the bloom rate of chaff and the resolution cell of a particular radar. The shorter the pulse width of a radar, the faster the chaff has to bloom to be effective. The narrower the horizontal and vertical beamwidths, the faster the chaff has to bloom to be effective.

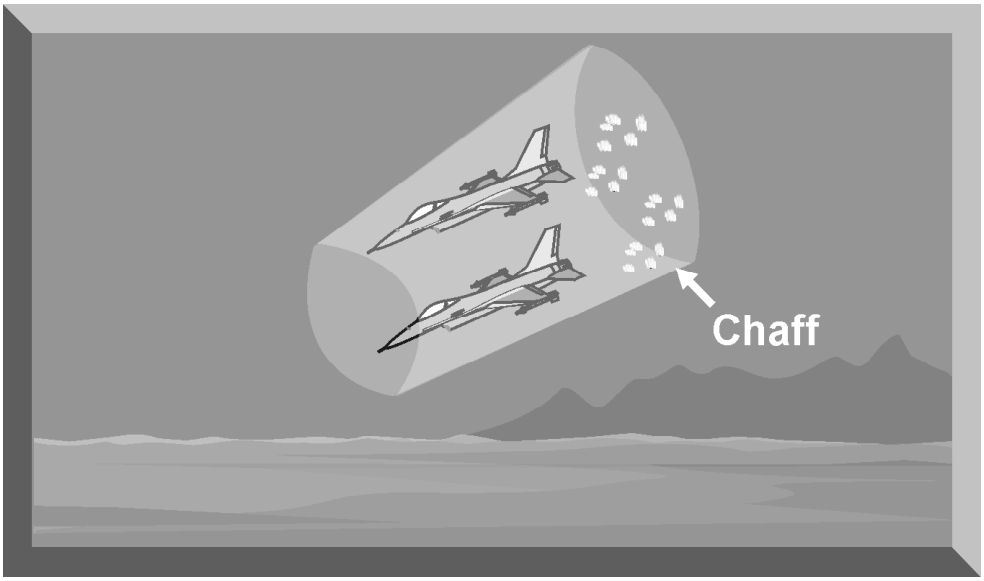


Figure 13-9. Chaff Bloom Rate and Radar Resolution Cell

d. Against Doppler radars, self-protection chaff is most effective when dispensed at or near the beam, relative to the threat radar. When chaff is dispensed in the airstream, the drag on an individual dipole is so great compared to its mass that it slows to the velocity of the surrounding air mass almost instantly. Since the relative velocity of the chaff, in relation to the radar, is zero, radar systems employing Doppler processing and tracking will not display the chaff. Doppler processing radars will continue to track the aircraft unless it also has a relative velocity of zero. This occurs when the aircraft is abeam the radar. Chaff corridor and area saturation tactics against Doppler tracking radars will have limited effectiveness.

e. Chaff persistence and polarization are two additional characteristics that are important employment considerations for area saturation or chaff corridor operations. These individual chaff element characteristics are directly related to the combined effects of aerodynamic, atmospheric, and gravitational influences.

(1) Chaff persistence is the length of time the chaff is at an effective altitude to screen ingressing aircraft during area saturation or chaff corridor operations. The time span depends on the fall rate of the chaff and varies according to the density of the dipoles. The prevailing atmospheric conditions, such as wind and temperature also affect chaff persistence. Generally, the longer cuts used for lower frequency radars fall faster than the shorter cuts used for higher frequency radars. Each type has its own rate of fall based on these conditions. The rate of fall is a critical mission planning consideration for determining the amount of time between chaff corridor or area saturation initiation and the arrival of the aircraft being screened. If the chaff is employed too early, it may not be at the correct altitude or may have dispersed to the point that it is not effective to screen ingressing aircraft.

(2) Each chaff strand is a polarized dipole with positive and negative ends. The orientation of these strands determine their polarity (Figure 13-10). Chaff cuts with the positive and negative ends oriented vertically are vertically polarized. Chaff cuts with the positive and negative ends oriented horizontally are horizontally polarized. Since chaff strands are initially buffeted by turbulence and airstream vortices, the dipole orientation and polarization, changes rapidly and randomly. Eventually, the strands separate into two groups; one descending horizontally, and one descending vertically. Since the vertically oriented strands tend to fall faster, the lower part of the chaff cloud tends to become more vertically polarized, while the upper portion is horizontally polarized. A threat radar that uses vertical polarization will receive minimal affects from the upper (horizontally polarized) portion of the chaff cloud. If the aircraft being screened are flying within this portion of the chaff cloud, they may be detected and engaged. This is another mission planning consideration for chaff area saturation or chaff corridor operations.

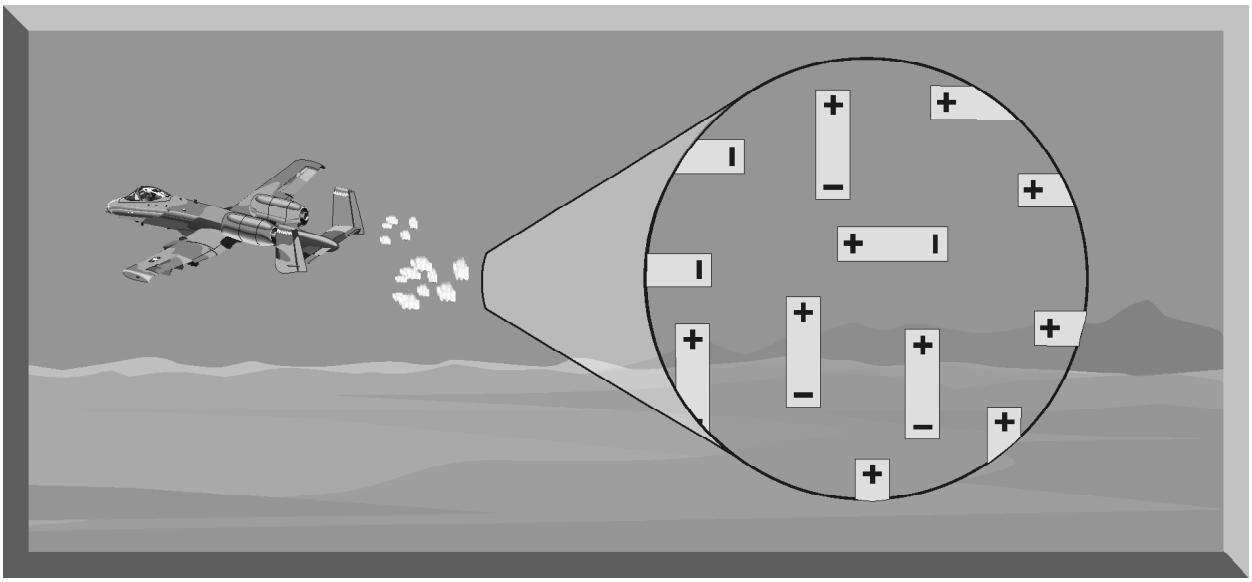


Figure 13-10. Impact of Chaff Polarization

3. CHAFF OPERATIONAL EMPLOYMENT

The two primary chaff employment tactics are force screening and self-protection. Force screening tactics include area saturation and corridor operations. Self-protection tactics include the reactive employment of chaff to negate a potentially lethal engagement. Different chaff dispensing techniques are used for each employment tactic and are important planning considerations for all chaff employment tactics. This section will discuss area saturation, corridor operations, and self-protection chaff employment.

a. The objective of area saturation operations is to present multiple false targets in a specific area in order to saturate radar systems and confuse the enemy integrated air defense system (IADS). Area saturation can be accomplished by fighter aircraft or drones equipped with chaff pods employing random chaff dispensing techniques. The chaff dispenser is set to release random bursts of chaff along the ingress and egress route of the attack package. Chaff pods may be supplemented with chaff bombs containing special fuses that provide false targets at varying altitudes. Attack aircraft can also contribute to area saturation by randomly dispensing self-protection chaff as they ingress and egress. However, this tactic can deplete the number of chaff bundles an attack aircraft may need to defeat a potentially lethal radar system encountered at a later time in the mission.

(1) The chaff cuts must provide frequency coverage for the threat radar systems. Also the RCS of each chaff burst should be large enough to present a realistic target to the victim radars. Multiple false targets created by chaff area saturation may confuse threat system operators and encourage them to expend missiles on false chaff targets.

(2) Saturation also masks the number of attacking aircraft (Figure 13-11). When used with false target deception jamming, area saturation can greatly enhance mission success. However, the technique is resource-intensive since aircraft employing chaff pods and chaff bombs cannot attack targets. These aircraft are vulnerable to attack and should be supported by standoff jamming. Area saturation tactics may have limited success against Doppler processing radars.

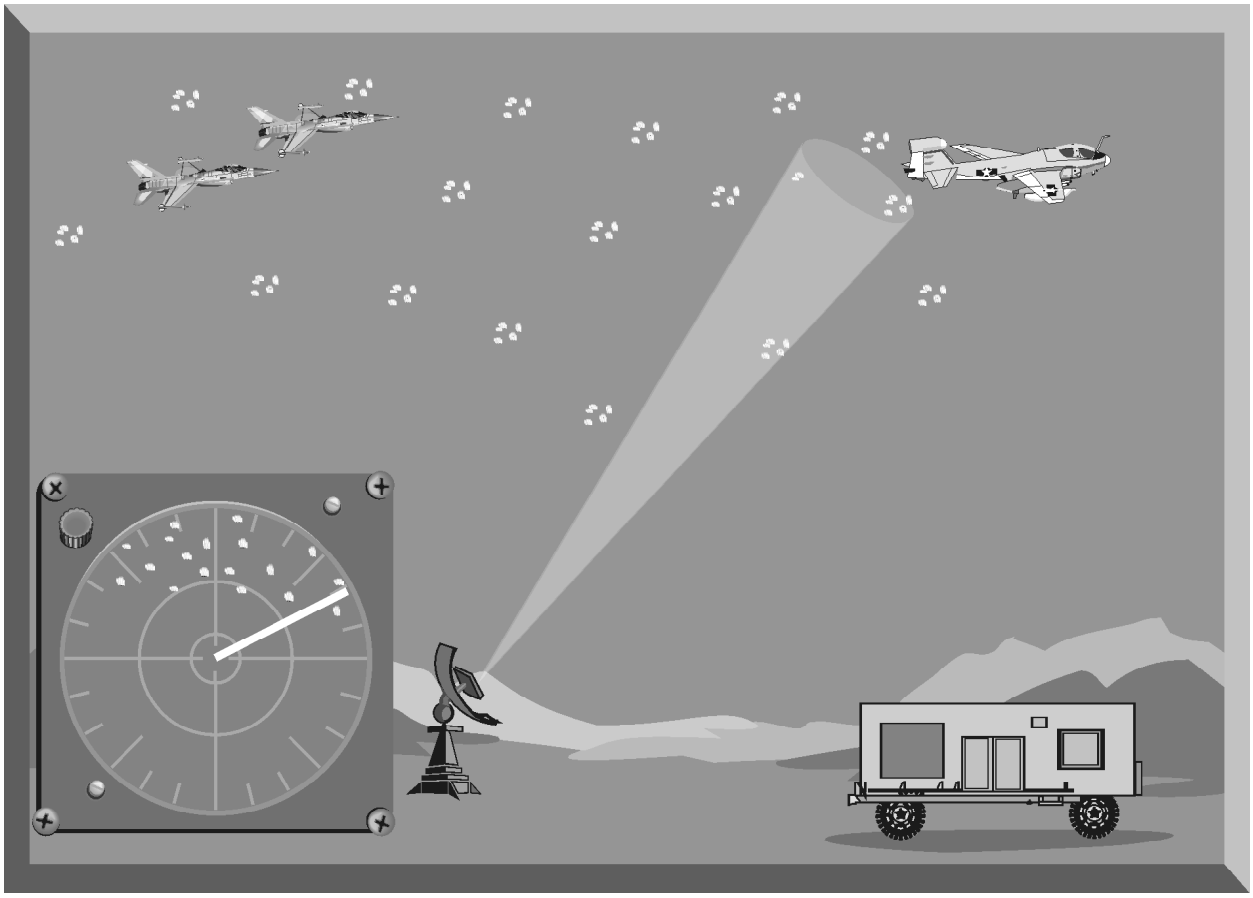


Figure 13-11. Area Saturation Tactics

b. The objective of chaff corridor operations is to screen the ingress and egress of an attack package by dispensing large quantities of chaff in a continuous "ribbon." Fighter aircraft, or drones equipped with chaff pods such as the ALE-38, employ a stream chaff dispensing technique to "lay" the chaff corridor. The pods are set to provide a continuous line of chaff dense enough to hide ingressing and egressing aircraft. The chaff cuts should provide frequency coverage for the radar systems that must be countered. Timing for the chaff aircraft in relation to the attack package must consider the fall rate and persistency of the chaff to ensure that the chaff corridor covers the required altitude for a time sufficient to allow the attack package to ingress and egress. An effective chaff corridor completely denies a radar's ability to distinguish between

the chaff and the attack aircraft. To do this, the radar cross section, or RCS, of the chaff within the resolution cell of the radar must exceed the RCS of the aircraft. This condition must be met throughout the length of the chaff corridor. When this condition is met, the chaff corridor will appear as a continuous return on the victim radar scope, and the attack package cannot be detected (Figure 13-12).

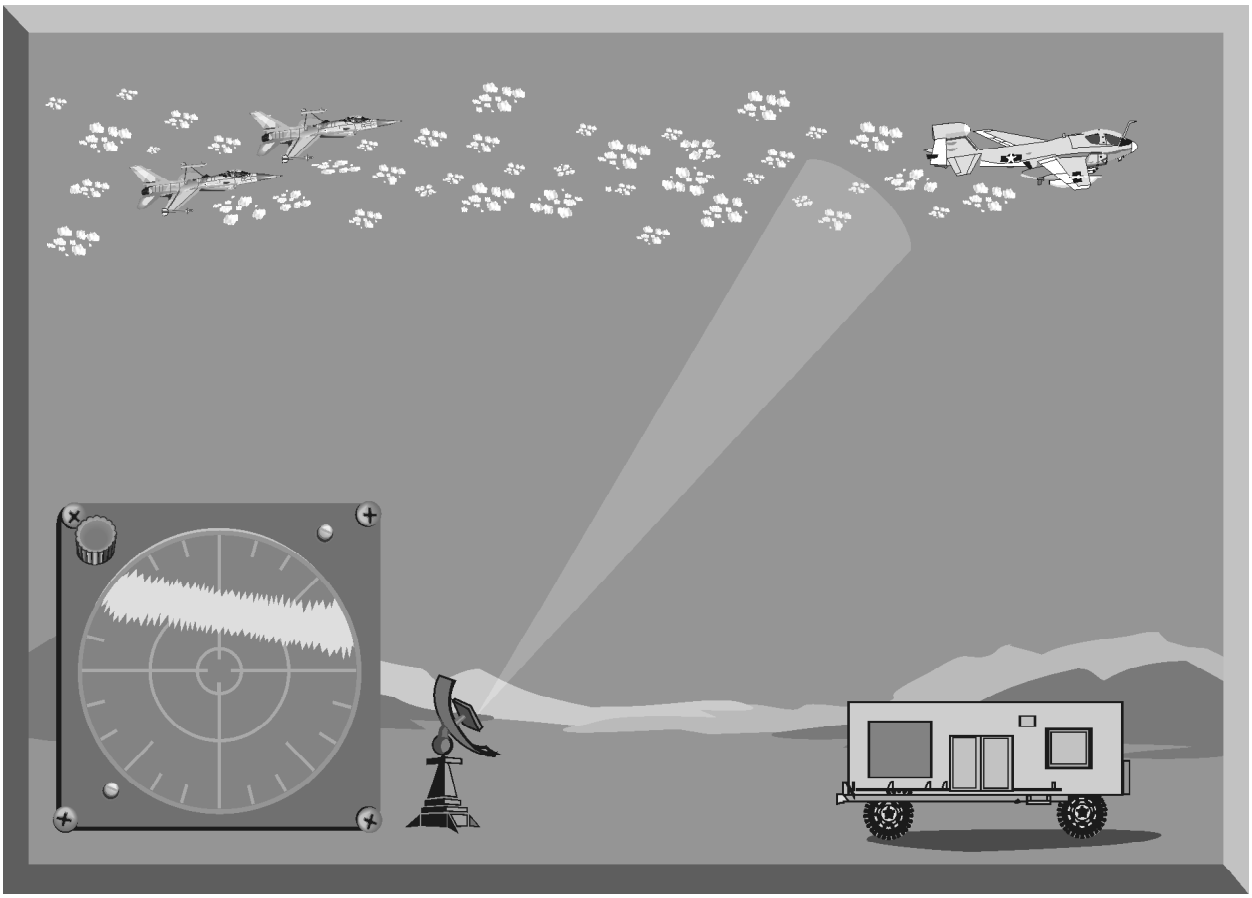


Figure 13-12. Chaff Corridor Tactics

(1) One advantage of a chaff corridor is that it can screen ingressing and egressing aircraft from pulse radar systems. However, chaff corridors are resource-intensive. Aircraft "laying" the corridor cannot strike critical targets. The chaff aircraft are also vulnerable to attack. Therefore, standoff jamming and self-protection jamming systems should be employed to provide some screening and protection for the chaff dispensing aircraft. Finally, chaff corridors may not be effective against radars with Doppler processing.

(2) To be effective, chaff corridor operations require detailed planning. Electronic combat (EC) planners must first determine that a chaff corridor is the most effective way to screen the attack force. This decision is based on the vulnerability of the attack aircraft to the anticipated threat radar systems and the availability of chaff assets. Once the decision is made to employ a chaff corridor,

planners must select the location, determine the length of the chaff corridor, select the ingress and egress altitudes, and establish the timing for the chaff aircraft and the attack package. Once the location of the chaff corridor is determined, planners must assess the threat radar systems that must be countered. The specific operating frequencies of the threat radars will determine the cuts of chaff that must be dispensed. The resolution cells of the threat radars will determine the density of chaff required. The length of the chaff corridor and the chaff density will determine the number of chaff aircraft required to seed the chaff corridor. The chaff fall rate and the atmospheric conditions impact the timing between the chaff aircraft and the attack package, and the altitude that the chaff dispensing aircraft must fly.

c. Self-protection chaff tactics are based on the use of chaff dispensers that use burst chaff dispensing techniques to defeat a TTR. Burst chaff dispensing, employed during the final phase of an engagement by air-to-air or surface-to-air weapons, can generate tracking errors or a radar break-lock. Burst chaff effectiveness is greatly enhanced when accompanied by jamming and evasive maneuvers (Figure 13-13).

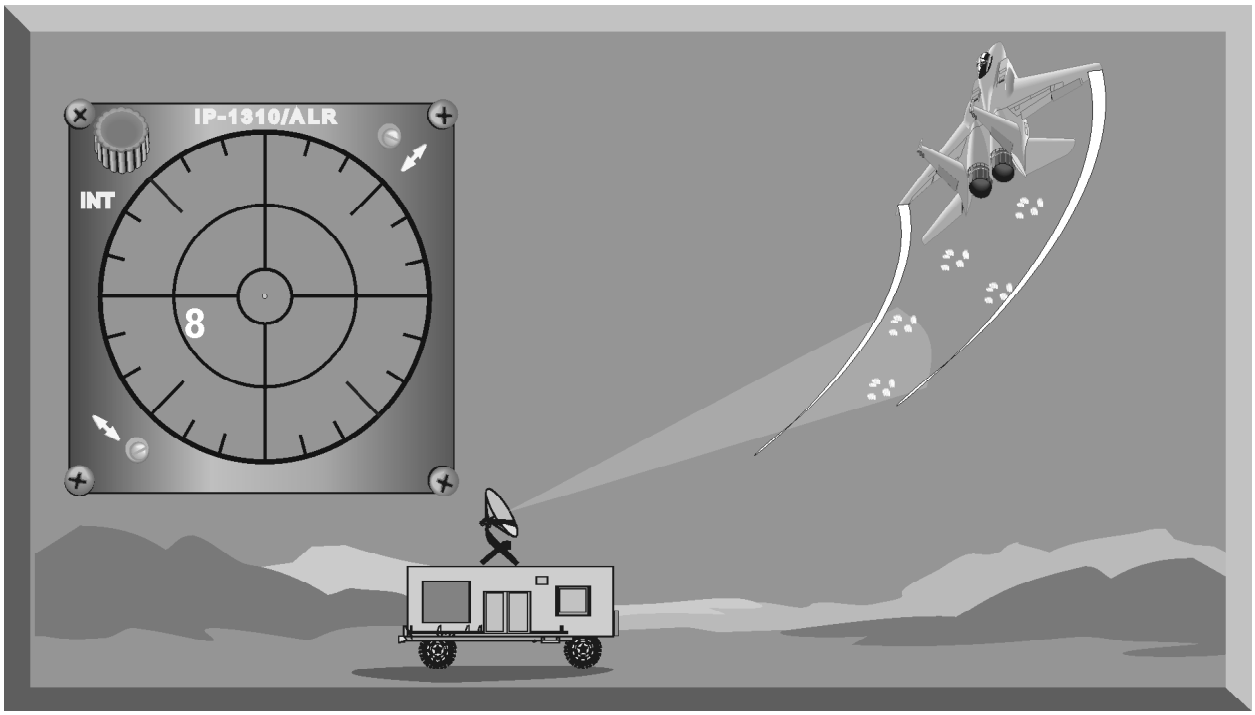


Figure 13-13. Self-Protection Chaff Tactics

(1) Self-protection chaff has proven effective against all pulse radar threat systems when employed with maneuvers and jamming. This is especially true for TTRs operating in an automatic tracking mode.

(a) Chaff employed against a track-while-scan (TWS) radar is designed to put multiple targets, with an RCS greater than the aircraft, in the resolution cell of the horizontal and vertical radar beams (Figure 13-14). Since the tracking loop tracks the largest return, the TWS radar will automatically switch to the chaff. After dispensing chaff, the pilot can maneuver vertically or horizontally to move the aircraft out of the resolution cell.

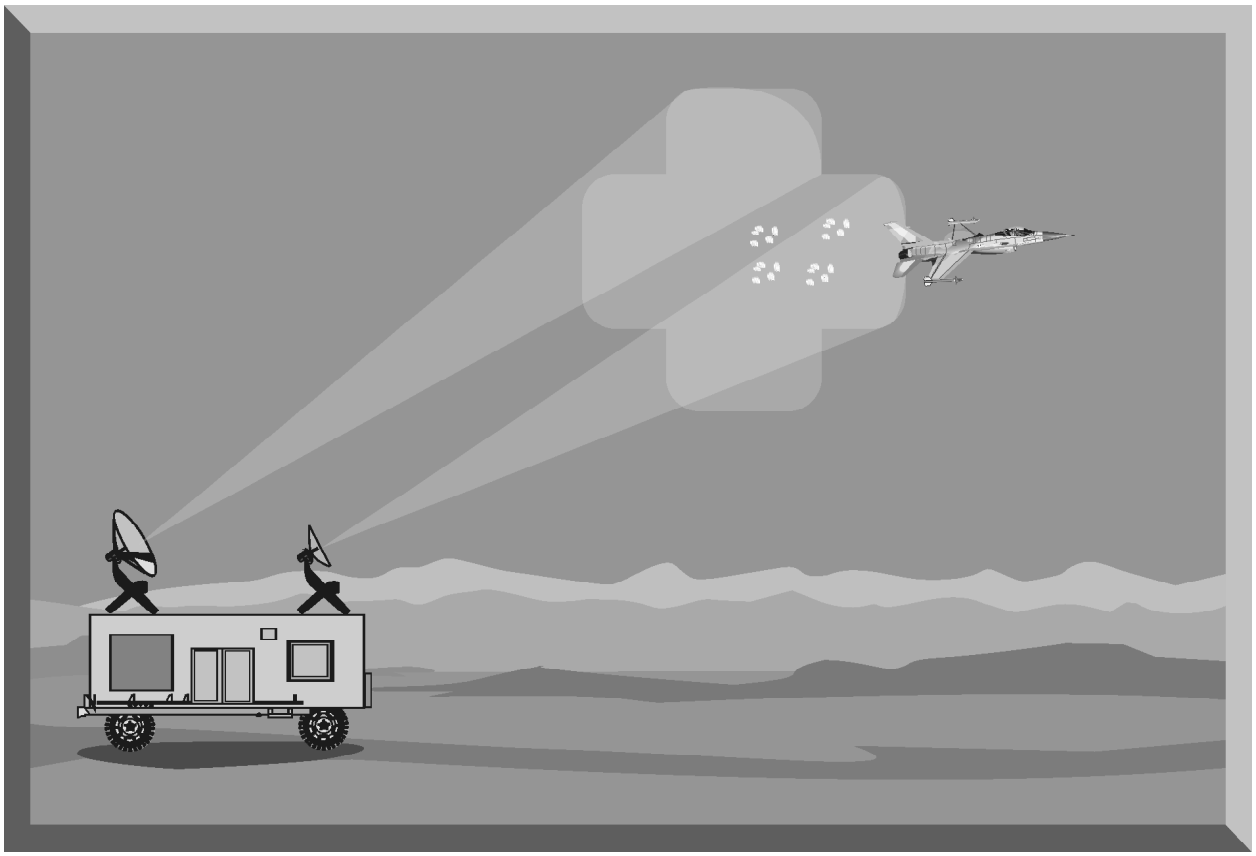


Figure 13-14. Self-Protection Chaff Effect on a TWS Radar

(b) Against a conical scan radar, chaff puts multiple, large RCS targets within the separate scans of the radar (Figure 13-15). These multiple targets generate error signals in the tracking loop and drive the separate scans off the aircraft return. As the conical scan radar tracking loop attempts to resolve these error signals, it will eventually lock on to the chaff. Maneuvering outside the overlapping scan area enhances chaff effectiveness and facilitates the transfer of radar lock-on to the chaff.

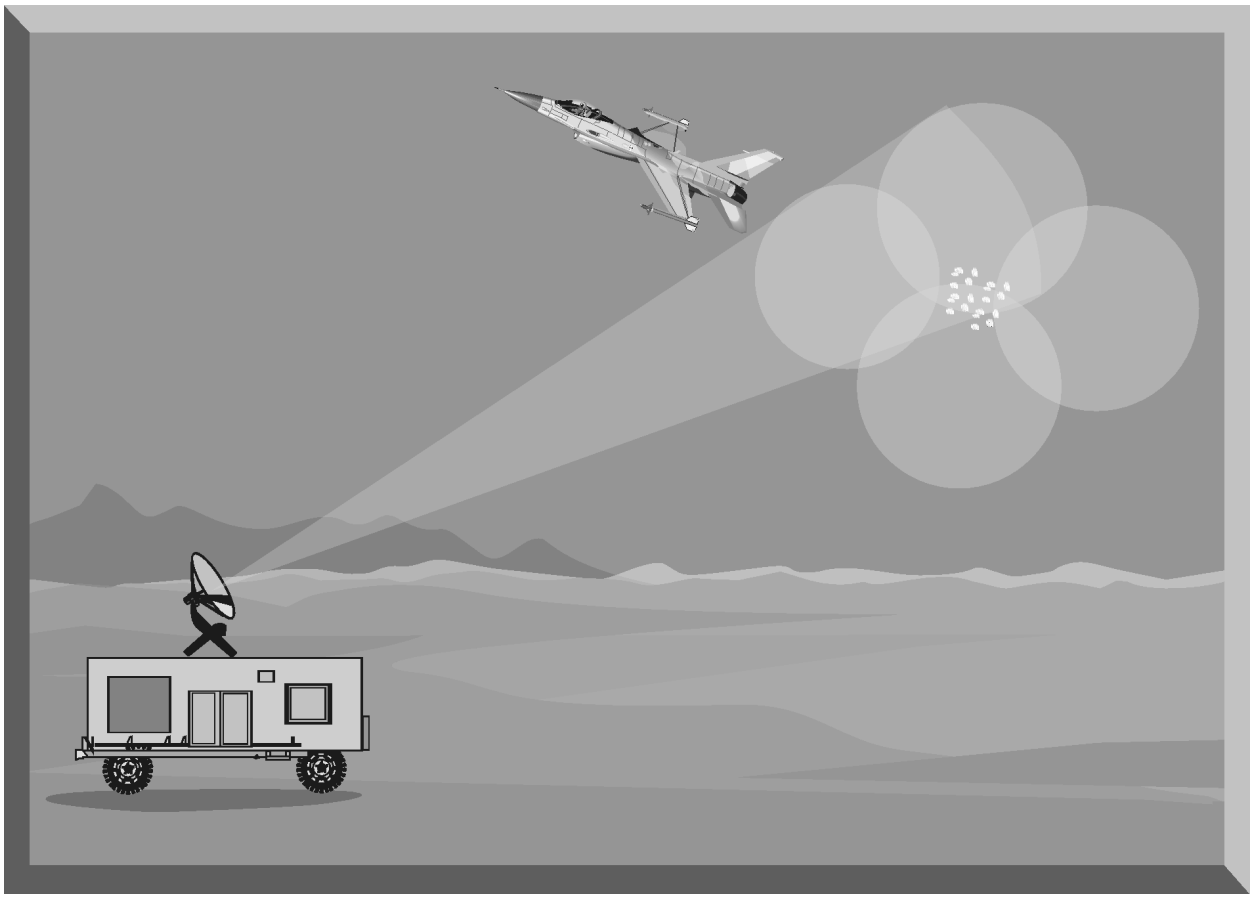


Figure 13-15. Self-Protection Chaff Impact on a Conical Scan Radar

(c) Chaff employed against a monopulse radar is designed to put multiple targets in at least two of the tracking beams (Figure 13-16). This generates errors in the azimuth, elevation, and range tracking circuits. Multiple chaff targets continue to generate azimuth and elevation errors that can eventually generate a break-lock condition, as the radar transfers lock-on to the chaff. Chaff is most effective against monopulse radars when employed on the beam in order to create the maximum angular tracking error.

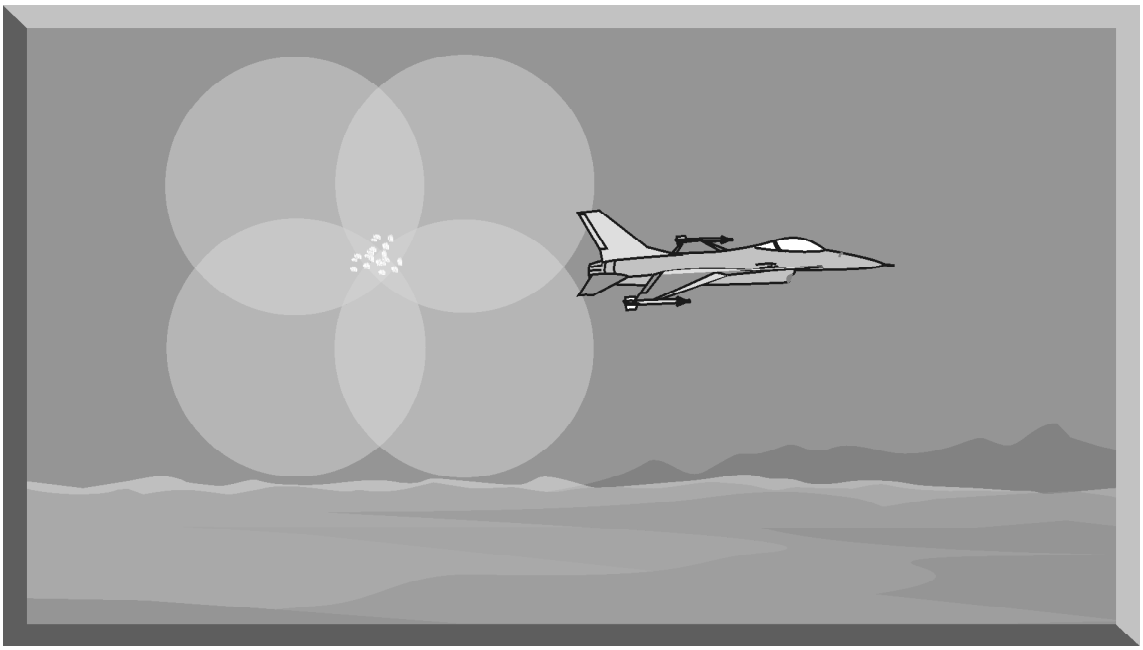


Figure 13-16. Self-Protection Chaff Impact on a Monopulse Radar

(d) Modern radars may employ some form of Doppler filtering to negate the effectiveness of chaff and other sources of clutter. Pulse Doppler and continuous wave radar systems track targets based on target velocity relative to the radar. Radars employing a moving target indicator (MTI) use relative target velocity to distinguish between targets and clutter. Chaff slows to near zero relative velocity almost immediately after dispensing. For self-protection chaff to be effective, the aircraft velocity relative to the radar site must also be near zero This occurs when the aircraft's aspect to the radar is 90°, or on the beam. By maneuvering to a beam aspect against a Doppler radar, the pilot is exploiting the "notch" where radar cannot discriminate targets based on Doppler frequency shift (Figure 13-17).

CHAPTER 16. RADAR ELECTRONIC PROTECTION (EP) TECHNIQUES

1. INTRODUCTION

Electronic warfare (EW) is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Nearly every military action, from command and control of an entire integrated air defense system (IADS) to precision guidance of an individual weapon, depends on effective use of the electromagnetic spectrum. Radar systems have become a vital element of nearly every military operation. Since these systems operate across the entire electromagnetic spectrum, much of the EW effort is concerned with countering radar systems. All of the jamming techniques discussed in Chapters 10 and 11 and the chaff employment options discussed in Chapter 13 are specifically designed to counter radar systems. These actions are classified as electronic attack (EA), which is a part of EW.

a. EW is somewhat like a chess game—a series of moves and countermoves within the electromagnetic spectrum. As we develop jamming techniques to counter radar systems, our adversaries develop counter-countermeasures to negate the effectiveness of these techniques. In response, we develop newer techniques and our adversaries respond with new modifications to their radar systems. This series of moves and countermoves can continue for decades. The development and application of radar counter-countermeasures are classified as electronic protection (EP), also a part of EW.

b. The continuing battle to control the electromagnetic spectrum for unrestricted radar employment has resulted in over 150 radar EP techniques. These techniques are designed to negate the effectiveness of electronic jamming and chaff on radar systems. These radar EP techniques can be incorporated into the design of a radar system or added to an existing radar system in response to a jamming technique. It is beyond the scope of this text to discuss all the radar EP techniques in use today. This chapter will discuss the most common EP techniques. They have been organized by function of the technique within the radar. These functions include radar receiver protection, jamming avoidance, jamming signal exploitation, overpowering the jamming signal, pulse duration discrimination, angle discrimination, bandwidth discrimination, Doppler discrimination, and time discrimination.

2. RADAR RECEIVER PROTECTION

The following are some of the most common radar counter-countermeasures designed to prevent receiver overload or saturation.

a. Sensitivity time control (STC) is used to counter close-in chaff or close-in clutter. Receiver gain is set at normal for long ranges and reduced for close-in ranges. One problem with using STC is that close-in targets may be missed if STC is improperly adjusted.

b. Automatic gain control (AGC) is used to counter chaff, clutter, and most types of transmitted jamming. AGC senses the signal level of a receiver's output and develops a back-bias, producing a constant output level. This technique has a slow response time compared to fast AGC and instantaneous AGC, both of which are employed instead of AGC. Also, it cannot maintain correct IF output levels for different intensity signals that are close in range because the bias voltage has a long buildup and decay time.

c. Fast automatic gain control (FAGC) is also employed against chaff, clutter, and most types of transmitted jamming. FAGC works by sensing the signal level of receiver output and develops a back-bias, tending to hold output constant. Response time is within milliseconds, permitting fast response and recovery as the antenna traverses the jammer's bearing. There are several precautions to note when using FAGC. First, targets may be suppressed and lost without the operator knowing that jamming is present. Second, a strong pulse or echo may cause ensuing weak targets to be lost. Lastly, FAGC has difficulty getting an accurate bearing on the jamming source.

d. Instantaneous automatic gain control (IAGC) is another technique to counter chaff, clutter, and most types of transmitted jamming. IAGC senses the signal level of each echo or jamming pulse and develops a back-bias that holds the stage output constant. Gain control response time is within milliseconds and extends the dynamic range of the receiver. There are several precautions to note when using IAGC. First, it is not effective against signals whose "in band" time is less than the IAGC response time. Also, with continuous duty cycle jammers, targets may be lost without the operator knowing that jamming is present. Finally, it is difficult to get an accurate bearing on the jamming source.

e. Automatic noise leveling (ANL) counters noise jamming and modulated or unmodulated constant wave jamming. ANL samples receiver noise content at the end of each PRF and sets the gain accordingly for the next pulse interval. Continuous jamming reduces gain to keep output the same as the original noise level. ANL also follows the scanning rate of the antenna so that receiver noise output is constant as the antenna rotates. When using ANL, targets may be suppressed and lost without the operator knowing that jamming is present. Also, receiver gain is unstable when pulses or swept jamming enter the sampling gate intermittently.

f. The logarithmic receiver (LOG) counters most types of transmitted jamming by amplifying and demodulating large dynamic-range signals in logarithmic amplifiers. This produces "amplitude compression" of the strong

signals. However, when using LOG, output is nearly constant so the operator cannot easily tell when jamming is present.

g. The logarithmic receiver with fast time constant (LOG-FTC) counters narrowband jamming, chaff, and clutter. This technique amplifies and demodulates large dynamic-range signals in logarithmic amplifiers, producing "amplitude compression" of the strong signals. Video is coupled through FTC circuits to eliminate rectified carrier and low frequency sideband products. There are problems with using LOG-FTC. First, the receiver output is nearly constant, so the operator cannot always tell when jamming is present. Second, LOG-FTC is not effective against wideband, or fast-swept, short pulse jamming. Lastly, LOG-FTC causes a broadening of displayed jam sector. as well as degrading bearing accuracy on the jam source.

h. Dicke-fix (DF) counters wideband and fast-swept jamming and is similar in employment to wideband limiting (WBL). DF amplifies without ringing, clips down all pulses to a common level, then amplifies the narrowband echo signal more than the wideband jamming. Noise level is held constant, independent of jamming intensity. There are precautions to note when using DF. Jamming that enters the wideband limiter can capture limiters, causing poor receiver sensitivity. Targets may be suppressed without the operator knowing that jamming is present. Also, resolution and target detection range are reduced, even in a non-jamming environment. Finally, DF is ineffective against extremely fast-swept spot jamming.

i. WBL is used to counter wideband jamming and fast-swept jamming. WBL amplifies without ringing, clips down all pulses to a common level, then amplifies the narrowband echo signal more than the wideband jamming. Noise level is held constant, independent of jamming intensity. However, jamming that enters the wideband limiter can capture limiters and cause poor receiver sensitivity. Resolution and target detection range is reduced, even in a clear environment. Targets may be suppressed without the operator knowing that jamming is present. Finally, WBL is ineffective against fast-swept spot jamming.

j. Adaptive video processing (AVP) counters chaff corridors, weather, sea clutter, and most types of transmitted jamming. AVP combines the adaptive threshold, beam-to-beam correlation, and wide-pulse blanking in frequency-scanning three-dimensional radars to avoid collapsing undesired returns on the PPI display. However, when using AVP, there is a decreased probability of detection in some multiple target situations. Also, targets may be suppressed without the operator knowing that jamming is present. Finally, AVP passes all point targets.

3. JAMMING SIGNAL AVOIDANCE

The following are some EP techniques used to avoid jamming signals.

a. Frequency agility (FA) counters narrowband jamming and some types of repeater and deception jamming. FA enables the radar to make rapid changes of transmitter and receiver operating frequency, sometimes on a pulse-to-pulse basis. Manual frequency changes may cause mutual interference with other radars and services.

b. Frequency diversity works against narrowband jamming and some types of repeaters and transponders. It is a multiple-radar coordination procedure in which radars are assigned operating frequencies that are separated to reduce mutual interference and their susceptibility to a single jammer. It is important to note that other radars may be operating at the same allocated operating frequency.

c. Polarization diversity is used to counter chaff, weather, and transmitted jamming. Polarization diversity attenuates jamming input to a radar receiver by using antenna polarization different from jammer polarization, and usually involves separate radars of different polarization. There are two precautions when using polarization diversity: (1) ground clutter worsens on vertical polarization, and (2) close coordination is necessary if separate radars are used; for example, one horizontally polarized search radar and one vertically polarized search radar.

d. Circular polarization (CP) works against chaff, weather, and transmitted jamming. CP attenuates jamming input to a radar receiver by using antenna polarization different from jammer polarization, and usually involves separate radars of different polarization. CP also improves target detection in rain clutter.

e. Conical-scan-on-receive-only (COSRO) is employed against inverse conical scan jamming to deny a jammer the ability to sense and upset scan angle tracking information. A constantly transmitted illumination beam is received and scanned to derive target angle information. However, the jammer can still degrade angle tracking if it can approximate the received signal scan rate.

f. Speedgate tracking is used against all types of transmitted jamming. The technique provides a very narrow bandpass having a center frequency related to Doppler shift. Only jamming within the restricted band is effective. It has the advantages of accurate target Doppler discrimination and good target tracking at low target levels. However, the speedgate can be stolen by gate stealers and some types of swept jamming.

g. Leading-edge track (LET) is used to counter an incoming target dropping chaff by allowing target tracking on the leading edge of the target. Trailing edge track (TET) is used to counter a receding target dropping chaff.

h. Track coast is used to counter chaff, clutter, multiple targets, range gate stealers, jam fades, and blinking jamming by placing tracking radar in a rate-aided coast condition. The system "estimates" target position to avoid interrupting the fire control solution. A lock-on or return to acquisition mode terminates the track coast condition. Track coast requires adequate storage of rate-aided information, and no true tracking information will be developed while track coast is operating.

i. Guard gates work against chaff, clutter, multiple targets, range gate stealers, jam fades, and blinking jamming. Guard gates provide automatic detection of a foreign signal and "estimates" target position to avoid interrupting fire control solutions. Like track coast, guard gates require an adequate store of rate-aided information with no true tracking information developed.

4. JAMMING SIGNAL EXPLOITATION

The following are some EP techniques that use the jamming signal for target acquisition and engagement.

a. Passive angle tracking (PAT) counters most types of transmitted jamming by allowing the radar to acquire and angle-track the source of jamming signals. There are some problems with this technique. Blinking jamming can cause severe instability, and the range of the jammer is unavailable until the target reaches burnthrough range.

b. Home-on-jamming (HOJ) counters most types of transmitted jamming by allowing the missile or radar to use the jamming signals, locate the source, and home on it. However, blinking jamming can cause severe instability, and the range of the jammer is unavailable until burnthrough.

c. Jamming signals produce recognizable sounds that help in their detection and identification. Aural recognition allows an operator to listen to the Doppler frequency associated with a moving target. It is used to counter most types of jamming.

d. The local oscillator off technique counters continuously transmitted jamming. No receiver output occurs unless a target echo signal and a jamming signal are present. Limitations of this technique include: targets only display in an area where jamming is present; and, if the antenna rotates away from the jammer, or if jamming is turned off, no targets are displayed on the radar scope.

e. The jamming strobe indicator counters any transmitted jamming with high-duty-cycle modulation. The indicator is a variable marker strobe on the radar display that moves in range proportional to jamming strength. The indicator traces an antenna lobe pattern on the display, showing the azimuth of the jamming source. There are some problems with the jamming strobe indicator. First, it interrupts normal video in some radars. Second, inverse or sidelobe

jamming can cause erroneous strobes. Finally, the jam strobe does not react to unmodulated CW or low-duty-cycle jamming for some radar systems.

f. The jamming indicator lamp, located on the operator console, is used on radars with automatic noise leveling (ANL) to counter continuous transmitted jamming. The lamp alerts the operator to the presence of jamming, and the ANL is manually shut off. This action allows the operator to determine jammer bearing.

g. Clean strobe generation (CSG) counters any transmitted jamming by using the sidelobe blanking circuits of a radar. An azimuth strobe appears when the jamming level in the main antenna exceeds the jamming level in the sidelobe auxiliary antennas. The operator is alerted to the presence and bearing of a jamming source, even with a constant false alarm radar (CFAR) receiver.

h. Jamming attenuation (JAM ATTEN) counters both clutter and any type of jamming. Receiver gain is reduced to avoid receiver saturation by inserting an attenuator pad that enables the operator to recognize presence, type, and bearing of a jamming source. When using JAM ATTEN, however, the reduced gain may cause loss of targets, even in non-jammed sectors. Also, any improvement in signal-to-jam ratio is not possible.

i. Receiver manual IF gain (MAN GAIN or IF GAIN) also counters clutter and jamming. Receiver gain is reduced to avoid jamming saturation by manually reducing stage gain, allowing the operator to identify jammer presence, type, and bearing. When using IF GAIN, the reduced gain may cause a loss of targets, even in non-jammed sectors. Also, any improvement in signal-to-jam ratio is not possible.

5. OVERPOWERING THE JAMMING SIGNAL

Following are some EP techniques a radar system can employ to overpower jamming and reduce the jamming-to-signal (J/S) ratio to less than one.

a. Burnthrough counters most types of transmitted jamming. Energy in the target pulse is raised by increasing the peak power, that is, the PRF or pulse width, or by increasing the time the radar illuminates the target by reducing the scan rate or scan angle. Some radars have modes in which the radar concentrates its power in narrow azimuth and elevation sectors about the suspected target position. However, burnthrough can degrade general radar performance by overloading the receiver if a large radar cross section target is detected. High power may impact radar operation in clutter or dense chaff environments.

b. Narrowband long pulse (NBLP or NLP) counters most types of transmitted jamming by using a high-energy long pulse. The signal uses a narrowband receiver for reception, and increases detection range for targets in jamming and

in the clear. Simultaneously, it reduces resolution, which causes poor radar performance in chaff and clutter.

6. PULSE DURATION DISCRIMINATION

The following are some radar counter-countermeasures that use pulse duration to discriminate between radar and jamming signals.

a. The fast time constant (FTC) is used to counter chaff, clutter, and narrowband jamming. A video circuit provides low frequency attenuation to reject carrier and low frequency modulation jamming. FTC passes normal radar pulse lengths with little attenuation, but causes some loss of receiver sensitivity.

b. Pulse width discrimination (PWD), clutter eliminate (CE), and wide pulse blanking (WPB) are designed to counter chaff, most types of jamming, EMI, and some types of deception jammers. A video coincidence gate, involving a delay line matched to the expected signal duration, senses if a return is the proper pulse width. PWD, CE, and WPB provide an enabling path for qualified signals. However, weak signals may be lost in the signal processing.

c. Pulse expansion-compression (PC) is used to counter most types of noise jamming and some types of deception jamming. An expanded pulse is coded for transmission. This expanded pulse is transmitted and decoded on return. Echo responses are then compressed in a decoding process. This expansion/compression is equivalent to NLP, which provides longer detection ranges, and wideband short pulse, which provides increased resolution. Using PC is not without problems. Unwanted residues may cause loss of weak targets. Additionally, range error proportional to the Doppler shift, or radial velocity, affects the accuracy of the PC.

7. ANGLE DISCRIMINATION

The following techniques use angle discrimination to distinguish between radar returns and jamming signals.

a. Sidelobe blanking (SLB) and sidelobe cancellation (SLC) are types of sidelobe suppression (SLS) used to counter sidelobe response to chaff, clutter, transmitted jamming, sidelobe jamming, and deception jamming. An auxiliary antenna approximates the pattern and gain of sidelobes of the main antenna and produces a signal for comparison with the signal received in the main antenna. If the signal in the auxiliary antenna is greater, the signal in the main antenna channel is blanked. This permits bearings to be obtained on a jamming source and rejects sidelobe jamming. SLB is useful only for determining the bearing to the jamming source.

b. Antenna manual positioning, antenna traverse and elevation angle offset, antenna jog, and antenna slow scan are EP techniques used to counter main

beam and sidelobe jamming and deception. These techniques are designed to increase the antenna scans across the jammed sector to increase the blip-scan ratio. These techniques increase the number of pulses integrated, as well as the operators' sorting capability.

8. BANDWIDTH DISCRIMINATION

The following are EP techniques that use bandwidth to distinguish between radar jamming and target returns.

a. Dicke-fix (DF) counters wideband and fast-swept jamming. A wideband limiter amplifies without ringing and clips all pulses down to a common level. Then an amplifier increases narrowband target echo signals more than the wideband jamming. There are some problems associated with DF. Any jamming entering the wideband limiter can "capture" the limiters and cause poor receiver sensitivity. Targets may be suppressed without the operator knowing that jamming is present. Resolution and target range is reduced, even in a clear environment. Finally, DF is ineffective, even harmful, when the jamming bandwidth is near the bandwidth of the desired echo signal.

b. Transmitter pulse lengthening (TPL) counters wideband and fast-swept jamming. TPL concentrates power into a narrow band about the carrier frequency by lengthening the transmitting pulse. While this allows use of a narrowband receiver, it impairs resolution, causing poor chaff and clutter performance.

c. Transmitter pulse shaping (TPS) counters wideband and fast-swept jamming. The sideband range is limited by shaping the transmitted pulse. This allows use of a narrowband receiver, but impairs resolution, causing poor performance in chaff and clutter.

d. Narrowband pulse limiting (NBLP or NLP) is a form of transmitter pulse lengthening that counters wideband jamming and fast-swept jamming. NBLP concentrates power into a narrow band in the carrier frequency by lengthening the transmitting pulse. This allows use of a narrowband receiver, but impairs resolution, causing poor chaff and clutter performance.

e. The fast time constant (FTC) is used to counter chaff, clutter, and narrowband jamming. A video circuit provides low frequency attenuation to reject carrier and low frequency modulation of jamming. FTC passes normal radar pulse lengths with little attenuation, but causes some loss of receiver sensitivity.

f. High video pass (HVP) is used to counter chaff, clutter, and narrowband jamming. It is similar to FTC. A video circuit provides low frequency attenuation to reject carrier and low frequency modulation jamming. HVP passes only the leading edge of the received pulses. HVP can cause some loss of receiver sensitivity.

g. The wideband short pulse (WSP) counters chaff, clutter, and narrowband jamming by transmitting a short pulse and using a wideband receiver for reception. Echo resolution and accuracy are improved, and performance against narrowband jamming is enhanced. However, the maximum detection range is decreased and system vulnerability to wideband jamming is increased.

h. Narrowband limiting (NBL) counters chaff, clutter and narrowband jamming. A narrowband filter positioned in the front of the amplifier section allows only the target signal bandwidth to enter the limiter, reducing wideband and off-frequency jamming. The limiter clips all signals and noise to a common level. This technique is useful only when followed by pulse compression or other "decode" techniques. NBL is not effective against wideband jammers capable of causing "ringing" of the NBL bandpass filters. Targets may be suppressed and lost without the operator knowing that jamming is present. Finally, target detection and resolution are poor.

9. DOPPLER DISCRIMINATION

EP techniques that use Doppler frequency discrimination between radar and jamming signals to negate jamming effectiveness include the following:

a. Moving target indication (MTI) is used to counter chaff and clutter. The phase of returned target echoes is compared on a pulse-to-pulse basis. Those with no phase change (no change in radial velocity) are cancelled using a delay-line canceler. Sensitivity using MTI is poor for weak targets, even in the clear. Also, it is blind to targets that have a Doppler frequency that is equal to a multiple of the radar PRF, unless PRF stagger is used. Finally, limited dynamic range does not allow full cancellation of strong clutter echoes.

b. Compensated coherent MTI, also known as compensated COHO MTI, counters chaff and clutter by comparing the phase of returned target echoes on a pulse-to-pulse basis. Those pulses with no phase change, that is, no change in radial velocity, are cancelled. Corrections to the coherent oscillator are applied to compensate for motion of the platform and radar antenna. Sensitivity is poor for weak targets, even in the clear, and it is blind to targets that have a Doppler frequency equal to, or a multiple of, the radar PRF, unless PRF stagger is used.

10. TIME DISCRIMINATION

The following EP techniques use time discrimination between radar and jamming signals to negate jamming effectiveness.

a. Video integration (VINT) and integrate-multiply (INT-MULT) counter any form of transmitted jamming not synchronous with radar PRF. The video continuously circulates through a delay line, delaying signals exactly one pulse recurrence time (PRT), then combines them with signals from the next PRT. Synchronous target signals add together to increase video output, but noise and

random pulses are suppressed. Unless MTI and FTC are employed, VINT and INT-MULT will enhance chaff, clutter, and jamming along with target returns. Also, feedback control, or loop gain, must be carefully adjusted for optimum results.

b. PRF stagger and jitter are EP techniques designed to counter quasi-synchronous jamming, EMI, MTI blind-speeds, "second trip" echoes, and repeater jammers simulating "closer-than-real" targets. The transmitter pulse interval is varied to break up synchronous patterns. Received signals must be "de-staggered" for use with MTI or integration. When using any of these techniques, video de-stagger balance must be accurate or "double video" occurs. These techniques are not effective against exact synchronous deception jamming.

c. Pulse-to-pulse correlation (PPC) is used to counter slow-swept blinking or pulsed jamming not synchronized with radar PRF, and some types of deception jammers. To be displayed, target video must exceed a threshold voltage for two successive pulses. The technique avoids displaying non-synchronous jamming and EMI, but is not effective against synchronous jamming, and may cause weak targets to be missed.

d. Beam-to-beam correlation (BBC) is used to counter slow-swept blinking or pulse jamming not synchronous with radar PRF and some types of repeaters and transponders. It is used in three-dimensional frequency scanning or frequency agile radars. To be displayed, the target return echo signal must exceed a threshold value in two adjacent antenna beams. BBC is not effective against synchronous jamming. It may also cause weak targets to be missed.

e. Single beam blanking (SBB) is used to counter slow-swept, blinking, pulsed jamming, and narrowband jamming. It is used in three-dimensional frequency scanning or frequency agile radars to avoid displaying vertical beams containing jamming. A blanking pulse is generated for vertical beams containing jamming so that they are not displayed. The technique is not used on RHI video. Also, it can cause a loss of targets at the jammed elevation angle on the PPI display.

11. SUMMARY

This chapter has discussed some of the most widely employed EP techniques designed to counter radar jamming. The capabilities of the individual radar operator were not discussed. However, the radar operator is as important as the EP techniques designed for the radar system. Many of the most effective EP techniques are designed to ease operator interpretation of the radar display. In the chess game of EW, the capabilities of individual radar operators can be as important as the sophisticated EP techniques in determining the final outcome.

CHAPTER 17. RADAR WARNING RECEIVER (RWR) BASIC OPERATIONS AND GEOLOCATION TECHNIQUES

1. INTRODUCTION

Radar surveillance and radar-directed weapons represent the biggest threat to aircraft survival on the modern battlefield. The first step in countering these threat systems is to provide the pilot or crew with timely information on the signal environment. The radar warning receiver (RWR) is designed to provide this vital information to the pilot. The RWR system is an example of an electronic warfare support (ES) system. The primary purpose of an RWR system is to provide a depiction of the electronic order of battle (EOB) that can have an immediate impact on aircraft survival. Though the RWR system is complex, the basic operations of the various components are straightforward. A step above RWR systems is threat geolocation. While an RWR provides the EOB for a single aircraft, threat geolocation systems can provide accurate threat location data for numerous aircraft over an entire region. Threat location data is used for aircraft threat avoidance and, more common today, the preemptive attacking of enemy radar sites. This chapter will discuss the functions of the various components of a RWR system including the antennas, receiver/amplifiers, signal processor, emitter identification (EID) tables, RWR scope, RWR audio, and limitations to RWR systems. This chapter will then go on to discuss three of the methods used to geolocate radar threat systems.

2. RWR ANTENNAS

Antennas are designed to receive radar pulses from threat radar systems. Factors that impact the operation of the RWR antennas include location, pattern, sensitivity, and polarization.

a. The physical location of the RWR antennas on the aircraft can affect its ability to detect a radar signal. Antennas are arranged to cover a predetermined area of horizontal and vertical space around the aircraft (Figure 17-1).

b. The antennas and their patterns play an essential part in displaying the spatial relationship of a threat radar to the aircraft. The antenna patterns are the areas, or "footprints," that the antennas are specifically designed to cover. These footprints are directly affected by the relative position of the antennas to the threat systems. This is because the signal processor measures and compares signal strength from all the aircraft antennas to compute threat signal location relative to the aircraft. This relative location is then presented on the RWR scope display. Aircraft movement and maneuvering shifts these relative positions during flight and can distort the true threat position on the RWR scope. Precise position determination is not possible with most RWRs.

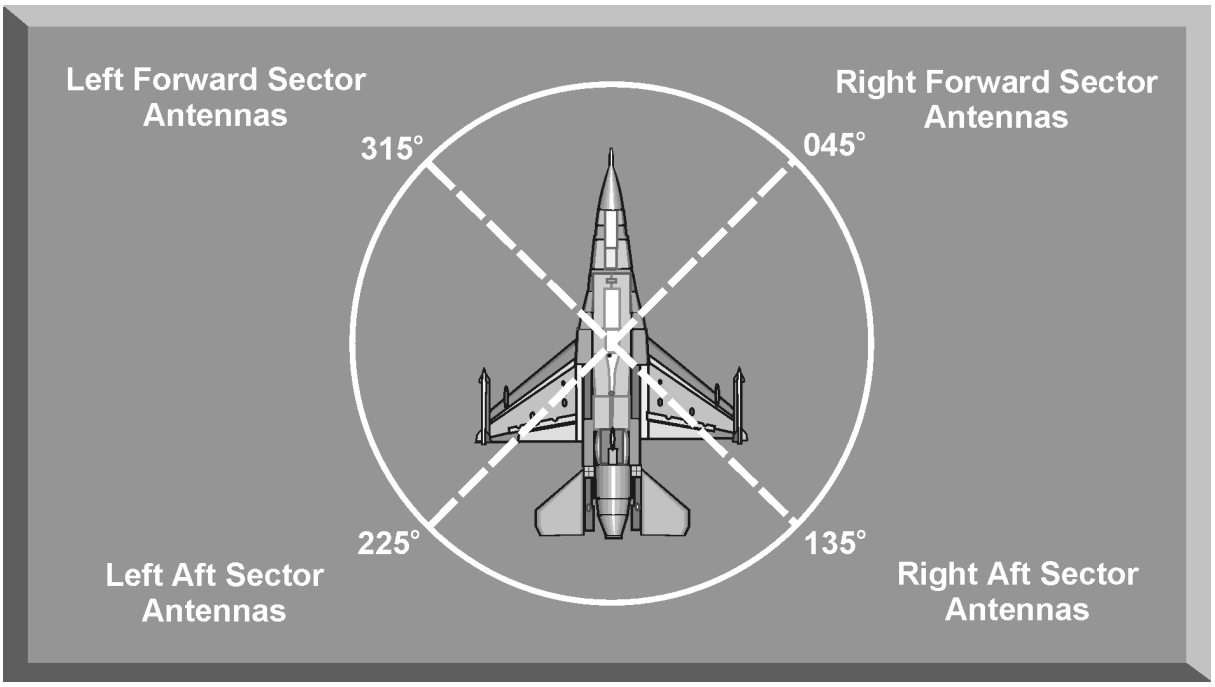


Figure 17-1. Radar Warning Receiver (RWR) Antennas

c. The sensitivity of an RWR antenna directly affects its ability to detect a radar signal. The more sensitive the antenna, the further it can detect a signal. The sensitivity of a system and its ability to intercept a radar signal is usually expressed in decibels relative to milliwatts or dBm units. A 10 dBm change in sensitivity can result in a 25 nm range difference in target detection. In general, sensitivity levels of -50 to -60 dBms are required to detect signals at long ranges (Figure 17-2).

Figure 17-2. RWR Antenna Sensitivity

d. Another factor affecting antenna detection range is the polarization of the antennas. If the polarization of the RWR antenna and the threat system antenna are mismatched, or cross-polarized, initial detection of a threat signal could be delayed until the aircraft is within the lethal range of a threat system. In this situation, the aircraft could be engaged with minimal warning (Figure 17-3).

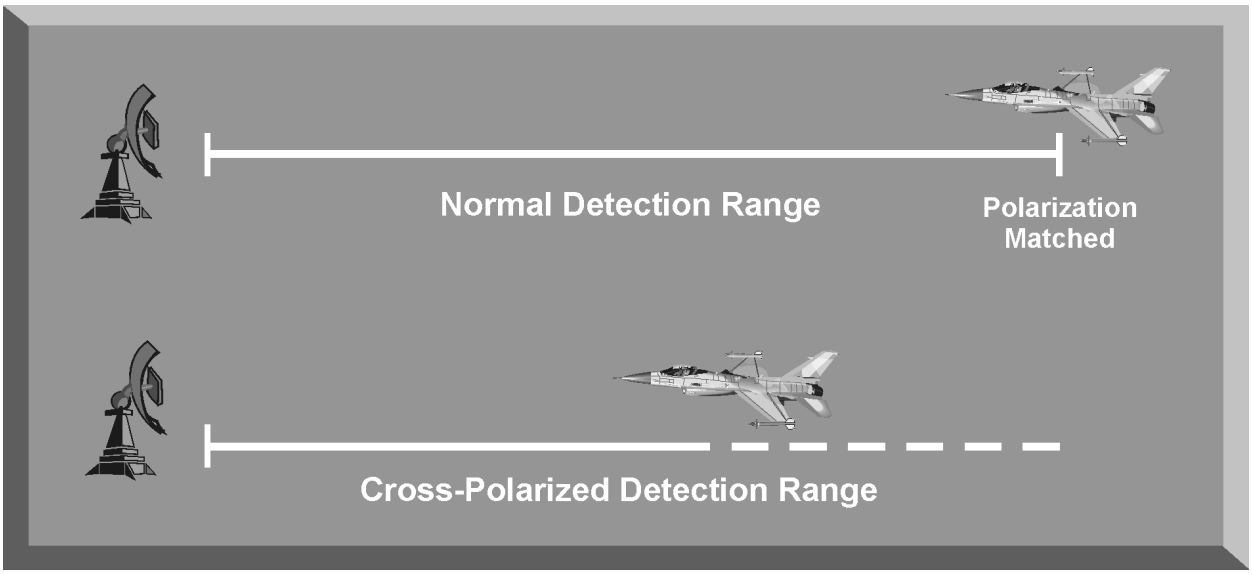


Figure 17-3. RWR Antenna Polarization

3. RWR RECEIVER/AMPLIFIERS

The RWR receiver/amplifier section processes the radar signals from the antennas. Most RWR systems use frequency bands to differentiate signals. Nominal band designations are summarized in Table 17-1. There are two types of receivers currently used in RWR systems: the crystal video receiver and the superheterodyne receiver.

Table 17-1. RWR Frequency Band Designators

RWR Frequency Band	EW Frequency Band
Band 0	Charlie-Delta Bands
Band 1	Echo-Foxtrot Bands
Band 2	Golf-Hotel Bands
Band 3	India-Juliet Bands

a. A crystal video receiver (CVR) is the simplest type of microwave receiver. It is used primarily for detection of pulse radar signals in the 2 to 18 GHz band. A CVR used in a radar warning receiver incorporates crystal detectors for each designated frequency band. A pulse radar signal is detected by the antenna and passed to the multiplexer. The multiplexer divides the received radar signals by frequency band and sends the signals to the appropriate band channel. The RF amplifier boosts the radar signal and passes it to the crystal detector (Figure 17-4).

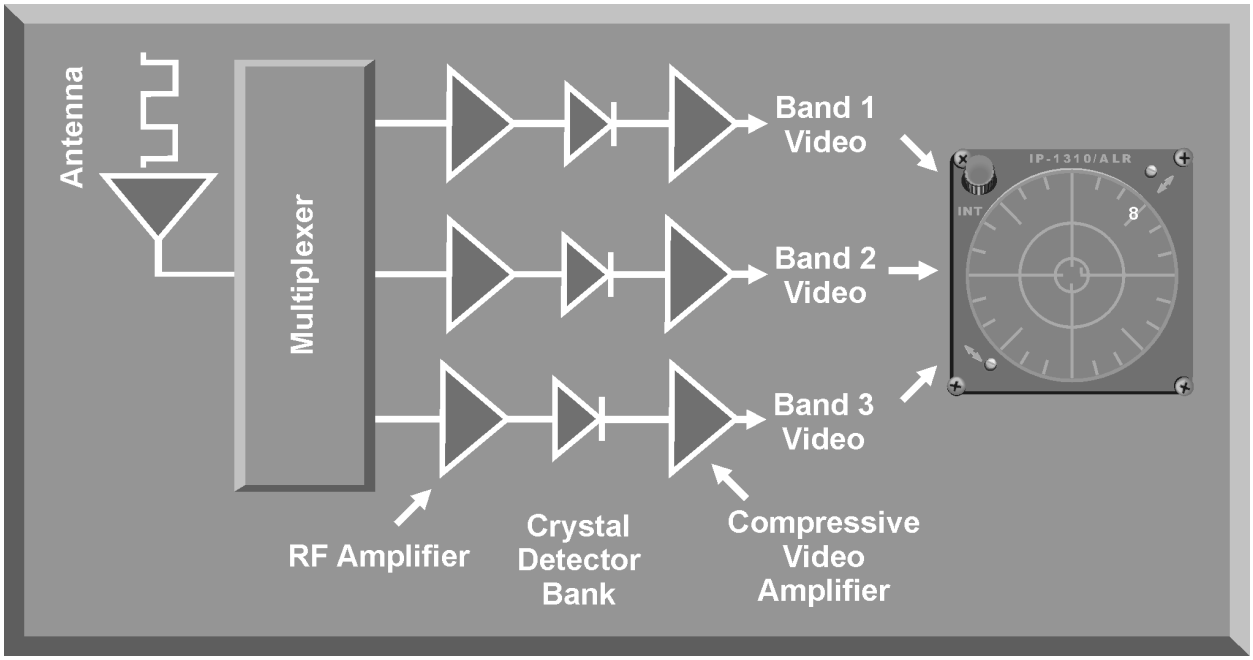


Figure 17-4. Crystal Video RWR Receiver

(1) The crystal detector is an RF diode, which converts the RF signal into a video signal. The voltage level of the output video signal is dependent only on the amplitude of the input signal and not on the frequency or phase. The sensitivity of a CVR is limited by the sensitivity of these crystal detectors. The sensitivity of crystal detectors currently available is generally adequate to detect main beam radiation from most threat radars. The video output of the crystal detectors is amplified by a high-grain compressive video amplifier and sent to the RWR scope for display.

(2) A CVR is extremely fast, sensitive, and covers a wide frequency range. These characteristics coupled with low cost and small size make CVRs ideal for use in radar warning receivers. The primary disadvantage of a CVR is that it is indiscriminate in reception and can be saturated in a dense signal environment. Multiple signals in the same band can cause amplitude distortion which can mask key threat signals.

b. A superheterodyne RWR receiver uses a pre-selector filter, mixer, and a local oscillator to translate the received signal to a lower intermediate frequency (IF). This lower IF allows the receiver to amplify and filter the received signal to provide greater sensitivity and frequency selectivity than a CVR (Figure 17-5).

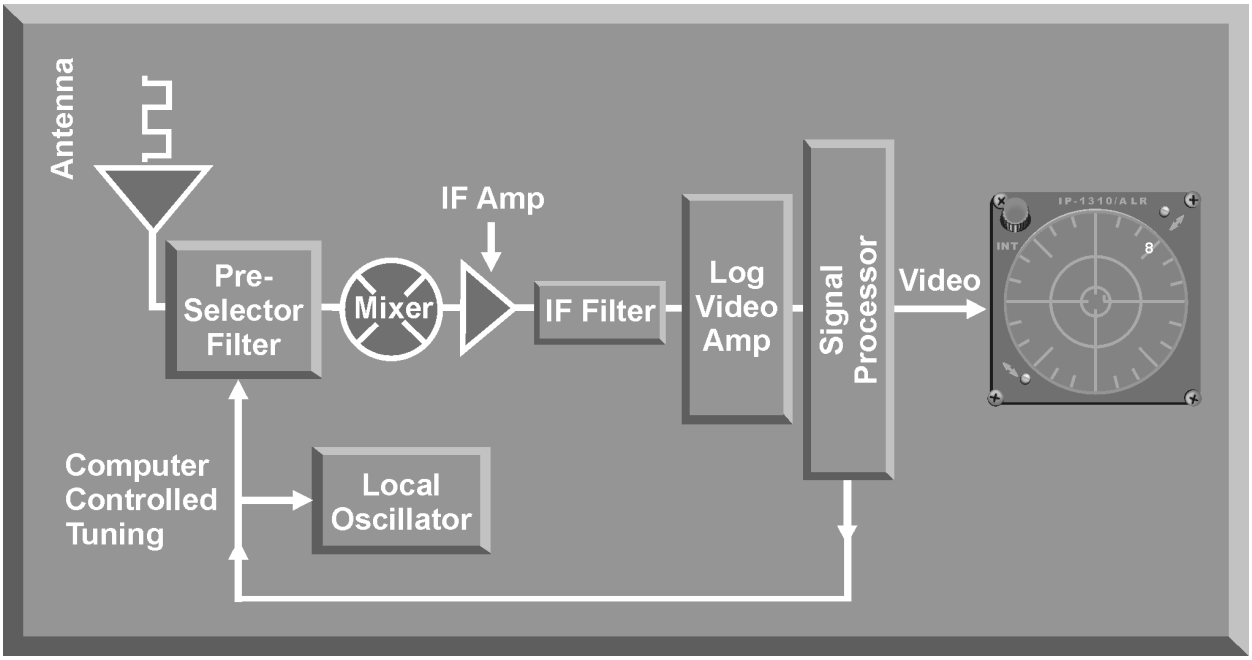


Figure 17-5. Superheterodyne RWR Receiver

(1) Superheterodyne RWR receivers use special scanning techniques controlled by the signal processor to tune the pre-selector filter and the local oscillator to rapidly scan selected threat system frequency bands. If the receiver detects activity in any of these bands, the scan stops to allow the processor to analyze the detected signals. The signal is combined with the local oscillator signal to lower the frequency to the IF. This signal is amplified, filtered, and amplified again before it reaches the signal processor. The signal processor classifies the threat and displays the proper threat symbol to the pilot. This entire process is accomplished in a matter of microseconds.

(2) The scanning superheterodyne receiver has important features that make it effective for RWR system application. It has excellent sensitivity and selectivity. It also has good frequency resolution. These features give the superheterodyne receiver a very low false alarm rate. The major disadvantage of the scanning superheterodyne receiver is its limited capability to receive signals from threat systems employing scanning antenna patterns. This limitation can be overcome with specific computer-controlled tuning to look for these threat signals.

4. SIGNAL PROCESSOR

The signal processor is the heart of the radar warning receiver. The signal processor is also known as the digital processor or analysis processor in different RWR systems. Its primary functions are to process numerous complex radar signals and identify, among the thousands of similar signals, those generated by lethal threat systems. The signal processor accomplishes this task continuously over the duration of the mission and displays the identified threat system to the aircrew almost instantly.

a. Signal processing begins when RF energy strikes the receive antennas on the aircraft. The received signals are then boosted in strength by intermediate amplifiers or antenna receivers. These amplified signals are then sent to the signal processor, or digital processor, where they are assigned a track file for reference to other signal characteristics. Data in these files is compared to those in the emitter identification (EID) table to process the signal for identification. Once identification is complete, a video and, if necessary, an audio signal, is sent to the cockpit display. The audio and video signals alert the aircrew to the electronic environment around the aircraft. This whole process takes less than a microsecond (Figure 17-6).

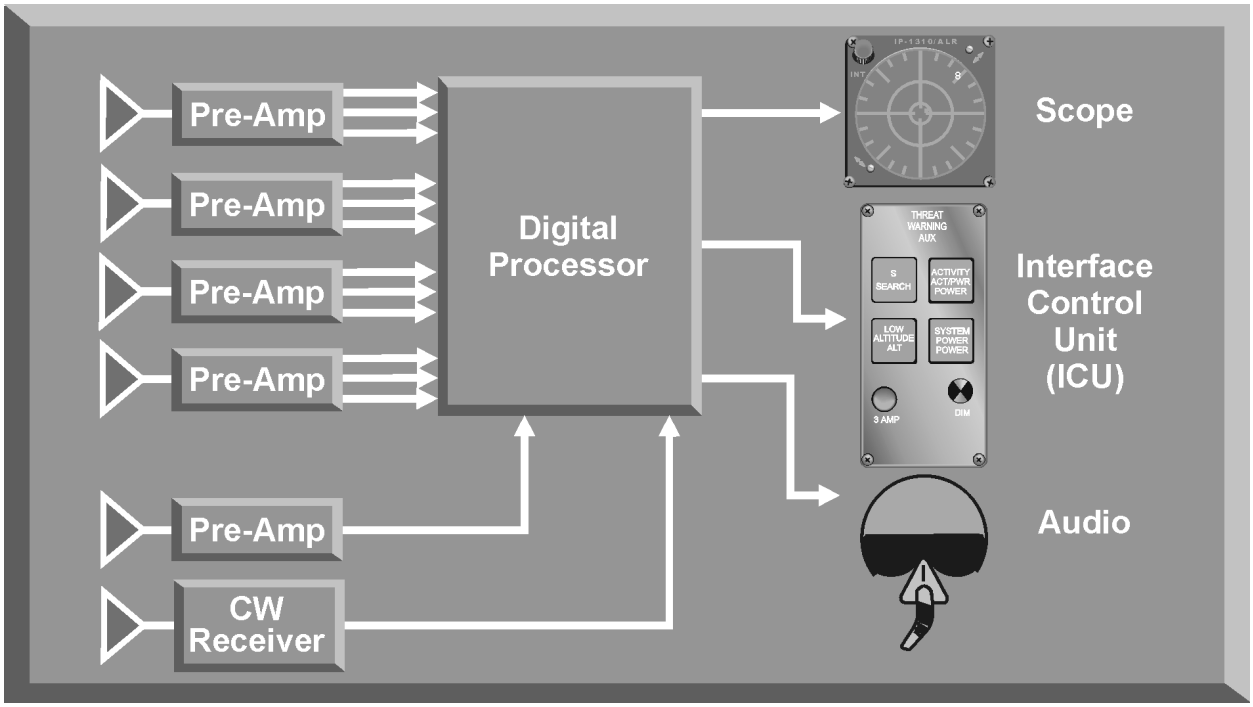


Figure 17-6. RWR System

b. Since many signals may be present, the amplifier detectors boost the signal strength, and also tag each signal by certain characteristics such as its time of arrival, direction of arrival, and/or frequency. These signals, along with their respective tags, are sent to the signal processor for further processing and

identification. The signal processor then makes a track file for each signal it receives from the amplifier detector.

c. The signal processor classifies each received signal and corresponding track file by its unique radar signal characteristics. Identifying characteristics used by a signal processor can include radio frequency, pulse width, pulse repetition frequency, EP techniques, and more. Characteristics of one signal may be identical to characteristics from different signals, while certain other characteristics can be as unique as a human fingerprint. The signal processor uses these primary characteristics to identify specific signals. When the primary characteristics of two or more signals are similar, the signal processor uses additional signal characteristics to resolve any confusion between two or more signals.

d. The signal processor ranks the track files based on priorities determined from tests it conducts on the signal characteristics and the threat priorities contained in the EID tables. It then quickly processes signals belonging to lethal threats before it processes signals belonging to non-lethal threats. For example, three signals enter the processor together and separate track files are established for each signal (Figure 17-7). A test on the first characteristic discriminant, frequency, will delay the further processing of Signal 3, since no lethal threat systems operate at a frequency less than 2000 megahertz. A further test on the remaining prioritized signals may eliminate Signal 2 as a threat system signal, leaving more processor time for the identification of the threat system which generated Signal 1. These tests do not stop the processor from attempting to identify all received signals. The signal processor merely delays the identifying sequence until all high priority signals have been processed.

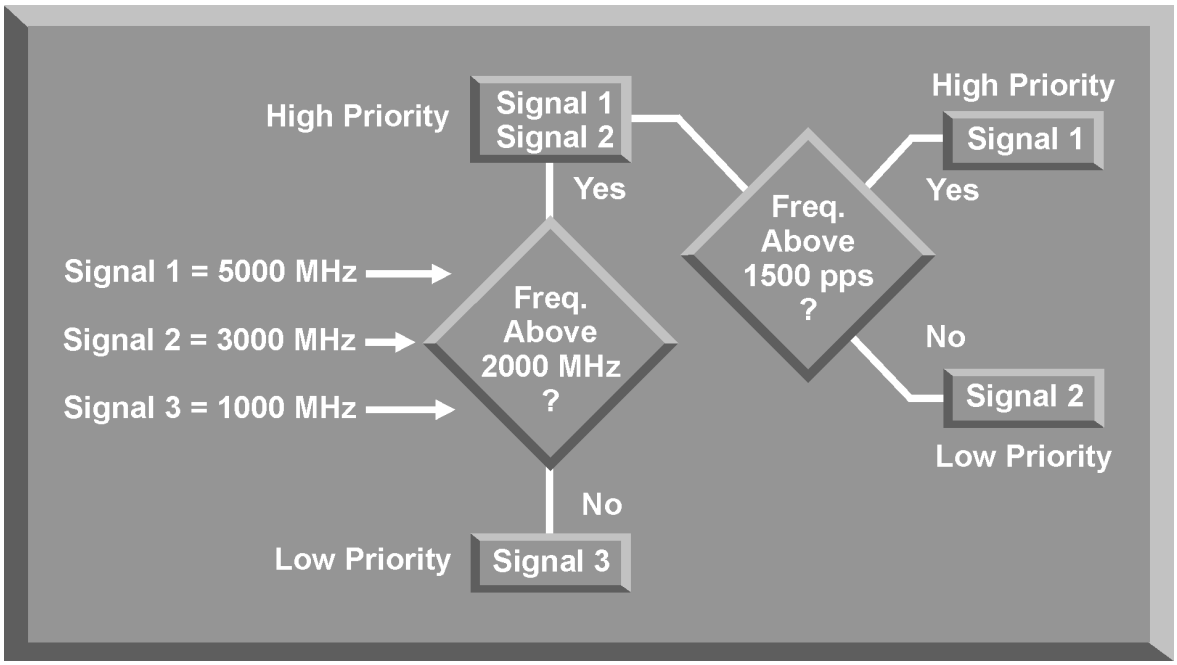


Figure 17-7. Signal Processor Signal Priority

5. EMITTER IDENTIFICATION (EID) TABLES

The signal characteristics in each track file are filled with processed data, and are constantly updated based on the time of arrival and location of the received signals. In addition, the track files are constantly compared to the EID table installed in the signal processor's computer memory. The EID table is a predefined table of radar characteristics associated with known radar systems (Figure 17-8). It is created from information gathered from electronic warfare support (ES) assets and intelligence sources. This table can be changed and updated as necessary to reflect the most current radar characteristics available for the anticipated threats in the planned theater of conflict. Each RWR system has unique procedures to reprogram the signal processor and update the EID tables. Emergency reprogramming actions, such as would be taken if a new threat appears that is not part of the current EID, are called a Pacer Ware.

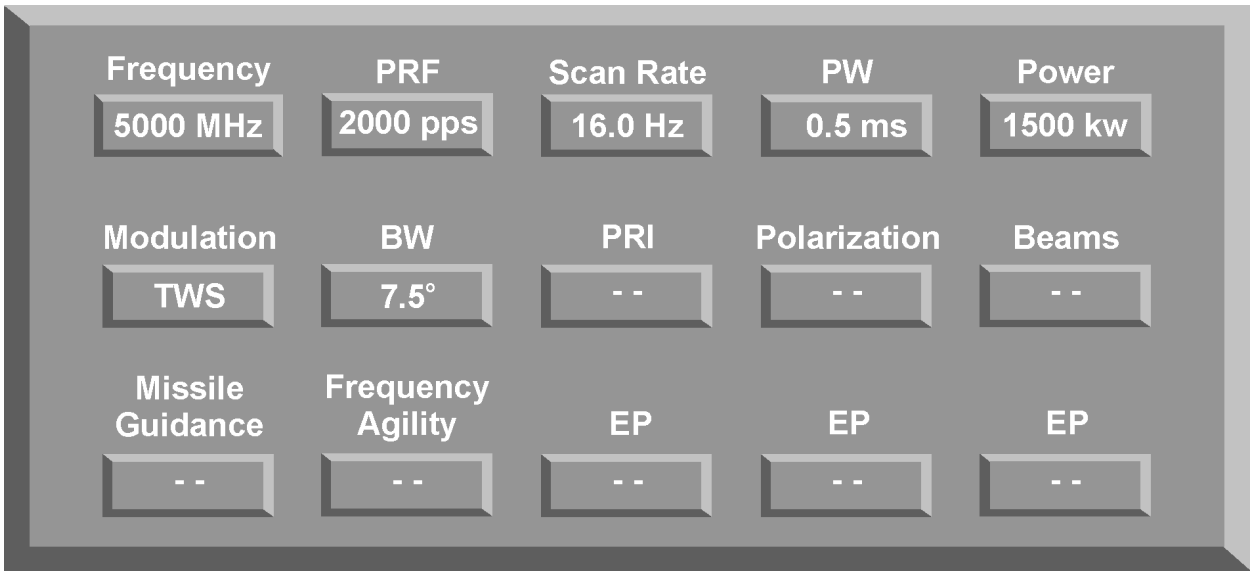


Figure 17-8. Sample EID Table

6. RWR SCOPE DISPLAY

The signal processor continually compares signal characteristics in the track files with the data in the EID tables. Once the signal processor has determined that enough of the signal characteristics match the information in the EID tables, it generates and positions a video symbol on the RWR scope. The video symbol represents a specific threat, and each threat system has its own unique symbol. In addition, an audio tone is generated to alert the pilot. The signal processor also generates symbols and audio associated with specific threat system actions, including search, track, and missile launch. The position of the threat symbol on the RWR scope always represents the relative position of the threat in relation to the aircraft which is the center of the RWR scope. The signal processor compares the received signal strength in the different antennas to determine the proper location of the threat symbol. Figure 17-9 depicts a situation where the two

forward antennas receive equal signal strength therefore the signal processor places the symbol at the 12 o'clock position.

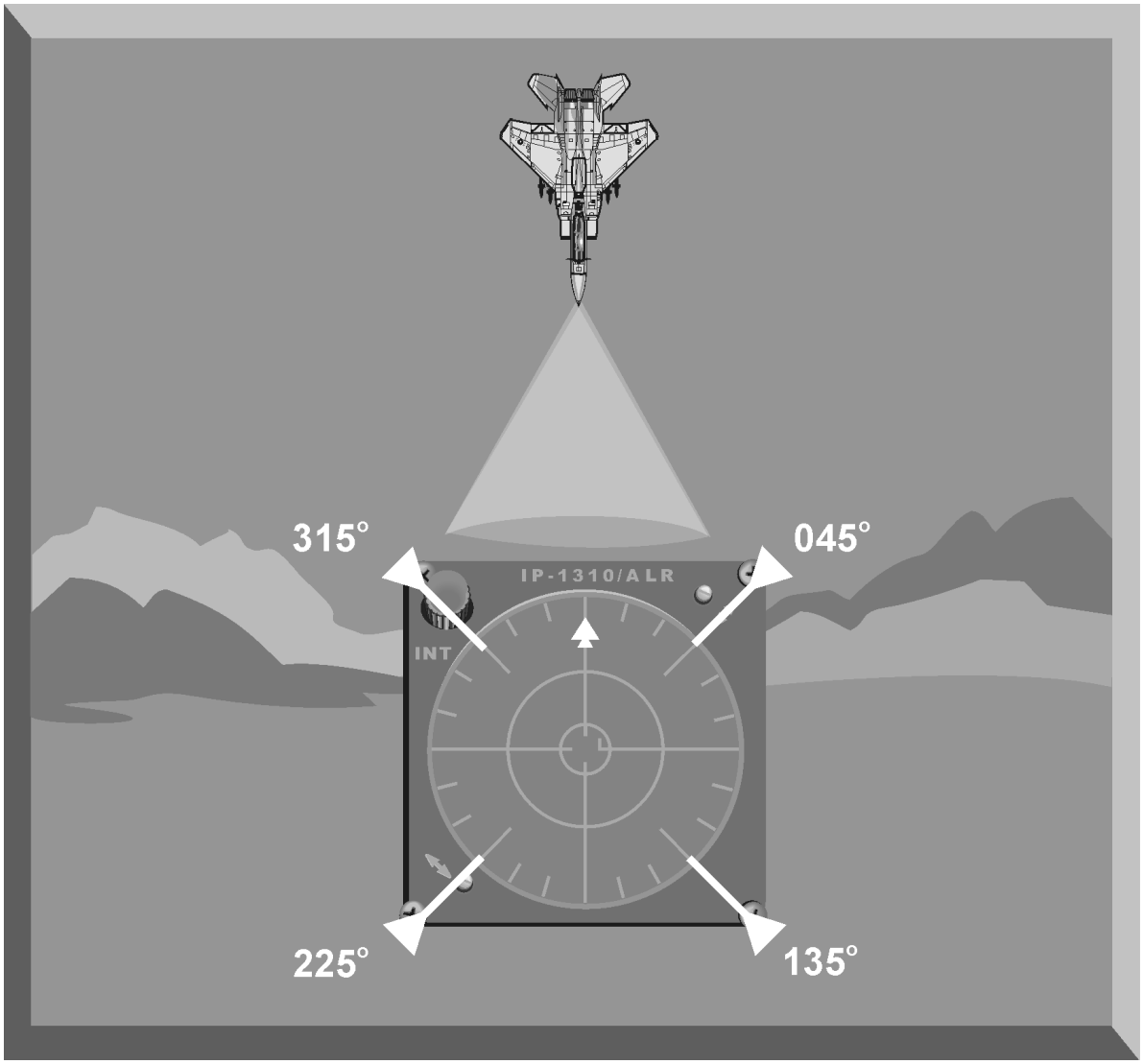


Figure 17-9. RWR Scope Azimuth Positioning

7. RWR AUDIO

In addition to generating threat symbols for each identified threat, the signal processor also generates threat audio. Threat audio first alerts the aircrew to the detection of a threat system. This RWR audio is generally referred to as "new guy" alert audio. The signal processor can also present constant audio from a selected threat. The aircrew controls this function through the interface control unit. The constant audio provided by an RWR system can be either "real" or synthetic. "Real" audio is normally based on the actual pulse repetition frequency (PRF) of the threat system radar whether the signal processor has identified it or not. Synthetic audio is based on the classification of the threat (SAM, AI, etc.) as

determined by the signal processor. The signal processor also generates a launch warning audio when the signal characteristics of the threat indicate a missile launch condition exists.

8. RWR INTERFACE CONTROL UNIT (ICU)

Every RWR system has some type of an ICU which provides the aircrew interface with the signal processor (Figure 17-10). The buttons on the ICU control specific functions of the signal processor. The ICU allows the aircrew to optimize the RWR system based on mission tactics. This optimization includes selecting appropriate priority lists based on ingress and egress tactics, controlling threat audio presentation, and determining the number and types of threats displayed. In addition, the ICU provides an additional visual indication of missile launch. All system test functions are controlled by the ICU to allow the aircrew to monitor the status of the RWR system.

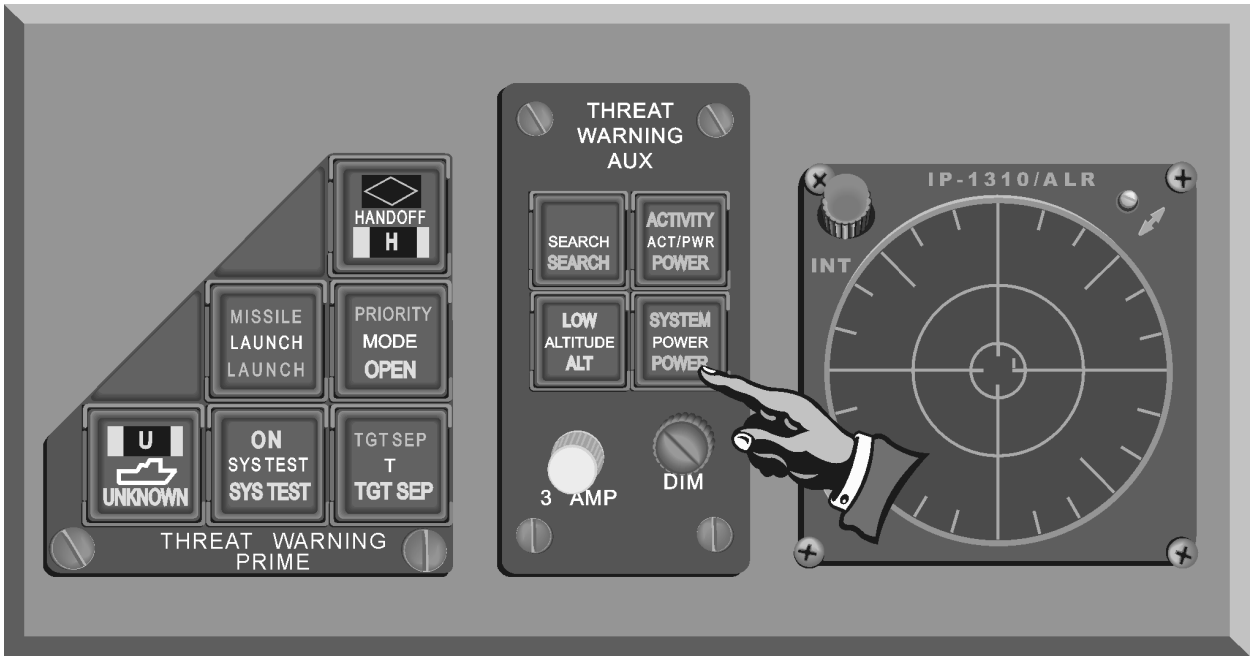


Figure 17-10. RWR Interface Control Unit

9. RWR LIMITATIONS

There are several limitations associated with all RWR systems. The most important limitations include ambiguities, impact of maneuvering, and electromagnetic interference (EMI).

a. The sheer number and diversity of radar systems associated with an enemy IADS greatly compound the problem of threat identification and warning for RWRs. Adding to this problem is the fact that many different threat systems use operating modes that are parametrically similar. When an RWR processes a

radar signal that has the same characteristics of a signal from a different system, an ambiguity may occur. An RWR ambiguity is defined as the display of more than one symbol for a specific threat signal. RWR ambiguities may occur from both enemy and friendly radar systems.

(1) Figure 17-11 depicts a number of friendly and threat signals that operate between 8000 and 10,000 megahertz. On any given combat mission, it is quite possible that the RWR will receive signals from one or more of these threat systems at the same time. If frequency is the only signal characteristic available for processing, the RWR will not be able to determine which system the signal represents. Since threat systems operating in this frequency range are potentially lethal systems, the signal processor will attempt to match the frequency with a threat system from the EID table.

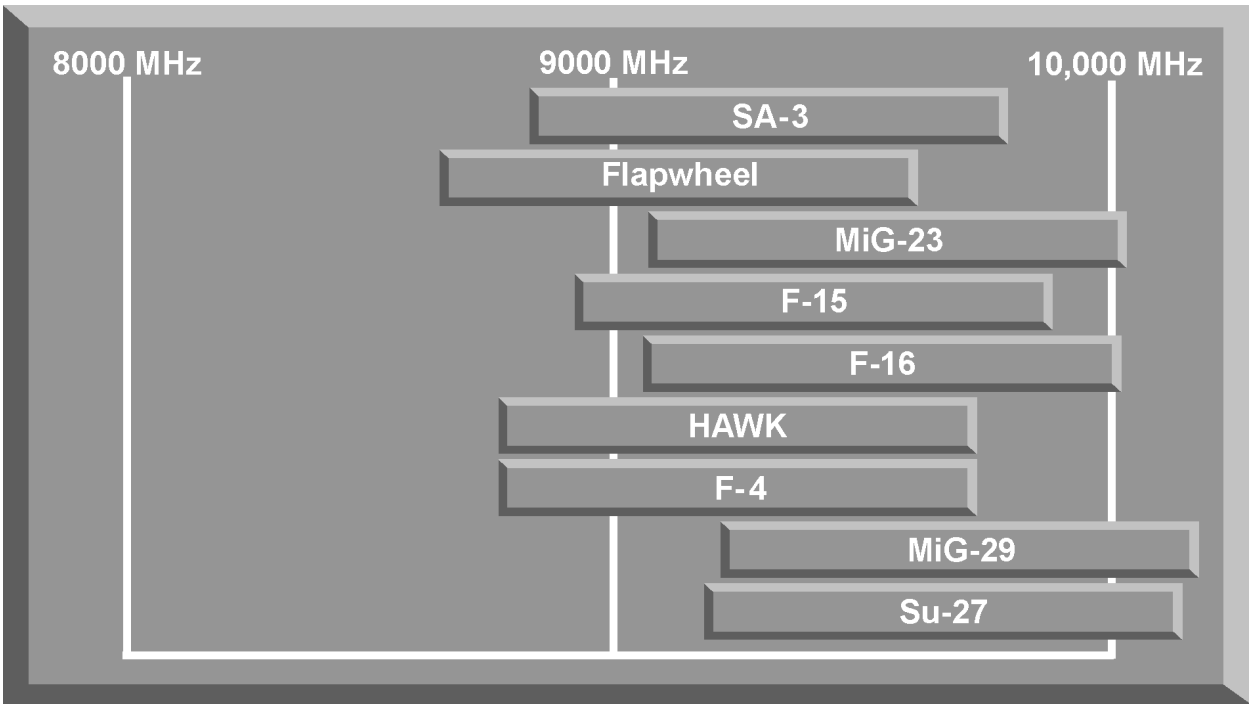


Figure 17-11. Signal Frequency Spectrum

(2) Matching partially processed signals to threat systems in the EID table may result in the wrong threat symbol being displayed, or numerous symbols being displayed on top of each other, making it difficult for the pilot to distinguish the exact threat. Incorrect threat symbology, or numerous combined symbols, are called RWR ambiguities.

b. RWRs are designed to provide accurate threat positioning information when the aircraft is flying straight and level. Most RWRs will also provide accurate threat positioning information when the aircraft is maneuvering up to certain limits of bank angle and turn rate. If aircraft maneuvering exceeds these

limits, RWR threat positioning data becomes unreliable. The two RWR limitations associated with aggressive maneuvering are inaccurate threat azimuth and multiple threat symbols.

(1) In Figure 17-12, the right forward and right aft RWR antennas detect a threat signal from a TTR. The left forward and left aft antennas are shielded by the aircraft and do not detect the signal. The signal processor determines the threat position, using the azimuth positioning algorithm, and displays the threat symbol at the 2 o'clock position.

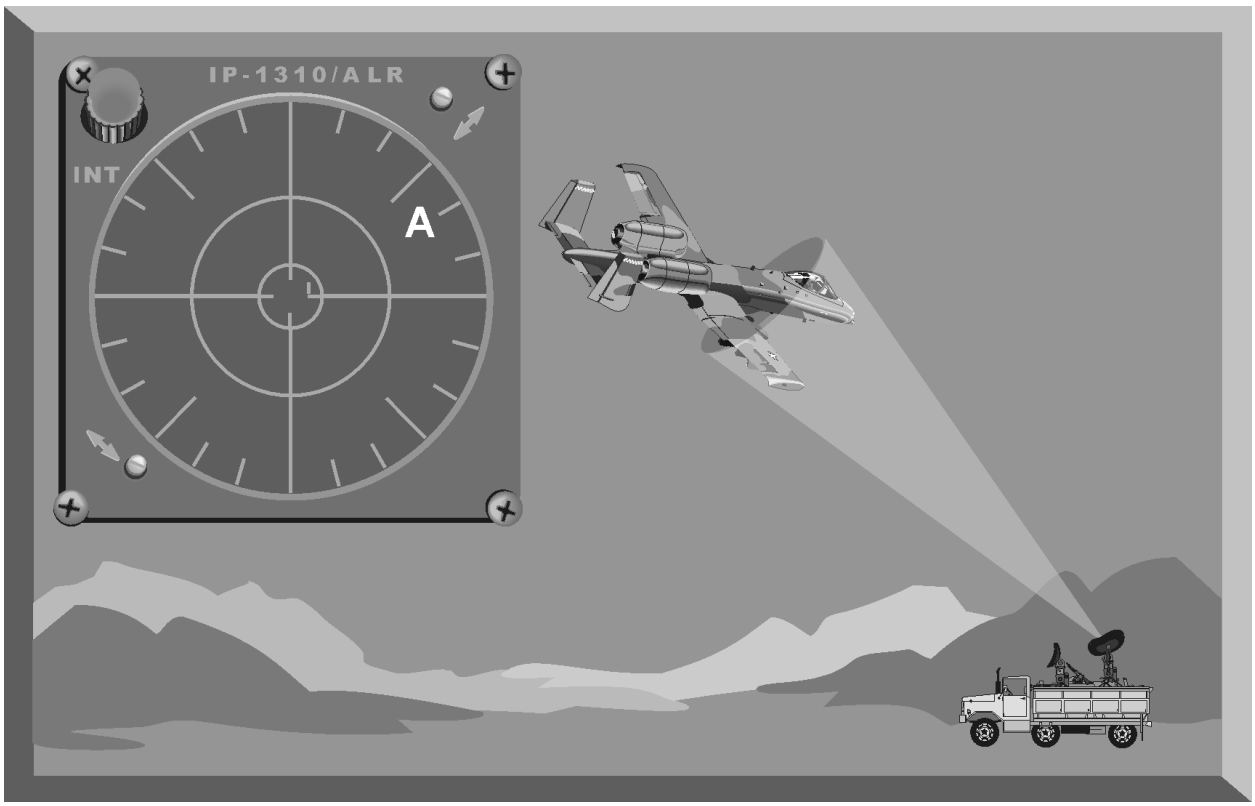


Figure 17-12. RWR Threat Azimuth Position Determination

(2) When the pilot maneuvers aggressively to put the threat symbol on the beam, he exceeds the RWR maneuvering limitations (Figure 17-13). Now all four RWR antennas detect the TTR signal. The signal strength in the right and left forward antennas is nearly equal. Based on this information, the signal processor displays the RWR symbol at the one o'clock position while the threat is actually at the three o'clock position.

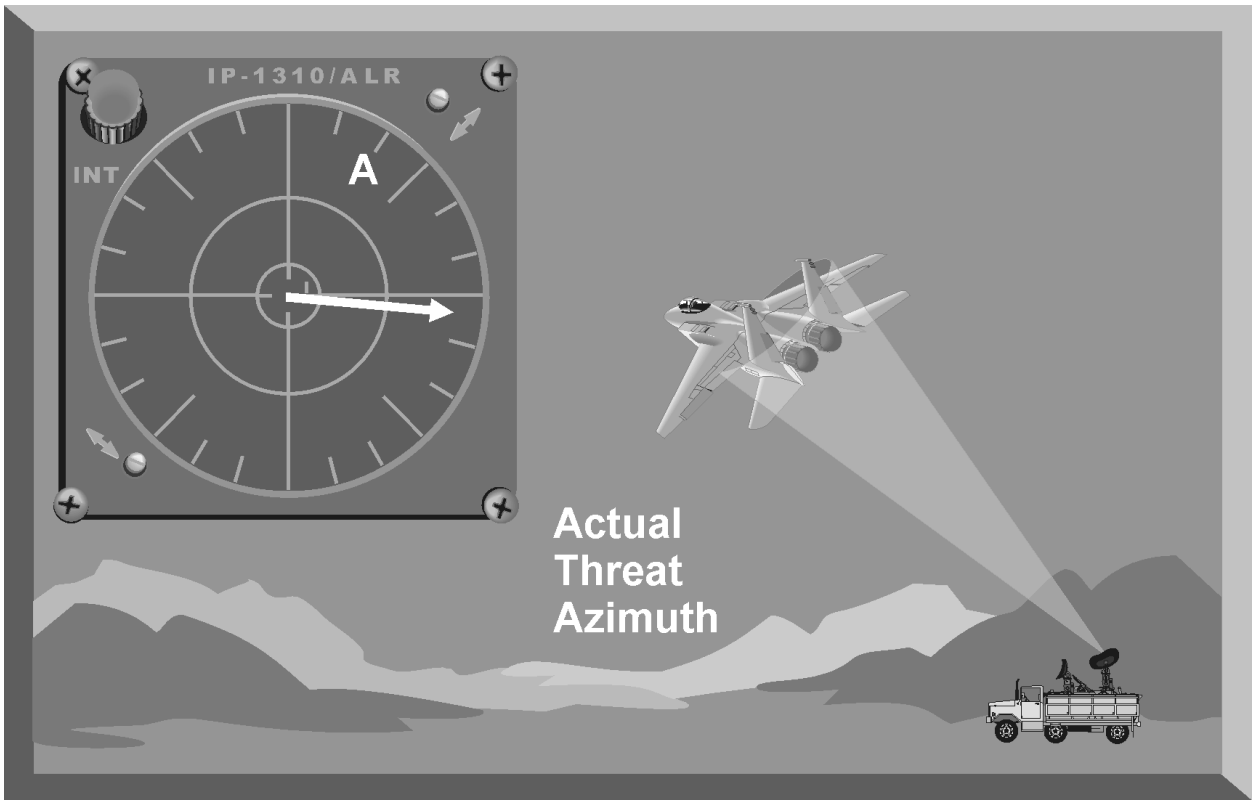


Figure 17-13. RWR Azimuth Error

(3) During aggressive maneuvering, the RWR signal processor may generate multiple symbols for a single threat emitter. In Figure 17-14, as the aircraft maneuvers, the relative azimuth of the threat position changes rapidly causing signal strength detected by each antenna to also change rapidly. The signal processor interprets these changing signals as new and different threat systems with the same signal characteristics. The number of "false" threat symbols displayed for a single threat is determined by the processing speed of the signal processor and a parameter called the symbol "age-out" time. Symbol age-out is the time, normally in seconds, that the RWR will continue to display a threat symbol after the signal processor has determined that the threat is no longer transmitting. The symbol age-out time is set for each threat in the EID tables.

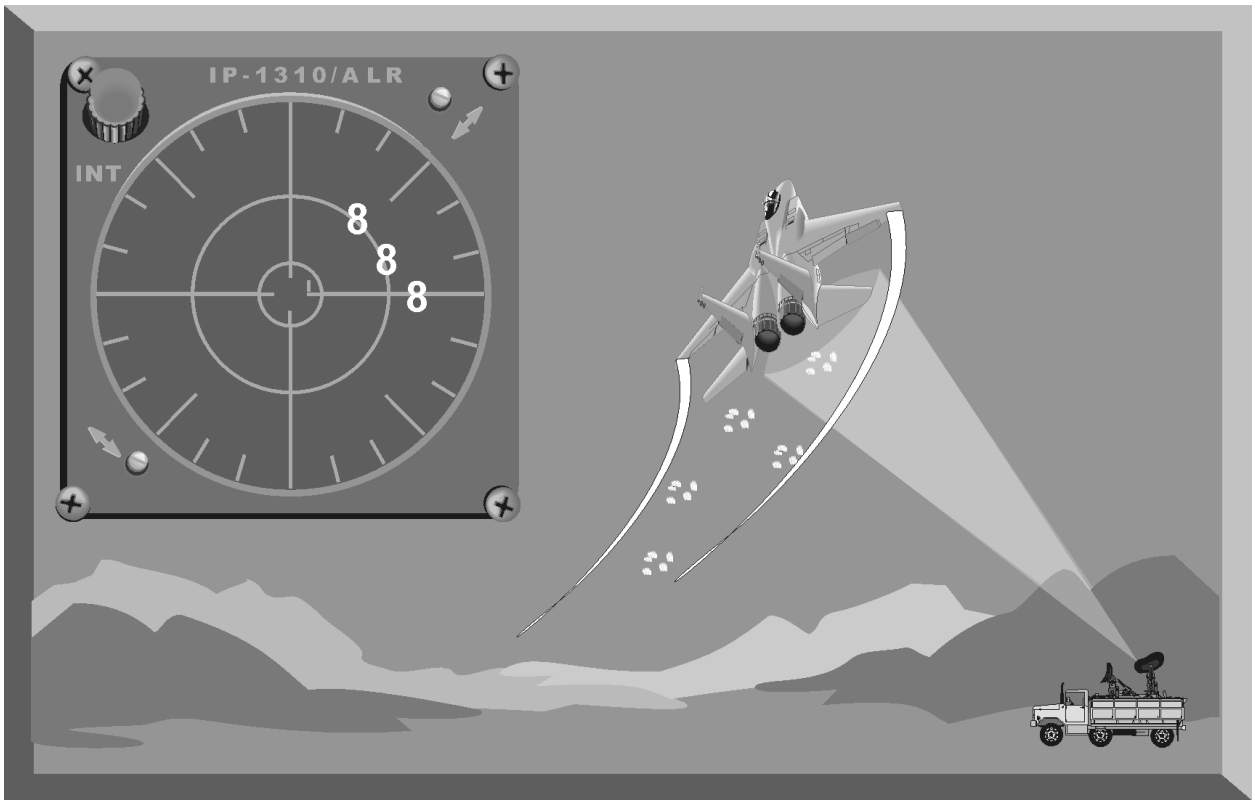


Figure 17-14. RWR Multiple Threat Symbols

c. Electromagnetic interference (EMI) is defined as any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronic systems. EMI can be induced intentionally, by way of jamming, or unintentionally as a result of spurious emissions and modulations. Certain RWR characteristics make them susceptible to EMI. Modern RWR systems are designed to receive and process signals in a wide frequency range, nominally 0.5 to 18 GHz, where most threats operate. This broad frequency coverage combined with the sensitive antennas make RWR systems susceptible to EMI. The primary source of EMI that impacts RWR operation is noise and deception jamming designed to counter enemy threat systems.

(1) High power noise jamming, such as that provided by a stand-off jamming aircraft, causes the RWR to raise the receiver threshold in the frequency band of the jamming. This effectively reduces the sensitivity of the RWR receiver and could delay the display of threat signals in that band. The reduction in sensitivity depends on the power that the jammer is transmitting, the beamwidth of the jamming beam, and the distance from the jammer to the aircraft. High power jamming may also generate multiple threat symbols on the RWR scope at the approximate azimuth to the jammer's position relative to the aircraft. Additionally, jamming from a wingman's self-protection system can generate multiple threat symbols and reduced sensitivity.

(2) A limitation of all RWR systems, related to EMI, is the problem of inaccurately identifying threat radar systems as friendly radar systems. This occurs when the parameters of a friendly radar are similar to the parameters of a threat radar system. The RWR will either display a threat radar symbol or an ambiguity associated with a threat radar. These RWR misidentifications are especially prevalent for AI radar systems.

(3) The impact of EMI on the operation of an RWR system depends on the signal environment. The pilot has little control over the number and diversity of friendly and enemy signals the RWR system must process. EMI is an unfortunate consequence of the reliance of modern military forces on operations in the electromagnetic spectrum. Aircrews should be keenly aware that EMI will impact RWR operation and be must be familiar with common RWR displays of EMI.

10. THREAT GEOLOCATION TECHNIQUES

The purpose of threat geolocation is to put a defined position, normally coordinates, on a threat radar. This information can be used to simply warn other aircraft about the threat or, if the coordinates are accurate enough, to allow for targeting and attack of the threat. Until recently, threat geolocation could only be performed by strategic assets and specialized tactical aircraft, specifically the F-4G Wild Weasel. Due to inherent time delays, data provided through strategic channels often did not apply to mobile threat systems. The mobile systems would relocate making the data obsolete. This section will discuss three techniques used to geolocate, also known as direction finding (DF), emitting radars that can be used by tactical assets to rapidly locate radar threat systems. The three are triangulation, interferometry, and time of arrival. All three techniques are heavily dependent upon the receiving aircraft's ability to accurately determine its present position, and the advent of GPS receivers has made this significantly easier.

a. Triangulation is the most basic form of DF available. It involves taking direction measurements from more than one source. The intersection of the azimuth measurements, called “lines of bearing”, is the likely location of the emitter (Figure 17-15). To be effective, the participating aircraft must have accurate data of their current positions when getting the lines of bearing.

(1) Triangulation can be carried out by multiple aircraft equipped with receiver equipment or by one aircraft over a period of time. The advantage of having multiple aircraft providing azimuth measurements is the increased angle-off and the speed of interception. In triangulation the best azimuth cuts are those that approach 90° angles. The speed of interception comes into play because threat emitters, knowing that DF operations are underway, attempt to transmit for as little time as possible. The disadvantage of multiple platforms is the communication required to ensure that all the platforms are measuring the same radar. In a dense radar environment this can be a difficult task.

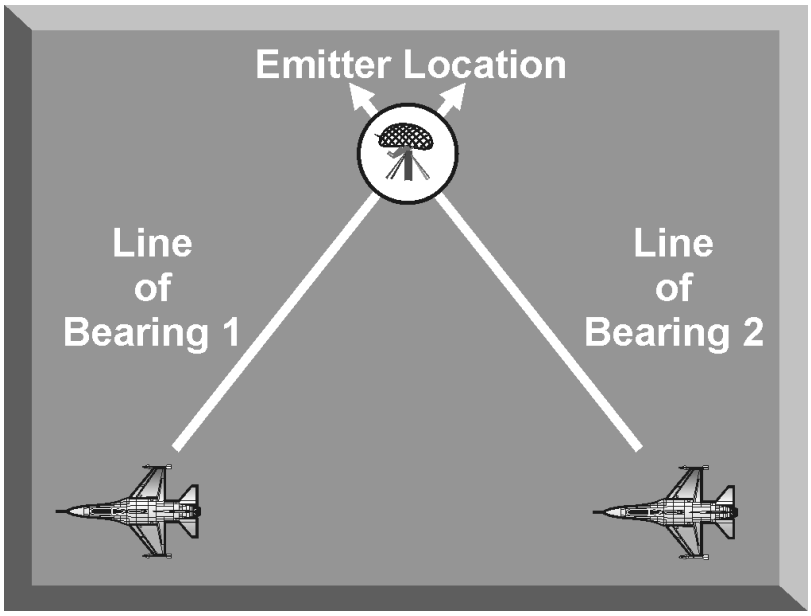


Figure 17-15. Triangulation

(2) Single aircraft triangulation eliminates the problem of signal coordination with other aircraft, but it also requires that the aircraft transit some distance to get multiple azimuth measurements. The accuracy of single ship DF operations is a function of the quality of the receiver equipment, distance away from the targeted radar, speed of the aircraft, and the amount of time that the targeted radar radiates.

b. The second technique is called interferometry. This technique is also known as phase interferometry, or phase difference of arrival. These systems operate by comparing the phase of a radar wave as it impacts two or more DF antennas; this phase difference is then used to compute an angle of arrival (AOA). For aircraft, the desire is to have these DF antennas on different parts of the same aircraft. Multiple AOA measurements are then used to provide the range and position of the threat.

(1) The key elements in an interferometer system are two antennas in fixed locations with matched receivers, a phase comparator, and a processor (Figure 17-16). An intermediate frequency output from each receiver is passed to a phase comparator, which measures the relative phase of the two signals. This relative phase position is passed to a processor, which calculates the AOA relative to the orientation of the two antennas (called the baseline). In most systems, the processor also accepts information about the orientation of the baseline (relative to true North or local horizontal) to determine the true azimuth or elevation angle to the emitter.

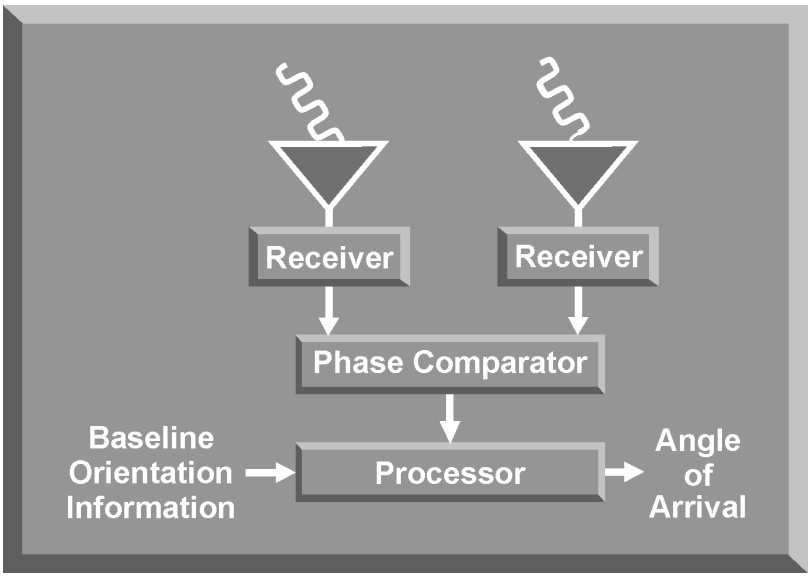


Figure 17-16. Interferometer Components

(2) To obtain rapid emitter locations some interferometer systems use multiple receive antennas in an array setup. This allows for simultaneous azimuth and elevation measurements to rapidly locate the emitter. An array allows for the mixing of long and short baselines in different patterns by selecting different pairs of antennas (Figure 17-17). The terms long baseline and short baseline are often used to designate the distance between the antenna elements in an interferometer system. Long baselines have the advantage of providing a quick and accurate location of the emitter, but they can suffer from ambiguities resulting from different wavefronts hitting the different antenna elements. In addition to the array depicted in Figure 17-17, a long baseline system could be created by using the existing RWR antennas on an aircraft, and supplementing these with a small short baseline system to compensate for the ambiguities.

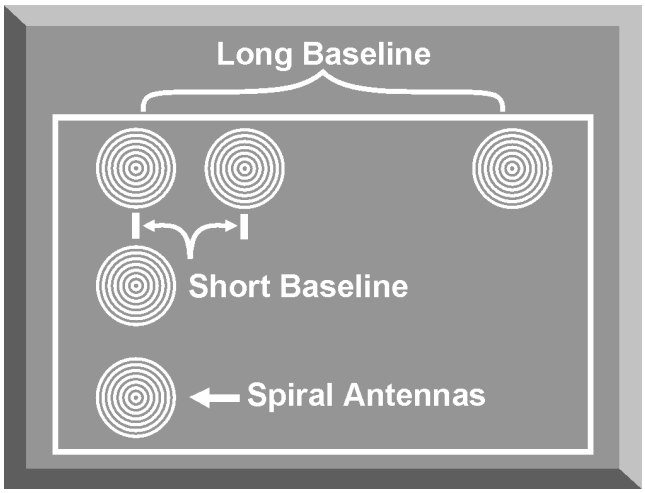


Figure 17-17. Interferometer Array

c. Time of arrival (TOA) and time difference of arrival (TDOA) techniques are the final type of location techniques to be covered in this section. Both techniques are based around the fact that radar signals travel at approximately the speed of light. Both techniques, using the speed of light as a constant, solve for the distance that the emitter is away from the receiver using the equation distance equals rate multiplied by time. Because there is not any directional information, the equation represents the radius of a circle around the receiving antenna; multiple distance measurements taken from multiple receivers are then overlayed. The intersection of the circles is the position of the emitter. If only two receivers are used, a simple DF technique can solve the ambiguity of which intersection represents the emitter (Figure 17-18).

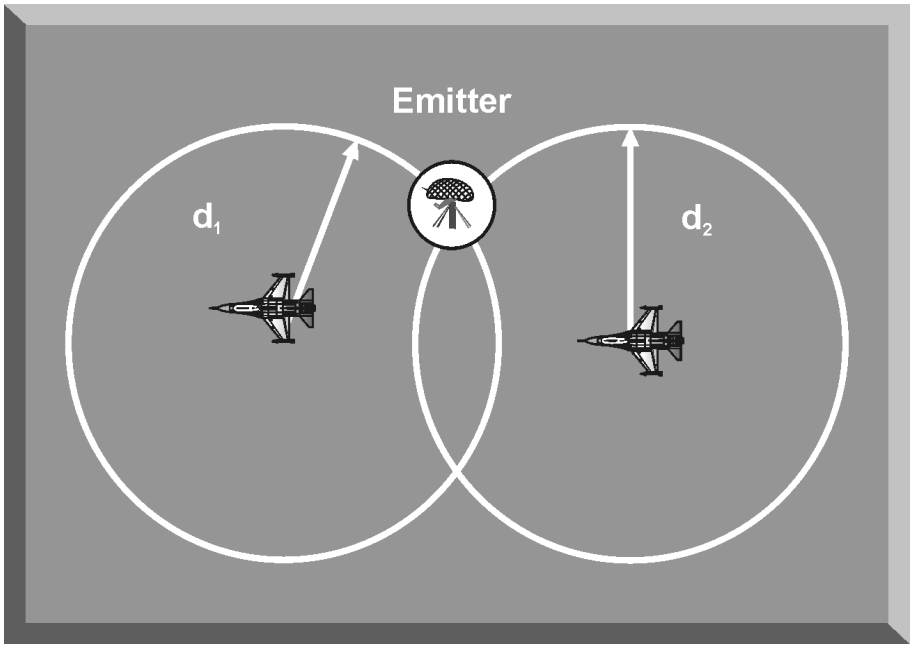


Figure 17-18. Time of Arrival Measurements

(1) TOA positioning is calculated by taking the time that a signal leaves a radar, measuring its arrival time at the receiver and mathematically solving for distance using the techniques described above. One of the primary challenges involved with TOA positioning is determining when the measured signal was transmitted, this requires either a very cooperative enemy or a radar signal with some type of exploitable time reference. Another challenge involves insuring that multiple receivers are timing the same signal. This is especially difficult in a threat intensive environment.

(2) TDOA is used when it is not possible to determine when a signal was transmitted. TDOA uses most of the same principles as TOA except that it must compensate for not knowing the time the signal was transmitted. It does this by using an extra receiver a known distance from the first receiver to generate a distance curve. The arrival of the signal is precisely measured at the two

receivers, the theory is that a signal that arrives at the two receivers at times t1 and t2 had to originate from a point on a curve defined by that difference in arrival time. For example, if the signal arrives at the two points at exactly the same time, then the transmitter must be equal distance from the two receivers. In this case the curve is actually a line of possible locations equal distance from the receivers and can easily be drawn. For situations where the signal arrives at different times at the receivers, a hyperbolic curve instead of a straight line denotes all the possible locations of the transmitter. Figure 17-19 shows an example of when the signal arrives at a different time, the constant value is the time difference multiplied by the speed of light yielding a distance. To solve for the emitter's location using TDOA another antenna receiver is required that is not in line with the first two receivers to generate an independent curve that will cross the first curve at the transmitter location.

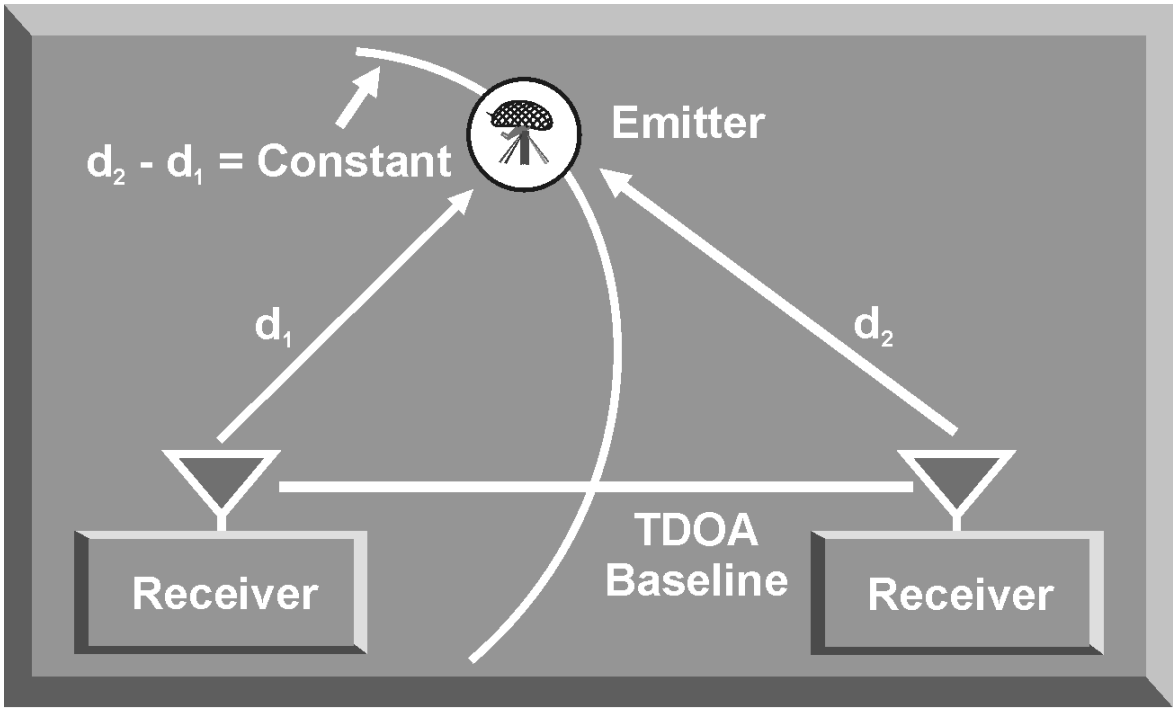


Figure 17-19. Time Difference of Arrival Measurements

(3) Timing techniques require very good timing accuracy in the receiving systems. If the receivers are far apart, such as different aircraft, then a separate time measurement is required at the source before sending to a processor. As with triangulation, one of the major challenges of multiple aircraft measurements is the coordination to ensure that the same signal is being looked at by all aircraft involved.

(4) Timing techniques are affected by the type of radar that they are trying to locate. Pure CW radars are not practical for a timing technique because there

is not a pulse to time. Pulsed signals, on the other hand, are much more susceptible to this type of location technique.

11. SUMMARY

An RWR system is designed to provide a picture of the electronic order of battle (EOB) operating in the vicinity of an aircraft. The signal processor is the heart of the RWR system and controls the function of all other system components. The signal processor, using inputs from the antennas and the receiver/amplifiers, compares the signal parameters with the parameters in the EID tables. The identified signals are displayed on the RWR scope with the appropriate audio. The ICU provides the aircrew interface with the signal processor to allow the aircrew to customize RWR operation for each combat mission. Modern RWR systems have some limitations that can effect aircrew survival. These limitations include ambiguous threat displays, maneuvering limitations, and EMI. Despite these limitations, an operational RWR system is one of the keys to survival on today's electronic battlefield. A product of advances on the electronic battlefield is rapid threat geolocation. New threat geolocation techniques are designed to provide advanced threat information to allow pilots to avoid, suppress, or destroy the mobile threat. The three most common techniques are basic triangulation using lines of bearing, interferometry using phase difference of arrival, and time difference of arrival using time differences to determine distance curves.

CHAPTER 18. SELF-PROTECTION JAMMING SYSTEM OPERATIONS

1. INTRODUCTION

Self-protection jamming systems are designed to counter surface-to-air missile (SAM), airborne interceptor (AI), and antiaircraft artillery (AAA) acquisition and target tracking radars. Self-protection jamming systems generate noise and deception jamming techniques to either deny threat system automatic tracking capability or generate sufficient tracking errors to prevent a successful engagement.

a. To counter the diverse array of threats and their associated frequencies in an integrated air defense system (IADS), a self-protection jamming system must be able to simultaneously jam multiple signals operating in a wide frequency range. The system must also be able to generate sufficient power to mask the radar return of the aircraft. Since many modern self-protection jamming systems are carried internally or externally on aircraft, their size, shape, and weight must be carefully controlled to minimize adverse effects on aircraft performance and handling. These design requirements may require a trade-off between additional power or capability and aircraft compatibility.

b. A self-protection jamming system must have receive antennas to receive radar signals, a system processor to identify received signals, a jamming techniques generator to produce an optimum jamming technique for the identified threat, and transmit antennas to transmit the required jamming techniques. These system components will be discussed in this chapter.

c. There are numerous internal and externally mounted self-protection jamming systems in use today. To simplify the discussion, the ALQ-184 pod will be used as an example of a modern, self-protection jamming system (Figure 18-1). The functions and operations of the ALQ-184 components are representative of currently deployed self-protection systems.

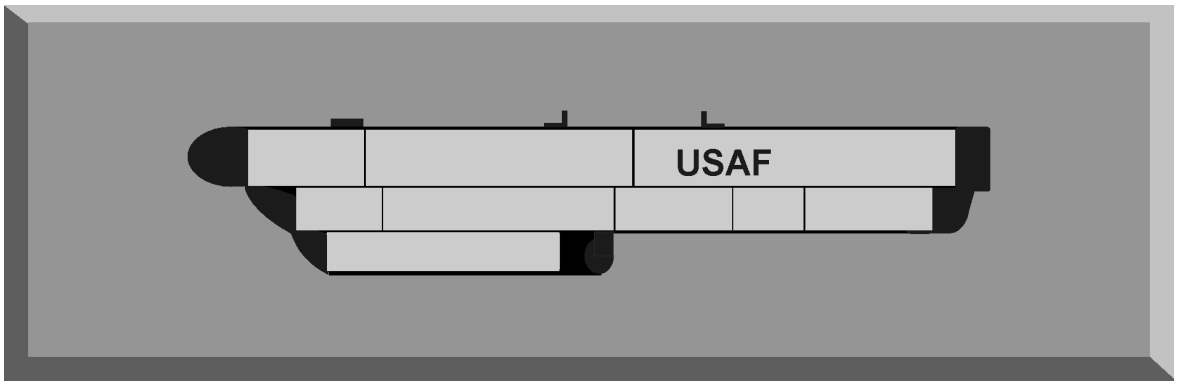


Figure 18-1. ALQ-184 Pod

2. RECEIVE ANTENNAS

The ALQ-184 pod has two sets of receive antenna assemblies located on the front and rear of the lower pod "gondola" (Figure 18-2). Each receive antenna assembly set consists of a low-band antenna and a mid/high-band antenna. The low-band antenna's signals are combined to form the input for the low-band receiver. The mid/high-band antennas provide signals to the separate mid/high-band portion of the pod.

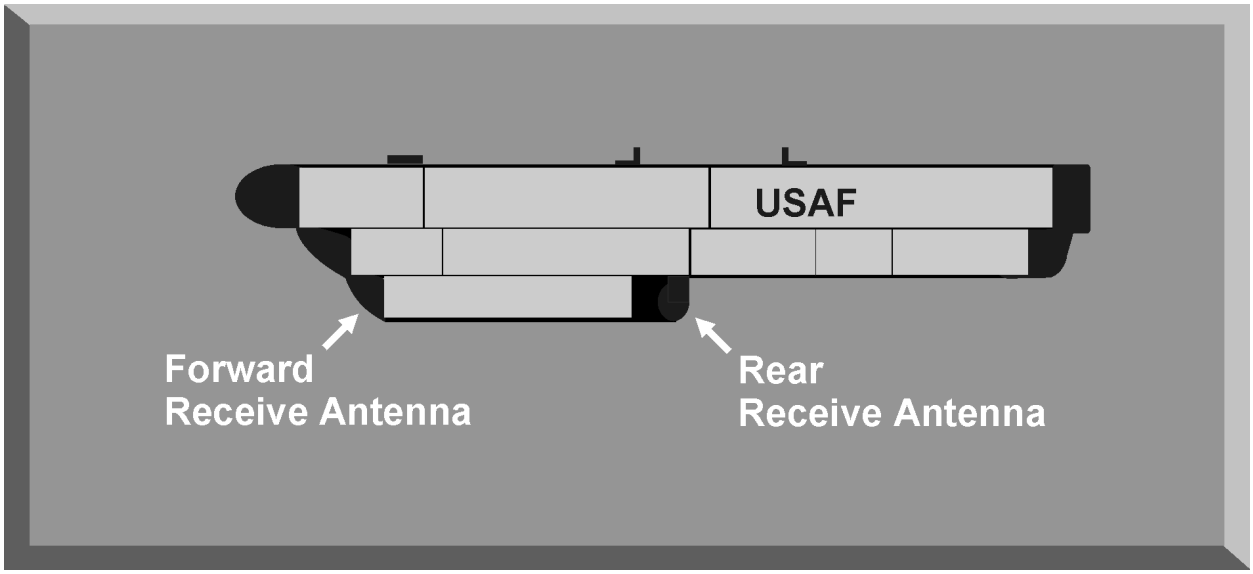


Figure 18-2. ALQ-184 Receive Antenna Location

a. The low-band receive antennas are circularly polarized spiral arrays. The mid/high-band receive antenna covers eight sub-bands via an eight element array that corresponds to the eight element transmit array. The mid/high-band antenna is also circularly polarized.

b. Each signal received via the receive antenna generates a corresponding transmit signal through a crystal video receiver. The angle of arrival (AOA) of each signal is determined by comparing the output of the crystal video receiver for each antenna.

3. RECEIVER SECTION

The forward and aft receive antennas detect radar signals and send them to the receiver section. The receiver section contains an AOA receiver and a multiplexer that separates frequencies. The AOA receiver determines the AOA of a signal based on the output signal level of each antenna element. The AOA data is passed to the system processor to control the angle of transmission of the jamming signal. The multiplexer separates all received threat signals into eight frequency sub-bands consisting of five mid-band and three high-band frequency

ranges. The multiplexer categorizes the received radar signals by sub-band and azimuth and then sends them to the system processor and the exciter.

4. SYSTEM PROCESSOR

The system processor is the "brain" of the ALQ-184 pod. It receives the threat signals from the receiver section that have already been categorized by sub-band and distinguished by AOA. Each received signal and its corresponding AOA is counted. When the signal count exceeds a pre-set threshold, the system processor validates the signal and identifies it using the emitter identification (EID) tables. Based on this threat identification, the system processor directs the techniques generator to initiate a jamming program through the exciter. At the same time, the system processor, through a signal switch control, directs the transmitter section to use either the forward or aft transmit antenna array, and specifies the transmit angle for the jamming program based on AOA.

a. The system processor also controls the low-band portion of the pod (Figure 18-3). The forward or aft low-band antenna receives and combines the threat signal and sends it to the multiplexer. The multiplexer channelizes this signal into one of two low sub-bands. The signal then passes to the modulator where the voltage controlled oscillators (VCOs) generate a jamming technique as directed by the system processor techniques generator. This ensures the jamming technique is at the proper frequency and modulation to provide maximum effect against the threat system. The generated jamming signal passes to a second multiplexer and then to a solid state amplifier for amplification. The amplified jamming signal is then sent to the two low-band traveling wave tubes (TWTs) and transmitted from the forward and aft low-band transmit antennas.

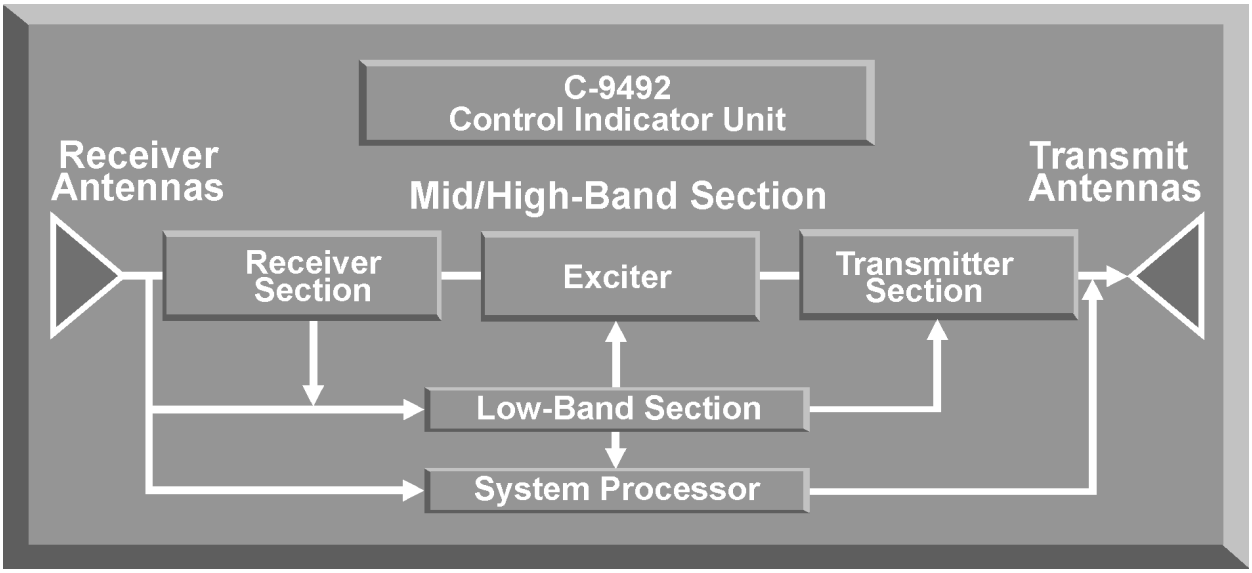


Figure 18-3. ALQ-184 Simplified Block Diagram

b. The system processor periodically performs a background built-in-test (B-BIT), to check the status and calibration of the ALQ-184. The system processor software is updated or reprogrammed as required from a memory loader verifier (MLV). The system processor uses two major software programs. The operational flight program (OFP) manages the receiver and transmitter functions, signal processing, and techniques generation. The mission data generator (MDG) contains the threat EID tables and the jamming techniques matrix for these threats.

5. JAMMING TECHNIQUES GENERATOR

The exciter section contains the VCOs and the keyed oscillators, which generate the jamming waveforms that are directed by the system processor. The exciter takes the threat signal from the receiver and modifies it with deception modulation or generates a noise program based on the techniques generator in the system processor. The selected jamming technique is then sent to the transmitter section.

6. TRANSMIT ANTENNAS

The transmitter section contains antenna switching circuits, a signal forming network, and TWTs. The antenna switching circuits are controlled by the system processor to ensure the transmitted jamming pulse is radiated at the proper azimuth. The signal-forming network controls the phase of each jamming signal. There are sixteen TWTs in the transmitter section, one for each front and aft antenna. The TWTs amplify the jamming signal for transmission from the appropriate transmit antenna.

a. The ALQ-184 has two sets of transmit antenna assemblies. One set is located on the front and one on the rear of the main pod assembly (Figure 18-4).

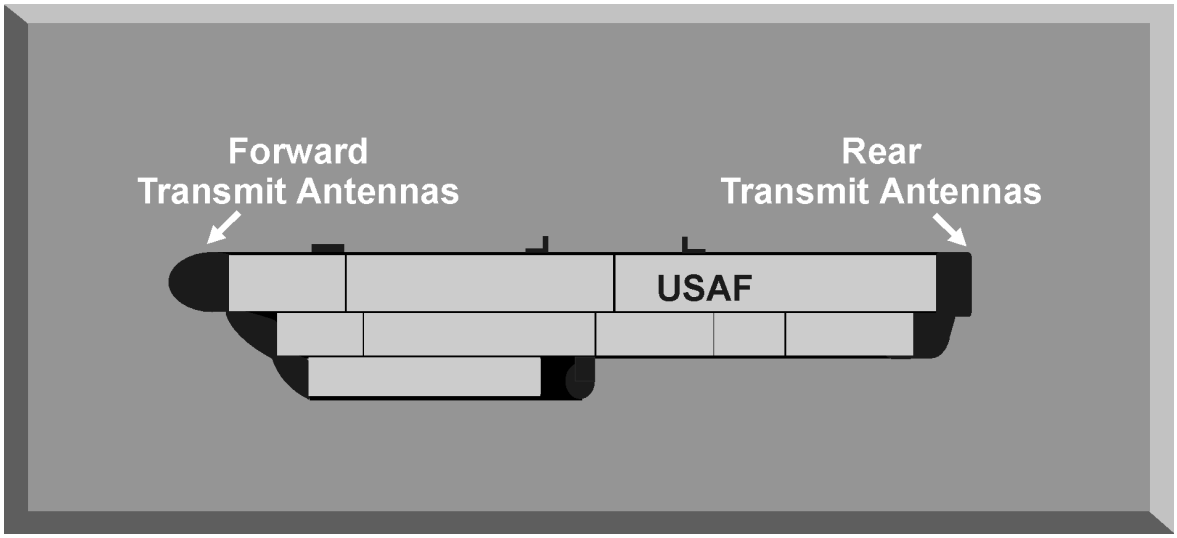


Figure 18-4. ALQ-184 Transmit Antenna Location

Each set has a low-band and mid/high-band antenna. The transmit antennas have opposite polarization from the receive antennas. This enables the pod to transmit and receive at the same time while preventing pod "ringing." Ringing occurs when the pod receives its own jamming signal and generates a jamming program to counter its own signal. This condition can highlight the aircraft to enemy radar and seriously degrade pod effectiveness.

b. The low-band transmit horn antennas are circularly polarized. The mid/high-band transmit antennas have the same eight-element array as the receive antennas. The transmit antennas generate a directional jamming signal for pulsed radar signals based on the AOA determined by the receive antennas. Detailed information on the antenna jamming pattern is contained in the ALQ-184 ECM Handbook.

7. C-9492 CONTROL INDICATOR UNIT

The C-9492 Control Indicator Unit (CIU) provides control of all functions of the ALQ-184. It allows the aircrew to control system power, select jamming techniques, and monitor system status (Figure 18-5).

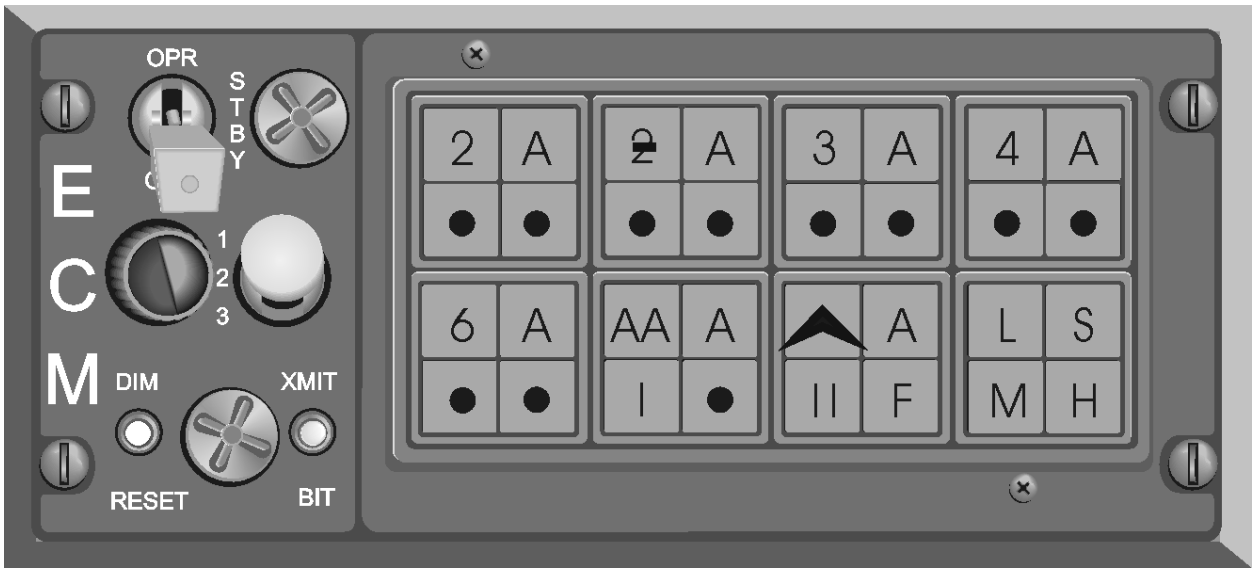


Figure 18-5. C-9492 Control Indicator Unit

8. JAMMING POD CONSIDERATIONS

Unfortunately, jamming pods do not make the aircraft completely invisible from enemy threat systems. When used in conjunction with the RWR, expendables, and threat countertactics they do drastically increase the probability of surviving a threat engagement. This section contains some items of consideration to ensure that your self-protection jamming is being properly utilized. These considerations include highlighting, burnthrough, and reprogramming.

a. If used improperly a self-protection pod can actually highlight the aircraft. This happens when a pod transmits a jamming program constantly or when another type of radar, not targeted for jamming but in the same frequency range, sees the jamming. Highlighting is normally associated with noise programs that transmit constantly. Most pods today avoid this by transmitting only when a threat requires it. Additionally, some aircraft have pod inhibit switches that allow the pod to remain in a standby condition until the pilot switches the pod to operate. What makes this system effective is that the switch is either on the stick or throttle allowing the pilot to rapidly go to operate without looking inside the cockpit (Figure 18-6).

Figure 18-6. F-16 ECM CMS

b. Burnthrough is described as the range that the aircraft's radar return is stronger than its jamming signal. Basically, the jet has gotten so close to the threat radar that the threat radar is overpowering the jamming pod. The range that this occurs varies for different radars, but it should be planned for particularly when there are threats in the target area. Burnthrough is also a consideration for support jamming systems; there is a range at which the support jammer's signal will be overpowered and the protected aircraft can be seen.

c. Many self-protection jamming systems are what is called software-reprogrammable. This means that jamming programs can be rapidly changed to adjust for changes in enemy radar systems. These updates can be made to

systems while they are still on the jet, and can take as little as 15 minutes using an MLV. The process of changing electronic warfare systems is known as a Pacer Ware change. An exercise to check the ability to make changes is known as a Serene Byte exercise. The pilot of the aircraft carrying the self-protection system has one responsibility in this process: to ensure that his jamming system is carrying the most current software program, usually referred to as a software version. While Pacer Ware changes are not common during peacetime operations, they do happen quickly during combat operations often to fine tune the jamming systems for the particular theater of combat.

9. SUMMARY

The effective employment of self-protection jamming is one of the factors that can mean the difference between success and failure on the modern battlefield. When employed in concert with chaff and maneuvers, self-protection jamming can be extremely effective in negating potentially lethal attacks. Despite their limitations, self-protection jamming systems are an important part of the "bag of tricks" aircrews can employ to put bombs on target.

EC-RELATED ABBREVIATIONS AND ACRONYMS

A

AAA	**Antiaircraft artillery**
AAM	**Air-to-air missile**
AAS	**ARM alarm sensor**
AC	**Alternating current**
ACET	**Automatic cancellation of extended targets**
ACQ	**Acquisition**
AC&W	**Aircraft control and warning**
ADA	**Air defense artillery**
ADF	**Automatic direction finding**
ADL	**Automatic data link**
AEW	**Airborne early warning**
AF	**Air Force/audio frequency**
AFB	**Air Force Base**
AFC	**Automatic frequency control**
AFRES	**Air Force Reserves**
AGC	**Automatic gain control**
AGI	**Auxiliary general intelligence (ship)**
AGL	**Above ground level**
AGM	**Air-to-ground missile**
AI	**Airborne interceptor**
AJ	**Anti-jamming**
AM	**Amplitude modulation**
AM-CW	**Amplitude modulated continuous wave**
AMOP	**Amplitude modulation on pulse**
AMP	**Amplifier**
AMRAAM	**Advanced medium range air-to-air missile**
AMTI	**Airborne moving target indicator**
ANG	**Air National Guard**
ANL	**Automatic noise limiting**
AOA	**Angle of arrival/angle of attack**
AOJ	**Angle-on-jam**
ARM	**Antiradiation missile**
ASK	**Amplitude shift keying**
ASM	**Air-to-surface missile**
ASR	**Air surveillance radar**
ASW	**Anti-submarine warfare**
ATC	**Air traffic control**
ATD	**Automatic target detector**
ATR	**Antenna, transmit receive**

ATV	**Automatic threshold variation**
AVNL	**Automatic video noise leveling**
AVP	**Adaptive video processing**
AWACS	**Airborne warning and control system**
AZ	**Azimuth**

B

BBC	**Beam-to-beam correlation**
BCC	**Battery control center**
BFO	**Beat frequency oscillator**
BIT	**Built-in test**
BMEWS	**Ballistic Missile Early Warning System**
BN	**Barrage noise**
BSE	**Boresight error**
BTE	**Battery terminal equipment**
BW	**Bandwidth**
BWO	**Backward wave oscillator**

C

C	**Degree centigrade**
C^2	**Command and control**
C^3	**Command, control, and communications**
C^2W	**Command and control warfare**
CAP	**Combat air patrol**
CAS	**Close air support**
CE	**Clutter eliminator**
CEP	**Circular error probable**
CFAR	**Constant false alarm rate**
CIJ	**Close-in jamming**
CIU	**Control indicator unit**
CM	**Countermeasures**
COHO	**Coherent oscillator**
COMINT	**Communications intelligence**
COMSEC	**Communication security**
CONSCAN	**Conical scan**
COSRO	**Conical scan-on-receive-only**
CPAC	**Coded pulse anti-clutter**
CP	**Circular polarization**
CRT	**Cathode ray tube**
CSG	**Clean strobe generator**
CSLC	**Coherent sidelobe canceler**
CV	**Coincident video**
CVR	**Crystal video receiver**

CW	**Continuous wave**
CWAR	**Continuous wave acquisition radar**
CWI	**Continuous wave illuminator**

D

dB	**Decibel**
dBm	**Decibels relative to 1 milliwatt**
dBw	**Decibels relative to 1 watt**
DBB	**Detector back bias**
DBF	**Digital beam forming**
DC	**Direct current**
DET	**Detector**
DF	**Direction finder/Dicke fix**
DINA	**Direct amplified noise**
DIFM	**Digital instantaneous frequency measurement**
DME	**Distance measuring equipment**
DOA	**Direction of arrival/dead on arrival**
DOF	**Degrees of freedom**
DPI	**Detected pulse interference**
DR	**Dynamic range/dead reckoning**
DRFM	**Digital radio frequency memory**
DSB	**Double sideband**
DTM	**Data transfer module**

E

EA	**Electronic attack**
EC	**Electronic combat**
ECCM	**Electronic counter-countermeasures**
ECM	**Electronic countermeasures**
ECP	**Electronic combat pilot**
EDAC	**Error detection and correction**
EHF	**Extremely high frequency**
EID	**Emitter identification (table)**
EL	**Elevation**
ELINT	**Electronic intelligence**
ELSCAN	**Elevation scan**
EMCON	**Emission control**
EMI	**Electromagnetic interference**
EMP	**Electromagnetic pulse**
EO	**Electro-optical**
EOB	**Electronic order of battle**
EP	**Electronic protection**
ER	**Electronic reconnaissance**

ERP	**Effective radiated power**
ES	**Electronic warfare support**
EVIL	**Evaluated vs. integrated log**
EW	**Electronic warfare**
EWO	**Electronic warfare officer**
EWWS	**Electronic warfare warning set**

F

F	**Degrees Fahrenheit**
FA	**Frequency agility**
FC	**Fire control**
FAAR	**Forward area alerting radar**
FAGC	**Fast automatic gain control**
FCR	**Fire control radar**
FCS	**Fire control system**
FEBA	**Forward edge of the battle area**
FFO	**Fixed frequency oscillator**
FFT	**Fast Fourier transform**
FLIR	**Forward looking infrared**
FM	**Frequency modulation**
FM-CW	**Frequency modulation continuous wave pulsed**
FMOP	**Frequency modulation on pulse**
FOJ	**Fuse-on-jam**
FOR	**Field of regard**
FOTD	**Fiber optic towed decoy**
FOV	**Field of view**
FRESCAN	**Frequency scanning**
FS	**Frequency sector**
FSK	**Frequency shift keying**
ft	**Feet**
FTC	**Fast time constant**

G

G	**Antenna gain/acceleration due to gravity**
GAS	**Ground aided seeker**
GCA	**Ground controlled approach**
GCI	**Ground controlled intercept**
GEN	**Generator**
GHz	**Gigahertz**

H

HARM	**High-speed antiradiation missile**
HAWK	**Homing all-the-way killer**
HBW	**Horizontal beam width**
HF	**High frequency/height finder**
HFDF	**High frequency direction finding**
HIPIR	**High-power illuminator radar**
HOJ	**Home-on-jam**
HOT	**Home-on-target**
HQ	**Headquarters**
HUMINT	**Human intelligence**
HVP	**High video pass**
HVPS	**High voltage power supply**
Hz	**Hertz**

I

I	**Improved**
IADS	**Integrated air defense system**
IAGC	**Instantaneous automatic gain control**
ICD	**Imitative communications deception**
ICW	**Interrupted continual wave**
IF	**Intermediate frequency**
IFC	**Instantaneous frequency correlator**
IFF	**Identification, friend or foe**
IPM	**Instantaneous position memory**
IR	**Infrared**
IRCM	**Infrared countermeasures**

J

JAT	**Jam angle track**
JAVA	**Jamming amplitude versus azimuth**
JCS	**Joint Chiefs of Staff**
JLT	**Jammer look-through**
J/S	**Jamming-to-signal (ratio)**
JTIDS	**Joint Tactical Information Distribution System**

K

K	**Degrees Kelvin**
kHz	**Kilohertz**
km	**Kilometer**

KO	**Keyed oscillation**
kV	**Kilovolts**
kW	**Kilowatts**

L

LASER	**Light amplification by stimulated emission of radiation**
LET	**Leading-edge tracker**
LF	**Low frequency**
LFMOP	**Linear frequency modulation on pulse (chirp)**
LIN	**Linear**
LIN-LOG	**Linear-logarithmic amplifier**
LLLTV	**Low light level television**
LO	**Local oscillator**
LOG	**Logarithmic**
LOG-FTC	**Logarithmic receiver with fast time constant**
LORO	**Lobe-on-receive-only**
LOS	**Line of sight**
LPI	**Low probability of intercept**
LT	**Listening time**
LVA	**Log video amplifier**

M

M	**Meter**
MALD	**Miniature air launched decoy**
MASER	**Microwave amplification by stimulated emission of radiation**
MANPADS	**Manportable air defense system**
MAWS	**Missile approach warning system**
MBB	**Main beam blanking**
MCG	**Midcourse guidance**
MCD	**Manipulative communications deception**
MDT	**Mission data type**
MDF	**Mission data file**
MDG	**Mission data generator**
MF	**Medium frequency**
MFAR	**Multifunction array radar**
MG	**Missile guidance**
MGC	**Manual gain control**
MHz	**Megahertz**
MIC	**Microwave integrated circuit**
MIJI	**Meaconing, Intrusion, Jamming, and Interference**
MLC	**Mainlobe cancellation**
MLV	**Memory loader verifier**
mm	**Millimeter**

MMIC	**Monolithic microwave integrated circuit**
MMW	**Millimeter wave**
MOE	**Measure of Effectiveness**
MOPA	**Master oscillator power amplifier**
msec	**Millisecond**
MTD	**Moving target detector**
MTI	**Moving target indicator**
MUX	**Multiplexer**
MW	**Megawatts**

N

NBFM	**Narrowband frequency modulation**
NBL	**Narrowband limiting**
NBLP	**Narrowband long pulse**
nm	**Nautical mile**
NLP	**Narrowband long pulse**
NOTAM	**Notice to airmen**
NSPS	**Nonsynchronous pulse suppression**

O

OFP	**Operational flight program**
OOB	**Order of battle**
OOK	**On-off keying**
OOK CW	**Interrupted CW**
OPDEC	**Operational deception**
OPSEC	**Operational security**
OTH	**Over-the-horizon**

P

PAM	**Pulse amplitude modulation**
PAR	**Pulse acquisition radar/precision approach radar**
PAT	**Passive angle track**
PC	**Pulse compression**
PCM	**Pulse code modulation**
PD	**Pulse Doppler/pulse duration (same as PW)**
PDM	**Pulse duration modulation**
PENAIDS	**Penetration aids**
PFM	**Pulse frequency modulation**
PFN	**Pulse-forming network**
PHOTOINT	**Photographic intelligence**
PIE	**Pulse interference elimination**

PISAB	**Pulse interference suppression and blanking**
PLD	**Pulse length discrimination (same as PWD)**
PM	**Phase modulation**
PN	**Pseudo noise**
PPC	**Pulse-to-pulse correlation**
PPI	**Plan position indicator**
PPM	**Pulse position modulation**
PPS	**Pulses per second**
PRF	**Pulse repetition frequency**
PRI	**Pulse repetition interval**
PRT	**Pulse recurrence time**
PSK	**Phase shift keying**
PW	**Pulse width**
PWD	**Pulse width discrimination**
PWM	**Pulse width modulation**

R

RADAR	**Radio detection and ranging**
RAGM	**Range angle gate memory**
RAM	**Radar absorbing material/repeater amplitude modulation**
RANRAP	**Random range program**
RC	**Resolution cell**
RCS	**Radar cross section**
RDF	**Radio direction finding**
RF	**Radio frequency**
RFD	**Radio frequency discriminator**
RFI	**Radio frequency interference**
RGM	**Range gate memory**
RGPI	**Range gate pull in**
RGPO	**Range gate pull off**
RHAW	**Radar homing and warning**
RHI	**Range height indicator**
ROB	**Radar order of battle**
ROR	**Range only radar**
R/P	**Receiver/processor**
RPD	**Random pulse discrimination**
RPJ	**Random pulse jamming**
RPM	**Revolutions per minute**
RPS	**Random pulse suppression**
RPV	**Remotely piloted vehicle**
RSBN	**Radio short-range beacon for navigation**
RT	**Recovery time**
R/T	**Receiver/transmitter**
RWR	**Radar warning receiver**

S

SAM	**Surface-to-air missile**
SAR	**Synthetic aperture radar**
SASE	**Semi-automatic support equipment**
SATCOM	**Satellite communications**
SBB	**Single beam blanking**
SCV	**Sub-clutter visibility**
SEAD	**Suppression of enemy air defenses**
sec	**Seconds**
SHF	**Super high frequency**
SIF	**Selective identification feature**
SIGINT	**Signals intelligence**
S/J	**Signal-to-jamming (ratio)**
SLAR	**Side-looking airborne radar**
SLB	**Sidelobe blanking**
SLC	**Sidelobe cancellation**
SLS	**Sidelobe suppression**
S/N	**Signal-to-noise (ratio)**
SOJ	**Stand-off jamming**
SORO	**Scan-on-receive-only**
SRM	**Swept rectangular modulation**
SS	**Swept-spot**
SSB	**Single sideband**
SSN	**Swept-spot noise/social security number**
SRW	**Swept rectangular wave**
SSW	**Swept square wave**
STALO	**Stable local oscillator**
STC	**Sensitivity time control**
SWC	**Scan with compensation**

T

TA	**Target acquisition**
TACAN	**Tactical air navigation**
TALD	**Tactical air launched decoy**
TBM	**Track break modulation**
TDD	**Target detection device**
TDOA	**Time difference of arrival**
TEL	**Transporter-erector-launcher**
TELAR	**Transporter-erector-launcher and radar**
TET	**Trailing edge tracker**
TEWS	**Tactical electronic warfare system**
TFR	**Terrain following radar**
TGT	**Target**
TJS	**Tactical jamming system**

TOA	**Time of arrival**
TOF	**Time of flight**
TOJ	**Track-on-jam**
TPL	**Transmitter pulse lengthening**
TPS	**Transmitter pulse shaping**
TTR	**Target tracking radar**
TV	**Television**
TVM	**Track-via-missile**
TWS	**Track-while-scan**
TWT	**Traveling wave tube**

U

UHF	**Ultra high frequency**
µsec	**Microseconds**

V

VCO	**Voltage controlled oscillator**
VDL	**Video data link**
VGPO	**Velocity gate pull off**
VHF	**Very high frequency**
VHSIC	**Very high speed integrate circuit**
VINT	**Video integration**
VLF	**Very low frequency**
VSRW	**VGPO with swept rectangular wave**
VSWR	**Voltage standing-wave ratio**

W

W	**Watts**
WBFM	**Wideband frequency modulation**
WBL	**Wideband limiting**
WPB	**Wide pulse blanking**
WSP	**Wideband short pulse**

Radar Fundamentals

Quick Review

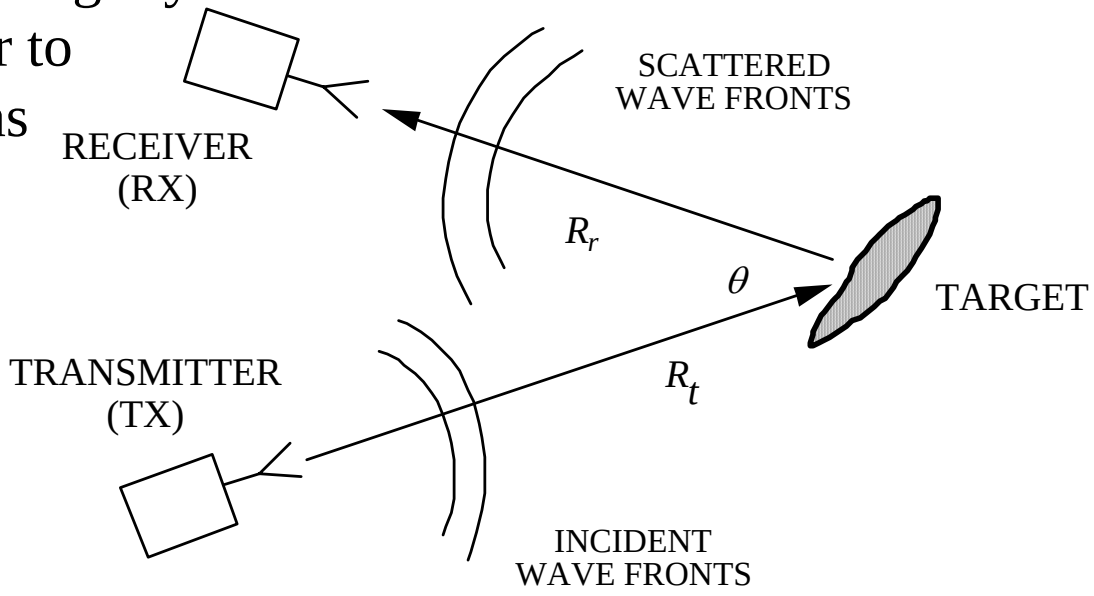
Assoc. Prof. Dr. Ahmed Saleh
EEE - Department of Radar
Military Tchnical College

Overview

- Introduction
- Radar functions
- Antennas basics
- Radar range equation
- System parameters
- Electromagnetic waves
- Scattering mechanisms
- Radar cross section and stealth
- Sample radar systems

Radio Detection and Ranging

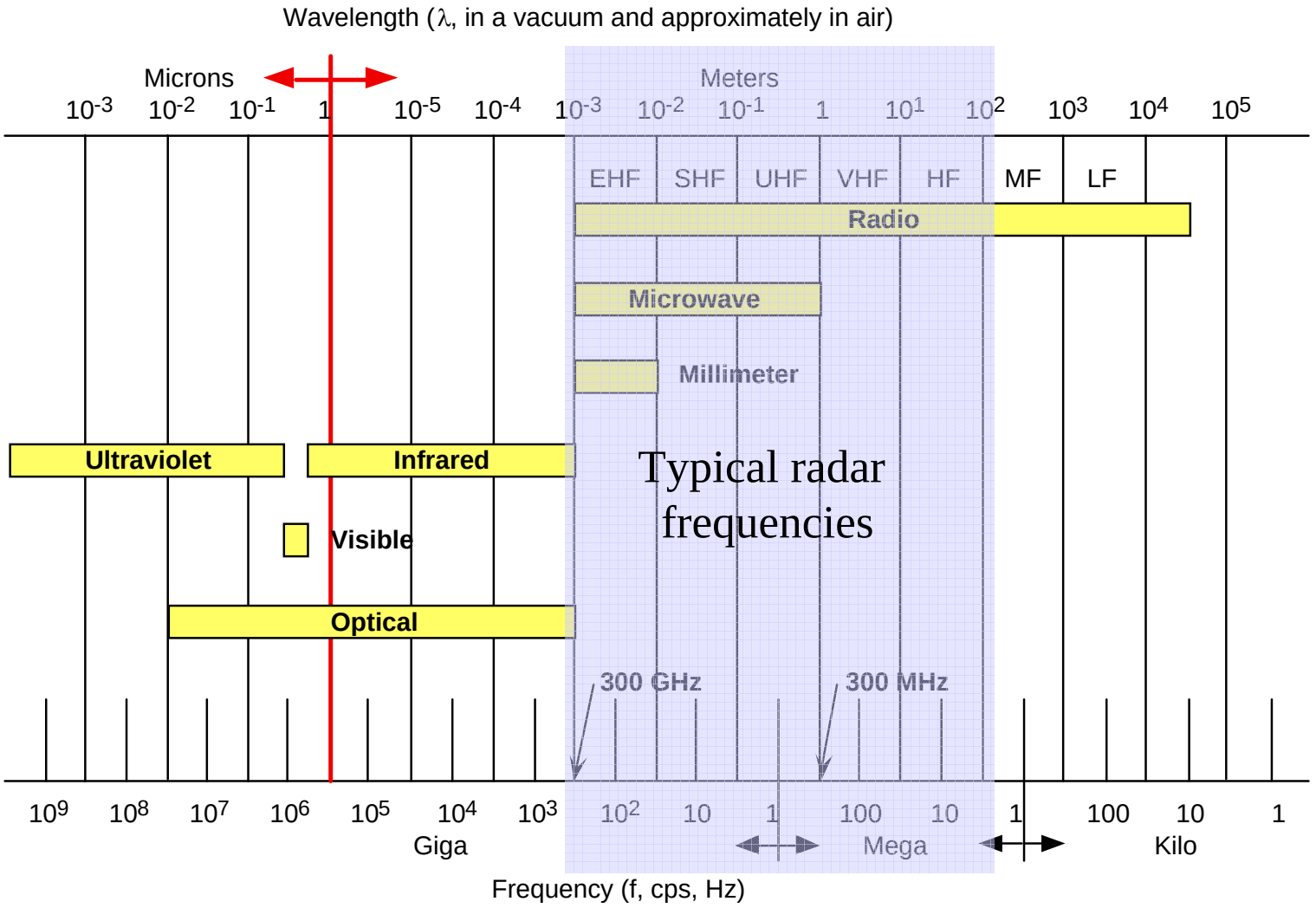
- Bistatic: the transmit and receive antennas are at different locations as viewed from the target (e.g., ground transmitter and airborne receiver).
- Monostatic: the transmitter and receiver are colocated as viewed from the target (i.e., the same antenna is used to transmit and receive).
- Quasi-monostatic: the transmit and receive antennas are slightly separated but still appear to be at the same location as viewed from the target (e.g., separate transmit and receive antennas on the same aircraft).



Radar Functions

- Normal radar functions:
    1. range (from pulse delay)
    2. velocity (from Doppler frequency shift)
    3. angular direction (from antenna pointing)
- Signature analysis and inverse scattering:
    4. target size (from magnitude of return)
    5. target shape and components (return as a function of direction)
    6. moving parts (modulation of the return)
    7. material composition
- The complexity (cost & size) of the radar increases with the extent of the functions that the radar performs.

Electromagnetic Spectrum



Radar Bands and Usage

Band Designation	Frequency Range	Usage
HF	3–30 MHz	OTH surveillance
VHF	30–300 MHz	Very-long-range surveillance
UHF	300–1,000 MHz	Very-long-range surveillance
L	1–2 GHz	Long-range surveillance En route traffic control
S	2–4 GHz	Moderate-range surveillance Terminal traffic control Long-range weather
C	4–8 GHz	Long-range tracking Airborne weather detection
X	8–12 GHz	Short-range tracking Missile guidance Mapping, marine radar Airborne intercept
K_u	12–18 GHz	High-resolution mapping Satellite altimetry
K	18–27 GHz	Little use (water vapor)
K_a	27–40 GHz	Very-high-resolution mapping Airport surveillance
millimeter	40–100+ GHz	Experimental

(Similar to Table 1.1 and Section 1.5 in Skolnik)

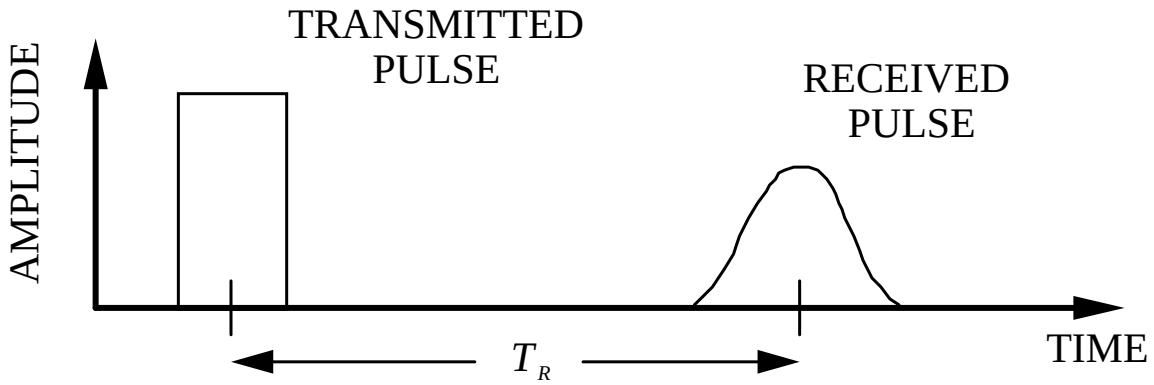
Time Delay Ranging

- Target range is the fundamental quantity measured by most radars. It is obtained by recording the round trip travel time of a pulse, T_R , and computing range from:

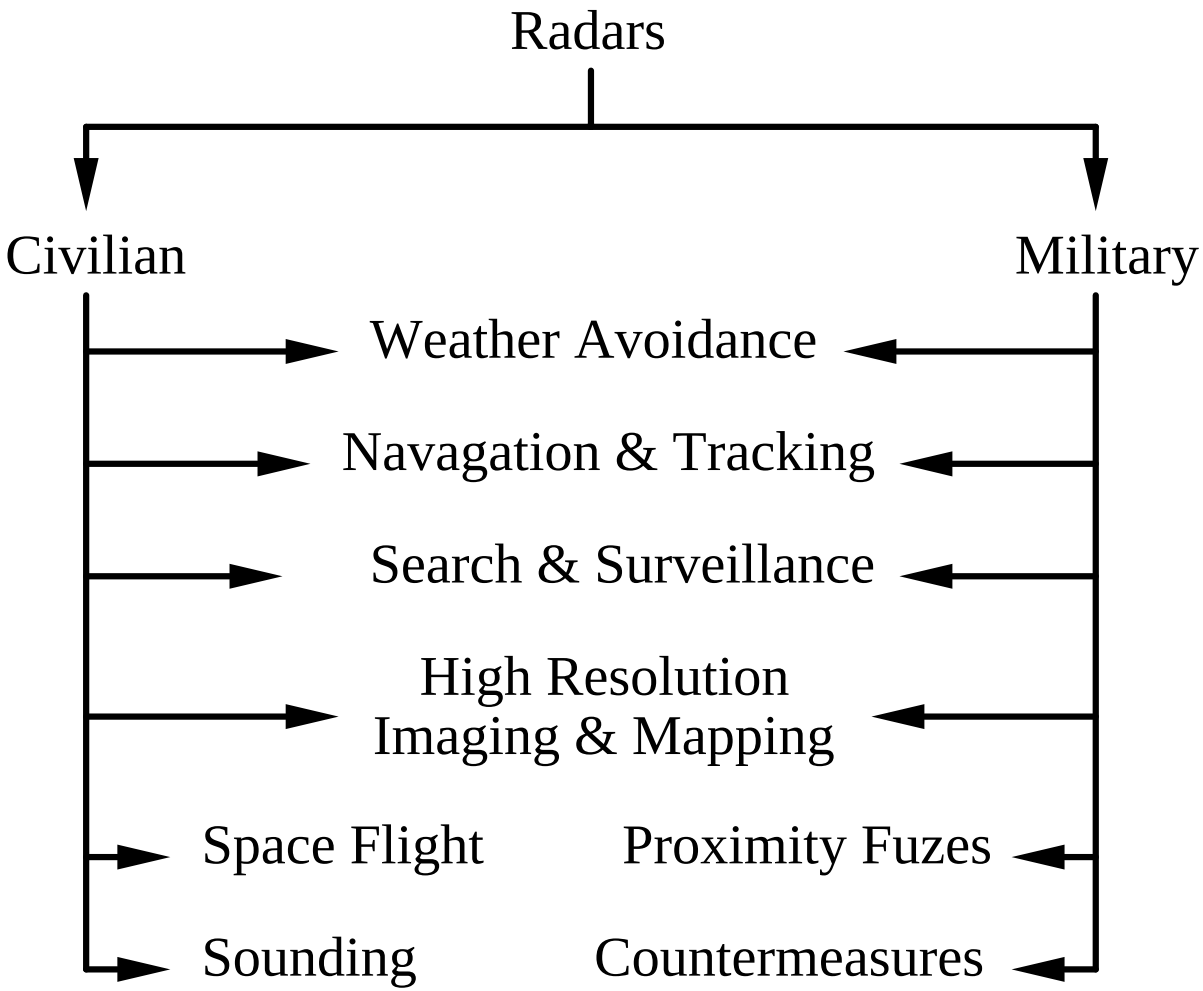
$$\text{Bistatic: } R_t + R_r = cT_R$$

$$\text{Monostatic: } R = \frac{cT_R}{2} \quad (R_t = R_r = R)$$

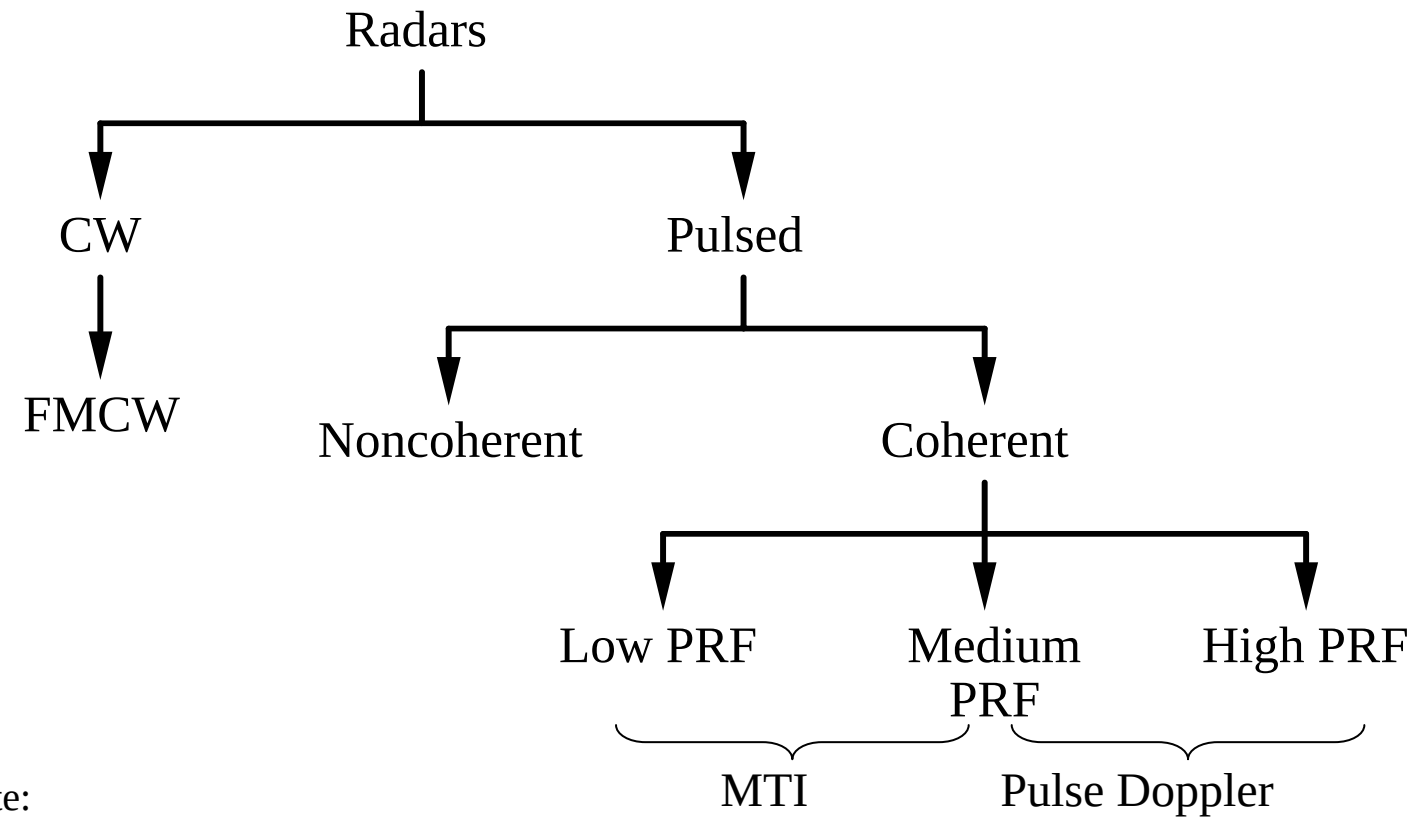
where c = 3x10^8 m/s is the velocity of light in free space.



Classification by Function



Classification by Waveform

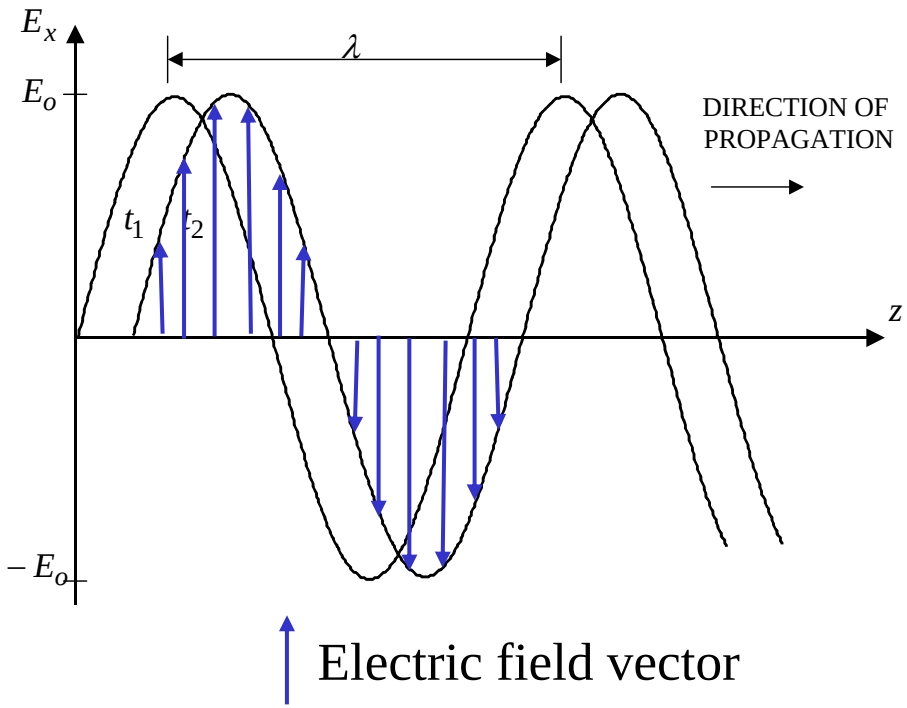


Note:

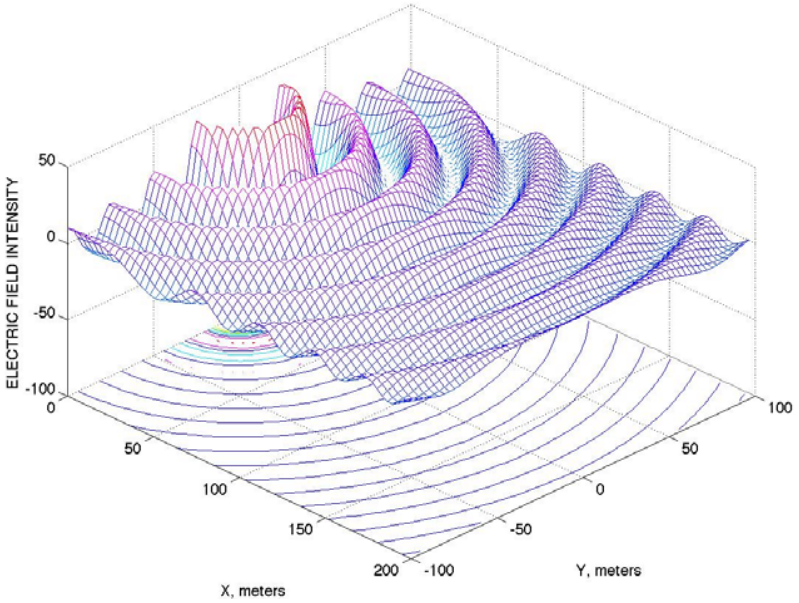
CW = continuous wave
FMCW = frequency modulated continuous wave
PRF = pulse repetition frequency
MTI = moving target indicator

Plane Waves

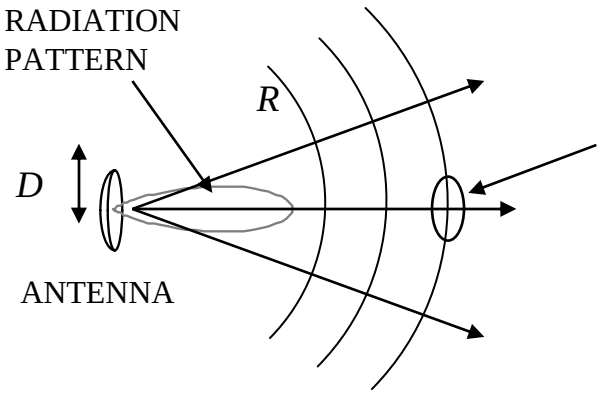
- Wave propagates in the z direction
- Wavelength, λ
- Radian frequency $\omega = 2\pi f$ (rad/sec)
- Frequency, f (Hz)
- Phase velocity in free space is c (m/s)
- x-polarized (direction of the electric field vector)
- E_o, maximum amplitude of the wave



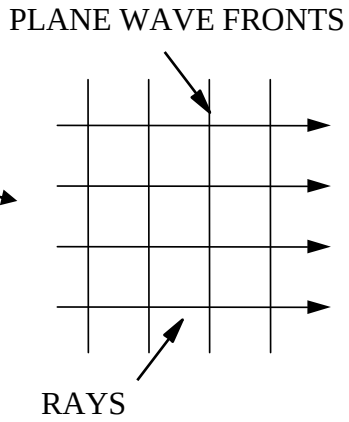
Wavefronts and Rays



- In the antenna far-field the waves are spherical $(R > 2D^2/\lambda)$
- Wavefronts at large distances are locally plane
- Wave propagation can be accurately modeled with a locally plane wave approximation

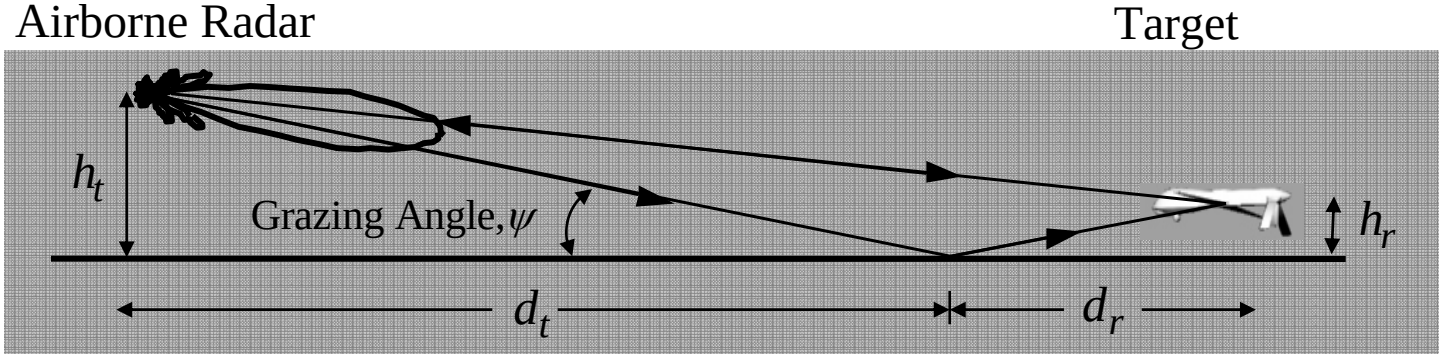


Local region in the far field of the source can be approximated by a plane wave



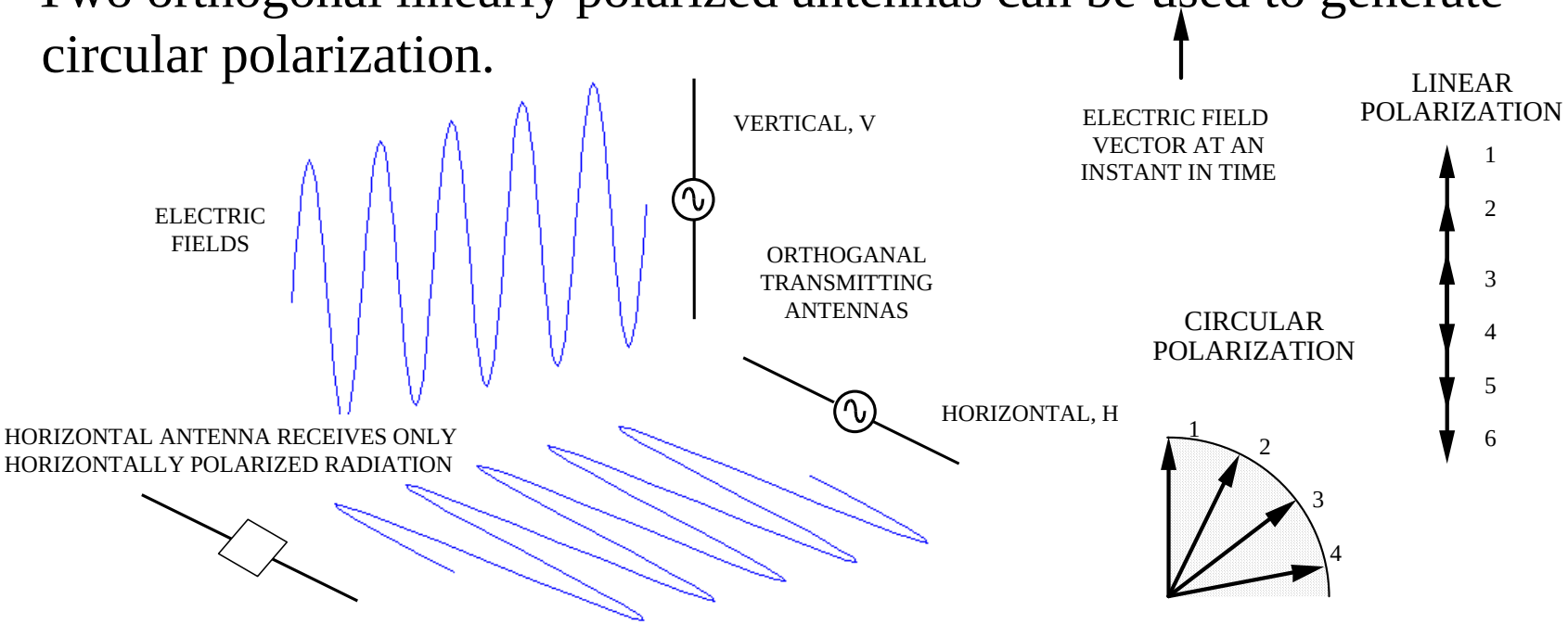
Superposition of Waves

- If multiple signal sources of the same frequency are present, or multiple paths exist between a radar and target, then the total signal at a location is the sum (superposition principle).
- The result is interference: constructive interference occurs if the waves add; destructive interference occurs if the waves cancel.
- Example: ground bounce multi-path can be misinterpreted as multiple targets.



Wave Polarization

- Polarization refers to the shape of the curve traced by the tip of the electric field vector as a function of time at a point in space.
- Microwave systems are generally designed for linear or circular polarization.
- Two orthogonal linearly polarized antennas can be used to generate circular polarization.



Antenna Parameters

- Gain is the radiation intensity relative to a lossless isotropic reference.
- Fundamental equation for gain:

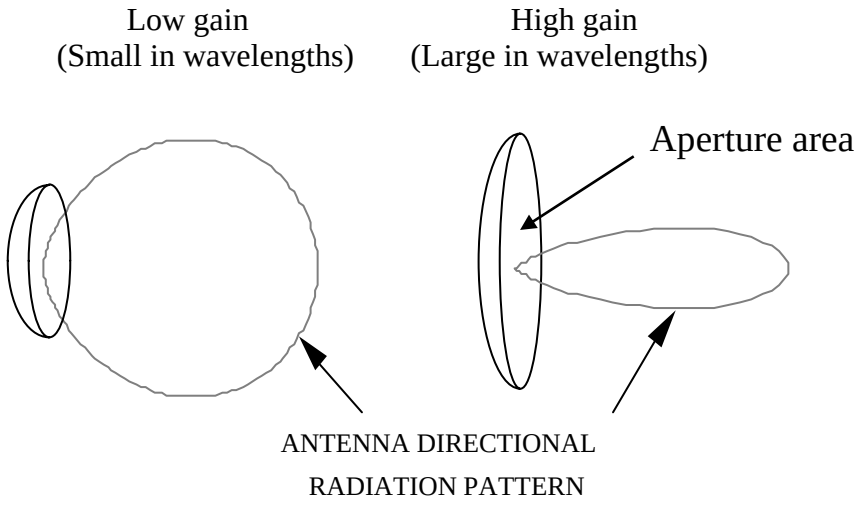
$$G = 4\pi A_e / \lambda^2$$

$A_e = A\varepsilon$, effective area

A = aperture area

ε = efficiency $(0 \le \varepsilon \le 1)$

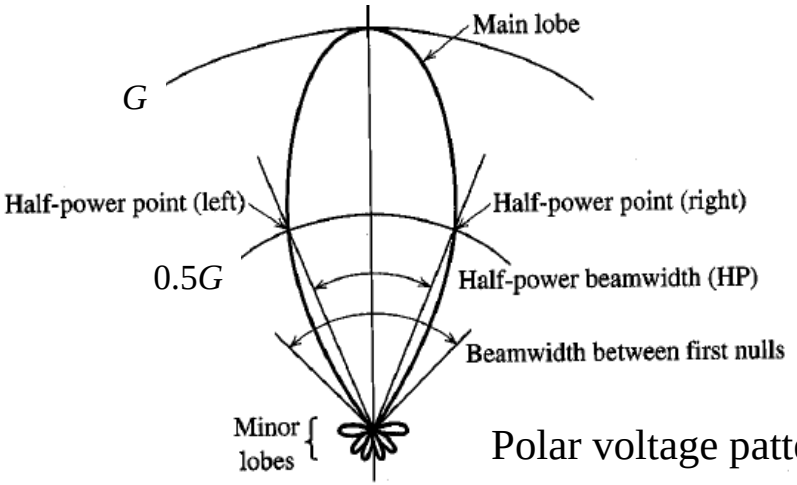
$\lambda = c / f$, wavelength



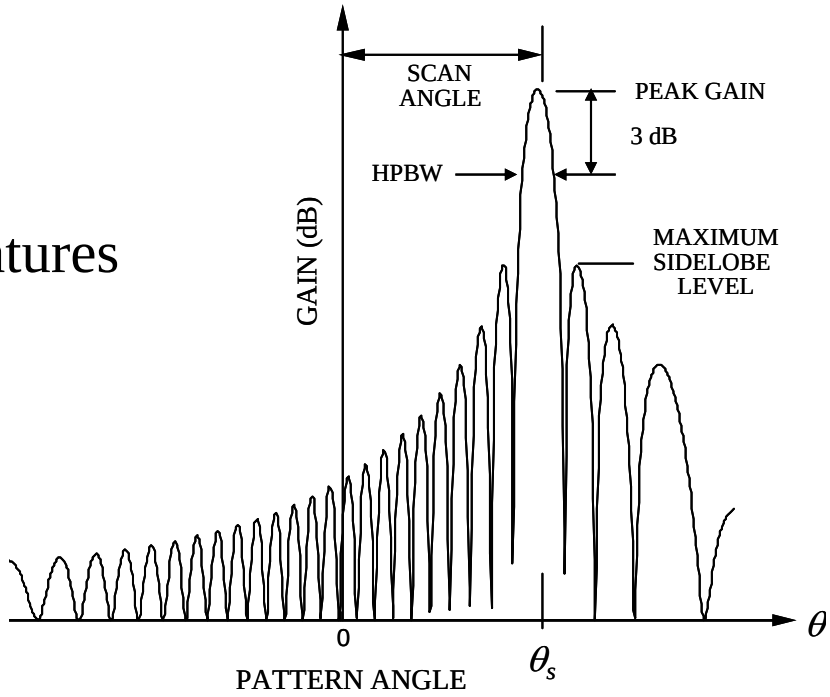
- In general, an increase in gain is accompanied by a decrease in beamwidth, and is achieved by increasing the antenna size relative to the wavelength.
- With regard to radar, high gain and narrow beams are desirable for long detection and tracking ranges and accurate direction measurement.

Antenna Parameters

- Half power beamwidth, HPBW (θ_B)
- Polarization
- Sidelobe level
- Antenna noise temperature (T_A)
- Operating bandwidth
- Radar cross section and other signatures



Polar voltage pattern plot



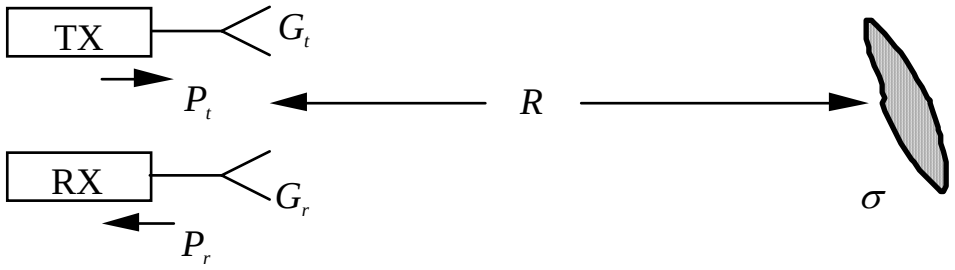
Rectangular dB pattern plot

Radar Antenna Tradeoffs

- Airborne applications:
  - > Size, weight, power consumption
  - > Power handling
  - > Location on platform and required field of view
  - > Many systems operating over a wide frequency spectrum
  - > Isolation and interference
  - > Reliability and maintainability
  - > Radomes (antenna enclosures or covers)
- Accommodate as many systems as possible to avoid operational restrictions (multi-mission, multi-band, etc.)
- Signatures must be controlled: radar cross section (RCS), infrared (IR), acoustic, and visible (camouflage)
- New antenna architectures and technologies
  - > Conformal, integrated
  - > Digital “smart” antennas with multiple beams
  - > Broadband

Radar Range Equation

- Quasi-monostatic



P_t = transmit power (W)

P_r = received power (W)

G_t = transmit antenna gain

G_r = receive antenna gain

σ = radar cross section (RCS, m^2)

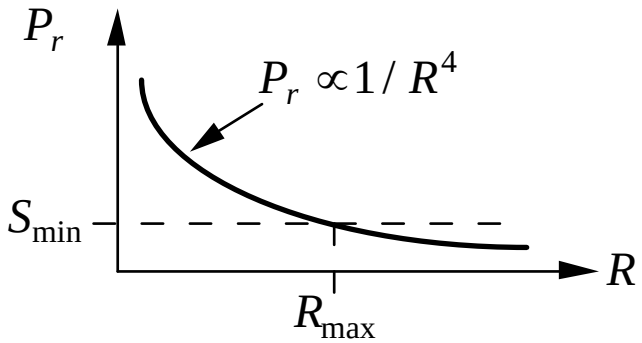
A_{er} = effective aperture area of receive antenna

$$P_r = \frac{P_t G_t \sigma A_{er}}{(4\pi R^2)^2} = \frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 R^4}$$

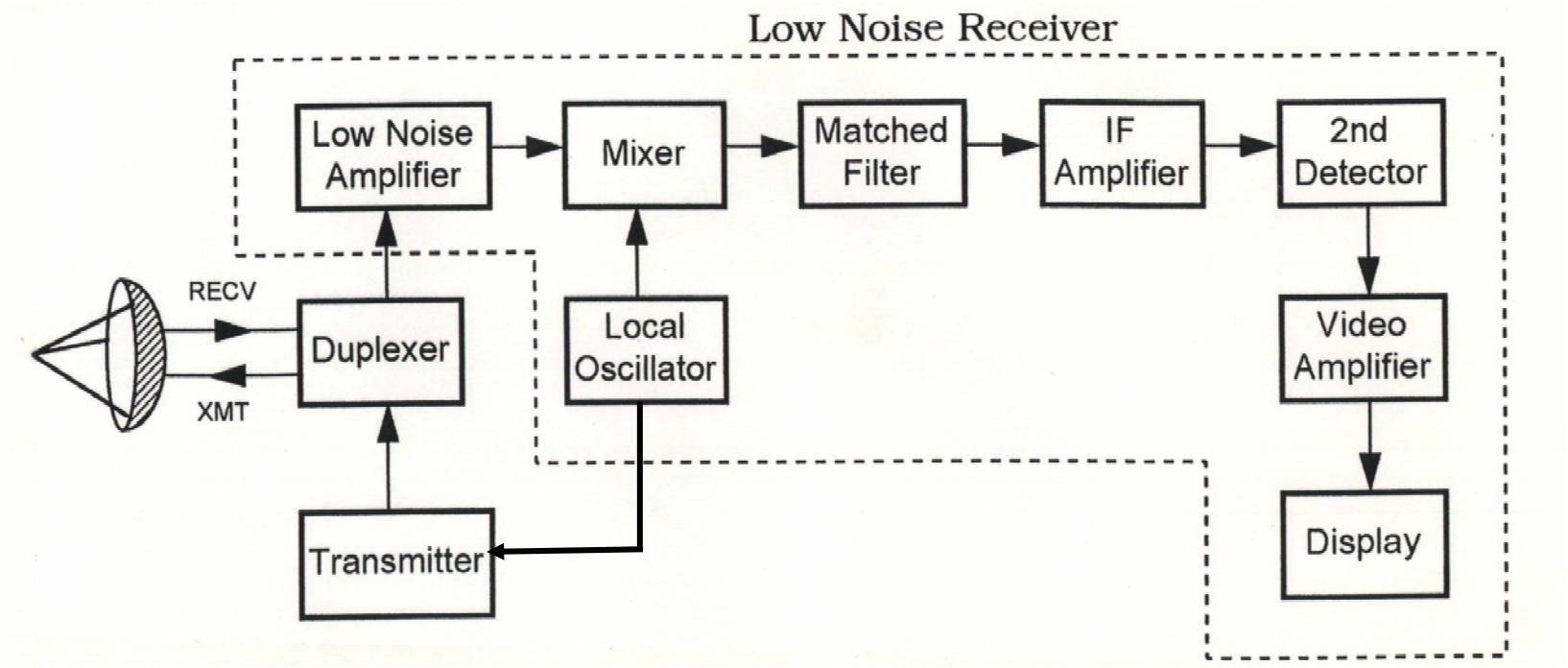
Minimum Detection Range

- The minimum received power that the radar receiver can "sense" is referred to a the minimum detectable signal (MDS) and is denoted $S_{\min}$.
- Given the MDS, the maximum detection range can be obtained:

$$P_r = S_{\min} = \frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 R^4} \Rightarrow R_{\max} = \left(\frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 S_{\min}} \right)^{1/4}$$



Radar Block Diagram



- This receiver is a superheterodyne receiver because of the intermediate frequency (IF) amplifier. (Similar to Figure 1.4 in Skolnik.)
- Coherent radar uses the same local oscillator reference for transmit and receive.

Coordinate Systems

- Radar coordinate systems

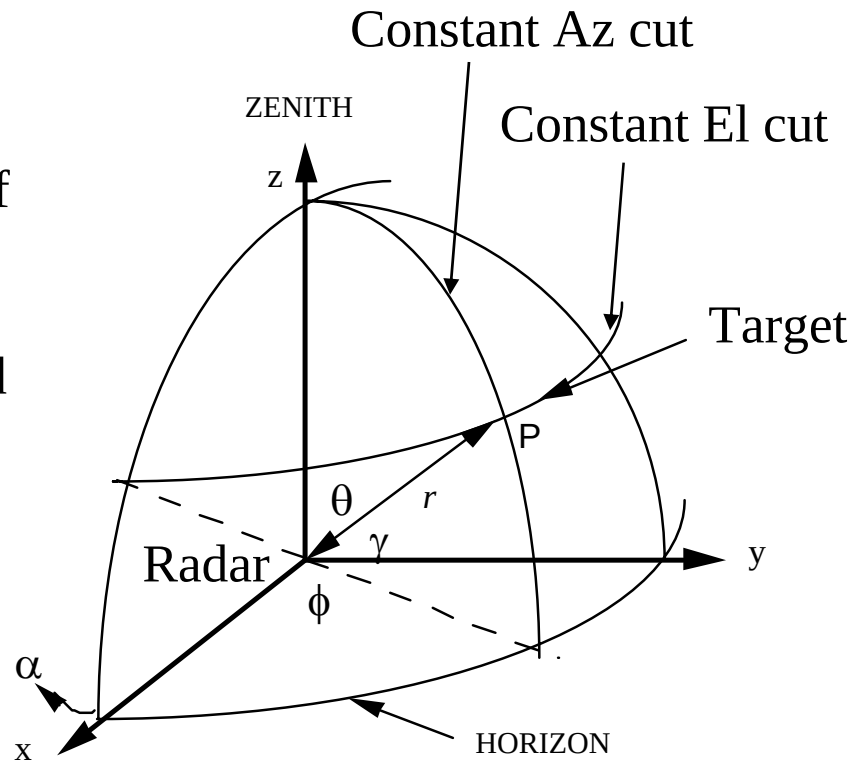
  spherical polar: (r,θ,ϕ)

  azimuth/elevation: (Az,El)

  or (α,γ)
- The radar is located at the origin of the coordinate system; the Earth's surface lies in the *x*-*y* plane.
- Azimuth (α) is generally measured clockwise from a reference (like a compass) but the spherical system azimuth angle (ϕ) is measured counterclockwise from the *x* axis. Therefore

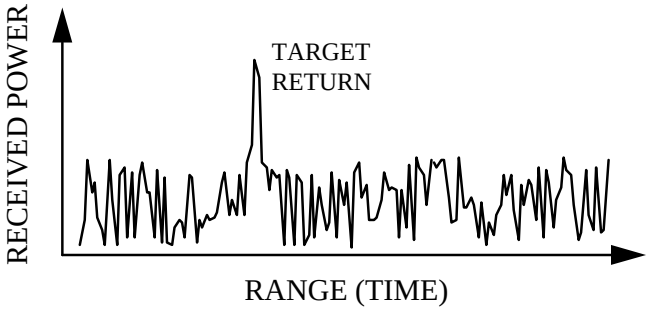
$$\gamma = 90 - \theta$$

$$\alpha = 360 - \phi$$

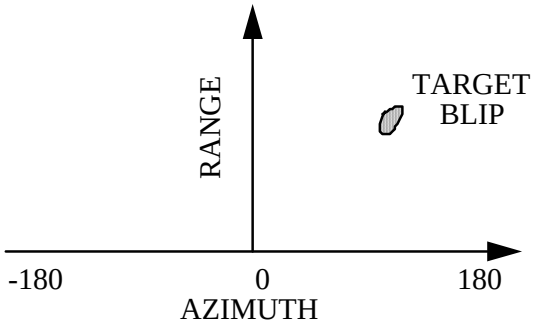


Radar Display Types

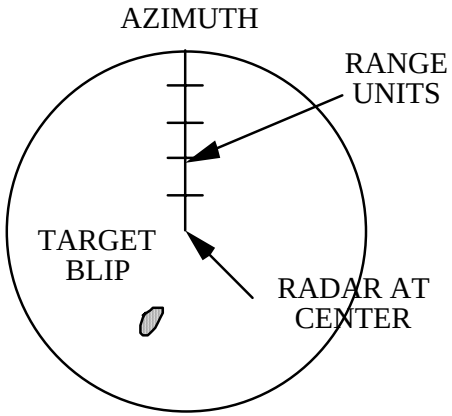
"A" DISPLAY



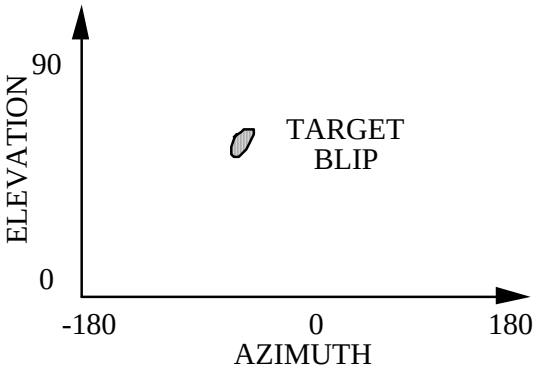
"B" DISPLAY



PLAN POSITION
INDICATOR (PPI)



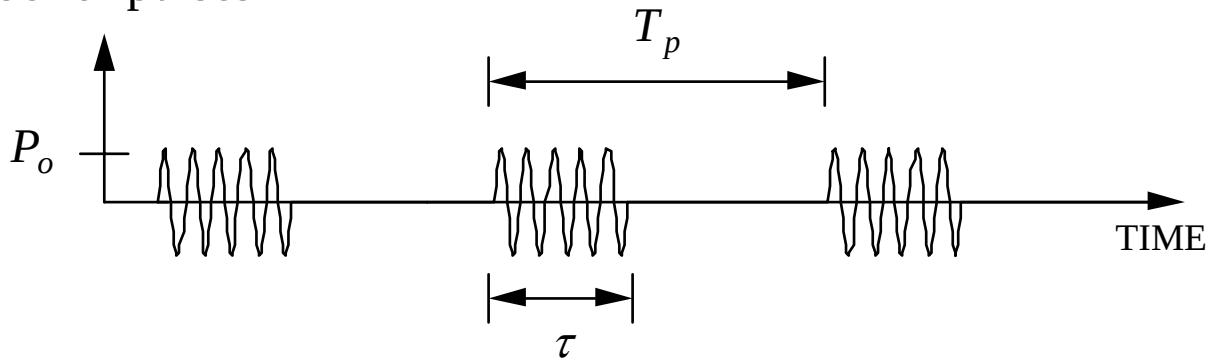
"C" DISPLAY



Pulsed Waveform

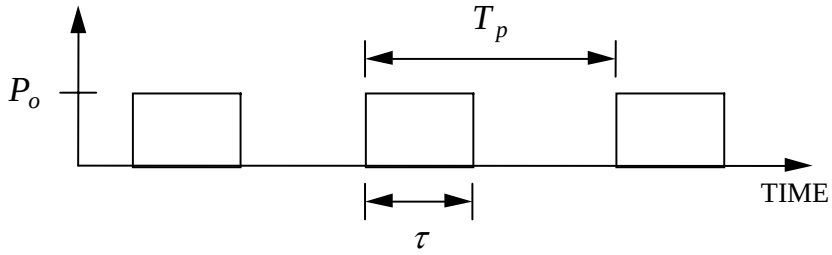
- In practice multiple pulses are transmitted to:
    1. cover search patterns
    2. track moving targets
    3. integrate (sum) several target returns to improve detection
- The pulse train is a common waveform

P_o = peak instantaneous power (W)
τ = pulse width (sec)
$f_p = 1/T_p$, pulse repetition frequency (PRF, Hz)
T_p = interpulse period (sec)
N = number of pulses

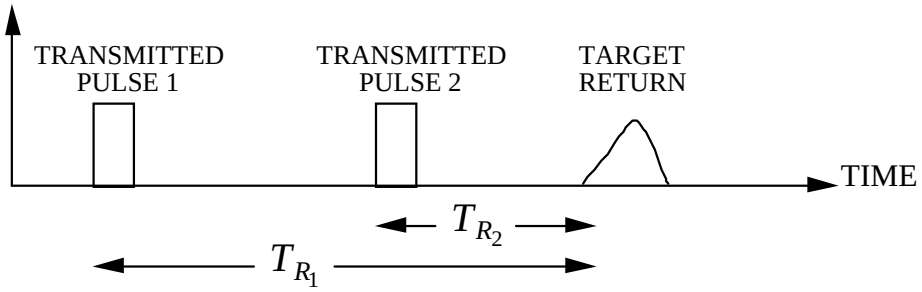


Range Ambiguities

- For convenience we omit the sinusoidal carrier when drawing the pulse train



- When multiple pulses are transmitted there is the possibility of a range ambiguity.

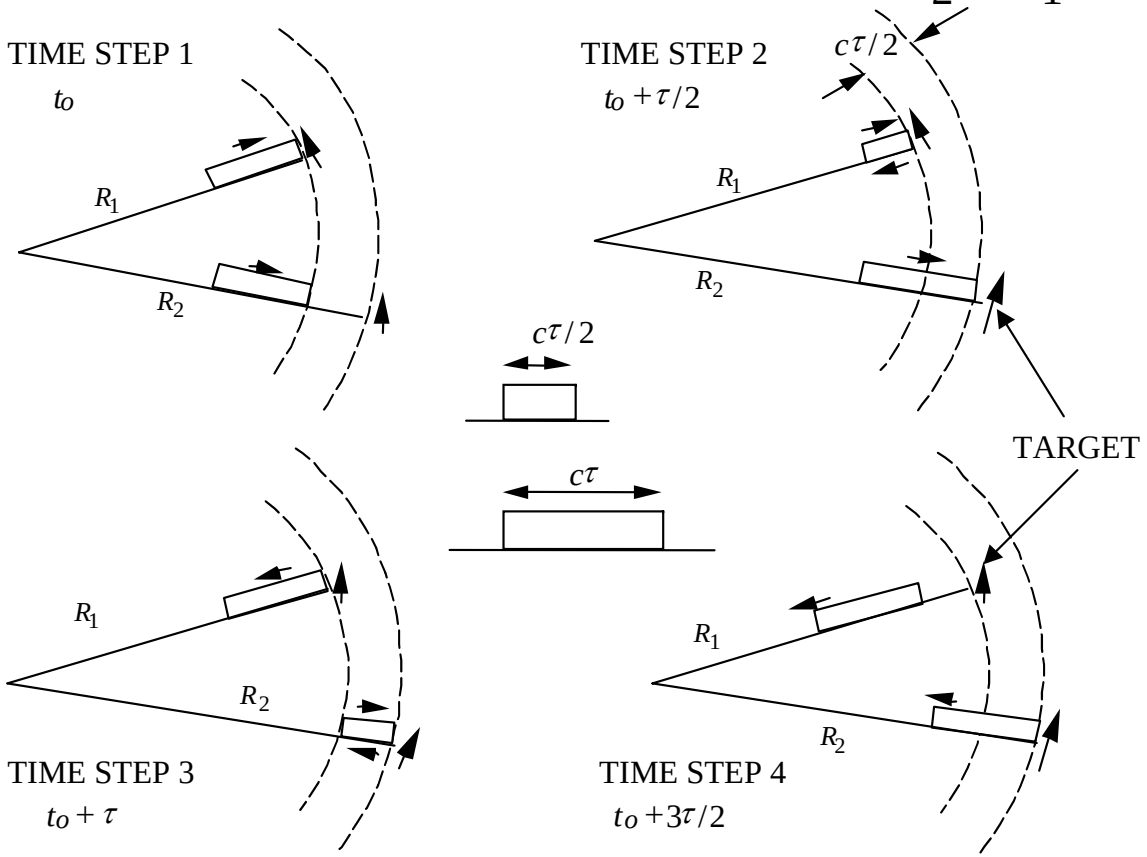


- To determine the range unambiguously requires that $T_p \geq \frac{2R}{c}$. The unambiguous range is

$$R_u = \frac{cT_p}{2} = \frac{c}{2f_p}$$

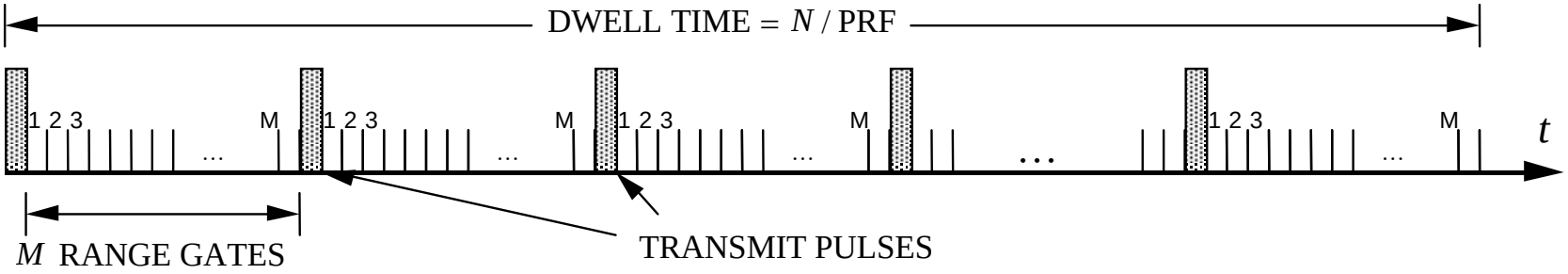
Range Resolution

- Two targets are resolved if their returns do not overlap. The range resolution corresponding to a pulse width τ is $\Delta R = R_2 - R_1 = c\tau/2$.

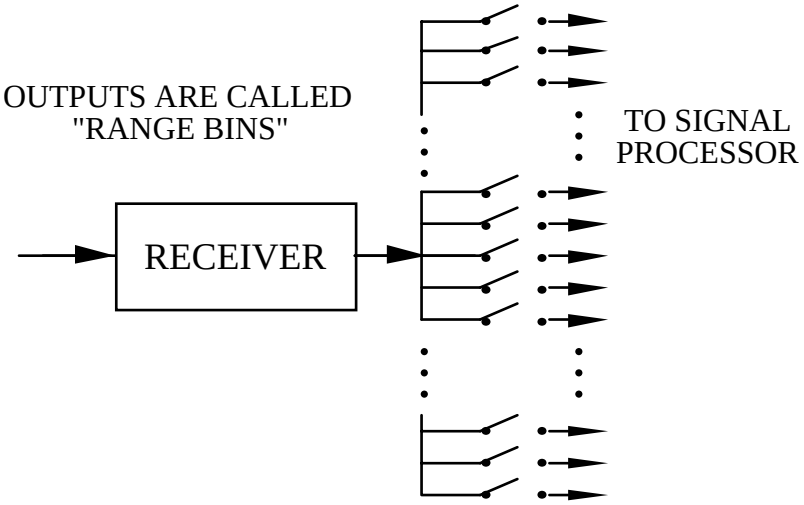


Range Gates

- Typical pulse train and range gates

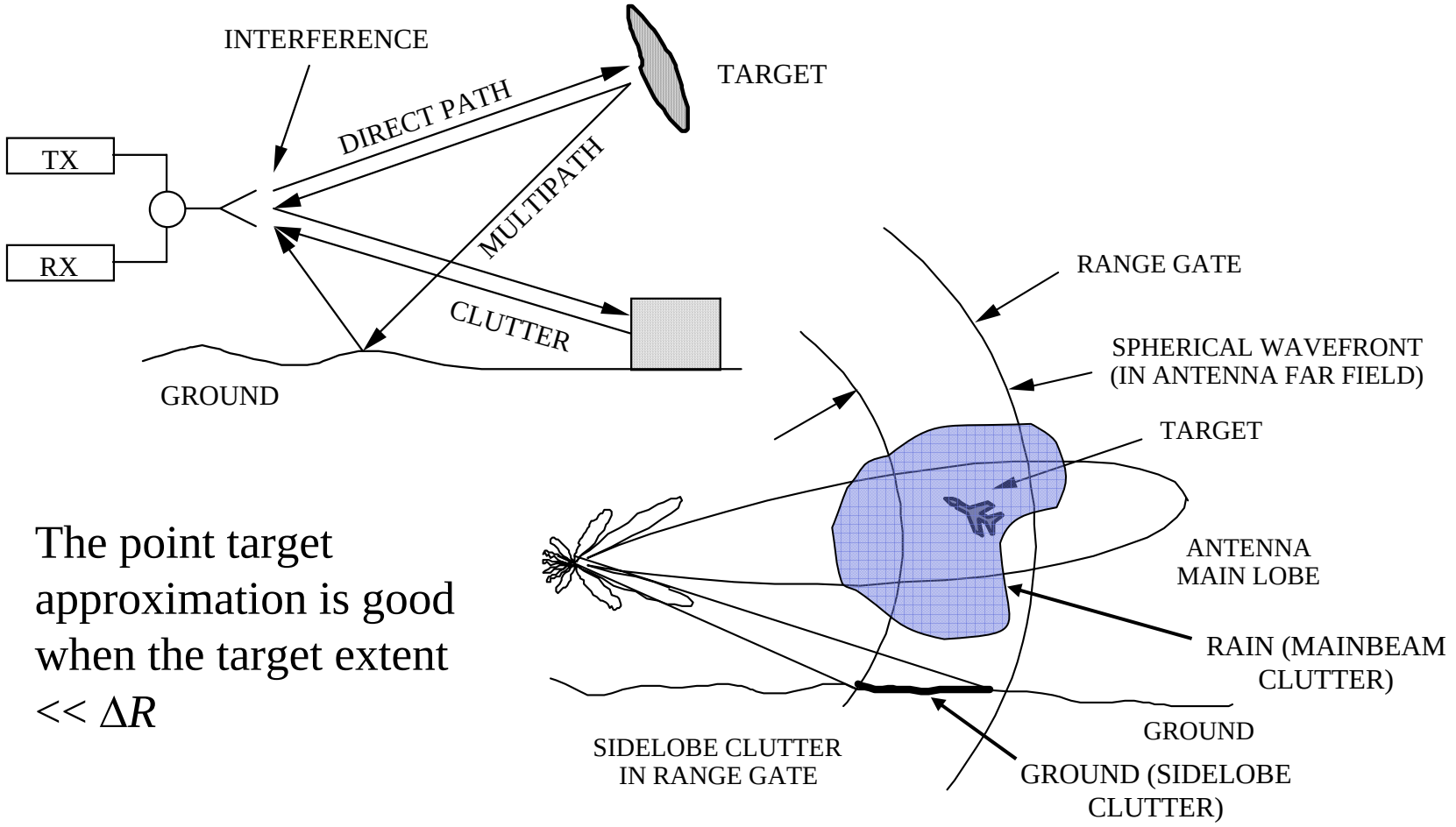


- Analog implementation of range gates



- Gates are opened and closed sequentially
- The time each gate is closed corresponds to a range increment
- Gates must cover the entire interpulse period or the ranges of interest
- For tracking a target a single gate can remain closed until the target leaves the bin

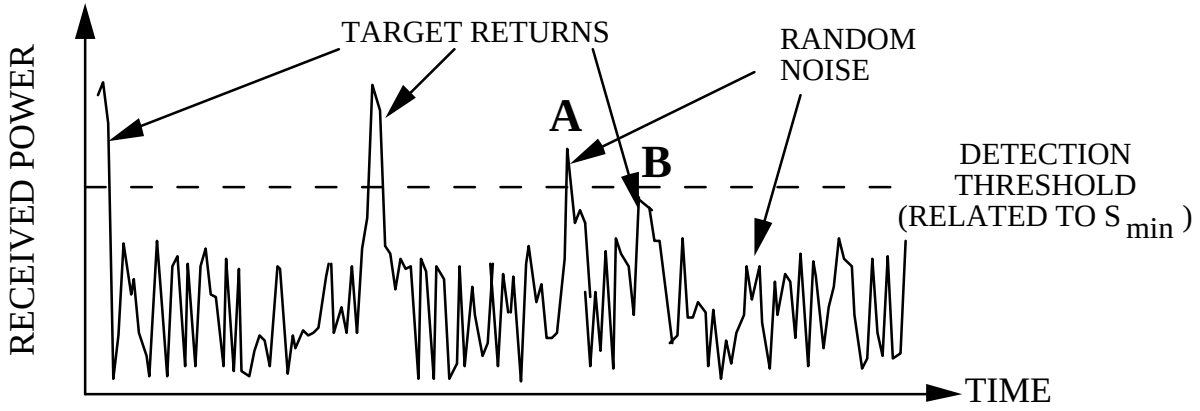
Clutter and Interference



The point target approximation is good when the target extent $<< \Delta R$

Thermal Noise

- In practice the received signal is "corrupted" (distorted from the ideal shape and amplitude) by thermal noise, interference and clutter.
- Typical return trace appears as follows:



- Threshold detection is commonly used. If the return is greater than the detection threshold a target is declared. **A** is a false alarm: the noise is greater than the threshold level but there is no target. **B** is a miss: a target is present but the return is not detected.

Thermal Noise Power

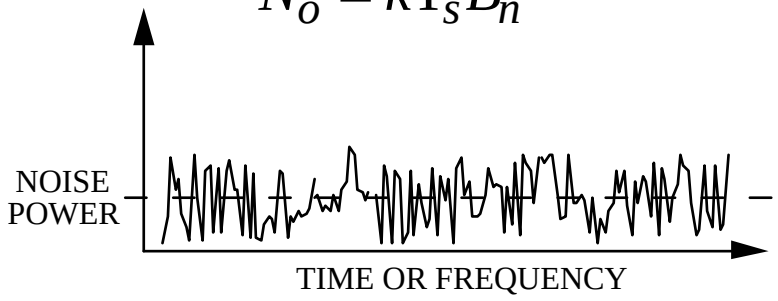
- Consider a receiver at the standard temperature, T_o degrees Kelvin (K). Over a range of frequencies of bandwidth B_n (Hz) the available noise power is

$$N_o = kT_oB_n$$

  where $k_B = 1.38\times10^{-23}$(Joules/K) is Boltzman's constant.

- Other radar components will also contribute noise (antenna, mixer, cables, etc.). We define a system noise temperature T_s, in which case the available noise power is

$$N_o = kT_sB_n$$



Signal-to-Noise Ratio (SNR)

- Considering the presence of noise, the important parameter for detection is the signal-to-noise ratio (SNR)

$$\text{SNR} = \frac{P_r}{N_o} = \frac{P_t G_t G_r \sigma \lambda^2 G_p L}{(4\pi)^3 R^4 k_B \text{T}_s B_n}$$

- Factors have been added for processing gain G_p and loss L
- Most radars are designed so that $B_n \approx 1/\tau$
- At this point we will consider only two noise sources:

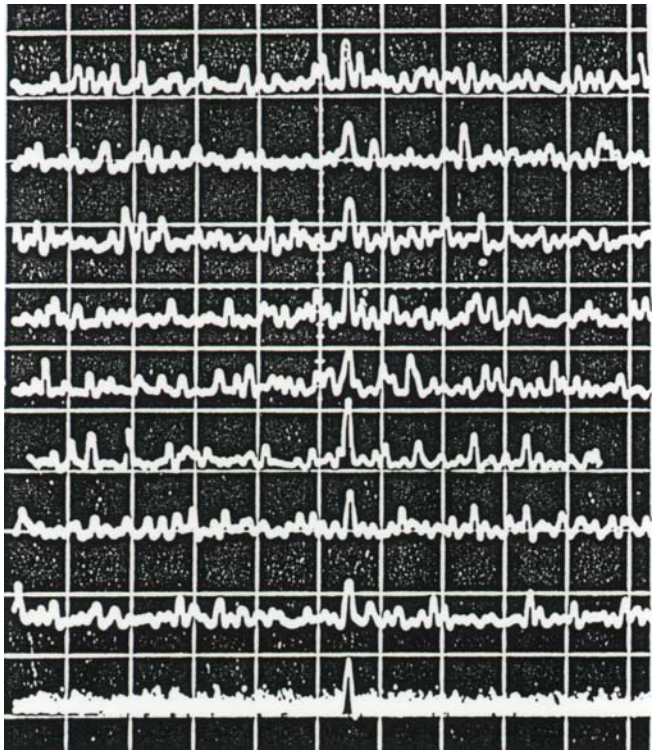
  1. background noise collected by the antenna (T_A)

  2. total effect of all other system components (T_o, system effective noise temperature)

$$\text{T}_s = \text{T}_\text{A} + \text{T}_e$$

Integration of Pulses

- Noncoherent integration (postdetection integration): performed after the envelope detector. The magnitudes of the returns from all pulses are added. SNR increases approximately as $\sqrt{N}$.
- Coherent integration (predetection integration): performed before the envelope detector (phase information must be available). Coherent pulses must be transmitted. The SNR increases as N.
- The last trace shows a noncoherent integrated signal.
- Integration improvement an example of processing gain.



From Byron Edde, *Radar: Principles, Technology, Applications*, Prentice-Hall

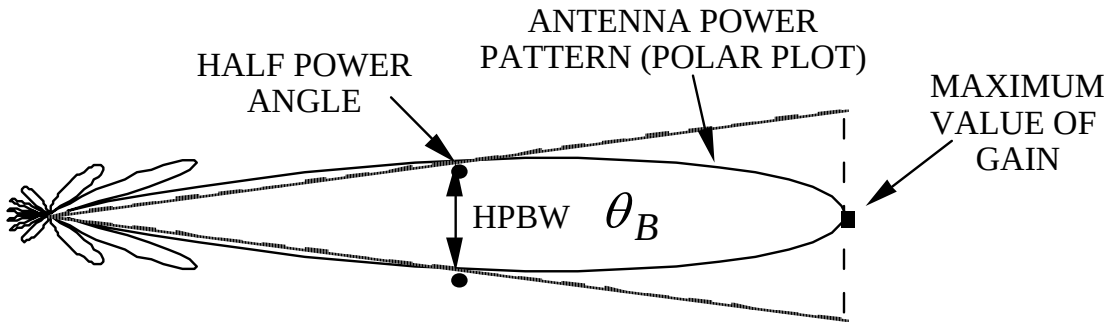
Dwell Time

- Simple antenna model: constant gain inside the half power beamwidth (HPBW), zero outside. If the aperture has a diameter D with uniform illumination $\theta_B \approx \lambda / D$.
- The time that the target is in the beam (dwell time, look time, or time on target) is t_{ot}

$$t_{\text{ot}} = \theta_B / \dot{\theta}_s$$

- The beam scan rate is ω_s in revolutions per minute or $\frac{d\theta_s}{dt} = \dot{\theta}_s$ in degrees per second.
- The number of pulses that will hit the target in this time is

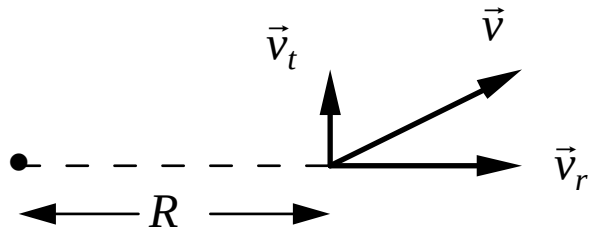
$$n_B = t_{\text{ot}} f_p$$

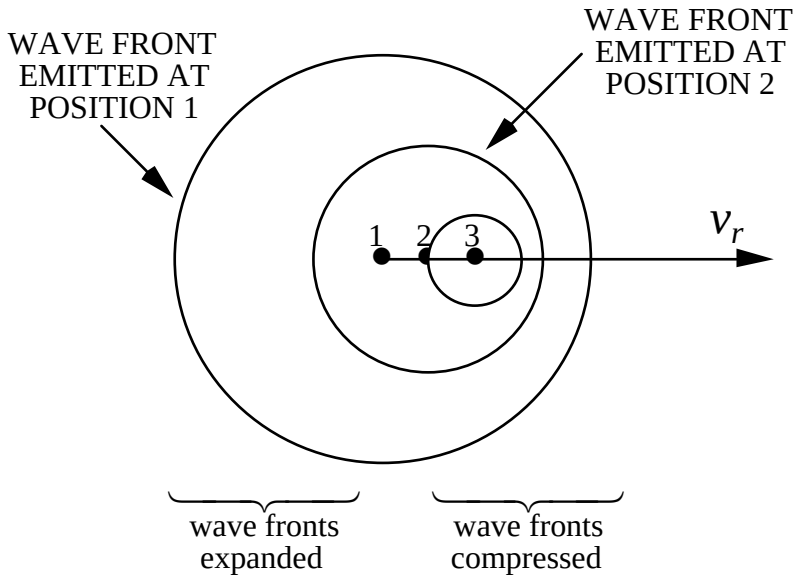


Doppler Shift

- Targets in motion relative to the radar cause the return signal frequency to be shifted.
- A Doppler shift only occurs when the relative velocity vector has a radial component. In general there will be both radial and tangential components to the velocity

$$f_d = -2v_r / \lambda$$



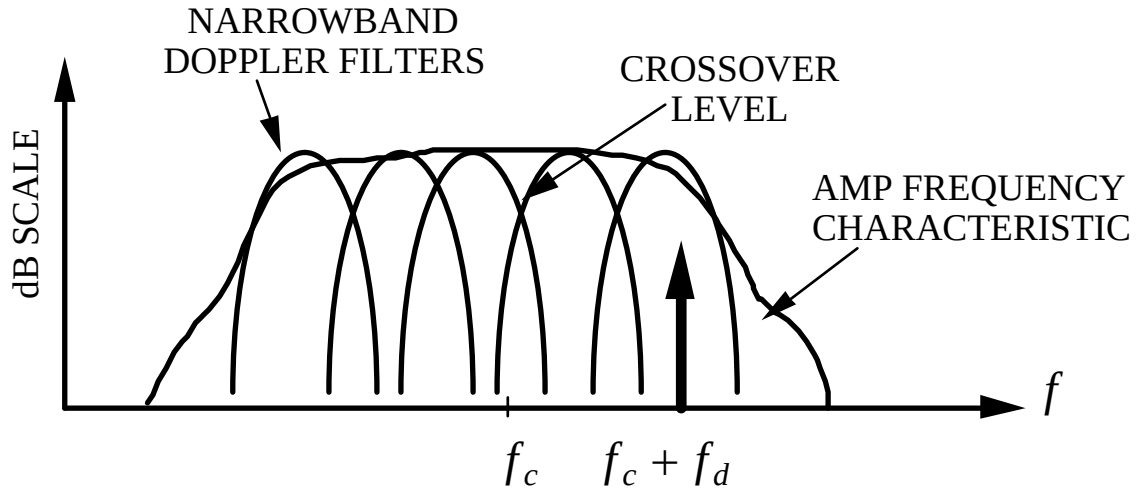


R decreasing $\Rightarrow \dfrac{dR}{dt} < 0 \Rightarrow f_d > 0$ (closing target)

R increasing $\Rightarrow \dfrac{dR}{dt} > 0 \Rightarrow f_d < 0$ (receeding target)

Doppler Filter Banks

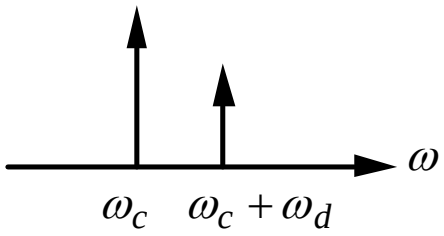
- The radar’s operating band is divided into narrow sub-bands. Ideally there should be no overlap in sub-band frequency characteristics.
- The noise bandwidth of the Doppler filters is small compared to that of the radar’s total bandwidth, which improves the SNR.
- Velocity estimates can be made by monitoring the power out of each filter.
- If a signal is present in a filter, the target's velocity range is known.



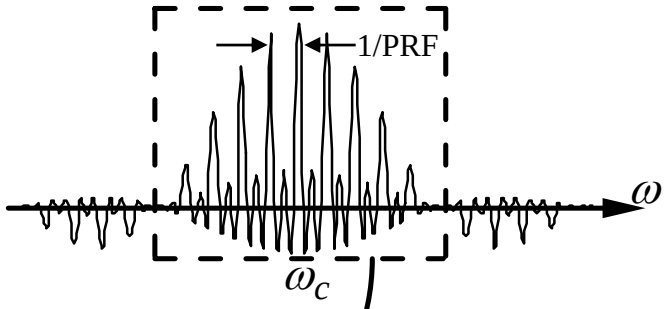
Velocity Ambiguities

- The spectrum is the Fourier transform of the pulse train waveform.

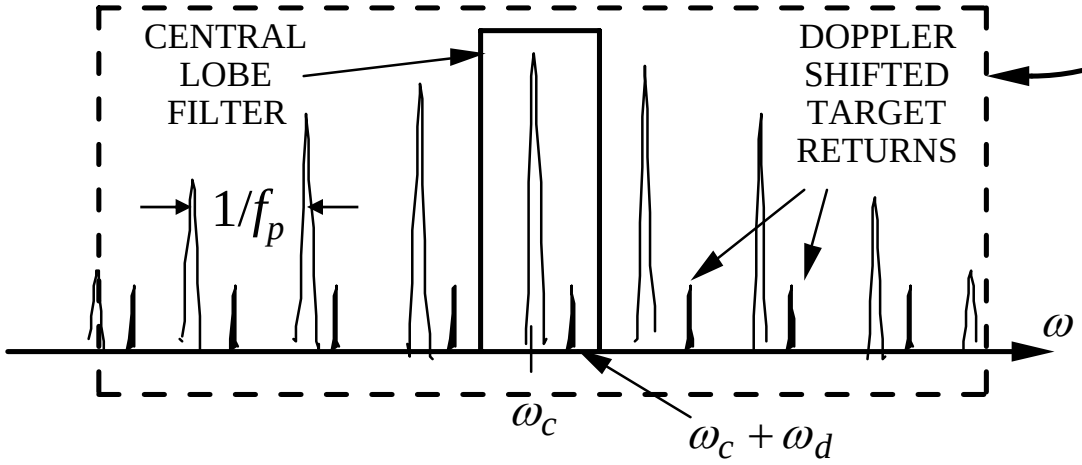
Spectrum of doppler shifted CW signal



Coherent pulse train spectrum (fixed target -- no doppler)



Expanded central lobe region with target doppler shift

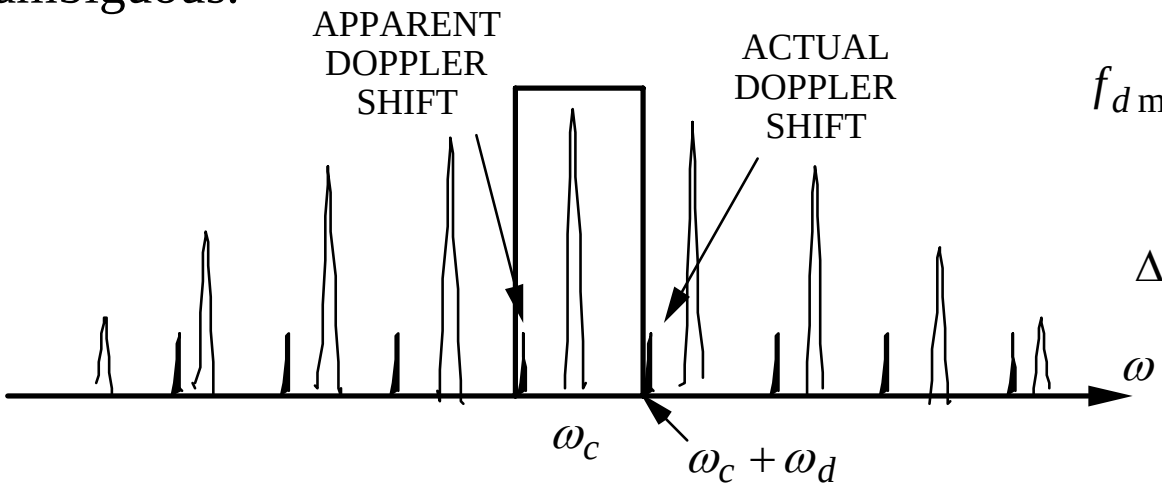


$$f_d|_{\text{observed}} = \frac{2v_r}{\lambda} \bmod(\text{PRF})$$

$$f_d = n\,\text{PRF} + f_d|_{\text{apparent}}$$

Low, High, Medium PRF

- If f_d is increased the true target Doppler shifted return moves out of the passband and a lower sideband lobe enters. Thus the Doppler measurement is ambiguous.



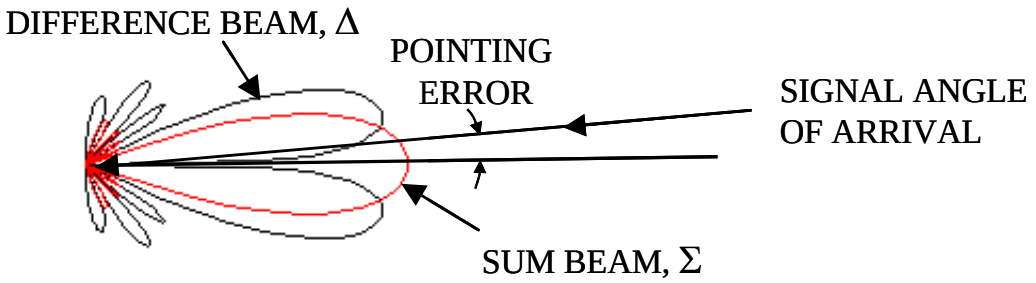
$$f_{d\max} = \pm f_p / 2$$
$$v_u = \lambda f_{d\max} / 2$$
$$= \pm \lambda f_p / 4$$
$$\Delta v_u = \lambda f_p / 2$$

- PRF determines Doppler and range ambiguities:

PRF	RANGE	DOPPLER
High	Ambiguous	Unambiguous
Medium	Ambiguous	Ambiguous
Low	Unambiguous	Ambiguous

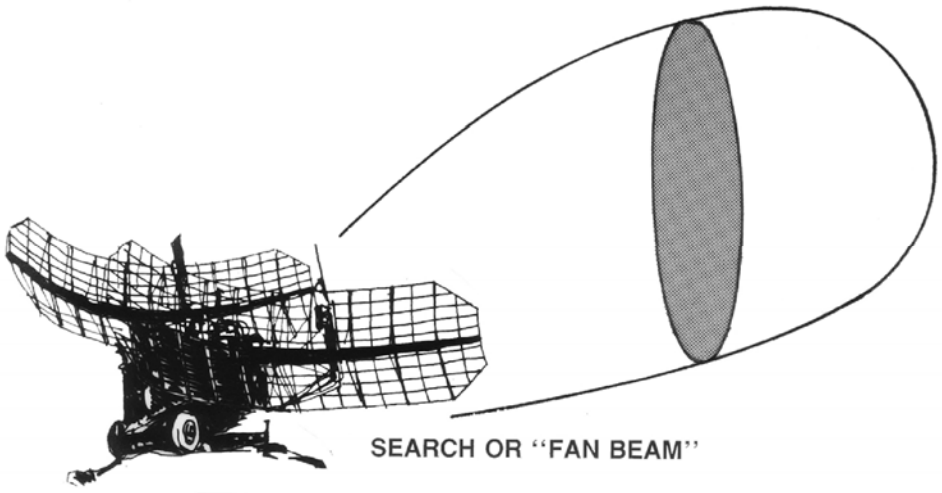
Track Versus Search

- Search radars
  - > Long, medium, short ranges (20 km to 2000 km)
  - > High power density on the target: high peak power, long pulses, long pulse trains, high antenna gain
  - > Low PRFs, large range bins
  - > Search options: rapid search rate with narrow beams or slower search rate with wide beams
- Tracking radar
  - > Accurate angle and range measurement required
  - > Minimize time on target for rapid processing
  - > Special tracking techniques: monopulse, conical scan, beam switching

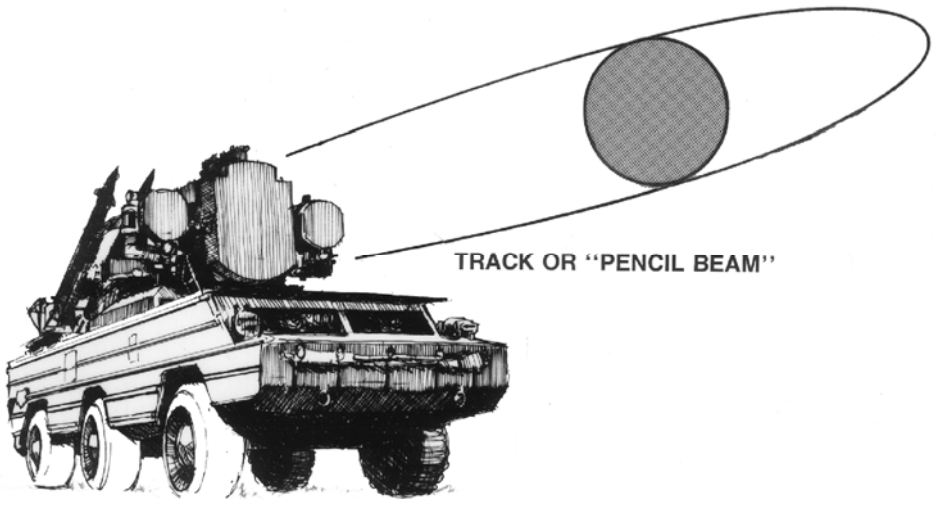


Monopulse Technique

Antenna Patterns



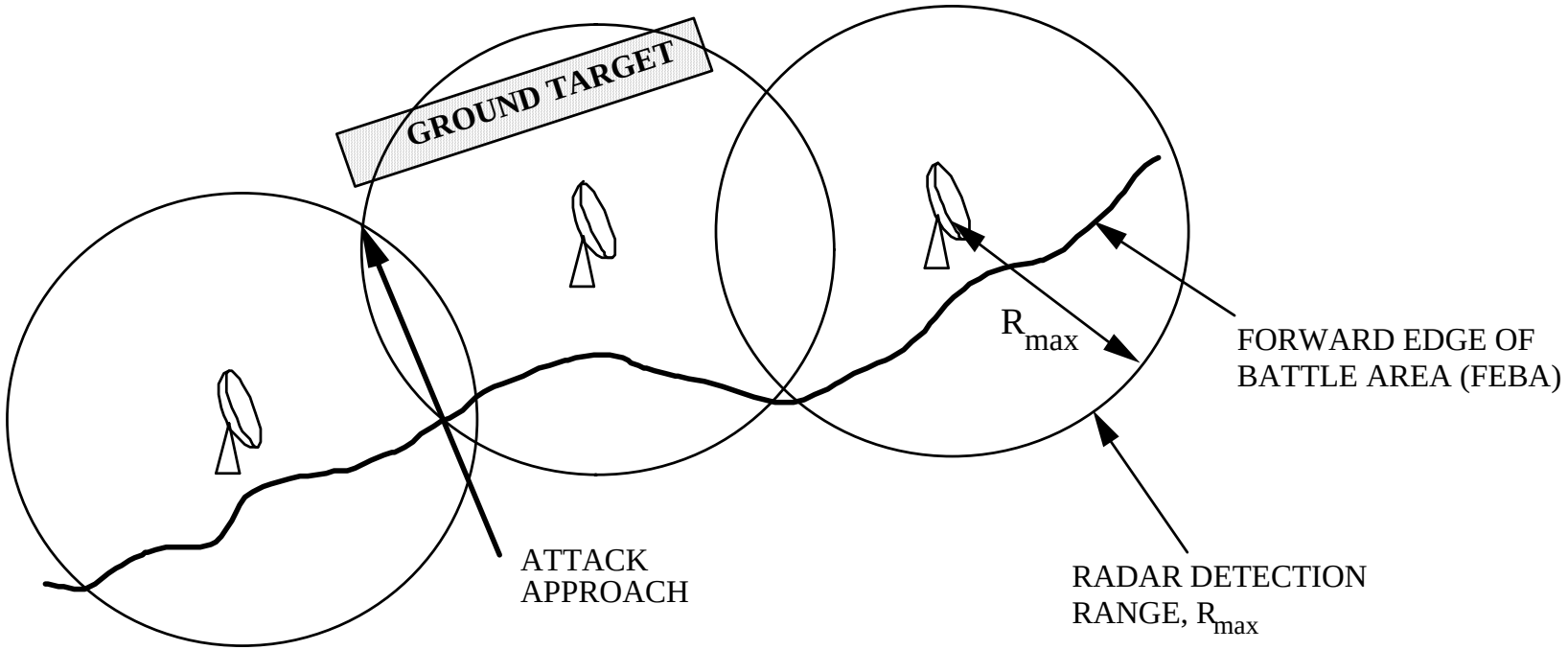
- Fan beam for 2-d search



- Pencil beam for tracking for 3-d search

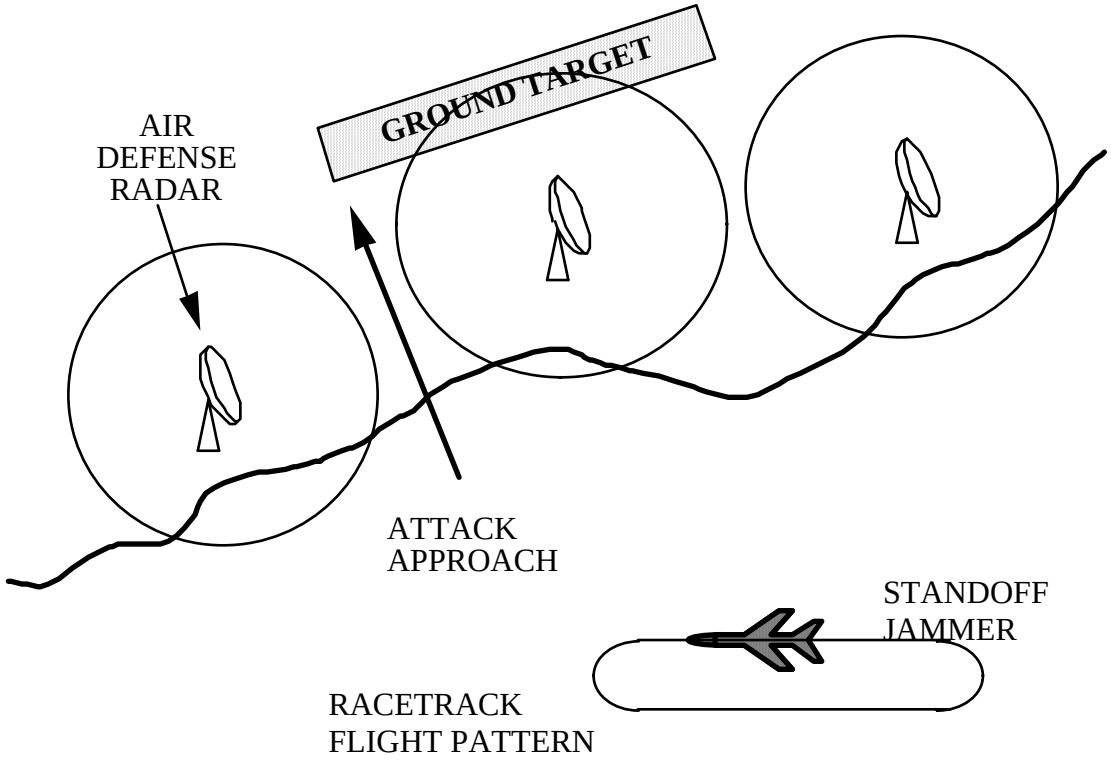
Attack Approach

- A network of radars are arranged to provide continuous coverage of a ground target.
- Conventional aircraft cannot penetrate the radar network without being detected.



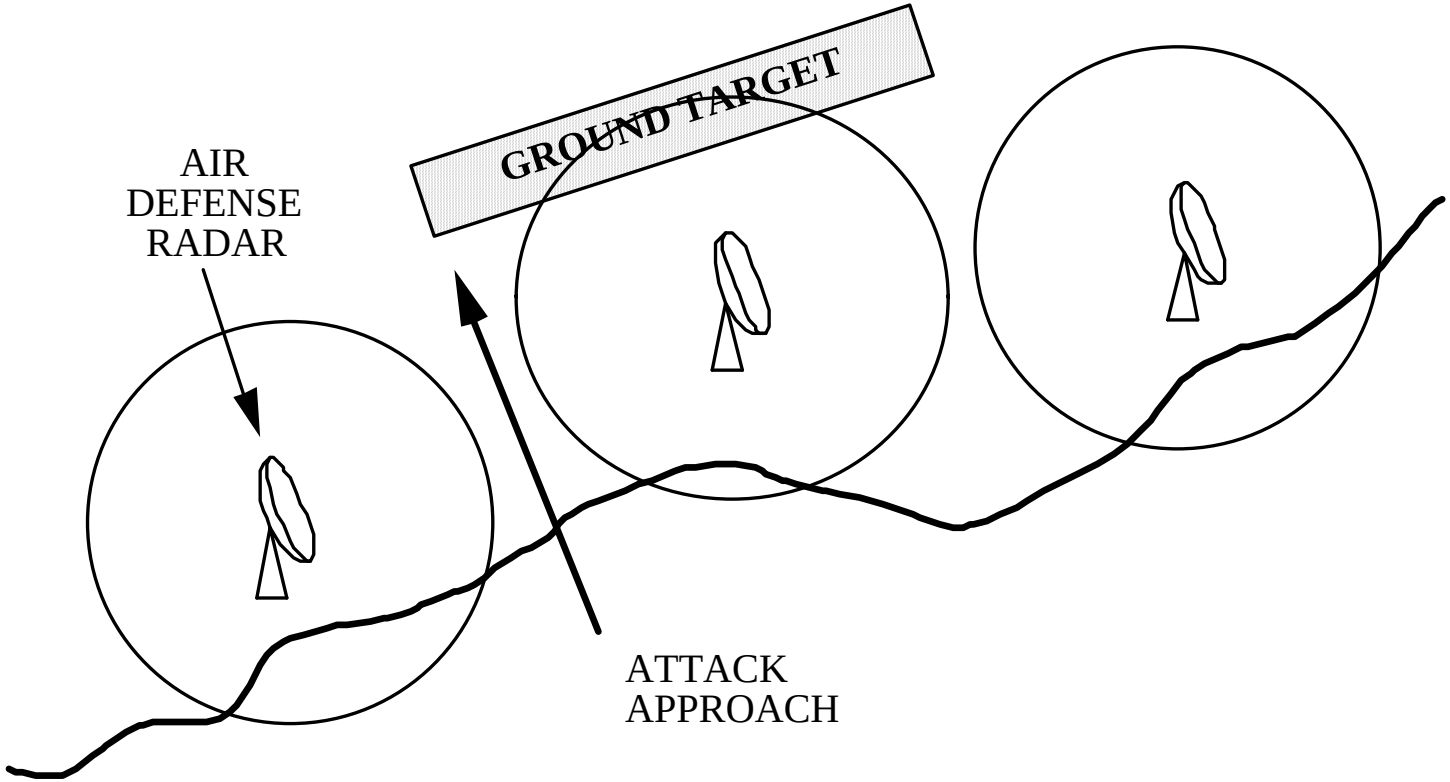
Radar Jamming

- The barrage jammer floods the radar with noise and therefore decreases the SNR.
- The radar knows it is being jammed.



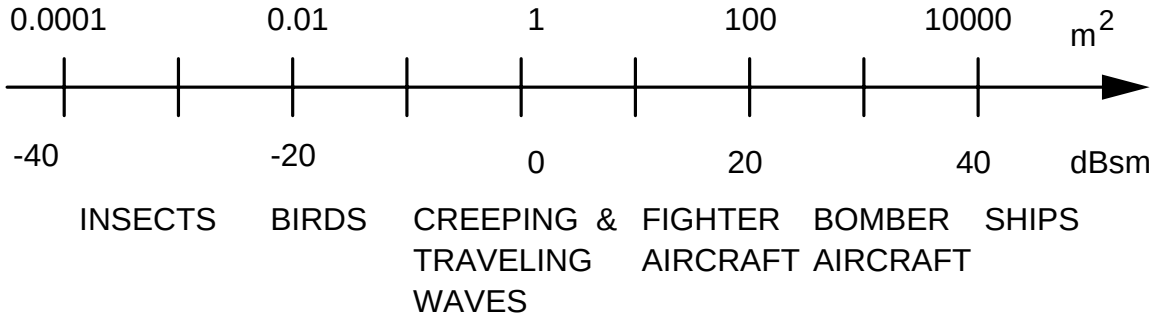
Low Observability

- Detection range depends on RCS, $R_{\max} \propto \sqrt[4]{\sigma}$, and therefore RCS reduction can be used to open holes in a radar network.
- There are cost and performance limitations to RCS reduction.



Radar Cross Section (RCS)

- Typical values:



- Fundamental equation for the RCS of a "electrically large" perfectly reflecting surface of area *A* when viewed directly by the radar

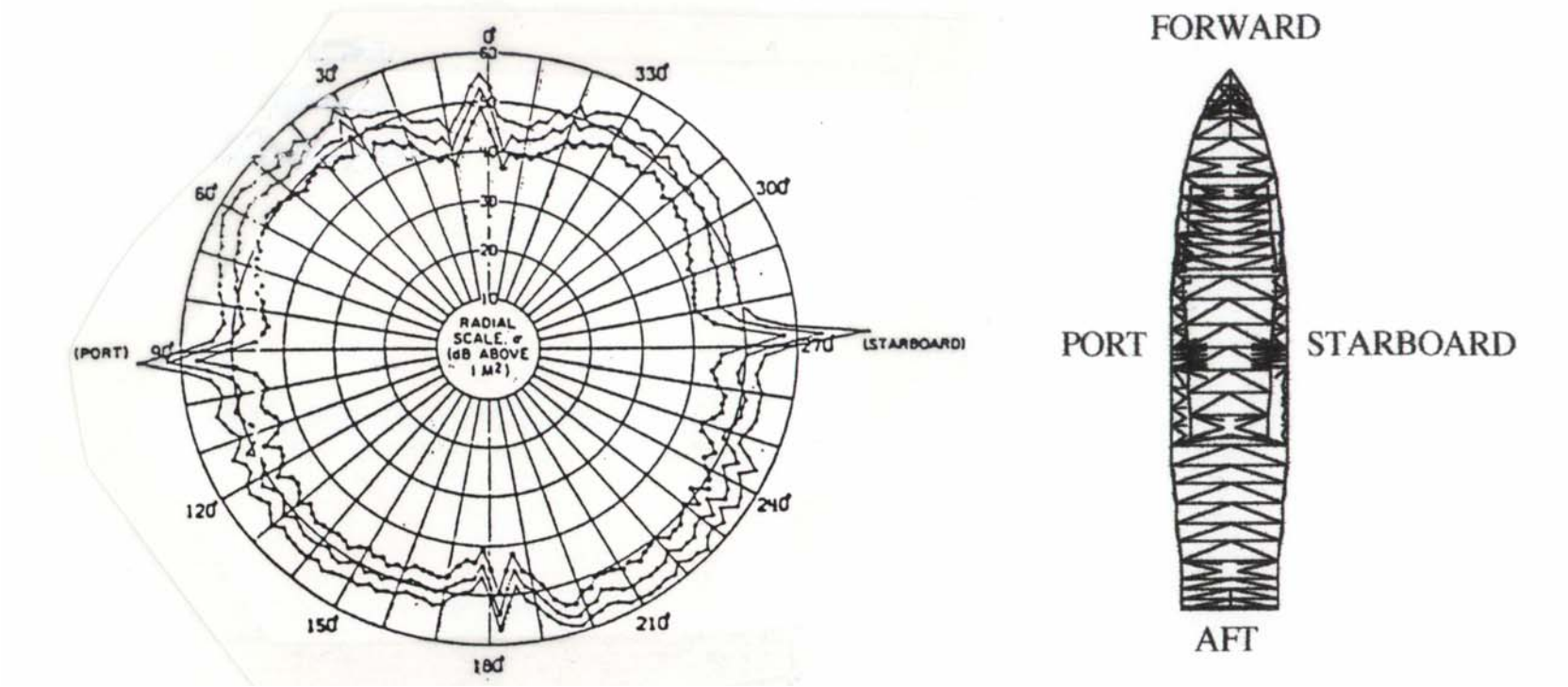
$$\sigma \approx \frac{4\pi A^2}{\lambda^2}$$

- Expressed in decibels relative to a square meter (dBsm):

$$\sigma_{\text{dBsm}} = 10\log_{10}(\sigma)$$

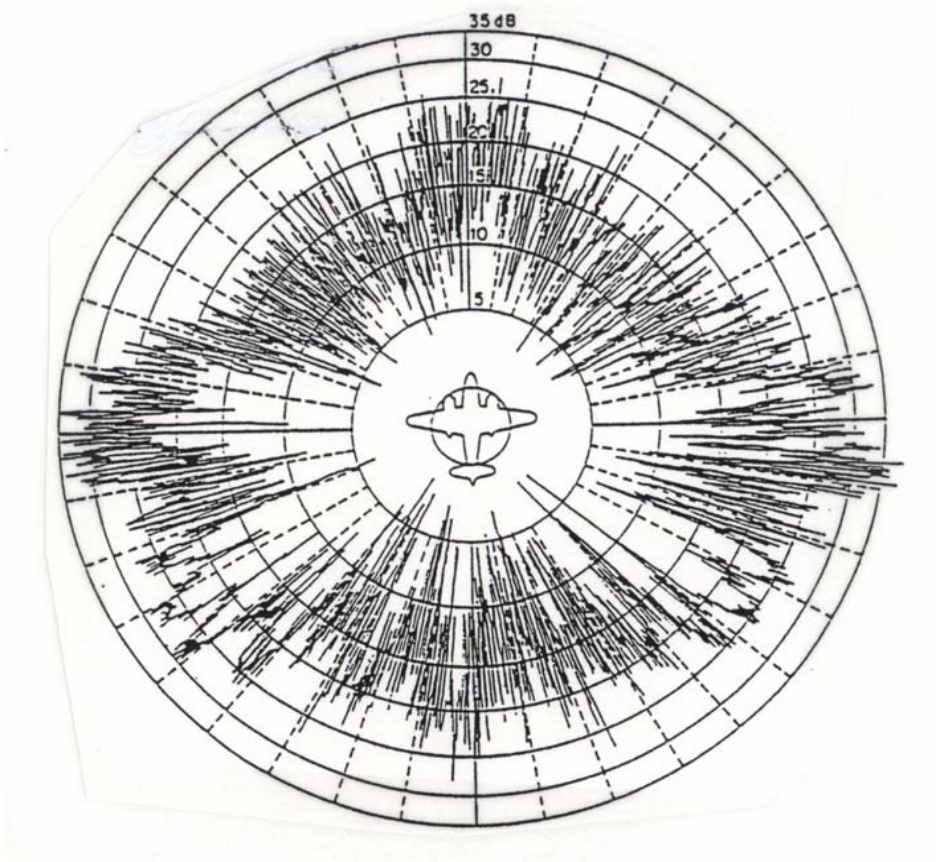
RCS Target Types

- A few dominant scatterers (e.g., hull) and many smaller independent scatterers
- S-Band (2800 MHz), horizontal polarization, maximum RCS = 70 dBsm



RCS Target Types

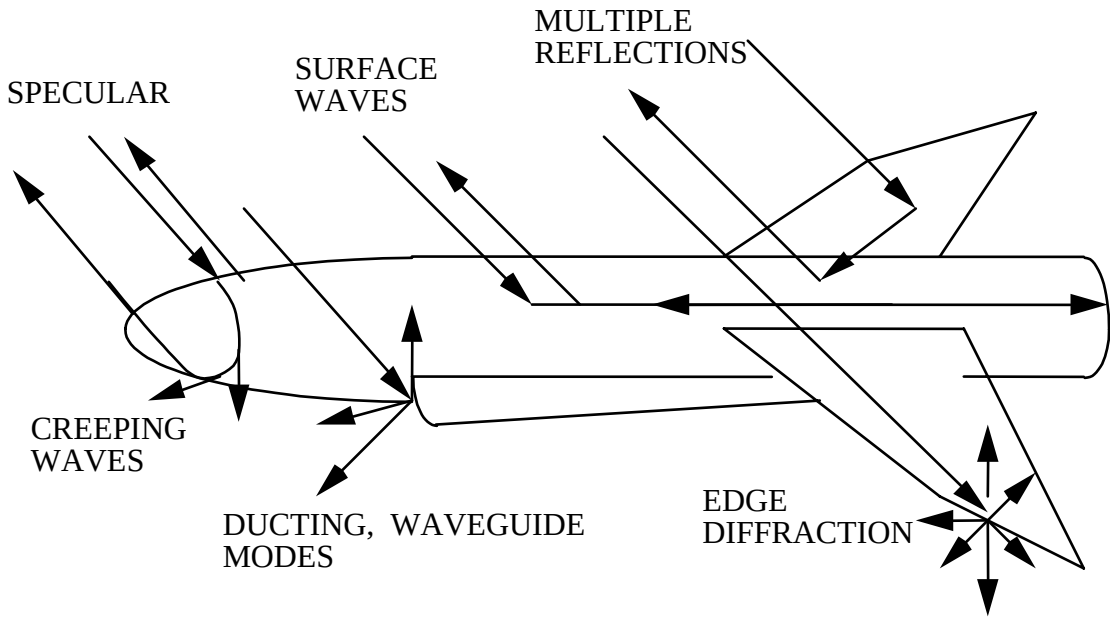
- Many independent random scatterers, none of which dominate (e.g., large aircraft)

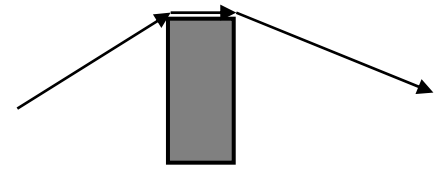


From Skolnik
- S-Band (3000 MHz)
- Horizontal Polarization
- Maximum RCS = 40 dBsm

Scattering Mechanisms

- Scattering mechanisms are used to describe wave behavior. Especially important at radar frequencies:
  specular = "mirror like" reflections that satisfy Snell's law
  surface waves = the body surface acts like a transmission line
  diffraction = scattered waves that originate at abrupt discontinuities



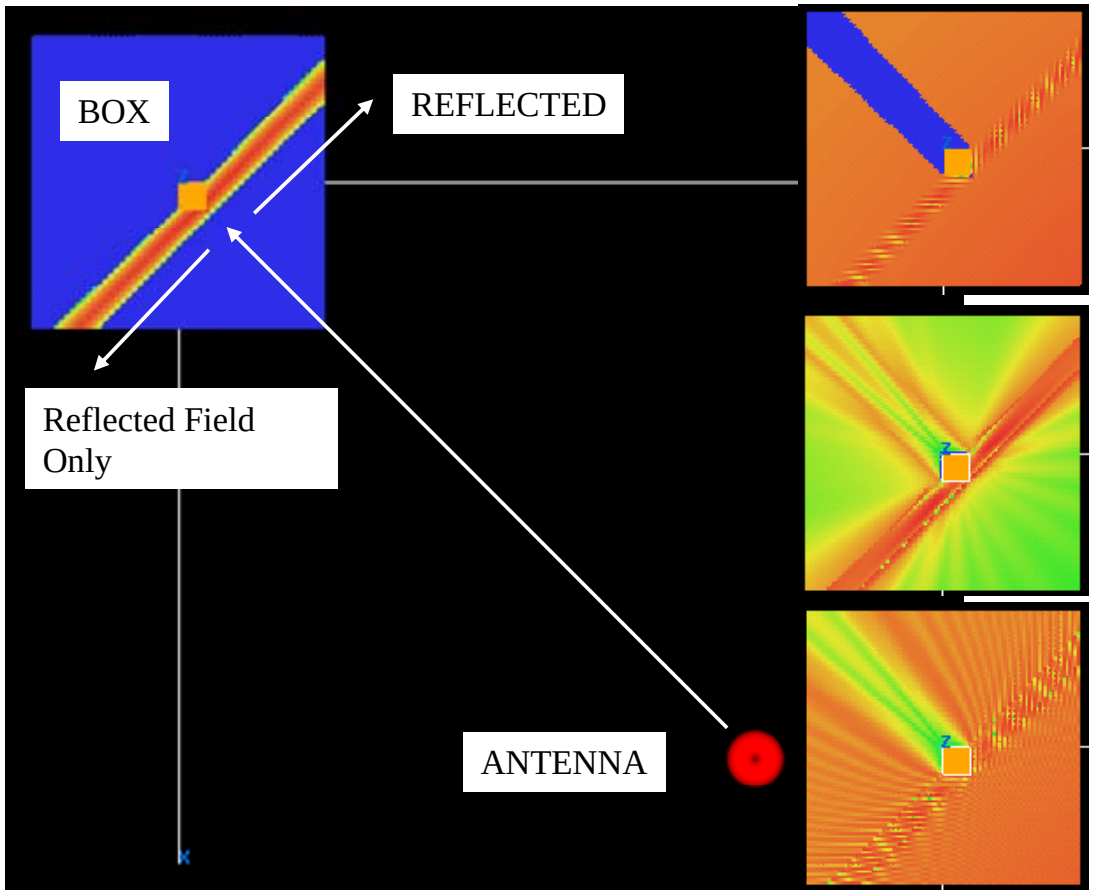


Double diffraction from sharp corners

Diffraction from rounded object

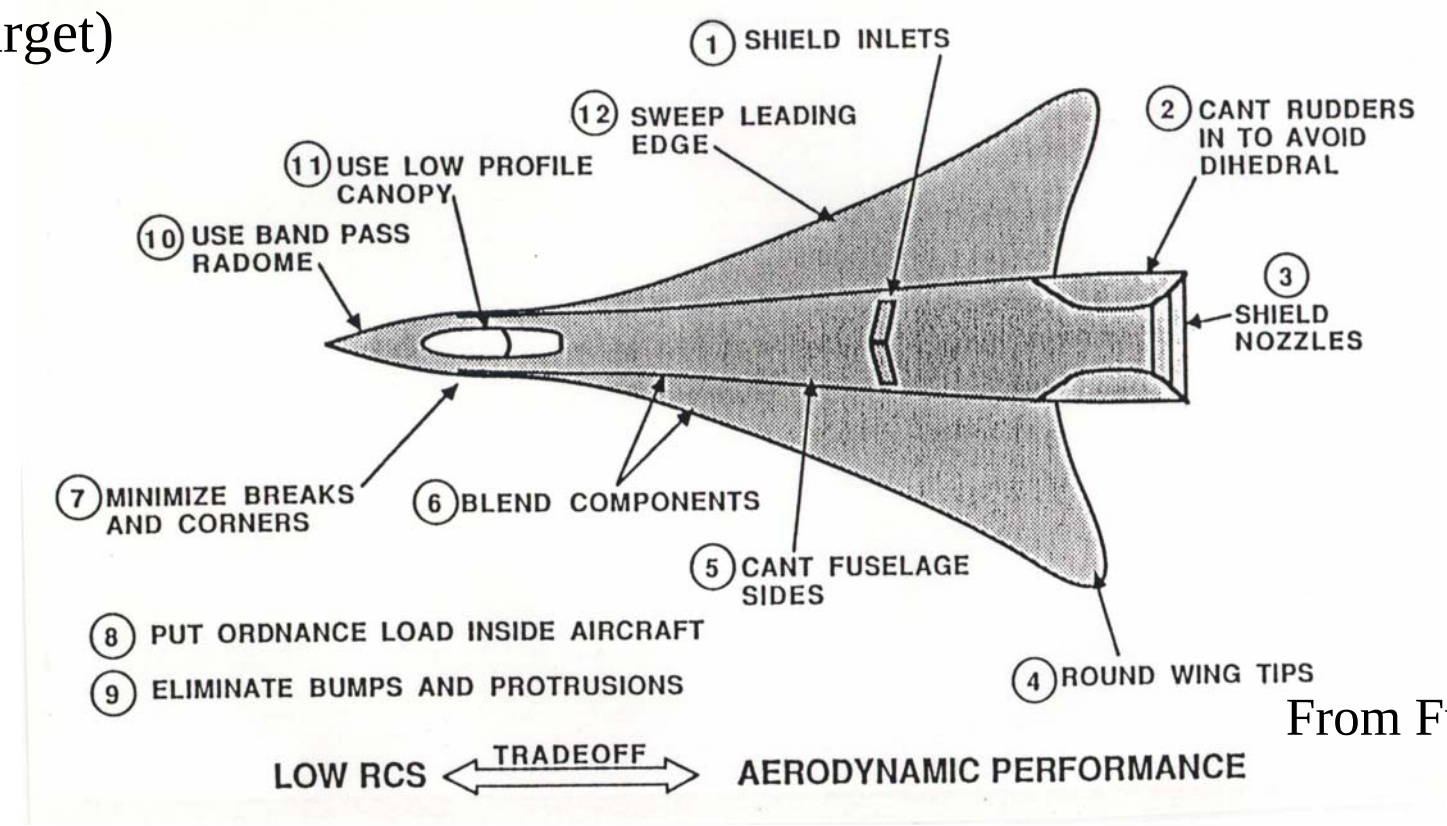
Example: Dipole and Box

- f =1 GHz, –100 dBm (blue) to –35 dBm (red), 0 dBm Tx power, 1 m metal cube



RCS Reduction Methods

- Shaping (tilt surfaces, align edges, no corner reflectors)
- Materials (apply radar absorbing layers)
- Cancellation (introduce secondary scatterers to cancel the “bare” target)

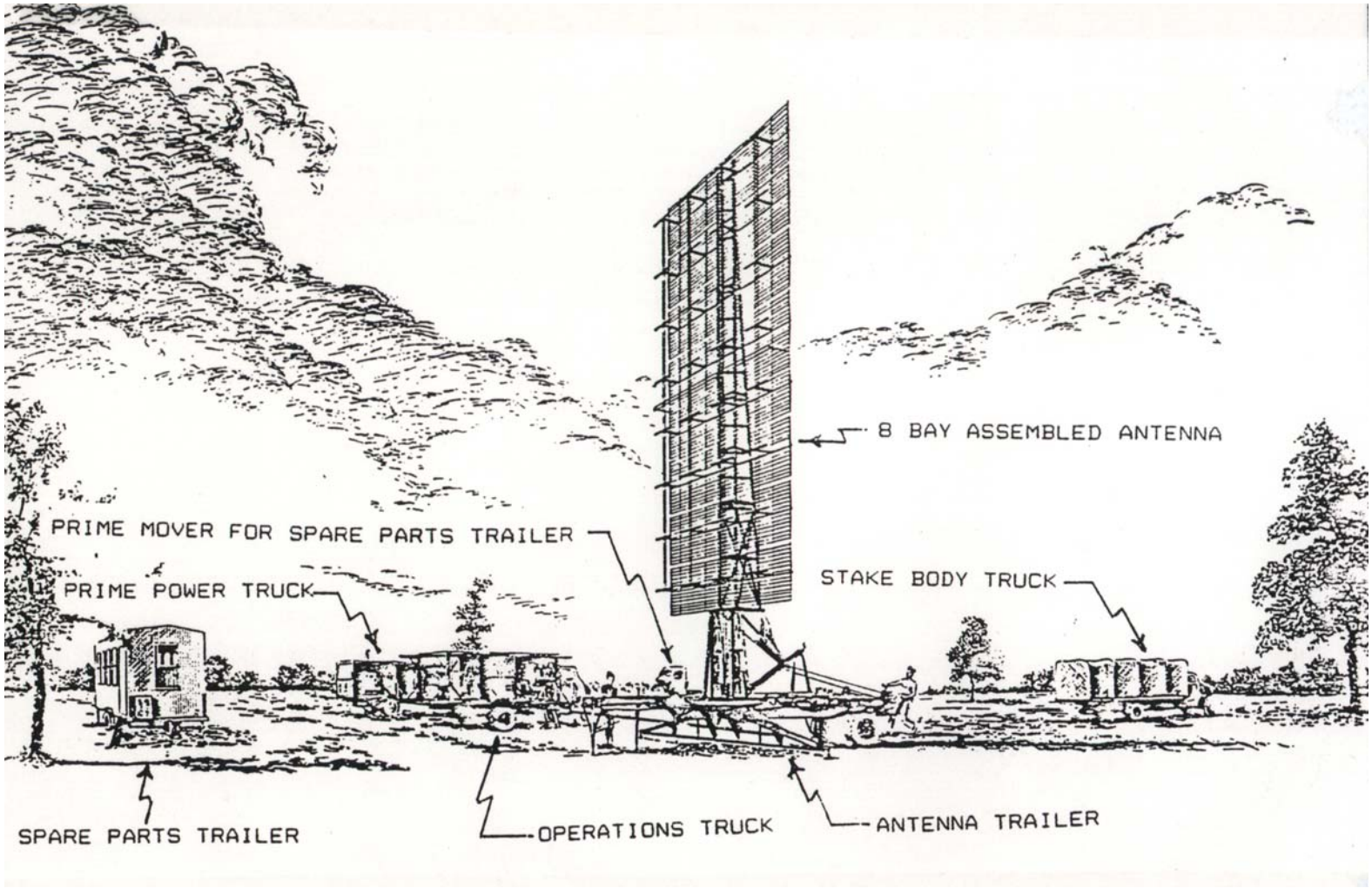


From Fuhs

AN/TPQ-37 Firefinder

- Locates mortars, artillery, rocket launchers and missiles
- Locates 10 weapons simultaneously
- Locates targets on first round
- Adjusts friendly fire
- Interfaces with tactical fire
- Predicts impact of hostile projectiles
- Maximum range: 50 km
- Effective range:
  Artillery: 30 km, Rockets: 50 km
- Azimuth sector: 90°
- Frequency: S-band, 15 frequencies
- Transmitted power: 120 kW
- Permanent storage for 99 targets; field exercise mode; digital data interface

SCR-270 Air Search Radar



SCR-270-D-RADAR

- Detected Japanese aircraft approaching Pearl Harbor
- Performance characteristics:

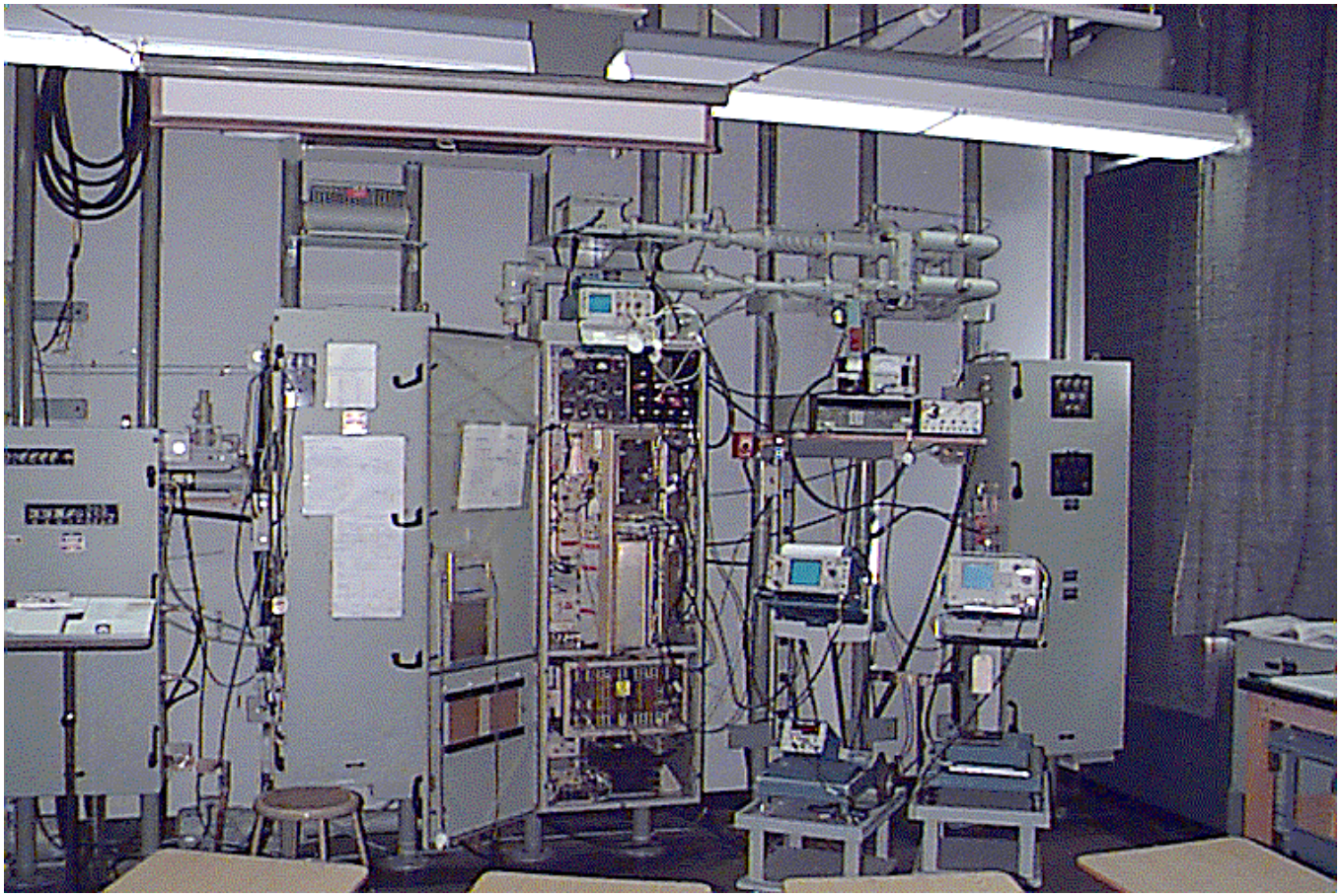
SCR-270-D Radio Set Performance Characteristics (Source: *SCR-270-D Radio Set Technical Manual, 1942*)

Maximum Detection Range	250 miles
Maximum Detection altitude	50,000 ft
Range Accuracy	4 miles*
Azimuth Accuracy	2 degrees
Operating Frequency	104-112 MHz
Antenna	Directive array **
Peak Power Output	100 kw
Pulse Width	15-40 microsecond
Pulse Repetition Rate	621 cps
Antenna Rotation	up to 1 rpm, max
Transmitter Tubes	2 tridoes***
Receiver	superheterodyne
Transmit/Receive/Device	spark gap

* Range accuracy without calibration of range dial.
** Consisting of dipoles, 8 high and 4 wide.
*** Consisting of a push-pull, self excited oscillator, using a tuned cathode circuit.

AN/SPS-40 Surface Search

- UHF long range two-dimensional surface search radar



AN/SPS-40 Surface Search

- UHF long range two-dimensional surface search radar. Operates in short and long range modes
- Range
  - Maximum: 200 nm
  - Minimum: 2 nm
- Target RCS: 1 sq. m.
- Transmitter Frequency:
  - 402.5 to 447.5 MHz
- Pulse width: 60 s
- Peak power: 200 to 255 kW
- Staggered PRF: 257 Hz (ave)
- Non-staggered PRF: 300 Hz

- Antenna
  - Parabolic reflector
  - Gain: 21 dB
  - Horizontal SLL: 27 dB
  - Vertical SLL: 19 dB
  - HPBW: 11 by 19 degrees
- Receiver
  - 10 channels spaced 5 MHz
  - Noise figure: 4.2
  - IF frequency: 30 MHz
  - PCR: 60:1
  - Correlation gain: 18 dB
  - MDS: –115 dBm
  - MTI improvement factor: 54 dB

ش ت ب/ش ت/ (ط-٤٦)
Military Technical College
Branch of Educational and Research Affairs
Educational Affairs

Branch : Electrical Engineering **Department** : Radar
Course Code: ERD402 **Course Name:** Radar Electronic Warfare

Year: 4th	Specialization: RA&GU
Term: Winter	Duration (weeks): 16
Type of the course : A	Type of the Exam. : W

Number of Hours	*Week Hours*			*Total Hours*		
	Lec.	*Ex.*	*Lab.*	*Lec.*	*Ex.*	*Lab.*
	3	*1*	*-*	*48*	*16*	*-*
Total Number of Hours	*4*			*64*		

Course Description:

Electronic counter measures, basic definitions, concepts, missions. Main radar ECM techniques, active & passive jamming techniques and active& passive deception techniques. Radar range performance under jamming. Main radar ECCM techniques for enhancement of security, survivability, immunity, and interference suppression. ECM receivers, classification, parameters measured, and IFM receiver as an example.

Course Objectives:

After completing this course, the student will be able to:

1- Evaluate the ECCM capabilities of different radar, or guidance systems.
2- To differentiate between different hostile ECM technique.
3- To calculate the effect of jamming on radar performance (maximum detection range.
4- To understand the mutual effects and the different links between ECM, ECCM and ESM measures.

Instructional Materials:

Lecture notes

References:

Electronic Warfare Fundamentals, November 2000.

ش ت ب/ش ت/ (ط-٤٨)

Military Technical College
Branch of Educational and Research Affairs
Educational Affairs

Branch :Electrical Engineering
Department : Radar
Course Code : ERD402
Course Name : Radar Electronic Warfare
Year : *4th*
Specialization : Radar & Guidance

Course Plan

Item No.	Theme	Hours				Remarks
		Tot	*Lec*	*Ex*	*Lab*	
1	Introduction	**6**	**6**	**-**	**-**	
2	Electronic Counter measures	**6**	**4**	**2**	**-**	
3	ECM Techniques	**12**	**10**	**2**	**-**	
4	Radar Performance under jamming	**10**	**6**	**4**	**-**	
5	ECCM techniques	**14**	**10**	**4**	**-**	
6	Ew receivers	**8**	**6**	**2**	**-**	
7	Control tests	**8**	**6**	**2**	**-**	
Total		**64**	**48**	**16**	**-**	

ش ت ب/ش ت/ (ط-٤٩م١)

Military Technical College
Branch of Educational and Research Affairs
Educational Affairs

Branch : Electrical Engineering **Department :** Radar
Course Code :ERD402 **Course Name :** Radar Electronic Warfare

Course Outlines

Week	Lec	Lecture	Hrs	Exercise	Hrs	Lab	Hrs
1	1	Introduction & Electronic counter measure	2				
	2	Introduction & Electronic counter measure	2				
2	3	Introduction & Electronic counter measure	2				
3	4	Introduction & Electronic counter measure	2	Assignment #1Active jamming	2		
	5	Introduction & Electronic counter measure	2				
4	6	ECM Techniques	2				
5	7	ECM Techniques	2	Assignment #2 Radar performance under jamming	2		
	8	ECM Techniques	2				
6	9	1st Control Test	2	1st Control Test			
7	10	ECM Techniques	2	Assignment #3 Performance under jamming conditions	2		
	11	ECM Techniques	2				
8	12	Radar Performance under jamming	2				
9	13	Radar Performance under jamming	2	Assignment #3 Performance under jamming conditions	2		
	14	Radar Performance under jamming	2				
10	15	Basic ECCM Techniques	2				
11	16	2nd Control Test	2	2nd Control Test			
	17	2nd Control Test	2				
12	18	Basic ECCM Techniques	2	Assignment #4 Interference suppression and noise standardization technique	2		
13	19	Basic ECCM Techniques	2	Assignment #4 Interference suppression and noise standardization technique	2		
	20	Basic ECCM Techniques	2				
14	21	Basic ECCM Techniques	2				
		EW Receivers	2	Assignment #5 IFM receiver	2		
15	22	EW Receivers	2				
	23	EW Receivers	2				
16	24	Revision	-	Revision			

Grading System:

Control Test 1	15 %	Control Test2	15 %
Teacher Opinion	10 %	Final Exam	60 %

Total **100 %**

Military Technical College
Branch of Educational and Research Affairs
Educational Affairs

Branch	: Electrical Engineering	**Department**	: Radar
Course Code	: ERD402	**Course Name**	: Radar Electronic Warfare
Year	: 4th	**Specialization**	: Radar& Guidance

Course Contents

Chapter1: **Electronic Counter Measures [ECM]**

1-1 Basic definition
1-2 Components of defiance system affected by ECM.
1-3 ECM concepts.
1-4 ECM missions
- stand off mission
- stand forward mission
- self screening (protection) mission
- Escort mission
-Mutual support mission

1-5 ECM Priorities

Chapter2: ECM Techniques

2-1 Active jamming techniques
- CW jamming
- Impulse jamming
- Spot noise jamming
- Barrage noise jamming
- Swept-spot noise jamming
- Smart noise jamming

2-2 Passive jamming
- Chaff
- Low flying
- Evasive maneuvers

2-3 Active Deception
- False target generation
- Range-gate stealer
- Velocity gate stealer
- Inverse gain
- Cross-eye angle deception
- Formation angle deception
- Blinking angle deception
- Cross- polarization

2-4 Passive deception
- Chaff
- Decoys
-Low observable

Chapter 3: Radar range performance under jamming
- The effective radiated jamming power(ERP)
- The effective radiated spectral density (ERD)
- The radar range equation in the presence of jamming (the burn through range considering different conditions of jamming)

Chapter 4: Survey of basic ECCM Techniques

4-1 Introduction

4-2 Security enhancement techniques
- Frequency camouflage
- Confusion techniques
- Deception techniques
- Masking techniques

4-3 Survivability enhancement techniques
- Burn through technique
- Prevention of receivers overloading
  - Feedback AGC
  - Feed forward AGC
  - Programmed AGC [STC]
  - Logarithmic reception

4-4 Interference immunity enhancement techniques
- Signal discrimination techniques
  - Spatial discrimination
  - Polarization discrimination
  - Frequency discrimination
  - Tracking techniques
  - Pulse width discrimination
  - Pulse reception frequency
- Identification techniques
- Optimization of signal processing
- System enhancement due to redundancy
  - Reliability and availability
  - Frequency divers radars
  - Frequency agile radar

4-5 Interference suppression and noise standardization techniques:

- CFAR processing
- Dicke-Fix
- MTI processing
- Doppler processing
- Side-lobe blanking
- Side-lobe cancellation

4-6 Techniques of mathematical game theory

Chapter 5: EW receivers

5-1 Introduction

5-2 Classification of intercept receivers

5-3 Parameters measurably EW receivers

5-4 Instantaneous Frequency Measurement receiver [IFM]

- Principle of operation
- Basic components
- The limiting amplifier
- Capture effect
- IFM receiver with multiple correlation
- Frequency digitizing window