

# Aerosystems Engineering & Management Training School

**Academic Principles Organisation** 

# AVIONICS PART 2 PHASE 3 Radar

BOOK 7
Electronic Warfare

# **WARNING**

These course notes are produced solely for the purpose of training. They are not subject to formal amendment action after issue and they must NOT be used for operating and maintaining the equipment described. Operation and maintenance of equipment is governed by the limitations and procedures laid down in the authorised publications and manuals which must be complied with for these purposes

# WARNING INTELLECTUAL PROPERTY RIGHTS

This course manual is the property of the Secretary of State for Defence of the United Kingdom and Northern Ireland (the 'Authority'). The course manual is supplied by the Authority on the express terms that it may not be copied, used or disclosed to others, other than for the purpose of meeting the requirements of this course.

© CROWN COPYRIGHT

# **ELECTRONIC WARFARE (EW)**

# SIGNAL INTELLIGENCE SYSTEM (SIGINT)

# **INFRA RED COUNTER MEASURES (IRCM)**

#### **OBJECTIVES**

**T.O.s** – 44.1, 44.2, 44.10, 44.11, 44.4, 44.9

#### E.O -

**S99-02 -** Describe Active Electromagnetic countermeasures.

**S99-04** - Describe the Aircraft Intelligence gathering systems.

**S99-03** - Describe the aircraft laser countermeasures system

#### KLP Ref -

\$99-02-01 - Describe the Noise Jammer

\$99-02-02 - Describe the deception Jammer

**\$99-03-01 -** Describe the laser countermeasures system

**S99-04-01 -** Describe the Signal Intelligence system (SIGINT).

#### Performance -

Describe Active Electromagnetic countermeasures.

Describe the Aircraft Intelligence gathering systems.

Describe the aircraft laser countermeasures system

# **CONTENTS:**

# **ELECTRONIC WARFARE**

	_
Definitions	5
Electronic Surveillance Methods (ESM)	7
Signal Intelligence (SIGINT)	
Electronic Intelligence Gathering (ELINT)	8
Threat warning	
Defence Aids Sub-System (DASS)	
Radar Warning Receiver (RWR)	
Electronic Defence	
Frequency Agility	
Frequency Diversity	
Non Electronic Defence Techniques	
Decoys	
Chaff	
Stealth	
Infra-red Homing Missiles	
ECM Jamming Techniques	
Noise Jamming	
Deception Jamming	
Noise	
Types of Noise Jamming	
Types of Deception Jamming	
The Laser	
Laser Fundamentals	
Laser safety	
Definitions	
The Laser Countermeasures system	
LAIRCM System	
LAIRCM LRUs	
LAIRCM Safety Precautions	
Future of IR Countermeasures	

# **ELECTRONIC WARFARE (EW)**

#### **EW Introduction**

1. "Electronic Warfare (EW) supports all types of military activity across the spectrum of conflict. It is used in platform, force or area protection, in Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), for defensive and offensive action and in support of other capabilities and strategies. To this end, EW relies on a combination of technical capabilities."

Source AJP-3.6(A) ALLIED JOINT ELECTRONIC WARFARE DOCTRINE DECEMBER 2003

- 2. The importance and widespread use of electronic devices in defence systems inevitably means that such devices become targets for attack, either by physical means or by more subtle electronic means Electronic Warfare (EW).
- 3. In modern warfare the electromagnetic spectrum, including radio, microwave, optical and infrared frequencies, is widely used in applications such as communications, target detection and tracking covert surveillance and laser ranging.

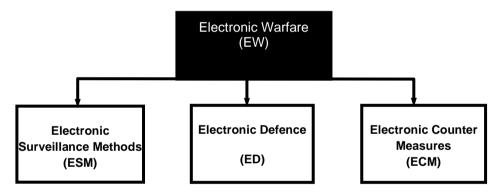


Figure 1 - The Three Branches of Electronic Warfare

#### **Basic Definitions**

4. **Electronic Warfare (EW)**. EW or Electronic Attack is defined as the military use of electronics involving actions taken to prevent or reduce an enemy's effective use of radiated electromagnetic energy and actions taken to ensure our own effective use of radiated electromagnetic energy. EW can be split into three branches (refer figure 1), as follows:

- 5. **Electronic Surveillance Measures (ESM).** ESM is that part of EW involving Surveillance of the Electromagnetic Spectrum (EMS) for immediate threat recognition in support of EW operations and other tactical actions such as threat avoidance, homing and targeting. It is the interception, location, recording and analysis of electromagnetic energy.
- 6. **Electronic Defence (ED)**. May also be known as Electronic Protection Measures is that part of EW involving actions taken to ensure our effective use of the electromagnetic spectrum despite the enemy's use of ECM. The principal object of ED is to permit radars to accomplish their intended functions.
- 7. **Electronic counter-measures (ECM).** ECM encompass actions taken to prevent or reduce an enemy's effective use of the EMS and is further sub-divided as follows:
  - a. **Electronic jamming** is the deliberate radiation, re-radiation or reflection of EM energy with the object of impairing the effectiveness of electronic devices, equipment and systems.
  - b. **Electronic neutralisation** involves the deliberate use of EM energy to either temporarily or permanently damage devices that rely exclusively on the EMS.
  - c. **Electronic deception** is the deliberate radiation, re-radiation, alteration, absorption or reflection of EM energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems.

Source: AP3002 Air and Space Warfare Third edition

# Describe the Signal Intelligence (SIGINT) system (KLP 99-04-01)

- 8. In explaining this KLP it is necessary to have a background knowledge of Electronic Surveillance methods these form part of what are known as of ISTAR techniques: Information Surveillance Target Acquisition and Reconnaissance. ISTAR assets will aid military commanders to link mission functions together to assist the combat force in employing its sensors and manage information they receive.
- 9. **ESM** is used to gain the advantage in EW by improving our ECM and ED techniques. To do this detailed information is therefore needed about the enemy's Radar and Electronic capabilities. This information is obtained from a thorough analysis of enemy Radar signal parameters.
- 10. **Signal Intelligence (SIGINT).** This is a very detailed process used to obtain a longer term electronic tactical advantage. Intelligence and security organisation sources collect the information; agencies such as the listening station at GCHQ detect and intercept electronic signals. Satellites may also be used to obtain information on the location of radar and signal emitters. This information will be analysed in detail and may be used to obtain a Strategic advantage in Electronic Warfare.
- 11. SIGINT methods involve detection and analysis of hostile communications / Radar signals

The Analysis Process of the signal in all three activities involves:

- a. Detecting and Receiving the signal
- b. Measure / Categorise the parameters
- c. Recognition / Identification
- d. Assessment and Reaction

From this information on the Electronic parameters of any detected signal can be examined and may be acted upon. The collection and analysis of this may give us information on the strength, intentions and role of the enemy.

12. **Electronic Intelligence Gathering (ELINT).** ELINT is information derived primarily from electronic signals that do not contain speech or text. ELINT can be gathered from electronic surveillance missions. These can be carried out by specialist Signals Intelligence Aircraft or Ships. One such aircraft is the RC-135W Rivet Joint it is equipped with a variety of sensors, allowing its multi-disciplined crew to intercept and exploit emissions across the electromagnetic spectrum, providing both strategic and tactical level intelligence.



Figure 2: RC-135W Rivet Joint RAF/MOD Crown Copyright 2013

13. **Threat Warning.** When an aircraft is on an operational sortie the aircrew must know when they are being illuminated by an Electronic threat (hostile radar) these could be land based, ship based or from another airborne platform. They may only have seconds to react if a Radar guided missile is detected. Consequently the aircrew want to know as much information about the signal as possible. Location, Frequency, what type of radar is being used etc. The rapid analysis and almost instantaneous display of this information hopefully allows the aircrew enough time to react to the threat. One item of equipment used for detecting Electronic Threats is the Radar Warning Receiver (RWR) which may form part of the Defence aids Subsystem.

#### Defence Aids Sub-system (D.A.S.S.)

- 14. An aircraft operating in a hostile military environment needs to be equipped with measures for self-defence. The crew will have been briefed on the threats in their area of operation.
- 15. During the mission the pilot must be warned of real tactical threats to the mission and must have the means to reduce their effectiveness.
- 16. Countermeasures include a means of detecting the threat and direct the threat away from the aircraft or causing the missile to detonate away from the aircraft.
- 17. The combination of sensor and countermeasure is called the Defensive Aid Subsystem (DASS)
- 18. A DASS system may include the following (Refer to figure 3):
  - a. Radar Warning Receiver (RWR)
  - b. Missile Warning Receiver (MAW)
  - c. Laser Warning Receiver (LWS)
  - d. Countermeasures dispenser chaff or flares
  - e. Towed decoy
  - f. Infra-Red Jamming

19. On military aircraft these systems may interface with each other and will interface with the aircraft mission avionics systems by using MIL-STD-1553B

databus.

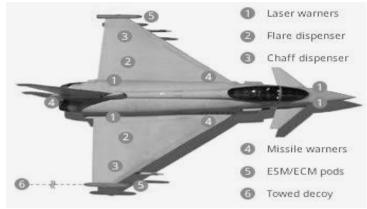


Figure 3 DASS system

20. **Radar Warning Receiver (RWR).** One of the main sensors of the D.A.S.S. is the RWR system A typical RWR system consists of four miniature directional antennas mounted either in the fin of an aircraft or in a wing-tip pod, which are used to cover several different frequency bands. It is desirable that these Signals are received at the earliest opportunity to alert the crew to any perceived threat. Each antenna feeds a receiver and the resulting signals are analysed to determine the bearing, strength and type of radar signal, including Pulse CW, TWS. The coverage and layout of the system is shown in figures 4a and 4b.

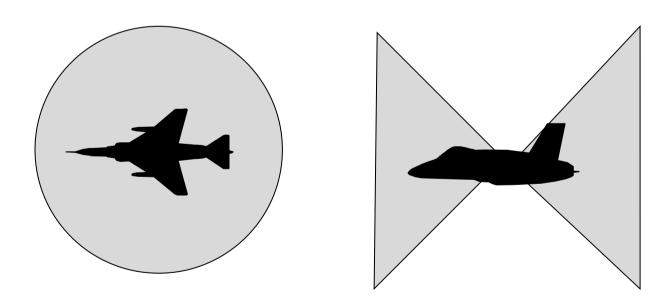


Figure 4a – RWR Signal Coverage (not to scale)

- 21. The RWR display shows positional information on the perceived threat. In addition, logic circuits analyse the threat posed by the radar (is it a missile control radar?) and illuminates appropriate warning lights. The detected signal may be analysed and fed to the aircrew as an audio tone based on the threat type of the radar signal.
- 22. The RWR antenna is a small compact unit. Small antennas can be used because the radar signal strength at a target (the RWR carrier) is many times greater than that reflected back to the illuminating radar; by the same token, a RWR can detect hostile radar before the enemy detects the carrier aircraft.
- 23. As mentioned It is desirable that the very widest band of frequencies are received and at the earliest opportunity to alert the crew to any perceived threat. Therefore low signal level detection is imperative. As a result the RF Cables connected to the Antennas in the fin and are routed though the aircraft to the receiver are specialised and more sensitive to handling than other types of RF cables. If bent or twisted they will lose their sensitivity to certain frequencies and this may impair the system's ability to pick up small signals consequently the RF cables are made of specialised materials/dielectrics and are to be handled with extreme care.

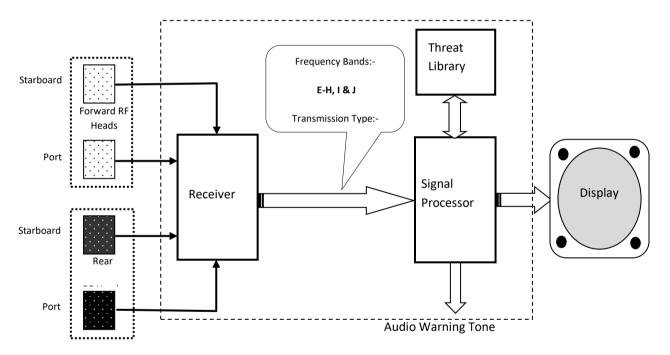


Figure 4b – RWR Layout

### **Electronic Defence (ED)**

- 24. Electronic Defence Techniques use a variety of techniques to maintain radar coverage in the face of hostile ECM. Two of these electronics techniques are Frequency Agility and Frequency Diversity there are others but they are outside the scope of this course.
  - a. **Frequency Agility**. The term 'Frequency Agile' is used to describe radar that is capable of operating at different frequencies within a given band of frequencies on a pulse-to-pulse basis. This means that the transmitted frequency for each pulse is slightly different making it more difficult to jam.
  - b. **Frequency Diversity**. Frequency diversity is the ability to operate radar system in different bands, thus avoiding barrage jamming techniques.

#### **Non- Electronic Defence Techniques**

- a. Decoys
- b. Chaff
- c. Stealth

#### **Decoys**

25. These are devices that are launched from or towed by target aircraft and which simulate genuine targets by reflecting enemy radar in such a way as to give the impression of being a genuine target. Or by actually transmitting deceptive information. Decoys can be free-falling or self-propelled and programmed or controlled to simulate tactical manoeuvres they could be drones or missiles with the reflection characteristics of the parent aircraft and may fulfil a dual role by having a warhead-carrying capability.

#### Chaff

- 26. The intention is that echoes from chaff should confuse an enemy radar operator either by giving the impression of large numbers of targets or by screening a friendly force. Both will cause tracking difficulties.
- 27. The effective echoing area of chaff is very large considering the small amount of material that is used and its lightness and compactness make it convenient for automatic dispensing from an aircraft or deployment using rockets and/or explosive dispensers.
- 28. The turbulence behind an aircraft makes the cloud of chaff initially spread out but then remains fairly constant in size. Chaff falls at between 50 and 300 feet per minute and drifts with the wind. A radar operator to distinguish between chaff and target can use the low speed of movement and this can be accomplished very easily using moving target indication (MTI). Because of this chaff is unlikely to screen targets from sophisticated modern radars and its main use is in confusing radarguided missiles.

#### Stealth

- 29. This is the name given to a range of techniques that reduce the radar returns of a potential target. Three main approaches are used:
  - a. **Radar Absorbent Materials**. Aircraft, or other targets, may be covered with materials that absorb radar energy. The penalty for this is increased weight and possibly extra drag.
  - b. **Radar Transparent Materials**. Aircraft can be constructed from non-metallic materials such as carbon fibre composite and fibreglass. This technique is applied to Cruise missiles.
  - c. **Design Features**. The shape of an aircraft design controls the radar echo strength.

# Infra-Red (IR) - Homing Missiles

30. Historically, most aircraft, which have been shot down by guided missiles, have been destroyed by the IR – homing type, so clearly the development of countermeasures to this threat is highly desirable.

### **Infra-Red Decoys**

31. **Flares.** The aim of infra-red decoys is to present a target to the missile which is more attractive than the aircraft. Decoys that are in the form of flares emit energy at all IR frequencies, and the missile guidance system will then transfer lock to either the flare or the power centroid (centre between heat sources) between the flare and the aircraft. As the flare drops away the aircraft is no longer in the missile "field of view" (FOV). The flare must have the capability to ignite quickly and be sufficiently bright while still within the missiles FOV, and then burn for long enough so that the aircraft can escape from the FOV.

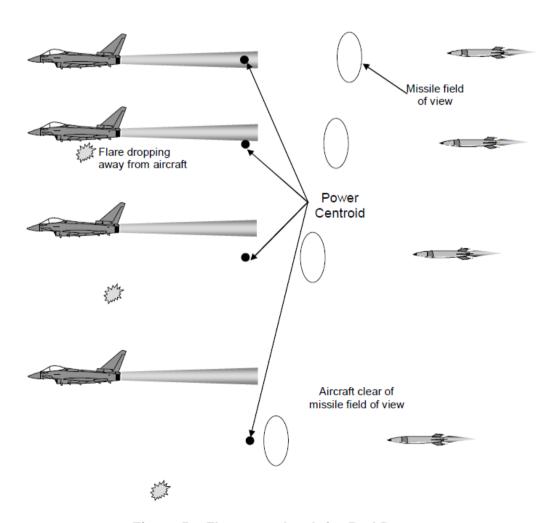
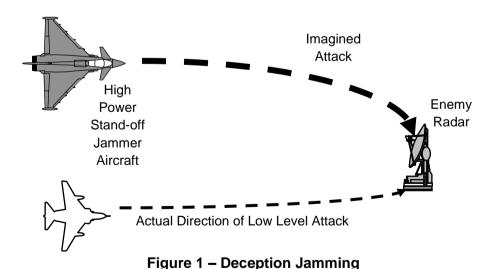


Figure 5 - Flares used as Infra-Red Decoys

# **ECM Jamming Techniques** (KLP 99-02-01/02)

- 32. ECM jamming techniques for use against radar may be divided into two general types:
  - a. Noise jamming
  - b. Deception jamming.
- 33. Depending on the type and role of the aircraft the Deception Jammer and Noise Jammers may be in an ECM pod or form part of a larger subsystem such as the Defence Aids Sub-system (D.A.S.S.) mentioned earlier.
- 34. **Noise Jamming**. The intention behind confusion jamming is to produce so many spurious returns on enemy radar displays that detection and interpretation of real returns becomes impossible. Noise jamming and the use of large clouds of chaff are good examples of confusion jamming.
- 35. **Deception Jamming**. Deception jamming is a more subtle form of ECM intended to make the enemy radar operator mistake a false target for a real one or to misinterpret the intentions of his opponent. The transmission of false signals, which deceive the radar into displaying incorrect information about the target, with regards to its slant range, and bearing are examples of deception, as is the use of small clouds of chaff intended to look like real aircraft or ships.
- 36. It is important to realize that some ECM techniques can be used for confusion or deception depending on its tactical deployment. For instance, noise (confusion) jamming could be used for deception purposes as shown in; figure 1, where the enemy radar operator is deceive into thinking an attack was coming from one direction while the real threat lies elsewhere.



#### **Noise**

- 37. Electronic noise as seen on a radar display (at video frequencies), consists of random signals whose amplitude varies with time so that no recognizable pattern occurs. The wanted target signals however, are recognized by the pattern they produce as determined by the pulse shape and the type of aerial scan.
- 38. If random electronic noise is mixed with the target signals, the recognizable signal pattern is gradually lost as the average power of the noise is increased. The result of noise jamming is therefore to degrade or obliterate the target signal pattern; therefore, the higher the noise power received by the radar, the more difficult will it be for the radar operator to detect targets and track them.
- 39. Radar transmissions cover a finite band of frequencies in the electromagnetic spectrum; e.g. a pulse radar using 0.5 µsec pulses might need a bandwidth (b/w) of 2 MHz centred on its carrier frequency, whereas a frequency-modulated CW radar might require a b/w of only 10 kHz.
- 40. For noise jamming to be successful, the noise b/w must be at least as wide as the b/w of the victim's radar. In practice, a jammer has a limited output power, but, by design, that power can be either concentrated in a narrow bandwidth (giving a high power output power unit b/w) or spread over a wide b/w (which results in a lower power per unit b/w); this is illustrated in figure 2.

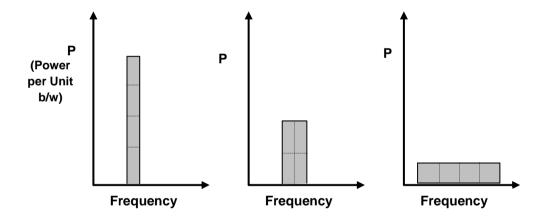


Figure 2 – Effect of Bandwidth on Power per Unit Bandwidth

#### **Types of Noise Jamming**

- 41. Although it is desirable to match the noise jamming to the characteristic of particular radar, it is sometimes necessary to use ECM to counter more than one radar (at more than one frequency) and it is not always possible to carry a separate jammer for each anticipated threat radar. It is advisable, therefore, to consider the ways in which noise jamming may be accomplished, there are:
  - a. Spot jamming
  - b. Sweep jamming
  - c. Barrage jamming
  - d. Multi-purpose jamming
- 42. **Spot Jamming**. Continuous jamming of individual radars is best achieved by spot jamming. The 'spot' in this instance is a narrow bandwidth sufficiently wide, however, to cover the spread of frequencies around the radar carrier frequency, a spread that is inherent in any pulse or continuous-wave radar. Although this method provides maximum jamming noise power, in a complex attack situation it suffers the severe limitation of only being able to jam those radars using that specific frequency.
- 43. **Sweep Jamming**. Jamming may be required over a relatively large band, but, in order that noise power arriving at any radar will be sufficient to jam it, it may be advisable to transmit over a small bandwidth and sweep that small bandwidth over the large waveband. Thus, if several radars each transmit at different carrier frequencies, or one radar changes frequency (frequency agility), the jammer can achieve a certain amount of success by sweeping. This means, of course, that each radar is not continuously jammed (thus reducing the effective noise power) and a good operator might overcome the problems arising from such jamming.
- 44. **Barrage Jamming**. If the enemy radars have frequency agility plus well-trained operators, it may well be possible for the operators to track targets despite the jamming methods so far described. However, wide frequency-band jamming called barrage jamming will enable jamming to be virtually continuous over a wide frequency band. But, as the available power is now distributed over a wide band, this method has the disadvantage that the jamming power in the given narrow band of operation of any radar is reduced compared with the jamming power of a spot jammer. Thus, for successful jamming the barrage jammer must have as high a power as possible.
- 45. **Multipurpose Jammers (MPJ)**. It is also possible to combine two or more jamming roles, e.g. barrage and pulse deception jamming. Electronic equipment can also be designed so as to be capable of simultaneously spot jamming at a number of different frequencies lying within a broad band of frequencies. All such equipment's are classed as multipurpose jammers (MPJ).

# **Types of Deception Jamming**

46. The object of enemy radar is to gain information on one or more of the parameters range, direction and speed of a target. To provide a countermeasure it is possible, instead of obliterating the radar display with noise jamming, to present either the radar operator or the radar circuitry with false information by electronic means. To successfully introduce such countermeasures, it is necessary to establish the enemy radar search pattern and to have some knowledge of the way the circuits of that radar operate.

Types of Deception Jamming include:

- a. False Target Generation
- b. Angle of Deception
- c. Range-Gate Stealing
- d. Velocity-Gate Stealing
- e. Noise Modulated Deception
- 47. **False Target Generation**. This form of deception results in blips that look like targets making it much harder for the enemy radar operator to able to tell the difference between false and real targets.
- 48. **Angle of Deception**. This technique feeds false angular position information back to the tracking radar; these angular error signals can be interfered with causing them to lose track of the target aircraft.
- 49. **Range-Gate Stealing**. If deception-jamming equipment were to transmit a false return pulse bigger than the true target echo, the victim radar would prefer the deception signal. Then by increasingly delaying the deception signals the is taken well away from the true targets position, and the enemy radar loses track of its real target and has to spend time re-acquiring it.
- 50. **Velocity-Gate Stealing**. CW Doppler-type radars determine primarily the velocities of targets and works in a similar way to range rate stealing of a pulse tracking radar. Once the velocity gate has been 'captured' by transmitting the appropriate deception signal velocity can be moved up or down, but must not be at a higher rate than the enemy radar is designed to achieve.
- 51. **Noise Modulated Deception**. This technique combines deception and noise jamming. For instance, deception signals could have noise modulation imposed, either randomly or in a prescribed way, or barrage noise could be arranged to contain large deception signals that an enemy operator may filter out as real targets.

#### **Laser Fundamentals Recap**

52. The word **LASER** is an acronym for:

<u>Light Amplification by Stimulated Emission of Radiation</u>

- 53. Lasers that operate in the near IR region  $(2.7\mu m)$  and which behaves in a very similar way to visible light (although IR is invisible to our eyes).
- 54. Lasers are particularly useful as range finders, target designators and for Laser Guided Bomb (LGB) guidance. By firing a laser ahead of the aircraft an accurate range can be calculated. The Laser Ranger and marked target Seeker (LRMTS) is an example of this sensor system. Target designation by laser was extensively used in Gulf War One where the Thermal Imaging and Airborne Laser Designator pod (TIALD) was used to deliver ordinance accurately onto targets in Iraq.
- 55. Lasers are devices that emit an extremely intense beam of energy in the form of electromagnetic radiation in the near ultra violet, visible or near infrared part of the electromagnetic spectrum. Light is a form of Electro-Magnetic energy that is made up of tiny packages of energy known as Photons.

#### **Characteristics of Laser Light**

56. Laser light (radiation) is different to any other known form of light and has four main characteristics, it is: monochromatic, coherent, intensely bright and has low divergence.

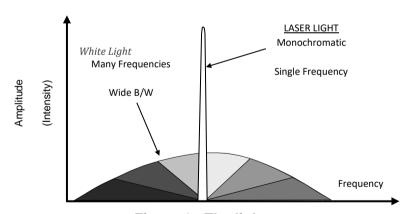


Figure 1 - The light spectrum.

57. This means that one colour or frequency. Therefore laser light has a very narrow frequency spectrum with a bandwidth (B/W) much narrower than that the wide bandwidth (B/W of normal white light that is made up of from light of many frequencies (or colours).

- 58. Coherent Laser light means that the emitted photons due to stimulated emissions are all of the same frequency and "in phase" with each other. Consequently the electro-magnetic waves of the laser beam are "in phase". White light is non-coherent and will have photons that are both "in phase" and "anti-phase".
- 59. A laser light is high in intensity because laser light is monochromatic and coherent the energy of the photons is "additive". Therefore lasers give out an extremely narrow intense beam of light. Unlike white light from a filament (bulb), which produces beams of light that are non-coherent and comparatively both broad and dim.

#### **Laser Safety**

- 60. There is always a danger to the eyes when working with lasers as they often use wavelengths that the cornea and the lens can focus well. The coherence and low divergence of laser light means that it can be focused by the eye into an extremely small spot on the retina, resulting in localized burning and permanent damage (or blindness) in seconds or less. Lasers are classified into safety classes numbered I (inherently safe) to IV (even scattered light can cause eye and/or skin damage).
- 61. JSP 390 Volume 1 sets out the MOD policy concerning the use of laser equipment. It is the MOD's policy to ensure that all laser use, training, test, research and trials are conducted in a safe manner which complies with or exceeds the requirements of UK Health and Safety legislation. JSP390 describes the approved procedures to be followed in the Military Air Environment (MAE) to ensure safety. Regulatory Article (RA) 4265 details the requirement for laser equipment maintenance and MAP-01 chapter 6.14.

RA 4265 - Laser Equipment Maintenance Rationale The operation of a laser can result in injury to the skin and eyes. The purpose of this Regulatory Article is to mitigate these risks by detailing the regulation for the maintenance of laser equipment. Contents 4265(1): Laser Equipment Maintenance Regulation Laser Equipment Maintenance 4265(1) 4265(1) The use of lasers in aircraft maintenance shall be strictly controlled Acceptable 1 Acceptable Means of Compliance is contained within MAP Chapter 6.14. Means of Compliance 4265(1) Guidance Guidance Material and associated processes are contained within MAP Chapter 6 14 Material 4265(1)

### The Laser Countermeasures System (99-03-01)

#### Large Aircraft Infra-Red Countermeasures (LAIRCM)

- 62. The Infra-Red Countermeasures (IRCM) in use today have undergone significant change from "IR lamp" based systems that emit IR energy in wide swaths to the more focussed laser based systems. The term Directional Countermeasures (DIRCM) is used for all directed laser defence systems. LAIRCM is one such evolution that uses a directional laser to defeat an IR guided missile.
- 63. The purpose of the Large Aircraft Infra-Red Countermeasure (LAIRCM), also known as AN/AAQ 24(V), system is to protect its host aircraft from ground launched Infra-Red (IR) guided missiles. It is designed to defeat a wide range of IR heat-seeking missiles.
- 64. LAIRCM operates as a fully autonomous system and requires no operator intervention. Once a missile has been detected, it is initiates defensive measures by tracking the missile and firing a high power laser at the missile guidance system to force the missile to lose lock. The targeted aircraft then has a high chance of survival as the missile is unable to guide to the target. If the LAIRCM loses track of the missile due to masking during aircraft manoeuvres or by sudden LAIRCM system fault then it launches a salvo of multi-spectral flares to seduce the missile guidance system.



Figure 2 – The DIRCM Nemesis<sup>1</sup>.

•

<sup>&</sup>lt;sup>1</sup> Crown Copyright (2015)

- 65. The LAIRCM system is composed of:
  - a. A high power, directional active infrared jammer.
  - b. A stand-alone IR self-protection system with treat surveillance and warning, threat tracking, threat jamming and flare release control.
  - c. A narrow beam directable IR transmitter that accepts threat handoff from an acquisition sensor (such as Missile Warning Receiver System MAWS and a closed loop tracking of the threat with a self-contained sensor.
  - d. A series of multi-spectral flare packs.
- 66. Aircraft emit a great deal of IR energy from hot engine parts, leading edges heated by aerodynamic friction and air conditioning systems. Aircraft IR emissions peak at around 1.5 and 6 micrometre wavelengths, just below the visible light spectra. It is this band of wavelengths that the missile seeker system is attempting to track.

#### 67. The LAIRCM LRUs are:

- a. A Signal Processor that controls the LAIRCM system operation.
- b. A number of Small transmitter Laser Assemblies, dependent on the size of the host aircraft.
- c. A Control Indicator Unit (CIU) that allows the operator to initiate the system, carry out Built-In Test (BIT) and warn of missile detection.
- d. Missile Warning Sensors which are placed around the periphery of the aircraft, in locations that maximise detection view from below the aircraft.
- 68. The LAIRCM engagement sequence falls into four distinct phases:
  - a. **Detect.** Following a missile launch, the MWS system detects the IR energy given by the missiles plume as it accelerates. This causes the MWS to send a launch signal to the Signal Processor.
  - b. **Handoff.** The Signal Processor evaluates the signal as a threat and directs the STLA onto the sightline of the missile.
  - c. **Track.** The STLA slews to the location of the threat and a Fine track Sensor (FTS) acquires the IR signal from the missile. It then tracks the position of the missile by moving the STLA to ensure the missile remains in view.
  - d. **Jam.** The STLA fires a modulated IR laser beam to jam the missiles' guidance system. The missile loses lock on the aircraft and acquires a false target.

#### **LAIRCM Safety Precautions**

69. The LASER used in the Large Aircraft Infrared Countermeasure (LAIRCM) system is a high-powered Class 4 LASER that requires strict safety procedures to be followed. To minimise individuals being exposed to LASER radiation. Each aircraft with LAIRCM equipment will have individual maintenance and safety procedures that must be observed by all personnel involved with maintenance of these equipment's.

### 70. Common LAIRCM safety procedures include:

- Maintenance of LASER equipment is to be undertaken only by qualified and authorised personnel.
- A safety cordon must be setup around the aircraft to ensure that no personnel, vehicles or aircraft are within the ocular hazard distance OHD. Warning signs must be displayed and if required a safety man.
- All personnel are wearing the appropriate protective clothing and eyewear prior to proceeding with testing. Personnel within the cordon undertaking live LASER firing must use the issued PPE and safety goggles.
- Personnel working in surrounding areas are to receive LASER Safety Awareness training. The LASER Safety Officer (LSO) is to be aware of all authorised personnel.
- A member of the team (normally the Control Unit operator) informs ATC that a LASER firing is taking place and is to remain in contact for the duration of the firing. The Supervisor remains present throughout the duration of the firing and in constant 2-way radio contact with all team members.
- Accidental Exposure. Any incident involving exposure or suspected exposure of a person to LASER radiation is to be reported immediately to the engineering and medical authorities. An eye injury will necessitate an immediate referral to a qualified ophthalmologist.
- 71. Please Note: This list is only an example of general IRCM safety precautions. Every IRCM Aircraft System/unit will have specific local orders that must be adhered to.



Figure 3 – The LAIRCM on the Hercules C130J<sup>2</sup>.

72. **The future of IR countermeasures:** The future for IR missile attack is still uncertain as new, intelligent missiles are produced. Therefore modifications to the LAIRCM system have produced the next generation of IR defence in the form of Common Infra-Red Countermeasures (CIRCM) which is currently used on rotary wing aircraft and sporting a very powerful Quantum Cascade Laser (QCL). BEA Systems have produced the Advanced Threat Infra-red Countermeasure (ATIRCM) which takes on a wide range of IR guided weapons.

<sup>&</sup>lt;sup>2</sup> Image copyright: 45153038 by Open Government Licence v3.0 Crown Copyright (2015)