Chapter 1 – INTRODUCTION TO EW TEST AND EVALUATION

1.1 PURPOSE AND SCOPE

This AGARDograph, which supersedes the original version (Volume 17, Issue 1, 2000), provides an overview of Electronic Warfare (EW) Test and Evaluation (T&E). This Handbook's primary purposes may be stated as:

- To introduce the novice to a disciplined approach to EW testing.
- To provide a concise reference for the EW T&E process and test resources for more experienced testers and programme managers.
- To aid NATO Nations in meeting the affordability challenges facing them. Failure to evaluate installed EW system performance adequately on the ground typically results in significantly increased flight test cost and lengthened schedules.
- To catalogue current T&E resources and capabilities available within NATO Nations (Annex A).

The Handbook offers guidance in applying available resources to meet identified test objectives and to aid cost-effective satisfaction of contractual and operational requirements.

Some caveats apply to this Handbook:

- EW systems and consequently T&E equipment operate in the same technical parameter space, since all operate generally with the same multi-spectral threat environment.
- This Handbook has been predominantly updated by its lead co-authors, who are US and UK EW Specialists. As a result, some unintentional US/UK bias may be detected by the reader. These co-authors are well aware that national variations exist in a number of areas across the Handbook and that differing views exist internationally on the relative importance of items and process elements described therein. The co-authors consider that when taken as a whole, this Handbook is sufficiently robust as a NATO-wide document and that any national differences can be adequately handled by each Nation's EW Experts. The co-authors welcome any comments that readers may have on the Handbook, with a view to inclusion in future updates.
- All system types are covered for EW T&E capabilities, but the concentration is on Radio/Radar Frequency (RF) and Infrared (IR) systems operating in EW frequency ranges.
- No requirement or numeric in the Handbook is intended to be associated with any specific System Under Test (SUT), platform or programme.
- Emitter databases, essential to EW systems and associated T&E equipment, are not discussed since they are nationally sensitive. For the same reason there is limited discussion of Low Observability (a.k.a. 'Stealth' or 'electromagnetic signatures') and directed energy weapons, although, where possible, a fuller discourse on their T&E is provided.
- All images and references to T&E facilities and resources are provided as examples only. They do not indicate that any one facility, resource or equipment is any better than another. Their inclusion in this Handbook does not constitute recommendation by the authors.
- The EW T&E engineer, armed with information in this Handbook, remains responsible for the timely identification, planning and execution of cost-effective tests, using appropriate facilities and resources, in order to satisfy their programme's requirements.

1.2 BACKGROUND

Developing and fielding modern EW systems is complex, expensive, and requires a disciplined test approach to ensure that limited programme resources are prudently applied. Therefore, an EW T&E professional's most important task is to determine the appropriate test objectives to satisfy the acquisition programme requirements. All acquisition programmes have milestones where system performance must be evaluated to determine if the system is ready to proceed to the next phase. Decision makers need timely and accurate information about the SUT. Test programmes should be structured such that they provide decision-quality information incrementally throughout the life of the test programme. This allows for system deficiencies to be identified early in the programme when the costs to resolve them are relatively low.

The scope of EW test programmes can vary greatly and it is the task of the EW T&E professional to construct a test programme to cost-effectively meet the programme needs. There are a wide variety of test resources and techniques available to accomplish this. A simple programme might entail taking a radar warning receiver of the type that has been previously proven on a fighter platform and re-hosting it on a transport aircraft. At the other end of the spectrum are programmes with several new EW systems operating as an integrated suite on a platform that is itself networked with other systems. In both cases, the EW T&E professional's task is to tailor a programme that tests the right things at the right time using the right resources.

This Handbook also provides a useful directory of key EW T&E resources available to NATO members, and examines lessons of the past which can be used to improve the productivity of future testing. While much of the content is aimed at personnel with relatively little experience in the field of EW T&E, this volume can also serve as a basic checklist of issues to be covered in planning, conducting, and evaluating EW tests. In order to gain an appreciation for current practices in EW T&E, some discussion of the history of EW system development, EW system application in modern warfare, and generic elements of disciplined testing are presented in this introduction.

With the rapid evolution of military electronics and computer science, the range, complexity, and sophistication of EW systems has grown significantly. This Handbook focuses on testing avionics systems for military aircraft, the primary purpose of which is Electronic Countermeasures (ECM) and Counter-Countermeasures (ECCM). This testing has much in common with the testing of any avionics system, especially in those areas that relate to availability, operability, supportability, and reliability.

1.3 HISTORY OF EW

Many would argue that EW dates back to the Crimean War and American Civil War and the advent of the telegraph as an important form of military communications. Early EW techniques included interruption of the enemy's communications by cutting the telegraph lines, and deceiving the recipients by sending misleading messages. These processes are similar to the current concept of Electronic Attack (EA). Listening in on the enemy's transmissions by tapping the telegraph lines may be the earliest form of EW Support (ES). While no radiated Electromagnetic (EM) energy was involved at this point, the rudimentary concepts of attacking, protecting, and exploiting electronic communications had begun. [1]

The pursuit of EW in military aviation first began in earnest during World War II. Radio beams were used to guide bombers to their targets; radar was used to detect and locate enemy aircraft; and radio communication was becoming the primary means of establishing command and control. As each new electronic measure was employed, the adversary developed a countermeasure or EA capability. In many instances, in order to preserve the advantage of the initial electronic measure in the face of countermeasures, counter-countermeasures or Electronic Protection (EP) were developed. [2]

One of the most significant EW events during World War II and one that highlights EW's role as a force multiplier was the first use of 'Window' by the British during a bombing raid on Hamburg in July 1943.

‘Window’ was the code name for an early version of chaff. The British had been encountering heavy losses from radar-directed German anti-aircraft guns and night fighters. The use of ‘Window’ totally surprised the Germans and completely disrupted the German gun direction and fighter control radars resulting in significantly reduced losses and the near complete destruction of Hamburg. [3]

The Vietnam War, with the backdrop of the Cold War, presented the next major flurry of EW activity. The North Vietnamese employed a Soviet-style Integrated Air Defence System (IADS). Throughout the war the North Vietnamese continued to upgrade the IADS and correspondingly the U.S. adapted to the upgrades with new countermeasures. While strategic bomber and reconnaissance aircraft have long used EW equipment such as Radar Warning Receivers (RWR) and Self-Protection Jammers (SPJ), Vietnam led to widespread use of these systems on tactical aircraft. The conflict also led to the development of specialised aircraft known as Wild Weasels to suppress enemy Surface-to-Air Missile (SAM) radars. The Wild Weasels employed sophisticated EW receivers and Anti-Radiation Missiles (ARMs) to accomplish their mission. Figure 1-1 shows an SA-2 Guideline missile of the type commonly used in Vietnam and an F-105G Wild Weasel aircraft. This era marked the beginning of modern requirements for survival in the presence of electronically-directed enemy fire control. [4]

Figure 1-1: SA-2 GUIDELINE Missile (top); F-105G Wild Weasel Aircraft with a Shrike ARM (bottom) – (U.S. DoD and USAF Photos).

The Arab-Israeli War in October 1973 provides a good illustration of what happens when the air defence threat posed by one adversary advances beyond the EW capabilities of the other. The war "lasted less than a month, yet it contained all the elements of a much longer war. It was an intense, bitterly contested conflict with each side well-equipped with the weapons for modern warfare. The Egyptian and Syrian air defences at that time, were developed from Soviet design. The design stressed overlapping networks of SAM and Anti-Aircraft Artillery (AAA) coverage. This formidable air defence network consisted of the SA-2, SA-3, SA-6, SA-7, the ZSU-23-4, and other AAA systems. While there were proven ECM from the Vietnam War for the SA-2 and SA-3 and IR countermeasures, such as flares for the SA-7, the SA-6 proved to be a surprise. The SA-6's radars operated in a portion of the electromagnetic spectrum never used before by the Soviets. The Israelis tried to compensate for their lack of ECM against the SA-6 by flying lower, trying to get under its radar coverage. This tactic placed them into the heart of the ZSU-23-4 threat envelope and contributed to the loss of numerous aircraft. This forced the Israelis to adjust their electronic equipment, modify their tactics, and seek additional ECM equipment, such as ECM pods and chaff dispensers from the U.S. However, before the tactics were changed and the new equipment arrived, the Israelis suffered heavy aircraft losses, which taught them a valuable lesson." [5]

The 1970s and 1980s also saw the coming of age of Low Observable (LO) technology. While LO principles have been applied earlier, the F-117A development marked the first time that LO principles would be the dominant design attribute for an aircraft. The F-117A, shown in Figure 1-2, became operational in 1985 and played a key role in Operation Desert Storm, where it operated with impunity in heavily defended airspace. Since the F-117A debut, LO technology has become an important consideration for all combat aircraft. [6]

Figure 1-2: F-117A Nighthawk: The First Operational Low Observable Aircraft – (U.S. DoD Photo).

Operation Desert Storm (1991) was spearheaded by an effort to suppress and destroy the Iraqi Kari IADS. This effort brought together all aspects of EW. Air-launched decoys deceived the Iraqi IADS into engaging them with radar-directed SAM systems such that Wild Weasel aircraft could target them with

High-speed ARMs (HARM). Support jamming aircraft jammed surveillance radars. F-117A aircraft attacked and destroyed key Command, Control, and Communications (C3) centres supporting the IADS. This initial coordinated EW activity was crucial to success of the ensuing coalition air campaign. [7]

Much of the historical EW perspective is still relevant to the modern electronic battlefield. What have changed are the speed, engagement range, communications network robustness, and lethality of the modern threat. The EW community must stay abreast of developments in the threat environment to ensure that aircrew do not face the type of surprises that the Israelis faced in 1973.

1.4 EW DEFINITIONS AND SYSTEM CLASSIFICATION

This section defines EW and related terms and describes the different classifications of EW suite architecture.

1.4.1 EW and Related Definitions

The definition of EW is broadly the same internationally, although EW components' definitions differ between NATO and some of its member and partner Nations. EW is defined in NATO as: 'Military action to exploit the electromagnetic spectrum encompassing: the search for, interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum, and actions to ensure its effective use by friendly forces.' [8]

The definition of EW does not make any reference to the equipment used, but rather is confined to a description of the task or mission. For the most part, the equipment used specifically in the accomplishment of EW is avionics. This relationship between EW and avionics establishes the domain of EW T&E in the aerospace environment. Testing and evaluating EW systems requires the application of the skills and insights requisite of testing avionics equipment in general, tempered with a view of the military actions to be accomplished using these devices. The functionality and military worth of EW systems is highly role, mission, and scenario dependent.

The U.S. Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13.1 addresses EW operational applications and also considers multi-national EW coordination. This document notes that while "'NATO Electronic Warfare policy' is largely based on US EW policy, the perspective and procedures of a Multi-National Force (MNF) EW Coordination Cell (EWCC) will be new to most." [9] The reader is referred to the NATO documents: Military Committee document 64/9 and STANAG 6018, both Restricted documents, for further information regarding NATO definitions of EW and its components. [10],[11]. The U.S. definitions will be used throughout this document unless otherwise stated.

In the NATO and U.S. Joint lexicon, EW has three sub-divisions: EA, EP, and ES. While minor national variations exist across NATO and its partner Nations, this lexicon has typical definitions:

- Electronic Attack (EA) – The use of electromagnetic energy, DE, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralising or destroying enemy combat capability and is considered a form of fires. [12]
- Electronic Protection (EP) – Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of electromagnetic spectrum that degrade, neutralise, or destroy friendly combat capability. [13] EP is also known as ED, Electronic Defence.
- Electronic Warfare Support (ES) – Actions taken by, or under direct control, of an operational commander to search for, intercept, identify and locate, or localise sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. [13]

Figure 1-3 shows the three EW sub-divisions and identifies some specific applications.

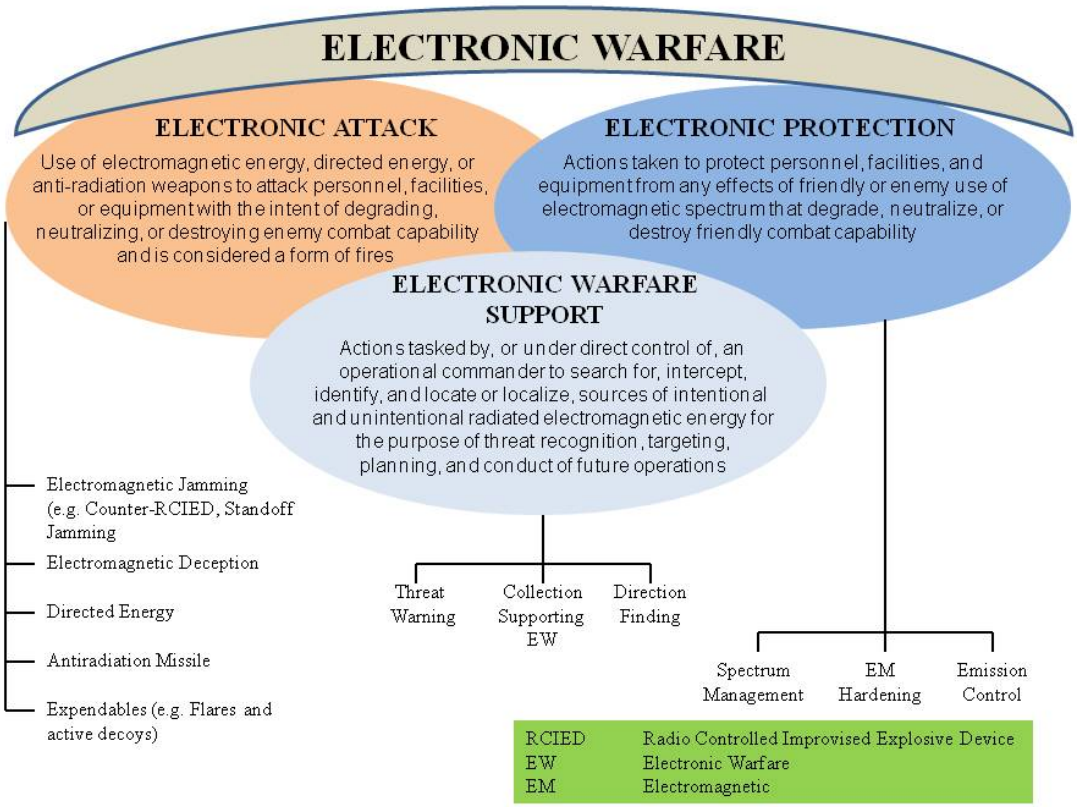

Figure 1-3: EW Sub-Divisions.

Electronic Intelligence (ELINT), Signals Intelligence (SIGINT), and Communications Intelligence (COMINT) have many similarities to ES. They are defined as:

- ELINT – Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. [14]
- SIGINT – A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted or intelligence derived from communications, electronic, and foreign instrumentation signals. [15]
- COMINT – Technical information and intelligence derived from foreign communications by other than the intended recipients. [16]

These mission areas are not considered EW under the US definition. However, the systems that perform these mission areas are functionally similar to ES systems and much of the information about ES systems and ES systems T&E in this Handbook applies to them as well.

1.4.2 EW System Architecture Classifications

There are a variety of EW system architectures in use, so it is difficult to separate them into neatly defined categories. Three general classifications, illustrated in Figure 1-4, will be used in this Handbook:

- **Stand Alone** – Each discrete EW system operates independently or nearly independently of every other EW system.

- **Federated** – Each EW system largely maintains its functional boundaries. The individual EW systems commonly share data via an EW data bus with the RWR serving as the bus controller. The individual EW systems also communicate via the avionics data bus to receive inputs such as aircraft attitude and flight data and to provide status information to the avionics system. The shared data also aids RF management; for example, the Fire Control Radar (FCR) can provide its operating characteristics such that the RWR and jammer will not process it as a threat.
- **Integrated** – All EW components, as well as other avionics systems, share common processing resources and databases. Data fusion algorithms are commonly used to enhance the information quality. Integrated systems can also schedule other aircraft system apertures and sensors to perform EW tasks, for example the FCR antenna is a high gain aperture capable of supporting secondary tasks. All controls and display information is routed by the central processor.

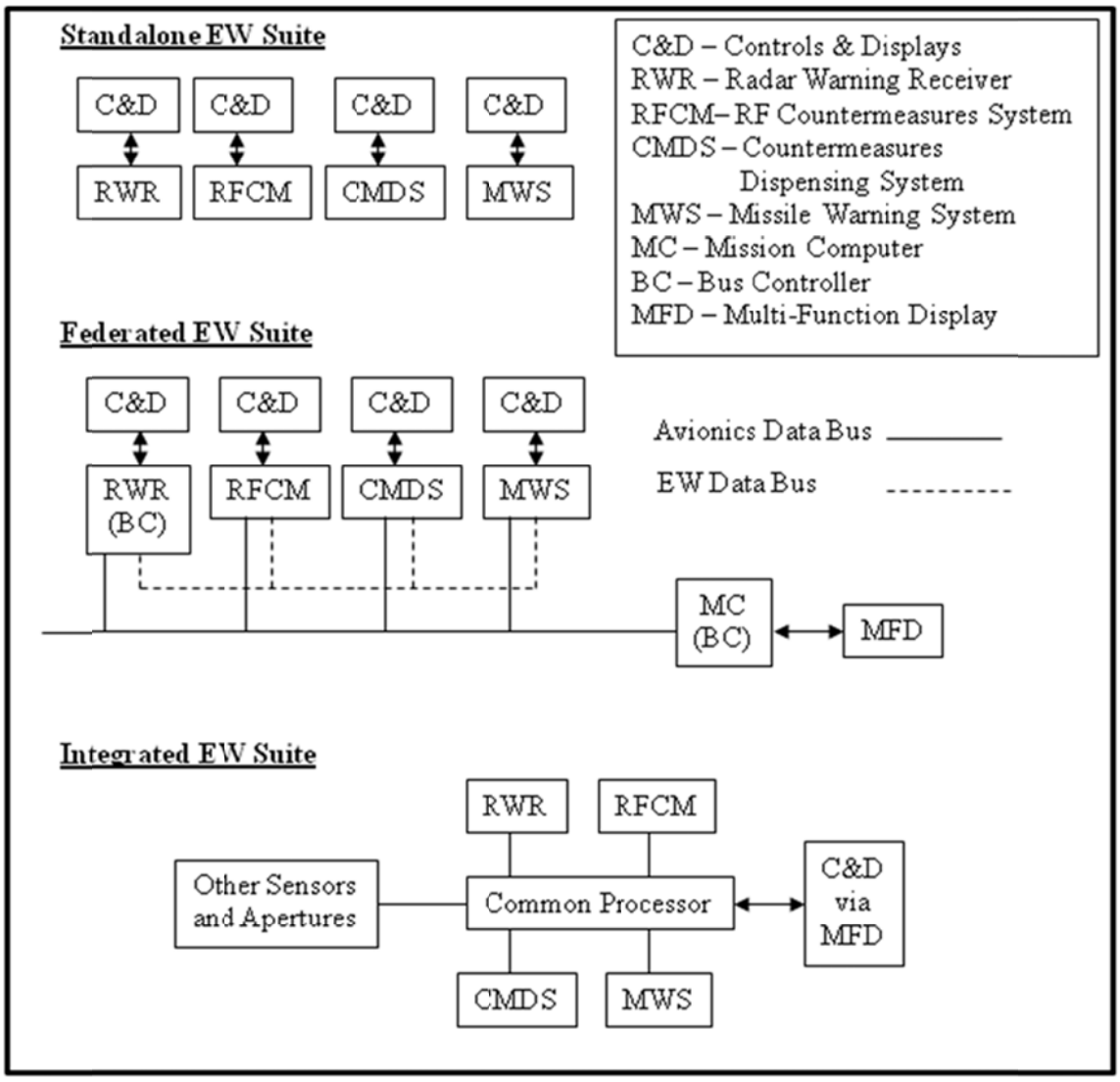

Figure 1-4: EW Suite Architecture Categories.

1.4.3 System Hierarchy

A weapon system is comprised of a number of elements. Table 1-1 identifies the individual elements and how they build up to form an entire weapon system.

Table 1-1: System Hierarchy.

Element	Description	Examples
Component	Constituent part of an LRU	• Circuit card assemblies
Line Replaceable Unit (LRU) also known as Weapon Replacement Assembly (WRA) or Module Replaceable Unit	An essential support item removed and replaced at field level to restore an end item to an operationally ready condition.	• RWR receiver assembly • RWR signal processor • RFCM transmitter
Equipment	A complete and functionally discrete piece of equipment	• RWR • RFCM System • MWS • CMDS
Sub-System	Comprised of the various equipments	• Defensive Aids Sub-System • Navigation Sub-System
System	Comprised of the various sub-systems	• Avionics System • Propulsion System
Weapon System	Comprised of the various systems	• Complete Aircraft

1.5 TEST RESOURCE CATEGORIES

EW system testing spans an enormous range starting with inspection of components and materials to be used in the manufacture of systems, and culminating with in-service support, including mission data and countermeasures validation and optimisation, problem investigation, and failure diagnosis. This Handbook concentrates on testing used to assess the capability of an EW system to comply with system-level specifications, perform its intended military role, and its potential to be serviceable and supportable in the field. These qualities are generally assessed using a combination of flight- and ground-based tests and employ a wide range of test resources.

Test resource categories applicable to EW testing include Measurement Facilities (MFs), System Integration Laboratories (SILs), Hardware-In-The-Loop (HITL) facilities, Installed System Test Facilities (ISTFs), and Open Air Ranges (OARs). A sixth resource category is Modelling and Simulation (M&S). See Figure 1-5.

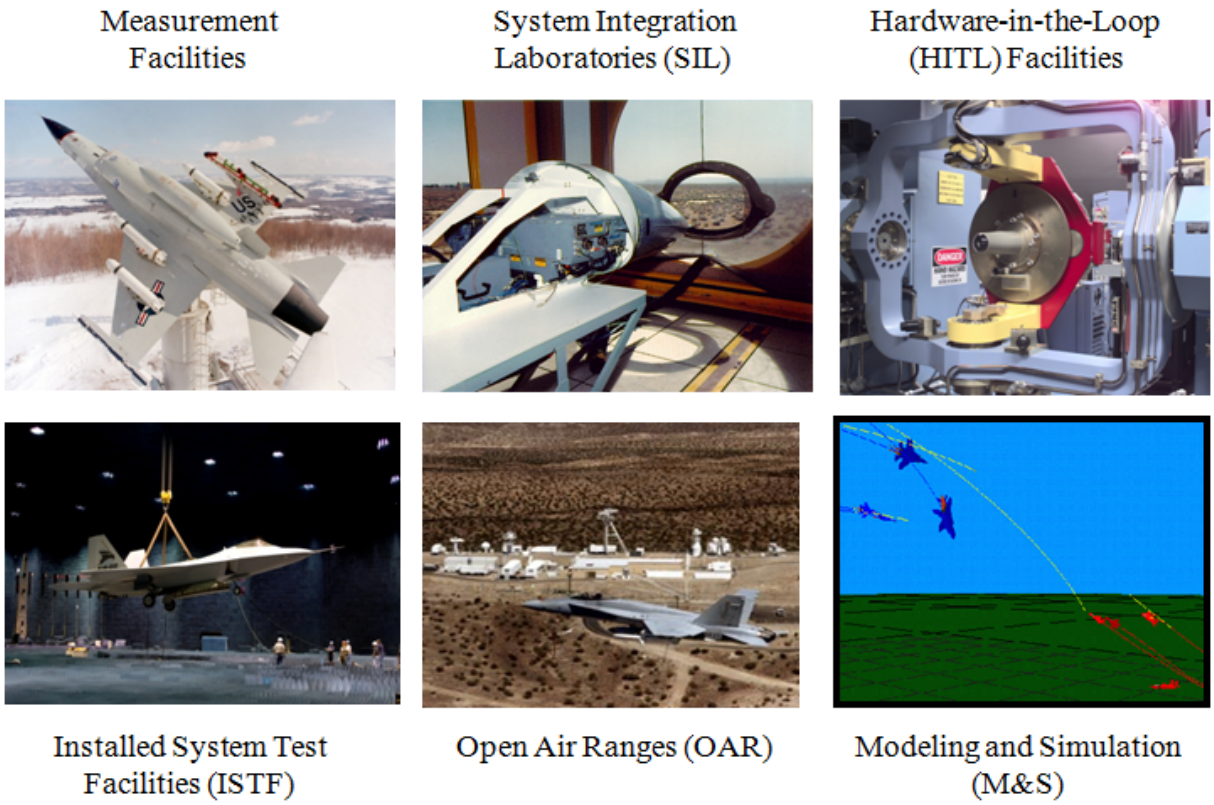

Figure 1-5: EW Test Resource Categories – (U.S. DoD Images).

It is tempting to equate 'types of tests' with specific test facilities. For instance, OARs provide an environment where aircraft can be operated in their intended flight regimes, and can often support testing of systems installed in the aircraft while the vehicle is on the ground. In this scenario, an 'installed system' type of test using an OAR resource category would be conducted.

Large anechoic chambers, capable of holding an actual aircraft, are frequently classed as Installed System Test Facilities. While this categorisation is applicable, it does not convey the full range of applications for which an ISTF may be suitable. Frequently, ISTFs are used to support HITL tests, integration activities, and simulations. If the resource category description is used to define the test types that the resource can support, there is a risk of inaccurate or incomplete understandings of the T&E value of many test resources.

This Handbook will use the term Test Resource Category to identify the primary role of a specific test facility and will use Test Type to reference the various levels of testing and system integration that may be accommodated at a given facility.

1.6 THE ACCEPTANCE PROCESS AND TYPES OF TEST

EW equipment manufacturers and Platform Systems Integrators (PSI) must ultimately prove that their system or systems meet the contractual specification requirements. The details of the process vary by country; however there are some common elements. The contractual requirements are typically tabulated in a matrix identifying the particular requirement, the acceptance method, and the venue for the activity. Table 1-2 identifies and defines the type of verification and the methods. [17]

Table 1-2: Verification Types and Methods.

TYPE	METHOD
Inspection	• Physical inspection, visual verification • Document review • Read-across by analogy, where prior evidence alone is used to fulfil a requirement
Analysis	• M&S, e.g., mathematical, statistical, physical • Read-across by evaluation, where prior evidence is used to partly fulfil a requirement • Technical evaluation of equations, charts, reduced and/or representative data
Test	• Laboratory – software test, rig test (by equipment manufacturer/supplier) and rig test (by manufacturer/supplier or Platform Systems Integrator – PSI) • Anechoic chamber (specialist equipment) • Aircraft ground test, e.g., Electromagnetic Compatibility and Interference (EMC/EMI) • Flight test – local or dedicated EW range
Demonstration	• Un-instrumented rig or aircraft test where requirement is met by observation alone

There is a hierarchy of test types which must take place in order to quantify the overall performance of the SUT. This sequence of T&E events tends to mirror the overall maturing of the SUT as it progresses through the development process.

Figure 1-6 depicts this process and helps to characterise an important attribute of the test process. It is a purposefully recursive process that continually refines the estimated performance of the SUT as it reaches higher levels of integration and maturity. Such a deliberate process may be difficult or even impossible to achieve due to fiscal, schedule, or test facility constraints. Each of the desired test events represents an opportunity to help reduce risk in developing the EW system. Here is where the tester's experience and application of statistically sound methods can construct a test programme that optimises the use of test resources while meeting budget and schedule constraints. Ultimately, the tester provides decision makers with quantifiable information about programme technical risks.

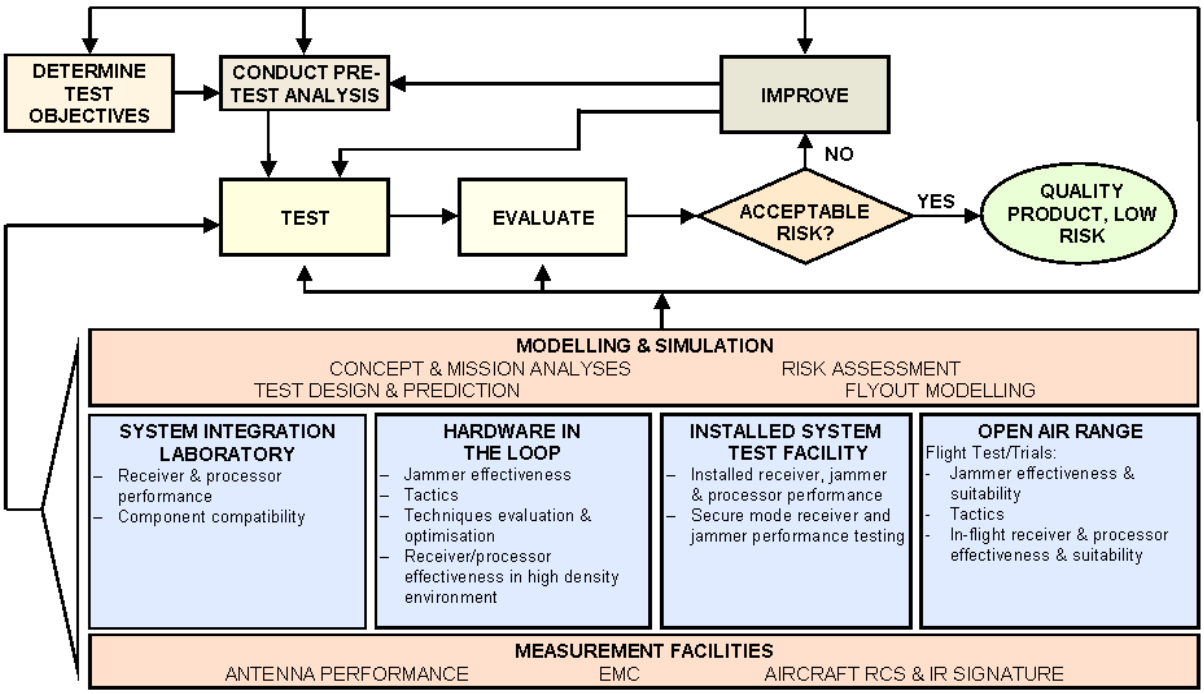

Figure 1-6: The EW T&E Process.

Some of the choices may not be obvious. For instance, flight testing is generally considered to be a more complete test than those events accomplished in an HITL or ISTF. The experienced tester, however, may determine that due to limitations of threat simulators available on the OAR, he can actually create a more realistic test scenario in an ISTF. This particular type of choice is frequently encountered when testing the effects of high threat or signal density. Most OARs are very limited in the quantity of threat simulators they can provide. On the other hand, HITLs and ISTFs can most often simulate very large numbers of threat signals with adequate fidelity.

1.7 EW SYSTEM APPLICATION IN WARFARE

As discussed earlier in this section, EW can be broken down into three primary divisions: EA, EP, and ES. While it is not the intent of this Handbook to fully describe the role of EW in military operations or to provide a detailed analysis of specific EW techniques, a brief overview of each of these primary divisions is given below to underpin a better understanding of the test requirements.

1.7.1 Overview of EA

EA is the use of electromagnetic or directed energy to attack personnel, facilities, or equipment. There are five basic sub-divisions of EA: jamming, deception, DE, ARM, and expendables. Jamming is generally defined as deliberate radiation, re-radiation, or reflection of energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum. With recent advances in technology and more frequent use of spectra outside the RF range, this definition can be extended to cover similar action against IR, Ultraviolet (UV), and electro-optical systems.

Jamming is the most prevalent form of EA and has two major sub-divisions: self-protection and support. In self-protection jamming, also known as defensive EA, the same vehicle being targeted by the enemy radar or sensor system carries the EA system. Support jamming, also known as offensive EA, has three sub-categories: stand-off, stand-in, and escort. In stand-off jamming, the EA platform normally operates

beyond the engagement range of the enemy air defence system and jams the surveillance elements of the air defence system in support of other attacking aircraft. Stand-in jamming is similarly directed at the surveillance elements of an enemy air defence system, but operates within the range of enemy air defence weapons. Stand-in jamming is normally performed by Unmanned Air Systems (UAS)[1]. In escort jamming, the jamming aircraft accompanies the strike package it is charged with protecting. This means that the escort jamming aircraft must have performance and range similar to the strike aircraft.

There are basically two types of enemy radar that must be jammed by EA:

- Surveillance radars perform two basic functions in an IADS: early warning, which provides overall situational awareness for forming the air picture, and target acquisition for terminal threat systems.
- Radars associated with the terminal threat systems, typically those performing target tracking and missile guidance. Terminal threat radars are usually given high priority in the hierarchy of EA threats because they are associated with the lethal phases of a weapon guidance system.

EA jamming techniques are used to disrupt or break the threat's range, velocity, or angle tracking capability and force the threat system to re-acquire the target and re-aim the weapon – a process which could provide the target the time to pass harmlessly through the threat's engagement envelope.

EM deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial enhancement, or reflection, of EM energy in a manner intended to convey misleading information to an enemy or to an enemy's EM-dependent weapons, thereby degrading or neutralising the enemy's combat capability.

DE is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or sub-atomic particles. The two most common manifestations of DE are High-Energy Lasers (HELs) and High-Power Microwave (HPM) devices.

ARMs are designed to home on RF emissions from enemy radar systems. These missiles aim to either destroy the targeted radar system or at least force it to cease operating to avoid destruction. These air-launched weapons normally receive targeting information from ES receiver systems on board the host platform. It is beyond the scope of this Handbook, but it is important to realise that these and other weapons systems are increasingly able to tap into networked systems that can provide targeting information from other sources via data links.

Expendable countermeasures are deployed from a host platform and normally perform self-protection functions. The three most common expendable countermeasures types are chaff, flares, and towed decoys. Chaff can be employed against search radars or as self protection against Target-Tracking Radars (TTRs) and missile guidance radars. Chaff is dispensed in bundles composed of many thousands of very thin conductive elements designed to reflect RF energy and confuse the victim radar. Flares are designed to protect aircraft from IR-directed threat systems by providing a more attractive target to the missile seeker than the targeted aircraft. Towed decoys attempt to provide the threat system a more attractive target than the platform they protect.

In addition to the above elements of EA, Emission Control (EMCON)[2], and Low Observable (LO) techniques are considered passive forms of EA. [18]

---

[1] UAS, which also means Unmanned *Autonomous* Systems, include UAVs (Unmanned Aerospace Vehicles) and UCAVs (Unmanned Combat Air Vehicles).

[2] EMCON is according to some sources a form of EP and will be treated as EP for the remainder of this handbook. [18]

1.7.2 Overview of EP

EP is that action taken to negate the effects of either enemy or friendly EA that would degrade, neutralise, or destroy friendly combat capability. EP techniques tend to be the result of developments of EA capabilities. Most EP techniques are defined in relation to how they counter a specific EA threat. Usually, the EP technique is some improvement in the sensor system design that counteracts the effect of a specific EA technique; therefore, it is difficult to understand the purpose of a specific EP technique without knowing the EA technique that it is designed to counteract. EMCON is also a form of EP. [19]

Usually, the design requirements of a system that operates in a jamming environment will exceed the requirements of a similar system designed to operate only in a friendly environment. For example, a radar receiver designed for use in a civilian environment can tolerate relatively wideband frequency response with only minimal degradation in performance. A similar receiver designed for use in a jamming environment would require narrowband frequency response to prevent skirt jamming.

The EP designer may utilise sophisticated transmitted waveforms and receiver processing that will make deception jamming difficult. This forces the enemy to use high-power, brute-force noise jamming. The EP designer can then use frequency hopping or multiple simultaneously transmitted frequencies so that the enemy must broaden the bandwidth of his jamming. This causes the enemy jammer to diffuse its energy over a wide bandwidth, thus reducing the effectiveness of the EA. A true, never-ending cat-and-mouse game between EA and EP designers then follows.

1.7.3 Overview of ES

ES is that division of EW concerned with the ability to search for, intercept, identify, and locate sources of radiated electromagnetic energy. ES is used in support of tactical operations for situational awareness, threat avoidance, homing, and targeting. Onboard radar warning and missile warning receivers, as well as many off-board surveillance systems, are considered elements of ES.

1.8 THE EW T&E PROCESS

The EW test process, as depicted in Figure 1-6, requires a disciplined approach to ensure that the required testing is accomplished in a timely and cost-effective manner that ultimately provides acquisition programme decision makers with accurate information about the SUT. The most important part of a test programme is determining the test objectives. The test objectives get to the heart of what is to be accomplished and thereby determine the direction and scope of the programme. If the test team doesn’t get the objective right, the programme runs a significant risk of not generating the necessary information to support programmatic decision making. The test objectives need to be coordinated between programme management and the test team to ensure that all participants understand the relationship between the financial resources available and the quality of information provided. A vital role of professional testers is to convey risk assessments to programme managers when financial resources are constrained and advise them on options.

1.8.1 Test Objectives

Test objectives derive from two basic sources: documented operational requirements of the military end user and contractual specification requirements. Ideally, these would be identical, but they sometimes differ in practice. The system programme office charged with acquiring the weapons system typically contracts with the manufacturer to provide specific quantifiable data about the performance of the acquired system. Test professionals representing the government generally participate in the Developmental Test and Evaluation (DT&E) phase to provide the programme office with an independent evaluation of the weapons system’s performance relative to specification requirements. DT&E is defined as any testing used to assist in

the development and maturation of products, product elements, or manufacturing or support processes. It is also any engineering-type test used to verify status of technical progress, verify that design risks are minimised, substantiate achievement of contract technical performance, and certify readiness for initial Operational Testing (OT). Development tests generally require instrumentation and measurements and are accomplished by engineers, technicians, or soldier operator-maintainer test personnel in a controlled environment to facilitate failure analysis. [20]

Additionally, the DT&E community must address military utility aspects of the SUT performance that are not addressed by the specification requirements. The role of DT&E above and beyond specification compliance assessments reduces the risk of finding problems in Operational Test and Evaluation (OT&E) that could preclude fielding the weapon system.

OT&E is the field test, under realistic conditions, of any item (or key component) of weapons, equipment, or munitions for the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users; and the evaluation of the results of such tests. [21] Test programmes that coordinate DT&E and OT&E throughout the programme's life greatly enhance their chance of successfully completing OT&E and fielding the weapons system.

Large acquisition programmes typically have a hierarchy of test objectives. A large programme charged with acquiring a new airframe that employs a number of potentially integrated sub-systems might have as an overall test objective: "Evaluate the performance of the F-XX aircraft". It could then have subordinate level test objectives such as: "Evaluate the defensive avionics suite", or "Evaluate the fire control radar system", etc. Further, an objective to evaluate the EW systems of an aircraft could be broken down into its components: "Evaluate the RWR performance", "Evaluate the expendable countermeasures system", etc. A small programme might have only a single stand alone objective, such as "Evaluate the performance of a new countermeasures flare". In any event, it is important that the EW tester be aware of how test objectives fit into the overall test programme.

1.8.2 Test Design

The DT&E test designers must ensure that two questions are answered. First, the test must determine if the manufacturer has met each of the contractual specification requirements. Second, the system must be evaluated to determine if the military utility is adequate to proceed to dedicated OT&E. It is possible for a system to meet all specification requirements but have sufficient military utility deficiencies to preclude a release to begin dedicated OT&E. OT&E testing is conducted under operationally realistic conditions to determine if the system is effective and suitable.

Figure 1-7 shows the main elements of test design. The programme objectives address both the specification compliance and the military utility and once they have been established, the test team must determine the measures by which the system performance or effectiveness will be evaluated. These are known as Measures Of Performance (MOPs) and Measures Of Effectiveness (MOEs). The MOPs are generally more applicable to DT&E and are generally tied directly to contractual technical performance requirements while MOEs apply to OT&E. This Handbook primarily addresses DT&E and will use the term MOP generically when discussing performance measures.

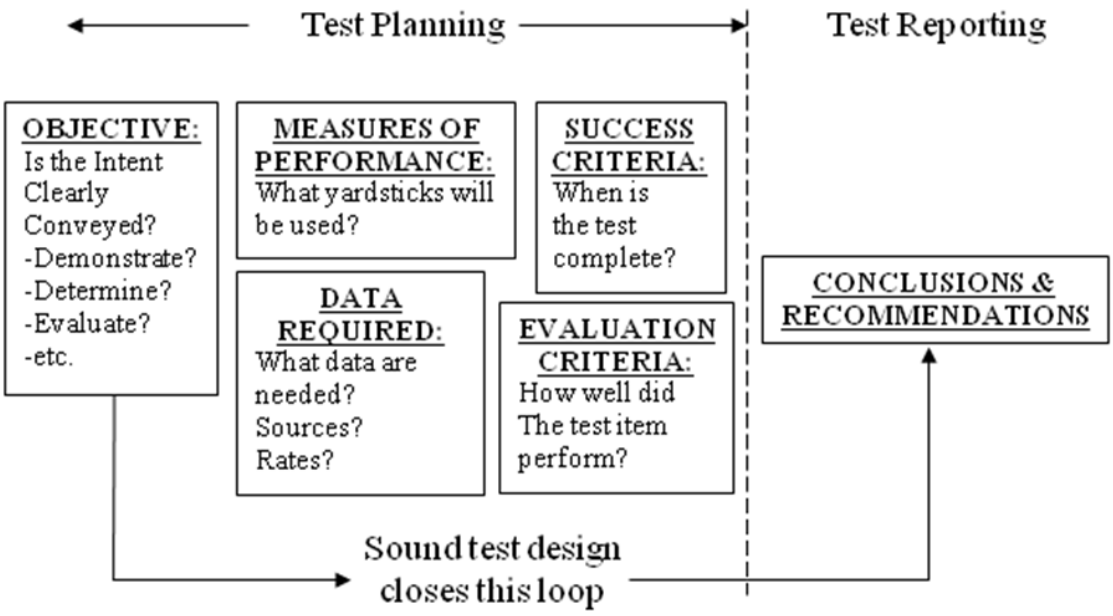

Figure 1-7: Test Design Elements.

The objectives must be testable, that is, the selected MOPs must be quantifiable attributes of the system that directly relate to operationally relevant functions. A specific type of MOP is the Critical Technical Parameter (CTP); the CTPs are parameters deemed vital to the desired capability of the weapon system. Two examples for an RWR include response time which relates directly to the warning time the system will provide the aircrew or angle of arrival measurement error which relates to the quality of the warning information provided. Note that MOPs are always nouns: time, error, etc.

Annex B discusses some common MOPs, to assist understanding measurements and what information they convey. It is intended to make the reader think about what details need to be addressed and documented in the planning stages, to avoid disagreements later in the programme when they are generally more difficult and costly to resolve.

System acquisition programme managers should involve experienced testers early in the system specification or contractual requirements development process. Experienced testers know what system attributes are meaningful, testable, and measurable. If a system attribute cannot be quantified or quantified in a useful manner, it is worthless.

Once the test objectives have been established and the MOPs identified, the amount of data required must be determined in order to estimate the values of the MOPs. This is critically important to programme managers because the amount will dictate the length and cost of the test programme.

Even the best designed tests only yield estimates of the true values of the SUT's measures of performance. MOPs are random variables generated from finite data samples. Therefore, it is impossible to establish the true value of a given MOP. A typical test will produce an estimate of the average value of an MOP, i.e., the mean or median and spread of the data, commonly expressed as the variance or the standard deviation. This means that each time a data set is collected it will produce a different result.

Many EW performance specifications are based on whether or not the estimated value of a MOP, such as response time, meets a required value. Even a well-conceived and executed test can result in a spread of the data collected. This implies that occasionally the estimated value will be sufficiently in error that the wrong conclusion about the system's performance may be drawn.

A key role that T&E professionals play on the acquisition team is to quantify the risk of such an error occurring and communicating that information to the decision makers prior to the test. This will ensure that decision makers understand the relationship between the resources expended and the quality of the answers that will be provided and ultimately the risk they will be accepting.

For example, if the response time contractual specification requirement for an RWR against a given threat radar beam is X seconds, the test team needs to design a test procedure to test the hypothesis that the system meets the specification requirement; the null hypothesis is that the system response time is less than or equal to X seconds. The hypothesis test can have four possible outcomes as shown in Figure 1-8.

		True (Unknown) State of SUT	
		System Meets Specification Requirement	System Does Not Meet Specification Requirement
Programmatic Decision	System Does Not Meet Requirements	Type I error – Rejected a Good System	Correct Decision
	System Meets Requirements	Correct Decision	Type II error – Passed a Bad System

Figure 1-8: Types of Decision Error.

Basically, a Type I error occurs when a ‘good’ system is incorrectly rejected for failing to meet the performance specification requirement and a Type II error occurs when a ‘bad’ system is incorrectly accepted as having met the performance specification requirement. There are many excellent references on the statistical techniques of determining probabilities. A typical approach is to specify the probability of a Type I error (the significance level of the test) and design the test procedure such that the probability of incurring a Type II error is acceptably small (this determines the power of the test). [22] Generally, the likelihood of incurring Type I or Type II errors can be reduced by increasing the sample size. Experimental design techniques can optimise the quality of information provided for given cost and schedule constraints.

When a mismatch occurs between the objective of the test and the resources available, the test team needs to work with programme management to bring the objectives and the resources into alignment. If the programme is under-resourced and the risk of incurring Type I or Type II error is deemed to be too great, programme managers can either provide additional resources to bring the risk up to an acceptable level or they can modify the objectives. Conversely, if the risk analysis shows a low risk of incurring Type I or Type II errors, programme managers might choose to reallocate the resources to other higher risk programme elements.

1.8.3 Programme Tailoring, Phasing, and Regression Testing

The purpose of a DT&E test programme is to ensure that the SUT meets all of its critical specification and military utility requirements, and is ready to begin dedicated OT&E. The test team must construct a test

programme that tailors the test objectives to the most cost-effective resources for accomplishing them. For example, if a test objective can be satisfied using a laboratory facility this will almost always be timelier and less expensive than accomplishing it in-flight on an OAR.

Testers should be aware that testing described in previous sections does not usually occur in a linear fashion. Each programme has unique requirements and related test objectives that drive where, how much, and in what order testing will occur. For example, most programmes require multiple SIL entries to check out hardware, software, and mission data changes throughout the programme.

SUT maturity is a major driver in determining which resources are needed. A new acquisition programme will likely employ multiple iterations of all types of test resources. Alternatively, a mature system with developed hardware and software being installed on a new aircraft would employ resources focusing on airframe installation effects and avionics integration. Most major acquisition programmes employ block cycle upgrades or other scheduled incremental capability deliveries. When these new capabilities are delivered the test philosophy should address two aspects: evaluating the newly delivered capability and performing regression testing to ensure that existing capabilities have not been inadvertently degraded.

Sequential testing using lower cost resources to validate performance before progressing to more expensive and less available resources is good risk management practice. If deficiencies are identified in the course of using less expensive test resources, they can be resolved before moving on to higher-cost, higher-fidelity test resources. The test strategy should always aim to find problems as early as possible in the programme using the most cost-effective resources.

Regression testing is a critical risk-mitigation component of a well-designed test programme. Regression testing is performed to ensure that when a change is made to one part of the system other performance aspects of the system have not been unintentionally degraded. Since the incremental approach is a planned activity, regression testing should be built into the schedule. Failure to properly plan for and conduct regression testing can result in lengthy and costly changes late in the programme.

1.8.4 An Integrated Test Approach

The system programme office has the overall responsibility for weapons system acquisition and ensuring that an integrated test programme occurs. There are two aspects to an integrated test approach. The first is organisational and deals with integrating the objectives of the stakeholding parties: the contractor, the government DT&E organisation, and the operational test agency. The second deals resource integration, i.e., ensuring that resources and facilities are employed in an efficient, cost-effective manner that avoids unnecessary duplication of effort. Figure 1-9 shows the resource categories and some examples of the types of activities that they support.

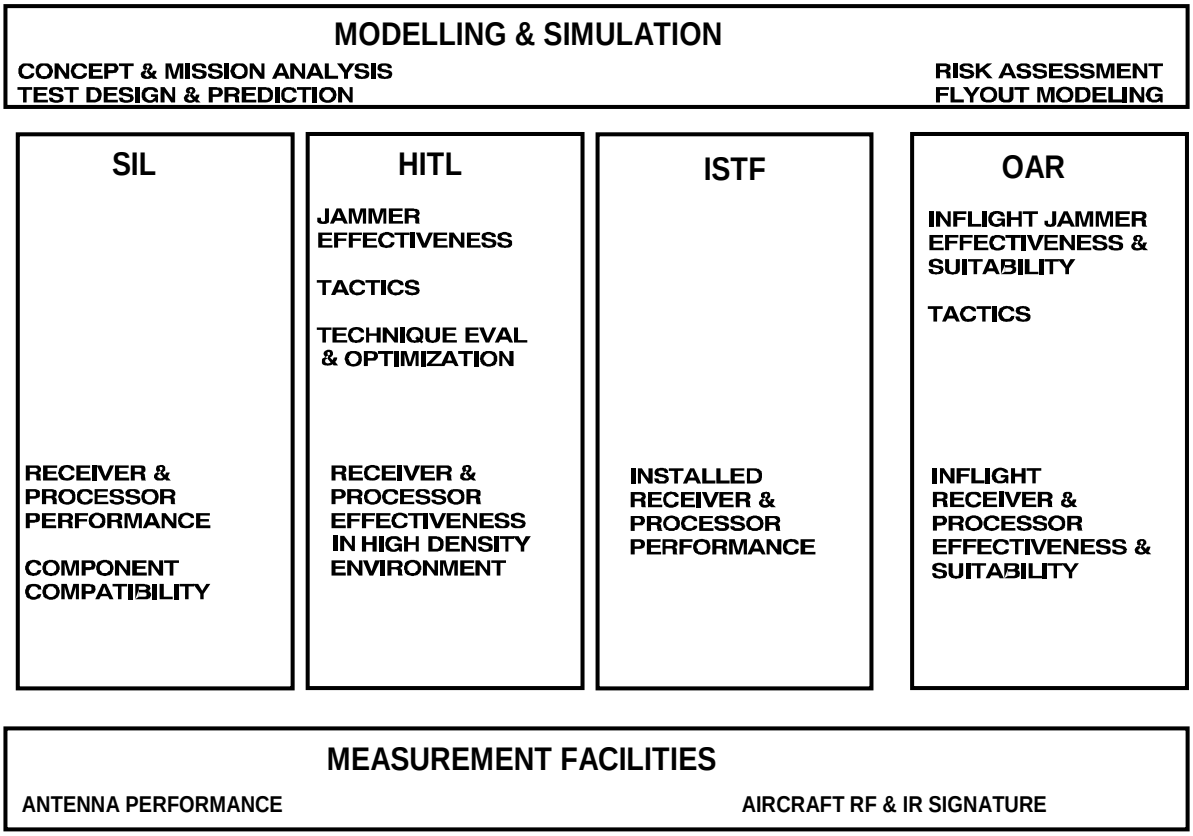

Figure 1-9: EW T&E Resource Category Examples.

The test community has a wide variety of resources available to address the established test objectives. Test managers must construct a test programme that optimises the employment of test facilities and resources to cost-effectively execute the test while maintaining technical credibility. Most test programmes will require the use of more than one facility or resource, frequently with more than one iteration. The more complex the development effort, the greater the facility or resource utilisation will be.

A typical RWR programme illustrates how a test programme should be tailored. Take the case where a new RWR is being developed for a fighter aircraft. This will involve nearly every type of resource available to the test community, starting with M&S to model antenna patterns, and detailed development testing at the contractor's facility, all the way through OAR testing.

Contrast this with the case where several years later after the RWR is fielded on the fighter platform, the same RWR is chosen to equip a transport aircraft. In this case, the RWR hardware and software are already developed. A new installation on a different platform will involve new antenna locations, and possibly new antennas. It will need to interface with a different avionics system. Also, the mission requirements of the transport aircraft will be different than the fighter aircraft and will necessitate different Mission Data Files (MDFs). Since the hardware and software are mature, the testing should focus on the risk areas specific to this programme such as installation, integration, and mission-unique attributes.

In some cases, test resources might not be available to meet the requirements of a test programme. This sometimes occurs when emerging technology outpaces the capabilities of existing test resources. In that case, the programme office might need to develop new test capabilities. Note that development and upgrading of test facilities is, in general, a lengthy process. There is a need for facility operators to identify potential future test requirements as far ahead as possible to maximise facility availability for testing.

1.8.5 Data Reduction and Analysis

The test itself only provides data, observations, and information to be subsequently evaluated. The bridge between testing and evaluation is data reduction. Often, this step is thought to be a simple act of feeding data to the computers and waiting for the output to appear on the engineer's desk. Experienced testers know differently; they are fully aware that factors such as selection of data, editing of outliers, and determination of statistical processes to be applied to the data can have a major effect on the outcome of the evaluation. A thorough understanding of experimental statistics is a prerequisite for the successful evaluation of any EW system.

1.9 EW T&E RESOURCE UTILISATION

1.9.1 Relative Cost

In general, the cost per test becomes higher as the testing moves to the right, as shown notionally in Figure 1-10. The use of models, simulations, and ground testing can reduce overall test costs since flight tests are the most costly.

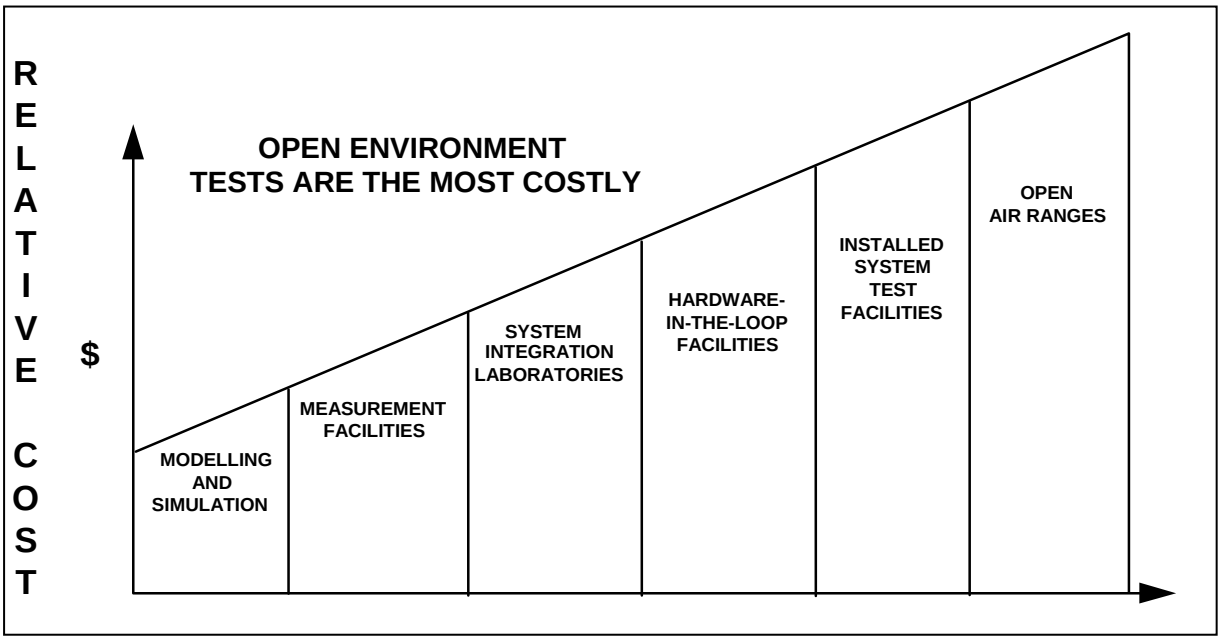

Figure 1-10: Relative Cost – T&E Resource Utilisation.

1.9.2 Relative Use

Due to the complexity of EW systems and threat interactions, modelling and simulation can be used in a wide range of progressively more rigorous ground and flight test activities. Figure 1-11, also notional, shows that M&S and MF are used throughout the test spectrum. It also shows how the number of trials/ tests should decrease as the testing proceeds through the categories.

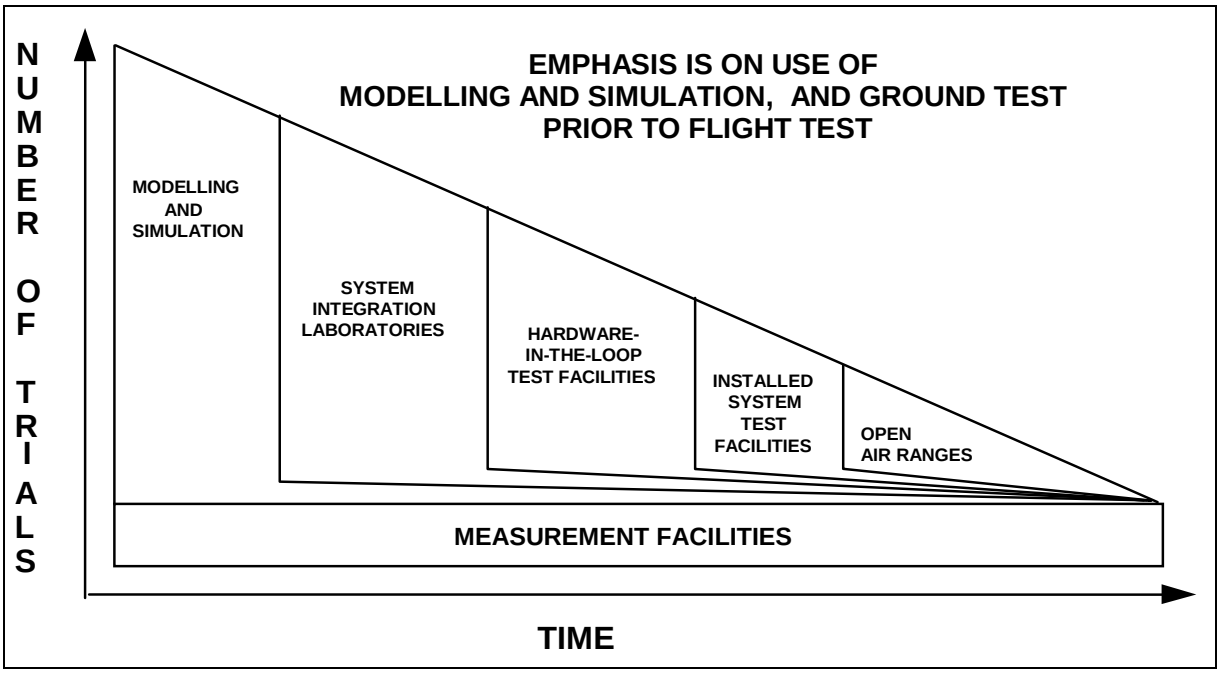

Figure 1-11: Relative Use – T&E Resource.

The key issue is to optimise cost, time, and risk of successfully gathering test evidence that allows SUT, system, and platform off contract and into operational use. To attain this two driving themes are:

- Move as much testing to the left of the development programme, i.e., from flight test to anechoic chamber ISTF and MF, and to M&S that has been subject to adequate Verification, Validation and Accreditation (VV&A).
- Only do in flight those tests that cannot be adequately achieved by ground test.

1.10 SAFETY CONSIDERATIONS

Specific safety procedures must be developed and observed for each type of test in each type of facility. The following hazards required particular attention when considering the T&E of EW systems.

1.10.1 Electrical Shock Hazards

Many EW systems utilise high-power transmitters requiring high-voltage excitation for the final output stages. In addition, nearly all EW systems make use of either 115 VAC or 28 VDC electrical power for operation. While these power sources are generally well protected when the system is installed in its operational configuration, they may be exposed and easily contacted during test activities. This is particularly true in the HITL and SIL environment.

1.10.2 Radiation Hazards

Effects of human exposure to high-intensity RF fields can vary from minor reddening of the skin to severe and permanent damage to internal organs. High power radiation can also cause equipment damage. The most common opportunity for such damage is in anechoic chambers. The Radar Absorbent Material (RAM) used in these chambers will absorb rather than reflect the RF energy from the systems in operation. The absorption of energy causes heating of the RAM. As a result, power levels must be carefully monitored

and constrained to levels below that at which the heating of the RAM will result in toxic smouldering or fire. Radiation hazards can exist in all test environments but are most frequently encountered in the ISTF and OAR testing phases.

1.10.3 Pyrotechnic Hazards

EW expendables such as chaff and flares typically rely on pyrotechnic (explosive) devices for ejection. One can easily imagine the results of an inadvertent firing of these devices during ground maintenance or test operations. Also, EW pods carried on centreline or wing stations of aircraft are usually capable of being jettisoned. Unintended firing of the explosive charges that initiate the jettison sequence may result in both personnel injury and equipment damage. These pyrotechnic hazards are most likely to occur during ground test or preparation for flight test in the OAR testing phase.

1.11 THE TEST PLAN

All test activities require careful planning to be successful. Test plans come in a multitude of forms and formats, each created to ensure a specific requirement or group of requirements are satisfied in the most complete and efficient manner possible.

1.11.1 Cost and Test Budget

Adequate budgeting for each test event is critical. It is difficult to accurately predict the cost of an unplanned or poorly planned activity. Early in the programme when test events are not clearly specified, the budgeted cost for testing will likewise be only a rough estimate. The sooner more complete test planning is accomplished, the sooner the test budget can be accurately determined. Generally, as the programme progresses, the potential for acquiring additional funding is reduced. Poor budgeting at the beginning of the programme will nearly always result in cost overrun or severe constraints on test execution and failure of the test effort to deliver the required information.

1.11.2 Schedule

As with the budget, the schedule for testing is affirmed through the development of detailed test plans. Test facilities that are needed to accomplish the desired testing may have full schedules. Access to the required facilities when needed is greatly increased if detailed test planning is accomplished early and this cannot be over-emphasised.

The schedule tends to be a major driver for the budget. Inaccurate schedule projections will generally lead to budget problems and, in the end, failure of the test programme to deliver the required information.

1.11.3 Test Efficiency

Accomplishment of test events in the optimal sequence can substantially reduce the amount of retest or regression testing required. Test planning is the primary tool to understand and analyse the best sequence of events. It is also the process where experienced testers accomplish the trade studies to assess how programmatic risk will be affected by the elimination or insertion of test events.

1.11.4 The Bottom Line

It is the test planning process that permits a logical sequence of test activities with reasonable expectations at each stage. Data reduction and analysis, safety, and certainly a meaningful evaluation are all virtually useless (and probably impossible to accomplish) without a carefully developed test plan.

1.12 TRAINING – A KEY TO SUCCESS

This Handbook primarily covers the EW T&E process and its underpinning facilities, tools and techniques. It must be recognised, however, that if the staff (engineers and other) involved in these areas do not have sufficient skill and experience, then the goal of programmes with minimum cost, duration and risk will be unattainable.

The EW T&E field is a complex one, requiring high levels of specialism and experience in a number of sub-disciplines *inter alia* microwave and optical engineering, mission systems engineering, platform design and development, electromagnetics, and rig and on-aircraft T&E.

EW and T&E training is therefore of great importance if the above goal is to be met. A number of Nations and agencies run EW and EW T&E courses that can satisfy this requirement. It has been shown that such training is a great experience accelerator for novices, allowing them to function at a much higher level than would otherwise be possible. This training can also enable experienced T&E engineers to solve difficult T&E problems and make contributions to their programmes by applying detailed technical knowledge obtained from the training. [23]

1.13 REFERENCES

[1] Price, A., “The History of US Electronic Warfare, volume 1”, The Association of Old Crows, September 24, 1984, pp. 1-2.

[2] Price, Vol. 1, pp. 12, 26.

[3] Pheasant, V.A., “Window on Gomorrah”, J. Electronic Defense, Vol. 26, No. 7, July 2003, pp. 56-59.

[4] Price, A., “The History of US Electronic Warfare, Volume II”, The Association of Old Crows, October 2, 1989, pp. 43-109.

[5] United States Air Force Doctrine Center, Air Force Doctrine Document (AFDD) 2-5.1, “Electronic Warfare”, 5 November 2002, p. 14.

[6] Rich, B. and Janos, L., “Skunk Works”, Boston, MA, Little, Brown and Company, 1994 (ISBN 0-316-74330-5), pp. 24, 85, 97-105.

[7] AFDD 2-5.1, p. 26.

[8] AAP-6 (2010): NATO Glossary of Terms and Definitions (English and French), 22 March 2010.

[9] United States Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13.1, “Electronic Warfare”, 25 January 2007, p. V-3. www.fas.org/irp/doddir/dod/jp3-13-1.pdf (Accessed 26 September 2011).

[10] NATO Military Committee (MC), MC 64: NATO Electronic Warfare Policy.

[11] NATO STANAG 6018: Allied Joint Electronic Warfare Doctrine – AJP 3.6(A). 5 February 2004.

[12] JP 3-13.1, p. I-2.

[13] JP 3-13.1, p. I-4.

[14] JP 3-13.1, p. GL-8.

[15] JP 3-13.1, p. GL-13.

[16] JP 3-13.1, p. GL-5.

[17] "Encylopedia of Aerospace Engineering (2010)", Edited by Richard Blockley and Wei Shyy. John Wiley & Sons, Ltd. (ISBN: 978-0-470-75440-5). Volume 7, Chapter 376 – Pywell, M. Electronic Warfare and Defensive Aids Systems Design and Development.

[18] AFDD 2-5.1, p. 8.

[19] JP 3-13.1, p. I-4.

[20] Defense Acquisition University, "Glossary of Defense Acquisition Acronyms & Terms", 12th Ed., Defense Acquisition University Press, Fort Belvoir, Virginia 22060-5565, July 2005, p. B-50.

[21] "Glossary of Defense Acquisition Acronyms & Terms", p. B-115.

[22] Montgomery, D.C., "Design and Analysis of Experiments", Hoboken, NJ, John Wiley & Sons, Inc., 2009 (ISBN 978-0-470-12866-4), p. 35.

[23] Welch, M.J., The Electronic Warfare Test & Evaluation University. U.S. Air Force T&E Days, 5-7 February 2008, Los Angeles, California, AIAA 2008-1602.

1.14 FURTHER READING

NATO Terminology Management System and Database (NTMS and NTDB). http://nsa.nato.int.

Joint Doctrine Publication 0-01.1 United Kingdom Supplement to the NATO Terminology Database. 8th Edition, September 2011.

Price, A., "The History of US Electronic Warfare, Volume III", The Association of Old Crows, September 2000 (ISBN 0-9703794-0-4).

"Jane's Radar and Electronic Warfare Systems 2011 – 2012". Jane's Information Group. ISBN: 978-0-710-62967-8.

"Encyclopedia of Aerospace Engineering (2010)", Edited by Richard Blockley and Wei Shyy. John Wiley & Sons, Ltd. ISBN: 978-0-470-75440-5. Volume 7, Chapter 376 – Pywell, M. Electronic Warfare and Defensive Aids Systems Design and Development.