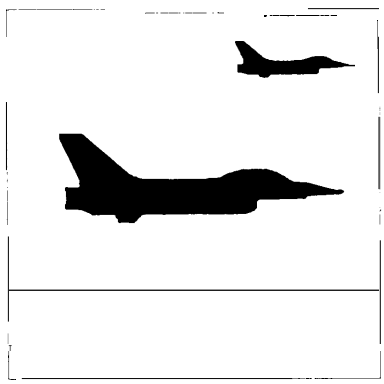
Avoiding Fratricide of Air and Sea Targets

4

As described in the previous chapter, reducing fratricide requires more than improving identification. This chapter discusses ways to improve both tactical knowledge and identification to avoid air fratricide. There are several technical approaches to better identification; each of these is described briefly below with a discussion of its advantages and disadvantages. The chapter ends with a discussion of the interaction of military identification systems with civilian air traffic control and a brief discussion of avoiding fratricide of ships.

BATTLE MANAGEMENT

"Battle management' includes collecting information about where combat resources are needed, setting priorities, and allocating resources to needs. The tactical knowledge or ''situational awareness' provided by battle management is so integral a part of air combat that its importance to avoiding fratricide is easily overlooked, Yet the foremost antifratricide measure is properly coordinating friendly forces.



Any efforts that improve coordination also improve combat effectiveness—and that typically is their primary justification—but these same efforts can help reduce fratricide. The Navy and the Air Force discovered during joint operations in the Persian Gulf War that air tasking orders (ATOs) were difficult to transmit between the Services' strike planners. Air Force and Navy radios were not always compatible and the ATOs were so voluminous that transmission was time ,consuming. These and other uncovered communication problems are now being corrected. The resulting improvement in attack efficiency will be obvious, but better communication and coordination also will make fratricide less likely.

At the tactical level, long-range surveillance can sometimes track an enemy airplane from the moment of takeoff. If a fighter can be seen taking off from an enemy airfield, few would argue with the assumption that it is an enemy airplane. This capability is partially in hand today with the AWACS. The limitations of the system are range and, more importantly, tracking. Once the enemy airplane gets close to a friendly airplane the radar may no longer see them as separate targets or the radar may loose track of the airplane when it flies behind mountains. Then, when a distinct radar echo is again detected, the tracking radar cannot tell whether the aircraft came from an enemy airfield.

AWACS can hand down information, but greater benefits accrue with a two-way communication between some central coordinating point and forward shooters equipped with IFF capabilities. For example, to avoid fratricide, surface-to-air missiles are specifically allocated defensive areas in which friendly aircraft are not to fly. Tests are currently underway to evaluate the feasibility of transmitting target identification down to individual missile batteries so that missiles and fighters can operate in the same area. But much of the information handed down from the center could come from analysis of data collected by the individual missile batteries in the field.

The ultimate goal for any identification and command system would be an array of individual shooters equipped with point-to-point identification of friend and foe (IFF) capabilities, collecting information and sharing it through some network so identifications are based on a composite picture built up from all available information. With the possible exception of the missile-fighter coordination, none of the communications improvements currently proposed or underdevelopment are being justified solely-or even primarily—as antifratricide measures, but their contribution to avoiding fratricide could be substantial. If allies can tap into the information-sharing network, they can still get the benefit of U.S. IFF information without acquiring the technology.

NONCOOPERATIVE IFF

Chapter 3 discussed how cooperative systems really only identified friends; noncooperative techniques are able to identify foes as well. Noncooperative identification of aircraft varies from the very simple-visual recognition—to detection, analysis, and classification based on extremely subtle differences among target aircraft.

The end of the Cold War will change the equations governing noncooperative IFF. In those future Third World conflicts in which the United States has overwhelming air superiority, positive identification of enemies-and hence noncooperative IFF--will be important. After all, any unidentified aircraft picked at random is likely to be friendly under those conditions, so failure to respond to an IFF query will probably not be justification to fire. At the same time, the technical challenge now will be in many ways much greater than during the clearer confrontation between NATO and the Warsaw Pact forces, since both Western and Soviet equipment are now widely proliferated. Therefore, allies and enemies might very well be using the same equipment, as they indeed did during the Persian Gulf War. The Services agree that no single measurement will be adequate to identify enemies, rather that a composite picture formed from many sources of information will be needed to be definitive. Some are discussed below.

Radio-Emission Intercept

Perhaps the simplest noncooperative technique—short of visual identification-is passive interception of radio and radar transmissions. Each radio and radar system transmits at characteristic frequencies, with characteristic signal modulation, and-at least for radars--characteristic pulse shapes and repetition rates. Some aircraft will transmit radio-frequency energy routinely, while others will at least occasionally transmit. It is also theoretically possible to induce enemy aircraft to transmit signals, perhaps by

sending false communications requiring answers or by appearing to threaten the aircraft in a way that forces the enemy pilot to turn on defensive radars or otherwise communicate with his command and control network.

Radar

Careful analysis of radar returns reveals much more about a target than just its bearing and range. Soon after the development of radar, operators noticed that the propellers of aircraft modulate the frequency of the radar return in a characteristic way. The modern equivalent is called jet engine modulation (JEM). The air intakes of jet engines reflect radar signals very efficiently. Some of the radar waves entering the inlets are reflected off of the rapidly rotating compressor or fan blades. The motion of the blades causes a slight Doppler shift in the frequency of the reflected waves. These subtle frequency shifts are readily detectable by sophisticated radars and are, moreover, characteristic of particular jet engines.

The principal limitation of identification by jet engine modulation is clear: the technique identifies engines, not aircraft. There are a limited number of military jet engines available worldwide and very different airplanes can be powered by the same type of engine, At the same time, individual aircraft in a particular fleet might have different engines. For example, some U.S. F-16s have been fitted with the General Electric F-1 10 engine while others have been fitted with modified Pratt and Whitney F-100 engine originally used in the F-15.

Jet engine modulation should at the very least distinguish fighter aircraft from transport aircraft, These two types of aircraft use very different types of engines: fighter engines typically have low bypass ratio engines and therefore have small, high-speed fans, while transports have high bypass ratio engines with much larger, slower fans. This method will not, however, necessarily distinguish military from civilian transports, For example, the commercial Boeing 757 and the military McDonnell Douglas C-17 both use the Pratt and Whitney F-1 17 turbofan engine.[1]

In addition, the technique is highly dependent on a proper geometry between the radar and the target. This dependence can restrict the technique's application in a dynamic air engagement.

More detailed information about the airplane structure itself will be available from high-resolution radars (HRR) under development. Radio or radar waves are just a form of electromagnetic radiation, like light, and travel at the same speed. Light travels about 300 meters in a microsecond. A typical radar sends out pulses, or bursts of radio waves, that are on the order of a microsecond in duration. This means that the radar pulses are many meters long. Resolving features much smaller than the radar pulse length is difficult; thus conventional radars are good at detecting objects but not much use for providing details of objects as small as airplanes. Targets appear just as blobs on the radar screen. If, however, a radar had a very compact pulse, perhaps the individual reflective surfaces of an aircraft could be resolved, which would allow identification. Such HRRs are currently in research and development. See figure 4-1.

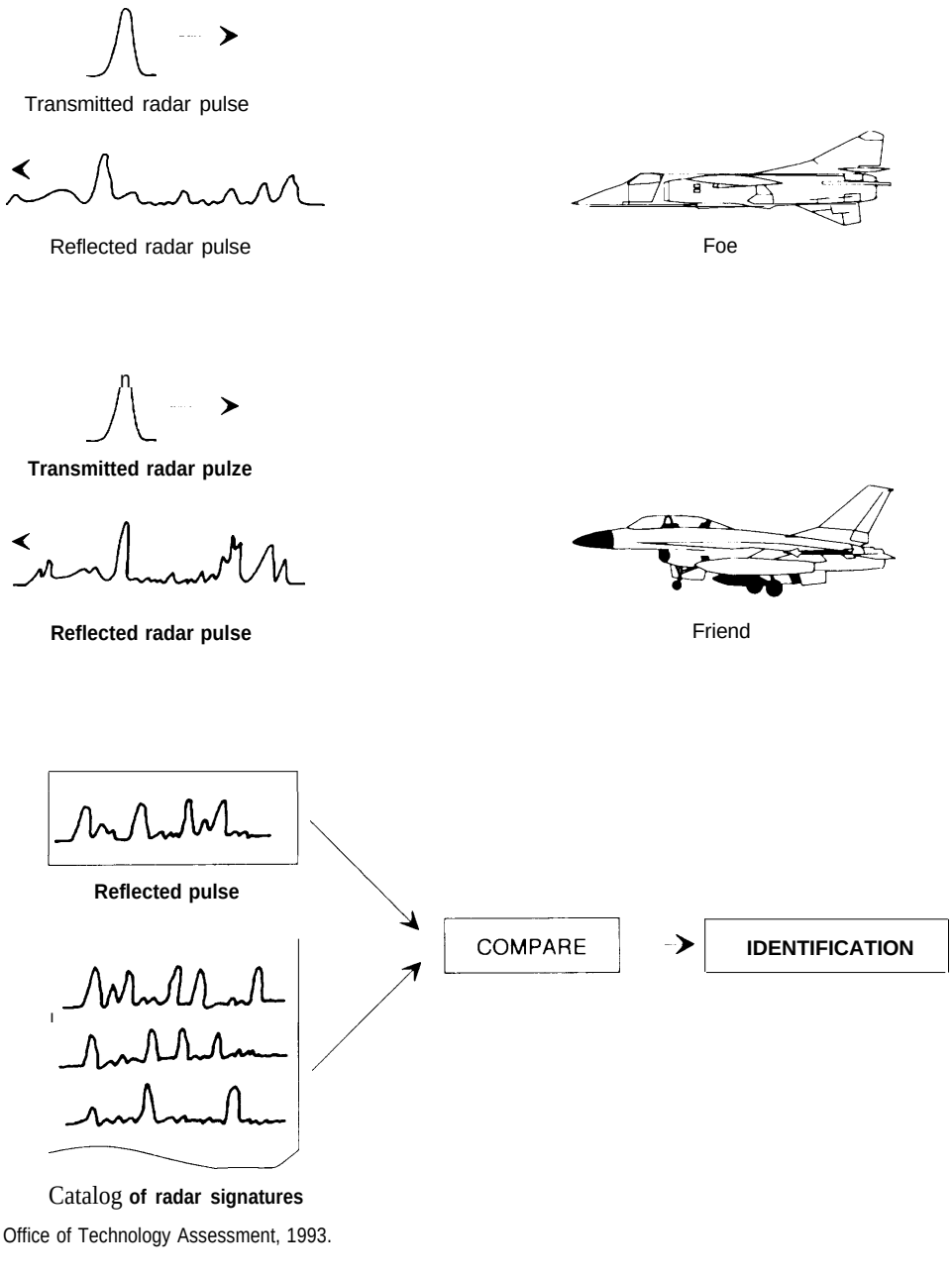
The challenges facing high-resolution radar development are substantial. First, of course, is designing and building a radar that can emit pulses with duration of only several nanoseconds (billionths of a second). Proponents of high-resolution radar are confident that the technology is available or can be developed. In addition, however, are the operational challenges. For example, each target will have a different echo pattern depending on the perspective of the viewing radar. Side views will look nothing like head-on views and data catalogs must be developed of all potentially hostile aircraft seen from all possible aspects.

---

[1] Mark Lambert, cd., *Jane's All the World's Aircraft* (Coulsdon, UK: Jane's Information Group, 1990), p. 748. The civilian designation for the engine is "PW2040.'

Figure 4-I—High Resolution Radar

Identification with High-Resolution Radar



Office of Technology Assessment, 1993.

Moreover, different aircraft can look similar from particular directions. For example, from a trade journal review of the Soviet Su-27 fighter: "From a head-on or trailing position, the Su-27 resembles the Navy/Grumman F-14, but has a thinner profile and is therefore more difficult to detect. From certain attitudes, if the range is not known, the forward portion of the Su-27 also resembles that of the USAF/General Dynamics F-16 because of its prominent bubble canopy and


MCDONNELL DOUGLAS CORP.

U.S.-built F-18 from the Australian Air Force flies below a similar-looking Su-27 from the former Soviet Union. Superficial resemblances of weapons can make quick identification difficult and unreliable.

its forward aerodynamic strakes, which blend into the wing leading edges."[2]

The algorithms used to discriminate among aircraft will not look at every detail but will extract and concentrate on certain defining characteristics. If an enemy knew which characteristics were used for discrimination, then it could try to suppress or alter them. Thus, the algorithms will need to be strictly secret and cannot be shared with all allies.

Surface-to-Air Missiles and Noncooperative IFF

Difficulties of working out aircraft identification has forced surface-to-air missiles (SAMs) and air interceptors into different zones of responsibility. Typically, SAMs defend strips of airspace from which all friendly aircraft are excluded; thus, anything entering the zone could be considered hostile and attacked. These areas are called Missile Engagement Zones or MEZs. Undefended corridors through the strips allow friendly aircraft to pass from one side of the strip to the other. Since enemy aircraft can track friendly aircraft and soon discover the locations of the corridors, the corridors must be moved frequently. Areas outside the MEZs are left to the interceptors. SAMs would not routinely engage any aircraft within these Fighter Engagement Zones, or FEZs.

The introduction of the Patriot missile changed the utility of this allocation of responsibility between interceptors and SAMs. The range of the Patriot is so great that, at least in the European theater of operations, there would be little area that was not accessible to both interceptors and Patriot. The Army, which operates the Patriot batteries, could severely and artificially restrict the engagement range of Patriot, but that obviously eliminates much of its capability and the justification for the cost of the system. To resolve this conflict, the Army and the Air Force started a program called Joint Air Defense Operations (JADO) to test a concept known as Joint Engagement Zones, or JEZs. The test of the feasibility of


HUGHES MISSILE SYSTEMS

An infantryman prepares to launch a hand-held surface-to-air missile against an attacking aircraft. The combined-arms battlefield is complex and dynamic, with many different types of weapons able to engage enemy targets, thereby greatly complicating and broadening friend and foe identification requirements.

[2]Donald E. Fink, "Sukhoi, Australian Pilots Fly in Joint Maneuvers," *Aviation Week and Space Technology,* Mar. 5, 1990, pp. 64-67.

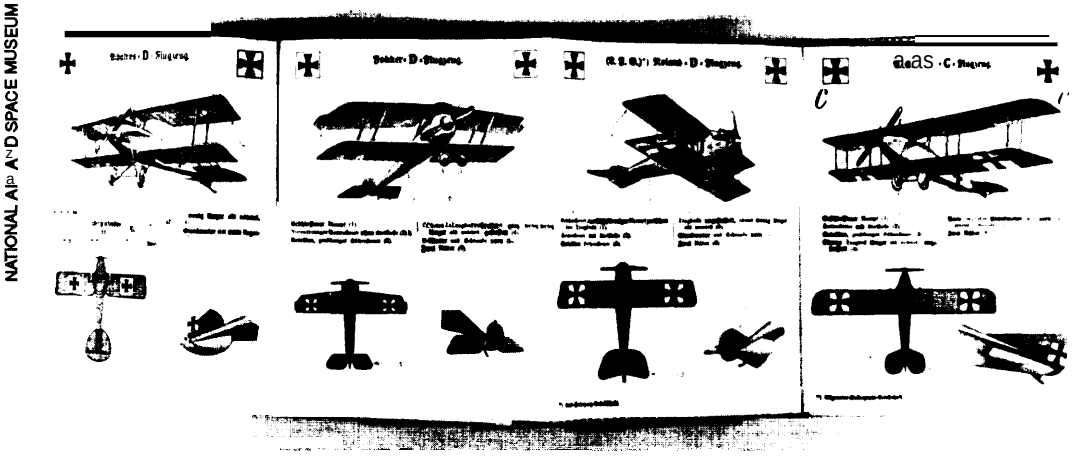
Box 4-A—History of Aircraft Identification

From the time aircraft were first used in combat in World War 1, fratricide has been a problem. Early fratricides motivated the application of national insignia on the wings and fuselages of aircraft and were at least part of the reason that some pilots-like the famed "Red Baron' 'resorted to garish color schemes.

Between the World Wars, the military gave some slight attention to the problem of identifying friendly aircraft beyond visual range, or in aloud or fog. As early as 1928, the British speculated on the possible use of sirens, whistles, or "singing" wires to create a signal that could be heard even if the aircraft could not be seen. Bomber command also considered schemes to use special light signals to identify returning aircraft.[1]

The problem of fratricidal attacks on aircraft and surface ships took its modern and familiar form with the development of radar. Early radar inventors foresaw immediately that radar-a device that allowed detection of aircraft and ships at long range, at night, and through clouds--created the difficult problem of identifying the detected object?

Early radar developers' first IFF attempts were to alter the radar returns of friendly craft in some characteristic way. Radar pulses are nothing more than radio waves that, when reflected from an object, create detectable echo pulses. The apparent size, or radar "cross-section," of an object determines the intensity of the radio waves reflected back. The cross-section in turn, depends roughly on the physical size, shape, and orientation of the object but also on the electrical characteristics of the object. For example, a conducting rod equal in length to half the radio wavelength will resonate with the radio waves, which causes a particularly strong reflection. If the resonant reflection could be turned on and off, then the radar return would vary in a way that could be used for identification purposes.



A German aircraft spotter's field guide used in World War I. From the very first uses of aircraft in combat, identification has been a challenge.

In 1937, the British mounted a few test aircraft with an antenna wire running the length of the fuselage. A switch at the center of the antenna was turned on and off in a regular pattern by a cam. Toggling the switch effectively changed the length of the antenna and hence the degree of resonance and the radar cross-section. Thus a radar operator would seethe "size' 'of the target changing in a pattern known to be characteristic of friendly aircraft. Tests on individual aircraft were very successful but the crude cams would not have worked for groups

1 Sean S. Swords, A *Technical History of the Beginnings of Radar*, Technical Report MEE1 (Dublin, Ireland: Department of Microelectronics and Electrical Engineering, Trinity College; 1983), p. 99.

2 Indeed, early radar developers coined the term "IFF" for "Interrogation, Friend or Foe" or, as some early operators referred to it, "Izzie friend or foe?" See Robert Morris Page, *The Origin of Radar* (Garden City, NY: Anchor Books, 1962), p. 166.

of aircraft: without perfect synchronization, one airplane's switch might open just as another's might close creating an indecipherable jumble and the system was never adopted.

In 1939, the U.S. Navy mounted atop a destroyer a set of half-wavelength rods on a pole. A motor rotated the pole and the rods along with it. The rotation changed the orientation of the rods, hence their degree of resonance with a distant radar and thus the strength of the radar echoes. The radar echo from the destroyer oscillated in an obvious way that identified it as a friend. This technique, while simple, had the same limitations as the aircraft system and because of its simplicity was easy for an enemy to copy.

The limitations of passive cooperative techniques led radar researches to active radar reply devices, now called "transponders." The first transponders operated at the radar's frequency; whenever the transponder detected a radar pulse it would transmit its own pulse at the same frequency. The radar would detect this pulse, interpret it as a powerful radar return, and the target would show up brightly on the radar screen.

The first transponders were the Mark I and Mark II developed in Britain and similar devices developed around the same time by the U.S. Naval Research Laboratory (NRL). These devices scanned all radar frequencies in use by friendly forces and retransmitted a pulse at the appropriate frequency whenever a radar was detected. In the early days of radar, this technique was possible because only two or three radars frequencies were common, but as more radar frequencies became available, this approach became untenable simply because the transponder could not handle the range of frequencies.

By 1941, the proliferation of available radar frequencies required that IFF devices go to a single frequency, independent of the radar's frequency. Thus, the radar could operate on whatever frequency was most appropriate and an *additional* signal, part of the so-called "secondary" radar, would query the target's identity. The Mark III was the first such device, sending and receiving signals in the 157-187 MHz (that is, megahertz or millions of cycles per second) frequency band.[3] The Mark III became the standard IFF device used by the American, British, and Canadian air forces during World War II.

The Mark IV, developed at the U.S. Naval Research Laboratory (NRL), was the first IFF system to use different frequencies for the query and the response--470 MHz and 493.5 MHz-but it never came into widespread use.[4] In 1942, the NRL began development of the Mark V, also called the UNB or "United Nations Beacon," which was to operate near 1 GHz (that is, gigahertz, or billion cycles per second). This program was not completed until after the war but is important because the frequencies used-1.03 GHz for queries and 1.09 GHz for replies-are still used today on both civilian and military transponders.

The next set of refinements appeared in the Mark "X," which had a dozen query and response channels available.[5] Mark X originally allowed aircraft to identify themselves as friendly but did not allow different responses from different friendly aircraft. A capability, known as SIF,[6] allowed different responses from different transponders. This capability, plus an encrypted query and response mode added to the Mark X became the current Mark XII. (The Mark XII used for civilian purposes without the encryption capability is still frequently referred to, especially in Europe, as the Mark X-SIF.)

The Mark XII is today used by U.S. aircraft and ships but is not widely used among U.S. allies.

---

3 The U.S. equivalent of the Mark III was called the SCR 595. See Swords, op. cit., footnote 1, p. 102. Transponders operating on this principle, now in near universal use on aircraft for civilian air traffic control as well as military IFF, are usually called "secondary surveillance radars." See Michael C. Stevens, *Secondary Surveillance Radar* (Norwood, MA: Artech House, 1988), p. 7.

4 Much of this and subsequent wartime development of IFF devices was a joint effort of U.S. and British scientists, called the Combined Research Group and headquartered at the Naval Research Laboratory.

5 The "X" was a place-holder until a decision could be made about whether a new Mark number was justified but it became, perhaps inevitably, the Roman numeral 10. Thus, there are no Marks VI, VII, VIII, or IX in the chronology.

6 U.S. sources state that the acronym stands for "Selective Identification Feature," but some British sources state that the "F' stands for "Facility."

this approach is called JADO/JEZ. Tests are now being carried out at or planned for Nellis and Eglin Air Force bases. Since the establishment of the test program, the Navy has become involved, to enable it to test operationally some noncooperative surface-to-air identification systems, such as the Shipboard Advanced Radar Target Identification System, or SARTIS. In February 1994, coordination of Army ground-based SAMs, Air Force interceptors, and Navy off-shore SAMs will be tested along the coast of Florida at Eglin Air Force Base.[3]

Patriot missiles belong to the Army but during joint operations their rules of engagement are typically set by the Air Force. The Air Force wants positive hostile identification before allowing the missiles to fire. Lacking any intrinsic capability to do so, Patriot batteries must depend on higher echelons to provide the information. During large-scale battles involving many potential targets, the transfer of information from high echelons down to individual fire control centers can saturate current data networks, causing delays in identification data transfer.

Any development of noncooperative IFF must consider SAMs from the beginning if they are to contribute to their full potential. For example, Patriot missiles, while gaining fame for their interception of Scud missiles in the Persian Gulf War, were on permanent weapons-hold status against aircraft targets. There were, therefore, no ground-to-air fratricides despite numerous violations of Army air defense areas,[4] but also, of course, Patriot played essentially no role in air defense operations.[5]

COOPERATIVE QUESTION-AND-ANSWER IFF SYSTEMS

Cooperative question-and-answer systems have been central to combat aircraft identification since World War II; indeed, some discussions of "IFF" really only treat this one approach. A description of the Mark XII and now-canceled Mark XV provides specific information on these two systems but also offer a convenient framework for presenting general design considerations for all question and answer IFF systems.

Although the early "Mark" numbers referred to specific types of hardware, the Marks XII and XV—and presumably future models—really refer to protocols. That is, "Mark XII" refers to an agreed format, or protocol, for sending and receiving information. This includes the relevant frequencies, the length of the radio pulses, the timing between them, the meaning of different pulses, and so forth. The Mark number does not specify the hardware configuration required, and Mark XII equipment has gone from vacuum tubes to transistors while using the same protocols. Of course, *some* hardware must embody the protocols, but any one of several interrogators and transponders can handle these formats and are, therefore, ''Mark XII" devices. For example, the UPX-23 and UPX-27 refer to two specific shipboard Mark XII interrogators while the APX-72 is an example of a Mark XII airborne transponder. Thus, the following discussion can combine specific questions related to protocols with general descriptions of hardware.

The current Mark XII sends out a query in the ''L" radar band, at a frequency of 1.03 GHz. The query is a pair of radio pulses. The time between the two pulses can be varied and the transponder will interpret the query differently depending on the separation time between the pulses. The immediate predecessor of the Mark XII, the Mark X, used three different pulse separations, each referred to as a ''mode. ' A pulse separation of 3 microseconds is "Mode l," 5 microseconds is

---

[3] Capt. Rocco Ersek, N6X1, briefing titled: "Introduction: JADO/JEZ, " (undated).

[4] Briefing entitled, ''Combat Identification: TRADOC Briefing," Lt. Colonel Mike Brown, U.S. Army Training and Doctrine Command (March 12, 1992).

[5] U.S. Congress, General Accounting Office, *Aircraft Identification System(U)*, GAO/C-NSIAD-92-13, p. 13.

"Mode 2," and 8 microseconds is "Mode 3.' These modes are still in use today.

The reply signal from the Mark X contained at least a pair of 1.09 GHz "framing" pulses 20.3 microseconds apart. These pulses indicate when the reply message starts and stops. Between the framing pulses of the response from the original Mark X lay six time slots 2.9 microseconds wide, each of which may or may not contain a radio pulse.[6] A pulse in a particular time slot represents a "1" and lack of a pulse represents a "O,' thus allowing transmission of binary numerical data. The improvements implemented for the Selective Identification Feature, or SIF (see box 4-A), and Mark XII included an increase to twelve slots between the framing pulses to allow for 4,096 possible replies. With the available number of possible replies, airborne transponders can give a distinct reply that identifies not just whether the aircraft is a friend but *which* aircraft it is-exactly as in civilian air traffic control today.

A simple transponder can be exploited easily by the enemy. If the enemy could get the transponder to respond to a query, friendly aircraft would reveal their positions and identities. To avoid this weakness, a program to develop an encrypted query mode was started in 1954. Mark XII IFF devices have this encrypted question-and-answer mode, called Mode 4. The Mode 4 query starts with four time synchronization pulses followed by up to 32 pulses that contain encrypted information telling the receiving transponder that the query is a valid, friendly query. Invalid queries are simply ignored by the transponder. The response to a Mode 4 query is a string of three pulses. The reply can start after any of 16 possible time delays; thus by changing the delay the reply can convey limited information. See box 4-B for the specifications of the interrogations and replies.

The IFF interrogators and transponders cannot work by themselves. If the transponder sent out a query in all directions and got a response back, the IFF interrogator would only know that there is somewhere out there at least one friendly aircraft. To query particular aircraft, interrogator antennas are mounted along with conventional radar antennas to point in a particular direction. When a target is detected by the radar, the IFF interrogator can send out a query in the same direction as the radar beam asking the aircraft to identify itself. The information from the reply can then be displayed on the radar screen directly.

The transponder can be simpler than the interrogator. When it receives a query, the answer need not be directed to the questioning radar; instead a simple omni-directional antenna is adequate and the interrogating radar can determine which aircraft is responding by correlating the response with the radar beam's direction.

Because of the difference in complexity, interrogators are generally more expensive than transponders. This affects the extent of their use; for example, some aircraft are fitted only with transponders. Ships and control aircraft like the E-2 are routinely fitted with the more expensive interrogators, but many interceptors are not.

The different modes can be used for military air traffic control. For example, an aircraft carrier's radar will show all the aircraft in its vicinity but this may be over a hundred aircraft in some crowded air corridors, such as over the Mediterranean.[7] The radar operator can use IFF modes to highlight friendly military aircraft.

---

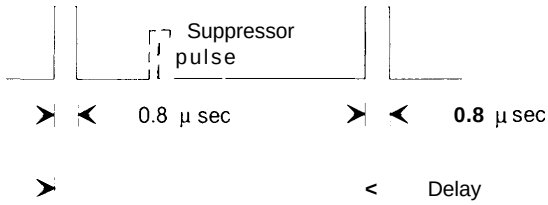
[6] Oral history at the Naval Research Laboratory holds that the time slots were intended to be an even 3.0 microseconds wide but the first delivery of delay lines for the prototype proved faulty, testing at only 2.9 microseconds. Rather than wait for new delay lines, researchers proceeded with what they had available. Thus, it came to pass that framing pulses of 20.3 (that is, 7x2.9) microseconds will be in use well into the twenty-first century. This tale illustrates how protocol standards should be developed carefully because they tend to stay with us for a long time.

[7] Briefing entitled ''Automatic Identification (AutoID), '' Applied Physics Laboratory, The Johns Hopkins University, (undated).

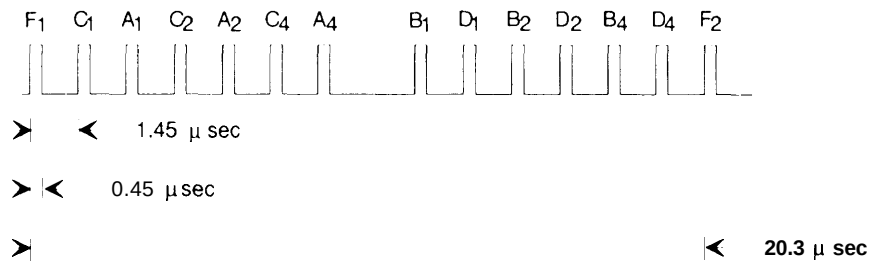
Box 4-B-Formats and Protocols for the Mark XII

Mark XII interrogations and replies are pulses of radio waves at 1.03 and 1.09 GHz. Information is conveyed by changes in the number and timing of the pulses. The interrogation for military Modes 1,2, and 3 and civilian Modes A, B, C, and D are a pair of pulses separated by a time delay, the length of which is specified by the particular mode. This format is illustrated in figure A.

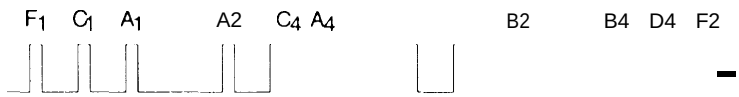
Mark XII interrogation format



Mode 3/A reply format



Mode 3/A reply pulse 7654



Mode 4 formats

SOURCE: NATO STANAG 4193 (Part 1) (Edition 2), 1990.

Box 4-B–Formats and Protocols for the Mark XII

No antenna is perfect, sending signals only in the direction wanted and no other. Energy leakage through "side lobes" could cause transponders to f ire even when t he radar is not pointed directly at them. To avoid this problem, some interrogators send out a suppressor pulse in every direction except the direction the radar is pointed. A transponder can compare the size of the two signals and if the suppressor pulse is larger than the framing pulses, the query is ignored.

Table A—IFF Modes

Delay (μ see)	Military mode	civil mode	Use
3	1		Military Function ID
5	2		Military Function ID
8	3 =	A	Aircraft identification
17		B	Not used internationally
21		C	Altitude
25		D	Not used internationally

SOURCE: NATO

Each interrogation mode has a different time separating the pulses, except that military Mode 3 is equivalent to civilian Mode A. The various Modes are shown in table 4-1. The pulse separation in Mode 1 is so short that not ail interrogators and transponders can handle the insertion of a suppressor signal in Mode 1.

The reply format consists of a pair of framing pulses 20.3 microseconds apart with up to 12 signal pulses between them, although not all modes use all the availabie signal pulses for information. The format is shown in figure B. Numerical values are transmitted in the replies in the form of four-digit "octal" or base eight numbers of the form ABCD. Each of the these digits is the sum of three pulse values. in the figure, for example, three of the pulses are labeled Al, A2, and A4. The first digit in the four-digit number is A which equals Al +A2+A4 where Al has a value of one, A2 a value of two, and A4 a value of four if a pulse is present in the appropriate time slot, and zero otherwise. Thus the decimal number 4,012, which is 7,654 in octal notation, would be represented by A=7=A4+A2+A1, B=6=B4+B2, C=5=C4+C1, and D=4=D4. The resulting pulse pattern is shown in figure C.

Mode 4 pulses, the encrypted mode, have a different format. The interrogation pulse starts with four time synchronization pulses. These are followed by up to 32 data pulses. The arrangement of these pulses validates that the query is indeed from a friendly interrogator and transponders should send a reply. The reply is a set of three pulse delayed by various amounts. These formats are shown in figure D.

Passive Cooperative IFF Measures

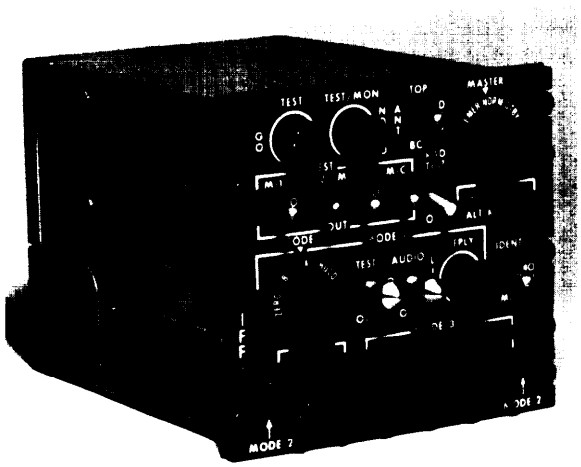
Cooperation by friendly targets could enhance the discriminating ability of passive friendly observers using the noncooperative IFF techniques described above. Few of these ideas are beyond the conceptual stage. They include adding radar highlights that would stand out on high-resolution radar, inducing vibrations that would show upon Doppler radars,[8] and even modulating or doping exhausts to make them stand out to infrared sensors. Application of any of these techniques will require first the deployment of the appropriate noncooperative identification technique.

Limitations of Mark X11, Improvements in Mark XV, and Next Generation IFF

This section briefly discusses some of the current and potential short-comings of the current Mark XII IFF system. These problems were to be corrected with the development of the Mark XV. The Mark XV development was canceled in December 1990 and the still-to-be-defined successor question-and-answer system is now referred to as the Next Generation IFF, or NGIFF.

[8] Briefing entitled, ' 'Achieving Covert Communications and Ground-Combat Identification Using Modulated Scatterers, ' E.K. Miller and D.M. Metzger, Mechanical and Electronic Engineering, Los Alamos National Laboratory (Mar. 11, 1992).

ALLIED SIGNAL AEROSPACE



A typical Mark XII airborne transponder. IFF formats and protocols can be handled by any of several types of interrogators and transponders.

As discussed in chapter 3, the three ways in which an enemy can defeat the purpose of an IFF system are exploitation, spoofing, and denial. An enemy exploits an IFF system by getting information from it. For example, if an enemy could record queries from a Mark XII interrogator and then rebroadcast them, then he could trigger the Mark XII transponders and have friendly aircraft identify themselves and reveal their positions. Even if recording valid queries were impossible, an enemy could *guess* at queries, hoping to hit upon a valid combination. With thousands of possible queries this may seem daunting, but in fact modem electronic devices should allow transmission of scores of guessed queries per second.

The Mark XV would have reduced or eliminated the possibility of enemy exploitation by changing the query codes rapidly. Valid Mark XII query codes are changed regularly but the process is cumbersome, involving the use of printed keys and the mechanical insertion of key values into the transponder. In the late 1960s, the Navy flight tested a system called TACIT (Time Authenticated Cryptographic Interrogator/Transponder), which allowed the rapid, automatic changing of query codes. Indeed, codes could be changed so rapidly that an enemy could not record and retransmit a code before it became obsolete

The Mark XV was to have a capability like TACIT. This means that all transponders, at least within a theater of operation and ideally worldwide, would switch codes in an agreed pattern, say, every second on the second. Clearly the requirements for time synchronization across literally thousands of platforms around the world is a major technical challenge. But modem developments in electronics makes the task possible if not easy; modem electronic clocks have accuracies of a fraction of a second per year. The encryption computer contained with each interrogator would be supplied with a "seed" key that would allow generation of a query code, then algorithms embedded in the computer would generate the next code from that seed and so on until a new seed were supplied.

An enemy's ability to appear friendly to an IFF system is called spoofing. Just as an enemy could try to exploit the Mark XII by recording or guessing at proper queries, an enemy could also try to spoof the Mark XII either by recording or guessing proper replies. The Mark XV would have incorporated several improvements to inhibit spoofing. These included a greater possible number of responses creating a greater barrier to straightforward guessing. The Mark XV would have used "spread spectrum" pulses, that is, a sharp pulse converted by the transmitter electronics into a broad frequency pulse that has lower peak energy at any given frequency, making interception more difficult. The receiver has similar electronics that operate in reverse, compressing the spread pulse into a sharp information pulse. A receiver that knows the proper spreading and compressing function gets substantial receiver gain, but an enemy that does not know the details of the function will have a difficult time resolving the signal from background noise.[9]

[9] Don J. Torrieri, *Principles of Secure Communication Systems, Second Edition* **(Bestow MA: Artech House, 1992),** pp. 95-99.

Also, the strength of the reply signal would have been adjusted for the distance of the interrogator, with the reply no stronger than it needed to be thus making more difficult the interception and retransmission of a valid reply,

An enemy might be able to deny the use of an IFF system, For example, jamming of the radio signals is one straightforward approach. Almost any radio can be jammed if an enemy is willing to invest adequate resources and can get jammers in the right places. Military radio and radar systems are designed to make jamming more difficult, but jamming can never be made impossible and the amount of effort that is appropriate to invest in electronic antijamming capability depends sensitively on 1) the presumed combat environment, 2) a judgment about the value of working in a jamming environment, and 3) a comparison with other approaches to solving the jamming problem (e.g., blowing up the enemy jammers).

Military users of Mark XII consider it easily jammed. Improvements contemplated for the Mark XV included significant antijamming capability. For example, the query and response pulses would be much longer than those of the Mark XII. Longer pulses mean the potential for greater total energy in the pulse and a longer signal integration time, which makes jamming more difficult, Each bit of information in a pulse would be spread over the whole pulse length, which makes reading the pulses in the presence of jamming more reliable. The spread spectrum electronics that contribute so much to communications security also make jamming more difficult. Finally, the structure of the pulses would allow for detection of transmission errors so that if jamming occurred, the operators would know that information received was faulty and should be rebroadcast.

Jamming is one potential threat, but an indirect form of denial is perhaps the most important: if the operators do not have confidence in the system, they turn it off. Several experienced pilots reported to OTA that during the Vietnam War, they turned off their Mark XII IFF systems as soon as they entered enemy air space. Other say that more recently, on missions flown near potentially hostile forces around the Mediterranean Sea, Mark XII were turned off. The reasons are the same in both cases: a fear that enemy-or even friendly--queries would trigger the transponders and thus reveal the aircraft's presence. Against the more sophisticated Soviet threat, pilots expected to turn off IFF transponders long before they crossed enemy lines. If the operator believes that an IFF system increases his danger, then it will not be used to its full potential, if it is used at all. Thus, the ON/OFF switch becomes another means of denial. Mark XV improvements would have mitigated the problem of inadvertent friendly triggering of the transponder but this is clearly more than just a technology problem and a solution requires careful coordination among the eventual users.

Despite its promised improvements, Mark XV development was canceled in 1990, both because of increasing technical complexity and the growing estimated cost of deploying the system. Over 40,000 Mark XII sets have been produced[10] and approximately 25,000 are still in use. With a huge number of platforms needing IFF devices—and a need for at least 17,000 Mark XVs was forecast—acquisition costs multiply rapidly. Indeed, the cost of the Mark XV would have precluded outfitting every vehicle with a device, which raises the distressing question of the value of an IFF system that is so expensive that it is not carried by all platforms.

The cancellation of the Mark XV program leaves the future of cooperative aircraft IFF uncertain. The original motivation for the program, obsolescence of the Mark XII, still stands, so some replacement capability is probably needed. Most studies by the military Services assume that

---

[10] Navy Briefing, "Defense Acquisition Board Milestone 'O' Review: Cooperative Friendly Aircraft Identification Presentation for C31 Systems Committee," July 22, 1992.

a cooperative IFF system will provide some part of that needed capability.

Perhaps the most obvious Mark XII replacement is a system with performance that is a compromise between that of the Mark XII and of the Mark XV. By backing off on the Mark XV performance goals, costs could be reduced for any replacement. Antijamming capability was one of the major determinants of costs. Justifying any particular antijamming requirement is difficult for any piece of electronic equipment. No one can ever be entirely sure what resources a future enemy might devote to jamming, how its jammers might operate, be deployed, and so on. Thus, making very conservative assumptions is enticing but has substantial cost consequences for electronic systems. Options for future IFF systems range from using the current Mark XII protocols and radio wave forms-that is, making no antijamming improvement to the Mark XII-to using the spread spectrum waveforms proposed for the Mark XV. In between are compromise solutions that include using a modified and reduced spread spectrum waveform or using directional antennas to reduce jamming interference. The Germans have made proposals for moving to a different frequency band altogether, in the S-band, which covers the range from 2-4 GHz. One advantage of S-band is that the airwaves are less crowded at those frequencies. As a general rule, however, the higher the frequency of radio transmission, the shorter the range. Thus, an S-band system has shorter range than an L-band system. The shorter range of S-band actually has one advantage: it is harder to jam with a few distant but powerful jammers. Short range is less of a handicap in the crowded European theater in which the Germans operate but it makes S-band unattractive for the worldwide operations needed by the United States.

Maintaining communications security was a secondary contributor to the cost of the Mark XV. The Mark XV was to have anew cryptocomputer, the KI-15, that would have provided very good security through electronic handling of cipher keys and rapid, automatic changing of keys that would have saved operational costs. While the cryptographic security component of the Mark XII is quite old, the whole system need not be junked. For example, according to the National Security Agency, new cryptocomputers could be added to the current Mark XIIs or to similar follow-on models. These would provide better security without the full cost of the Mark XV's capability.

The important point is that the Mark XV improvements were not all-or-nothing; compromises in performance are possible. DoD could build a system better than today's Mark XII but cheaper than the Mark XV. The performance goals for the Mark XV were established during the Cold War. Now that war with Russia seems far less likely and the more likely opponents are far less challenging, backing off on the performance requirements of the Mark XV should be given serious consideration. The exact emphasis is, of course, subject to judgment, but technical experts interviewed by OTA felt that the end of the Soviet threat has probably reduced the need for antijamming improvements more than the need for communication security improvements.

COORDINATION WITH CIVILIAN AIR TRAFFIC CONTROL

Civilian Airborne Transponders

A mid-air collision on December 16, 1960 between a United DC-8 approaching Idlewild (now Kennedy) airport and a TWA Super Constellation approaching LaGuardia killed the 128 aircraft occupants and eight others on the ground and highlighted the limitations of the air traffic control system even when aircraft were under positive control.[11]

---

11 Richard J. Kent, *Safe, Separated, and Soaring: A History of Civil Aviation Policy,* 1961-1972 (Washington DC: U.S. Department of Transportation, Federal Aviation Administration; 1980), pp. 6-7.

The New York City mid-air collision accelerated adoption of several technical improvements for civil air traffic control, for example, secondary radar transponders on civilian aircraft. By 1953, Mark X frequencies and protocols had been released for international civilian use.[12] The civilian airliners were given use of Mode 3, which in civilian use is called Mode A. Civilian airliners use the 4,096 possible combinations of reply signal to identify the aircrafts' flight numbers, with some numbers reserved for special messages; for example, any aircraft that responds to a Mode A query with a "flight number' of octal code 7700 is saying that it has an emergency.

Additional civilian modes called, not surprisingly, Modes B, C, and D have been added subsequently, but only Mode C, with a 21-microsecond delay between query pulses, is commonly used. Ground-based radars can determine ground coordinates directly but are not able to determine aircraft altitude. Therefore, most aircraft now have transponders connected to the aircraft altimeter allowing the transponder to report automatically the aircraft's altitude in response to a Mode C query, The use by civilians of military IFF frequencies and protocols has important implications anywhere the two types of aircraft expect to share the same airspace.

Mode S

Secondary surveillance radar has become so useful and important to civilian air traffic control that it has become a victim of its own success. In some particularly heavy air corridors-for example, Europe and the east and west coasts of the United States—aircraft can receive identification requests from dozens of radars. This may include air corridor radars and overlapping radar coverage from closely spaced airports. Moreover, not all nations' air traffic control procedures are identical or even particularly well-coordinated, so neighboring countries may simultaneously query the same aircraft for information important to their air traffic control.[13]

The multitude of interrogators can result in hundreds of queries each second. This volume can saturate the airborne transponders, making them unavailable when essential radar queries come through. Moreover, all of the aircraft are sending out identification calls more or less continuously; interrogators are receiving the replies from properly designated aircraft and a multitude of stray replies that are picked up as interference.

The ongoing, but gradual, adoption of a new mode-Mode S, where 'S' stands for 'select"—is the internationally agreed technical solution to these problems. In Mode S, interrogating radars will *not* routinely send out a general ' 'who's out there" query with every sweep. Mode S requires that each aircraft have a unique, permanent identifying number. A Mode S interrogator will occasionally send out an ''all-call' message to establish the identities of all of the aircraft within its coverage. The radar and interrogator can then send out specific messages to specific aircraft, requesting altitude, for example. As an airplane leaves the coverage area of one radar, the information about that specific airplane can be sent by land lines to the next radar, which will be expecting it.[14]

Proponents of the Mode S system claim that it will reduce transponder information loads by at least two-thirds. It will also allow denser air traffic near airports. One current constraint on traffic density is the resolution of air traffic radars, not just safe separation distances. Two closely spaced aircraft will respond to the same Mode A or Mode C query and their answers will overlap when received by the interrogating radar, which

---

12 Michael C. Stevens, *Secondary Surveillance Radar* (Norwood, MA: Artech House, 1988), p. 9.

13 Lief Klette, "Europe's Crowded Skies: Managing Civil-Military Airspace, " *International Defense Review,* July 1992, pp. *659-662.*

14 *Radio* Technical Commission for Aeronautics, " Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S) Airborne Equipment, " Document Number RTCA/DO-181 (March 1983).

will not be able to make sense of either of them.[15] With Mode S, a radar could interrogate one airplane and then, a millisecond later, send a separate interrogation to the second airplane. This time lag is so short that it will not affect air safety but will allow electronic separation of the replies. Thus, while Mode S is not needed by the U.S. military, it is part of a much-needed world-wide civilian standardization and modernization effort, of particular importance in Europe.

Mode S will allow messages longer than the current Mode A and C 12-bit messages. The greater number of message bits plus the unique identification numbers for aircraft allow limited two-way digital and text data transfer between aircraft and the ground that would be impossible with today's free-for-all interrogation system. For example, just as Mode C now queries altitude, Mode S could, in principle, query aircraft speed, bearing, rate of decent, destination, even fuel load. These data would be used by air traffic controllers to better manage aircraft in dense traffic.

Information can also be sent up to the aircraft. For example, changes of air traffic radio frequency could be sent automatically when aircraft move from one control zone to another. Weather advisories or changes in flight plan instruction could be sent up, then written or otherwise stored so they would be available to the pilot at a time of her choosing.

The basic Mode S is called "Level l;" "Level 2' includes the ability to receive short commands of 56 bits; "Level 3" includes the ability to receive longer command sets of 112 bits and transmit short ones; "Level 4" includes the ability to receive and transmit long commands. Since the system is not yet operational, all of the ultimate uses for the data transmission channels of Mode S are not clear but enough is known now to see that they will be useful to civilian pilots, but less so to military pilots.

Mode S will be adopted in phases in the United States. Large commercial passenger carriers must have Mode S transponders operating by the end of 1993. Commuter carriers and general aviation will acquire Mode S capability more gradually. Perhaps within 10 years, all aircraft, even general aviation, will need Mode S if they are to operate in dense air-traffic areas of the United States.

The military must operate in a world where the overwhelming majority of airspace is under civilian control (at least in peace time). This means that the military must adopt at least some of the Mode S capability into any future IFF system. The Services have two major problems with Mode S, neither of which is insurmountable but each of which must be handled. First is cost.

The cost to the military of Mode S will be more than just the cost of the equipment. Another black box can always get squeezed into a transport, but every cubic inch on a fighter plane is already occupied. That means redesigning existing equipment, placing antennas, dealing with waste heat from more electronics, and so on. Mode S was to be an integral part of the Mark XV. With its cancellation, DoD must find some other way to outfit its aircraft with Mode S or come to some accommodation with civilian air traffic control.[16]

The benefits of Mode S are greatest in the densest air traffic. Service resistance to the cost of Mode S is easy to understand because dense traffic areas are just those in which military aircraft are *least* likely to fly, at least in the United States. But since commercial aircraft can hardly avoid these areas, they will need Mode S. Then,

---

15 This is due to the finite speed of the radio waves sent out by the transponders. Since radio travels about 300 meters per microsecond, a 20-microsecond reply is 6,000 meters long and any two aircraft whose distances from the interrogator differ by less than that will send messages that will overlap, or be 'garbled,' at the receiver. Note that the aircraft need not be dangerously close; since air traffic control radars normally do not discriminate aircraft altitude, two airplanes with substantial vertical separation can still have very close ground tracks.

16 Letter from Barry Lambert Harris, Deputy Administrator, Federal Aviation Administration, U.S. Department of Transportation, to Richard G. Howe, Acting Chairman, Policy Board on Federal Aviation, Office of the Secretary of Defense, Apr. 20, 1990.

when Mode S is widespread, it doubtless will be used-even if not essential-in the less heavily traveled airspace where military aircraft *do fly*.

The FAA does not foresee Mode S message capability as a requirement for operating in general U.S. airspace, but requirements will be imposed on aircraft that wish to operate near the Nation's busiest airports. In principle, military flights could simply avoid those areas. Currently the DoD foresees that fighters eventually will be outfitted with Mode S/Level 2 and cargo transports will be outfitted with Mode S/Level 4.[17]

The second problem is more subtle: the information that Mode S might provide to potential enemies. This is not a wartime problem—pilots would just turn civilian modes off in war theaters and the military would take over air traffic control. It is, rather, a problem of long-term peacetime intelligence information loss. Current Mark X-SIF identifies an airplane by its flight number for that day. Mode S will identify each airplane uniquely by its tail number. The Services will not tolerate this since it would allow a potential enemy to build up over time a valuable database. For example, long-term compilation of aircraft tracks might reveal how often particular aircraft shuttle between deployment areas and depot maintenance sites. One solution is to allot to the Services a block of numbers that they could mix around at random. Civilian and foreign air traffic controllers would then know that the aircraft is a U.S. military aircraft but not which one,

The military may object to even this much information being available, but presumably the United States is also interested in clearly identifying civilian airliners as such. Any system that loudly proclaims all civilian aircraft inevitably identifies military aircraft as well, at the very least by default, since any airplane not proclaiming loudly will be assumed military. Thus, this weakness may bean inevitable price that has to be paid for the protection of civil aircraft from accidental attack.

Other Areas Requiring Civil-Military Coordination

Today the military and the FAA jointly operate air traffic control (ATC) systems covering the United States and the air approaches to it, with the military providing about a fifth of the ATC assets. The Nation is in the process of converting to a unified system, called the ARSA-4, to be operated solely by the FAA. The unified system should be more capable and cheaper. The Air Force will receive data from the FAA radars and interrogators, which will be used for the identification of aircraft approaching the United States .[18] Some of the current Air Force air traffic control computers cannot keep up with the high traffic densities in the Nation's busiest corridors, but sections of radar coverage can be systematically blocked out from the Air Force data link to allow the Air Force system to concentrate on only those sectors that are important to it. In the future, all Service ATC equipment and computers will be comparable with FAA equipment.

The FAA plans also for the gradual adoption of an automatic system to help pilots avoid mid-air collisions. Currently, aircraft pilots have visual information, on-board radars, and secondary information relayed up from ground radars. Ground radars can interrogate the transponders carried on aircraft but currently the aircraft cannot interrogate each other's transponders. The Traffic Alert and Collision Avoidance System (TCAS) will allow aircraft to use Mode-S transponders to get information from other aircraft in the area which will allow on-board computers to calculate and recommend collision avoidance maneuvers. TCAS will be in place for airlines by the end of 1993. TCAS may eventually place some requirements

17 Frank Colson, OSD liaison to FAA, personal brief.

18 Tom McNiff, *'Air Force, FAA Working on New Radar System, ' *Journal of Commerce* (Sept. 21, 1992), p. B3, (and personal briefings from Richard Lay, FAA in-route radar manager)

on military aircraft even if none are in place now. The first phase of TCAS for general aviation or commuter carriers is planned for implementation in 1995.[19]

If cooperative IFF systems are to be used by allies or even by U.S. forces operating in allied countries, then frequency allocation problems must be resolved. For example, the current Mark XII transponders can cause interference in Germany, where their use comes under some restriction. The converse problem is getting everyone onto the *same* frequency. For example, communications between military and civilian aircraft are not always easy since military fighters primarily use UHF frequency bands for communication while commercial airliners use VI-IF bands.

IDENTIFICATION OF SHIPS

The problems of identification of friendly and enemy ships are more like those of airborne targets than they are like those of land surface targets. Ships use a combination of tactical information and direct target identification to separate friends from foes.

Navy ships now have both Mark XII interrogators and transponders that allow positive friendly identification. The ships are equipped with sophisticated navigational and communications equipment, thus antifratricide efforts among ships through sharing of tactical and navigational information comes naturally.

Chapter 2 related several historical incidents of friendly fire between ships, and these are not unknown today .20 With the strong emphasis on carrier-based airpower, however, U.S. ships probably face a greater fratricidal danger from friendly aircraft. The consequences would be much more severe than for attacks on other aircraft but fortunately the likelihood may not be as great. Since the United States and its European allies will have total control over the sea in most foreseeable conflicts, there may be theaters in which there is no reason for a friendly aircraft to attack any ship.

There are several reasons to believe that avoiding fratricide of ships will be easier, or no more difficult, than avoiding fratricide of aircraft. Modem warships are not as widely proliferated around the world as are aircraft. Ships can afford to carry more powerful transponders, surveillance, and communications equipment. Ships are larger and slower than aircraft so some approaches to noncooperative identification of aircraft, for example, high resolution radar, should work at least as well. Some noncooperative techniques, for example, analysis of radio emission should work for ship identification just as they do for aircraft identification, although ships and aircraft will have different rules about radio and radar silence. Other techniques, jet engine modulation, for example, are simply not applicable. But still others might work better for ships than aircraft: examples include, synthetic aperture radars, laser radars, and high resolution infrared imaging. Because the country has far fewer ships than aircraft, cost per platform is less important for ships than for aircraft. Furthermore, while perhaps not spacious, ships have much less of a problem with packaging, power supply, waste heat removal, and antenna placement than do fighter aircraft.

Submarines

There is little current concern about fratricide of submarines. Few nations possess them and most that do are U.S. allies, so all submarines could be assumed friendly in most limited conflicts. Furthermore, U.S. submarines are substantially different from those of other nations. In the future, the problem may become worse, however. Some countries hope to export small diesel-electric submarines. One can easily imagine a

---

19 U.S. Department of Transportation, Federal Aviation Administration, "Introduction to TCAS II," March 1990.

20 During NATO exercises in October 1992, the U.S. aircraft carrier *Saratoga* accidentally fired missiles at the Turkish destroyer *Muavenet*, killing five and wounding at least 15. See Eric Schmitt, "U.S. Missiles Hit Turkish Ship, Killing 5," New *York Times*, Oct. 2, 1992, p, A8.

conflict like that in the Persian Gulf War, taking place perhaps a decade hence, in which both local allies and local enemies are equipped with the same German- or Russian-built submarines.

In principle, submarines could use cooperative and noncooperative IFF systems analogous to those used on aircraft. But whereas the aircraft systems would depend primarily on radio-frequency electromagnetic energy, submarines would use sound waves, magnetic fluctuations, or some other signature. But submarines are different. The hard part of killing a submarine is not attacking and destroying it—although that can be a challenge under some circumstances; the hard part is finding it. Submarine designers devote considerable attention to further increasing the difficulty of detecting submarines, largely by making them as quiet as possible. Submariners would strenuously resist any effort to have submarines actively broadcast in response to some identification hail, or to somehow increase their boat's signature to make cooperative-passive identification easier.

For the foreseeable future, therefore, avoiding submarine fratricide will be based on the current procedures for careful command and control of areas of operation. Submarines now patrol individual, well-defined areas; any other submarine that enters that area is considered hostile and open to attack. Moreover, within assigned patrol areas, surface ships do not engage in antisubmarine activity (that is left to the resident submarine), but any submarine found outside of assigned areas is assumed hostile and could be attacked by surface and airborne forces. This approach works but is very flexible only with good communication between submarines and surface ships. If assigned patrol areas can be reliably updated several times a day, ships above and below the surface can cooperate smoothly.

A COMPREHENSIVE IDENTIFICATION SYSTEM

No cooperative IFF system is perfect, so pilots and ships' crews hesitate to fire based solely on the assumption that *lack* of an IFF reply means a target is an enemy. Any shooter would prefer to have positive evidence that a target is an enemy, hence the motivation for noncooperative IFF systems. Yet neither are noncooperative systems perfect. Exercises on test ranges indicate that with current technology a few percent of targets identified as hostile are, in fact, friendly. This error rate may be acceptable in a struggle for survival, as was expected between NATO and the Warsaw Pact. However, if in the future the United States is engaged in a lesser conflict with overwhelming force ratios, then most of the aircraft in the air at any given time will be friendly and even a small rate of mistakenly identifying friends as foes can result in the loss rates from fratricide being as high as those from enemy action.

Cooperative and noncooperative systems can work together to make each more effective than either could be alone. Assume that a cooperative question-and-answer type system were, say, 90 percent reliable. If this system were used to sort all targets, then 10 percent of targeted friendly forces would be classified as hostile, clearly an unacceptably high value. But if a noncooperative system were also 90 percent reliable, that is, it classified friendly vehicles as hostile 10 percent of the time, and all hostile-classified targets were also queried by the cooperative system, then only 10 percent of 10 percent, or 1 percent, would slip through both, assuming the two systems are independent.[21] These numbers are picked only to be illustrative, whether a 1 percent error rate is acceptable will depend on the tactical situation and political and military judgment.

Cooperative systems can even help identify enemies, if operated in conjunction with noncooperative systems. Many noncooperative identifi-

2. In the real world, the systems may not be independent. Battle damage, for example, might both change the noncooperative signature and put IFF transponders out of commission. In war, nothing is neat.

cation techniques will discriminate friend from foe on the bases of subtle differences, but will require expensive, hence perhaps scarce, equipment. If this equipment is unable to examine all possible targets, then cooperative question-and-answer systems could concentrate efforts on ambiguous targets. For example, only those targets that do not respond to a cooperative IFF queries would be examined by noncooperative techniques.

Currently, the technology required for cooperative question-and-answer IFF systems is more developed than that for most noncooperative systems. The Services see the advantages of noncooperative IFF but that longer term goal should not erode efforts to improve the reliability of cooperative question-and-answer IFF by the application of technology that is near-term or in-hand.