



Journal of Aerospace Technology and  
Management

ISSN: 1948-9648

secretary@jatm.com.br

Instituto de Aeronáutica e Espaço  
Brasil

Wurts, Eric Julius

A identificação amigo-inimigo nativa do Brasil: perguntas e respostas

Journal of Aerospace Technology and Management, vol. 2, núm. 3, septiembre-diciembre, 2010, pp.  
371-386

Instituto de Aeronáutica e Espaço  
São Paulo, Brasil

Disponível em: <http://www.redalyc.org/articulo.oa?id=309426554012>

- Como citar este artigo
- Número completo
- Mais artigos
- Home da revista no Redalyc

redalyc.org

Sistema de Informação Científica  
Rede de Revistas Científicas da América Latina, Caribe, Espanha e Portugal  
Projeto acadêmico sem fins lucrativos desenvolvido no âmbito da iniciativa Acesso Aberto

Eric Julius Wurts  
Exército Brasileiro  
Rio de Janeiro – Brazil  
ericwurts@superig.com.br

## A identificação amigo-inimigo nativa do Brasil: perguntas e respostas

**Resumo:** Este artigo trata do Sistema de Identificação Amigo-Inimigo (IFF) com tecnologia genuinamente nacional, incluindo o Modo 4 com criptografia autóctone. São apresentados fratricídios reais e os métodos do país para reduzi-los. Aspectos técnicos dos sistemas IFF em uso pela Organização do Tratado do Atlântico Norte (OTAN), são revistos e atualizados com base nas Normas de Padronização da OTAN 4193. A análise mostra que o estágio atual de desenvolvimento da Indústria Nacional de Defesa, combinado à sua capacidade de integração com os centros tecnológicos das Forças Armadas, bem como as disponibilidades orçamentárias para a pesquisa e o desenvolvimento, fruto da Política de Defesa Nacional, são fatores para o êxito do projeto. Também expõe a importância da combinação da defesa aérea e controle do tráfego aéreo no Brasil como fator de sucesso do trabalho. A solução deve ser baseada na manutenção dos padrões da OTAN das características técnicas dos interrogadores e transponders do IFF Mark XII, mantidos os processos de interrogação e “resposta”. Indica-se a necessidade de subsídios para estudo da incorporação do Modo 5 e Modo S, em segunda etapa.

**Palavras-chave:** IFF nacional com Modo 4, Fratricídios, Indústria Nacional de Defesa, Tecnologia autóctone.

## The native identification friend-foe of Brazil: questions and replies

**Abstract:** This paper discusses the System of Identification Friend-Foe (IFF) with genuinely national technology, including Mode 4 with native encryption. Actual fratricides are illustrated and the Brazilian processes to reduce them are shown. Technical aspects of IFF systems in use by the North Atlantic Treaty Organization (NATO), are reviewed and updated based on the standards of NATO Standardization Agreement (STANAG 4193). The analysis shows that the current stage of development of the industry of National Defense, coupled with its ability to integrate with the technological centers of the Armed Forces, as well as the availability of budget for research and development, resulting from the National Defense Policy, are factors for the success of the project. Also, it exposes the importance of combining air defense and air traffic control in Brazil as a determinant factor for the success of the task. The solution should be based on maintaining the standards laid down in STANAG 4193 technical characteristics of interrogators and transponders of IFF Mark XII, keeping the processes of interrogation and “response”. Results indicate the need of providing grants to study the incorporation of Mode 5 and Mode S, in a second step.

**Keywords:** National IFF with Mode 4, Fratricide, National Defense industry, Indigenous technologies.

Nota: Este artigo reflete a opinião do autor e não necessariamente de sua Instituição.

Received: 13/09/10

Accepted: 28/09/10

## INTRODUÇÃO

No moderno combate aeroespacial, aí inclusos os embates aéreos (ar-ar) e a defesa antiaérea (terra-ar e mar-ar), são crescentes as buscas para incrementar o alcance dos armamentos: às aeronaves incorporam-se mísseis ar-ar e ar-superfície além do alcance visual (BVR – *beyond visual range*), conferindo alta possibilidade de acerto sem “o reconhecimento visual”; os sistemas antiaéreos de solo, de plataformas terrestres ou navais, aumentam seu raio de ação, buscando estender a letalidade de seus mísseis aos vetores de ataque com armas “fora do alcance” (*stand off weapons*) e em voo na casa dos 15 mil metros, também sem chance de identificação a vista pelos artilheiros antiaéreos. Aumentar o alcance significa maior probabilidade de vitória.

A identificação a vista dos alvos torna-se inexequível diante dos alcances estendidos das modernas armas de combate, apesar de a percepção (reconhecimento) visual de objetivos ser motivo de intenso treinamento para pilotos e integrantes da artilharia antiaérea de todos os países; portanto, aumenta-se o risco de fratricídios com o combate.

No controle de tráfego aéreo, surgem pleitos para atender ao vertiginoso aumento do número de aeronaves em circulação e para identificar aeronaves em situação de arresto, o que é preocupante nos dias atuais.

Este artigo aborda o desenvolvimento nacional do Sistema de Identificação Amigo-Inimigo (IFF – *Identification Friend or Foe*), que inclui a criptografia autóctone (Modo 4) e o interrogador e *transponder* compatíveis para o controle aéreo (militar e civil), contido no convênio firmado pelo Ministério da Ciência e Tecnologia com o Comando da Aeronáutica (Brasil, 2008a), num momento em que soluções nacionais para produção de sistemas de armas e meios de comando e controle têm crescido no ritmo da Política de Defesa Nacional (Brasil, 2008c) e da Estratégia Nacional de Defesa (Brasil, 2008b).

## OS FRATRICÍDIOS E OS MÉTODOS DE RECONHECIMENTO DO BRASIL

O emprego do vetor aéreo no combate moderno e a crescente capacidade dos armamentos por ele utilizados, num ambiente envolvendo forças blindadas de deslocamento rápido, não têm sido acompanhados por igual desenvolvimento nos sistemas de identificação. Agrava-se o risco de fratricídios nos dias atuais.

O pico do problema ocorreu nas Guerras do Golfo de 1991 e 2003, em que as perdas causadas por fratricídios nas forças americanas e aliadas atingiram índices alarmantes:

na Guerra de 1991, cerca de 17% do total (Lum, 1995), índice também apresentado com o valor de 25% (Hess, 2003); na guerra de 2003, o índice foi de 28% (Hess, 2003). A média, se considerados todos os conflitos envolvendo os Estados Unidos no século 20, é de 15% (Lum, 1995).

Na Guerra do Golfo de 1991, os incidentes foram limitados ao engajamento de alvos terrestres por plataformas aéreas e entre alvos terrestres. Já na Guerra do Golfo de 2003, fratricídios no combate aeroespacial aumentaram os índices. Como exemplos envolvendo aeronaves e a artilharia antiaérea (Hess, 2003), ficaram marcados o míssil *Patriot*, que abateu um tornado da *Royal Air Force* (Fig. 1), e a destruição de uma unidade de tiro *Patriot* por um *F-16*. Posteriormente, em 2 de abril de 2003, um míssil *Patriot* abateu um *F-18* a oeste de Karbala, no Iraque. O corpo do Tenente Nathan White, de 30 anos, foi resgatado numa operação com cerca de uma centena de militares da Marinha, dos Fuzileiros, Exército e Forças Especiais no dia 12 de abril de 2003. Hoje jaz, para o sofrimento dos militares e da família, no Cemitério Nacional de Arlington, Texas, Estados Unidos (Riggs, 2004).



Figura 1: Tornado abatido por *Patriot*. Fonte: Trim (2007).

Tais fratricídios revelam-se ainda mais assustadores dada a farta disponibilidade de meios de identificação e o amplo aparato de comando e controle dos Estados Unidos.

A Guerra das *Falklands* (Malvinas) deixou na memória dos militares argentinos recordações dolorosas, conforme relato de combate real do Major Luiz Alberto Puga Ramirez, da Força Aérea Argentina, em entrevista à Revista Aeronáutica (Souza, 1983, p. 19):

*[...] tem que se mencionar o gesto heróico, em que perde a vida o Cap GARCIA CUERVA, que é abatido pela própria artilharia. Este homem regressava de um provável ataque ao Hermes, que não foi até hoje confirmado, mas como o avião estava intacto [sic] mas não tinha combustível para chegar ao Continente, quis salvá-lo pois o país necessitava dele. Então tentou pousar em Porto Argentino [Port Stanley].*

No Brasil, os acréscimos de células na Aviação do Exército e Naval, somados à difusão de mísseis antiaéreos portáteis (*IGLA 9K-38*, *IGLA S* e *MISTRAL*) nas três Forças Armadas, sem sistemas de IFF como os da Fig. 2, aumentam os riscos de fratricídios em combate no país e sugerem maior coordenação entre as forças. Contudo, a adoção do Radar SABER M60 na artilharia antiaérea (AAAe) de baixa altura, dotada de mísseis portáteis (1ª Bda AAAe, 2007) com IFF incorporado nos Modos 1, 2 e 3/A (Tabela 1), reduz o problema, mas ainda carece do Modo 4, com criptografia.



Figura 2: Interrogadores para sistemas de artilharia antiaérea de curto alcance: AN/TPX-56 IFF Interrogator Set (esquerda) e AN/TPX-57(V) Common MK XIIA/ Mode 4/5 IFF Interrogator (direita). Fonte: Raytheon (2006, 2007).

No Brasil, evitam-se os fratricídios nos combates aeroespaciais com os processos ora disponíveis (Brasil, 2001), a saber:

- a identificação eletrônica amigo-inimigo do IFF (Seção 3) entre as plataformas aéreas, terrestres e navais que já possuem os equipamentos, principal forma de evitar o fogo amigo e controlar a localização de vetores; o Brasil está carente do Modo 4, mas estará acessível após o convênio (Brasil, 2008a) citado na Introdução;
- análise espectral de sinais do sensor primário do Radar SABER M60, capaz de indicar o modelo de

Tabela 1: Modos de Funcionamento (Operação) do IFF Mk X(A), XII e XII(A)

Modos militares	Modos civis	Utilização	$\Delta t$ entre P1 e P3 ( $\mu s$ )	Mk (OTAN)
1	-	Controle e identificação de tráfego aéreo militar	3	X(A)
2	-	Utilização militar em combate (regulado nas Normas Operacionais do Sistema de Defesa Operacional Brasileiro – NOSDA)	5	X(A)
3	A	Controle e identificação de tráfego aéreo civil e militar (compartilhado)	8	X(A)
	B	Controle e identificação de tráfego aéreo civil	17	-
-	C	Transmissão automática da altura da aeronave	21	-
	D	Utilização civil	25	-
4	-	Modo militar com criptografia	-	XII
5	-	Modo militar com espalhamento espectral	-	XII(A)

Fonte: The United States of America (2000b) (adaptado).



aeronaves de asas rotativas constante de seu banco de dados. O SABER diferencia alvos de asas fixas dos de asas rotativas (helicópteros), pela análise espectral do sinal refletido, que produz características específicas no caso dos helicópteros. Pode-se apontar o modelo do helicóptero pelo número e frequência de giro das pás, o que complementa o uso do radar secundário na identificação das plataformas. Por exemplo, se somente as forças amigas possuem o tipo de helicóptero indicado, este será identificado como amigo. Esse método possui limitações, pois há plataformas iguais em diferentes países e a alimentação do banco de dados depende da detecção do vetor para gravar a onda refletida ou de dados precisos das asas rotativas;

- identificação (percepção) visual das plataformas amigas e de outros países, processo incansavelmente treinado nas forças armadas, limitado ao alcance da vista humana e dependente da luminosidade, mas que pode ser incrementado por instrumentos óticos, como binóculos e câmeras com amplificação e dispositivos de visão noturna;
- análise do comportamento em voo das plataformas e das regras de circulação aérea nos volumes de responsabilidade da artilharia antiaérea. Se um vetor “quebra” as regras, como, por exemplo, ingressando no setor de defesa fora de um “corredor de segurança” arbitrado e com velocidade acima da permitida, poderá ser identificado como inimigo.

A capacidade adquirida para o reconhecimento de vetores aéreos pelo Sistema SABER M60 merece destaque, pois avanços significativos foram alcançados graças aos estudos da Universidade Estadual de Campinas (Unicamp), em parceria com a Orbisat da Amazônia Indústria e Aerolevantamento S.A., sob a coordenação do Centro Tecnológico do Exército (Unicamp, 2008).

Para evitar os fratricídios na terceira dimensão do combate, exercer o controle e executar as medidas de coordenação é fundamental, assim como o conhecimento prévio dos critérios de identificação no combate aeroespacial (ar-ar, superfície-ar e ar-superfície).

As ações de controle da artilharia antiaérea (superfície-ar), que podem ser válidas também de ar para superfície e entre vetores aéreos, desenvolvem-se sob as formas de:

- controle positivo, alicerçado na obtenção de dados em tempo real por emissões eletromagnéticas: sistemas de IFF, sensores primários que permitam a análise espectral do sinal recebido, processadores e enlaces de comunicações;

- controle de procedimentos que complementa o positivo e baseia-se na delimitação do espaço aéreo por volumes e no estabelecimento de estado de ação (grau de liberdade para abrir fogo das armas – Fogo Livre, Restrito, Interdito e Designado);
- controle misto, método completo, uma vez que engloba os dois anteriores (Brasil, 2001).

A definição de ação hostil é particularmente importante para os critérios de identificação de vetores amigos. A ação hostil classifica automaticamente como inimigo o vetor aéreo que a comete e acarreta a imediata abertura do fogo antiaéreo (ou aéreo).

Uma aeronave ou veículo aéreo não tripulado comete uma ação hostil quando ataca força amiga ou aliada; ataca instalações militares ou civis, amigas ou aliadas; ataca aeronave amiga ou aliada; executa ações de guerra eletrônica contra forças ou instalações, amigas ou aliadas; lança paraquedistas ou desembarca material de uso militar em território sob controle de forças amigas ou aliadas, sem a devida autorização.

Uma aeronave que adentra um volume de responsabilidade de uma defesa antiaérea ou o raio de ação de um vetor aéreo pode ser classificada como amiga, inimiga ou desconhecida (Brasil, 2001).

Será amiga, a menos que cometa uma ação hostil, quando for reconhecida como tal por um centro de controle da Força Aérea ou centro de operações de artilharia antiaérea; seu comportamento em voo a faz reconhecida como amiga; é reconhecida a vista como amiga ou emite código de reconhecimento eletrônico correto que permite sua identificação (IFF), ou a análise espectral indica ser de padrão de aeronave amiga (Brasil, 2001).

Será classificada como inimiga quando cometer uma ação hostil; quando for reconhecida como inimiga por um centro de controle da Força Aérea ou centro de operações de artilharia antiaérea como tal; quando seu comportamento em voo a faz reconhecida como inimiga; quando for reconhecida a vista como inimiga; quando permanecer em silêncio diante da interrogação ou emitir código de reconhecimento eletrônico (IFF) incorreto ou diferente do código em vigor, ou a análise espectral indica não ser de padrão de aeronave amiga (Brasil, 2001).

Será desconhecida quando for reconhecida como tal por um órgão de controle da Força Aérea ou centro de operações de artilharia antiaérea, ou não for possível identificá-la como amiga ou inimiga (Brasil, 2001).

## O SISTEMA *IDENTIFICATION FRIEND OR FOE*

### Generalidades

O Sistema IFF é uma “forma de reconhecimento” entre plataformas navais, terrestres e aéreas, executada por intermédio de uma “pergunta” padrão (pulso de interrogação) – feita por um “interrogador” a bordo de uma das plataformas, para a qual é emitida – e uma “resposta” codificada (pulso de resposta) por um *transponder* em outra plataforma.

Caso a “resposta” esteja correta, ou seja, conste de uma lista de códigos do sistema de inteligência, o possível alvo pode ser reconhecido como amigo. Se o alvo não “responde”, ou seja, permanece “passivo”, não é possível identificá-lo eletronicamente.

Uma só plataforma pode estar equipada com interrogadores e *transponders*, caso típico de aeronaves destinadas à interceptação aérea e de navios destinados ao combate naval; Sistemas IFF (*Combat Id*) ainda são raros em viaturas terrestres blindadas de combate, existentes em relação seleta de países, em uma lista que não inclui o Brasil.

O Sistema IFF difere do radar primário, pois não há simples reflexão de energia pelo alvo; no caso do IFF, há uma comunicação codificada entre as plataformas interrogadora e interrogada. Pode-se dizer que o IFF complementa o radar primário, sem dispensá-lo. Por esse motivo, também é dito “radar secundário” (SSR – *Secondary Surveillance Radar*).

O radar primário é essencial em combate, dada a falta de “resposta” de inimigos; no caso do controle do tráfego aéreo, o SSR sobressai em importância, por ter maior probabilidade de detecção e permitir troca de dados.

O Sistema IFF possui formas diferentes de operação, ditos Modos de Funcionamento (Operação), que definem os padrões do sinal, conforme mostra a Tabela 1.

O Pulso de Interrogação do IFF nos modos convencionais (exceto nos Modos 4 e 5) é formado por “trem” de três pulsos (P1, P2 e P3) e o tempo em microssegundos ( $\mu s$ ) entre P1 e P3 define o Modo de Interrogação; P2 destina-se à supressão dos lóbulos secundários. As “respostas” dos *transponders*, mesmo dos mais simples como o da Fig. 3, nos modos convencionais (exceto 4 e 5), têm a mesma estrutura, com dois pulsos (F1 e F2) separados por um tempo fixo ( $\mu s$ ). No tempo entre F1 e F2 encontram-se até 12 pulsos, cujas presenças ou ausências permitem obter as combinações, os “códigos” (STANAG 4193).

As plataformas navais e terrestres normalmente têm os dispositivos eletrônicos associados fisicamente e com



Figura 3: ARC (Cessna) RT-359A *Transponder*. Fonte: Bennet Avionics (2010).

antenas solidárias, por vezes com emissão defasada em  $180^\circ$ , como no caso do Radar SABER M60: a antena do radar primário emite para frente e a do secundário, para trás do dispositivo (Fig. 4).



Figura 4: Radar SABER M60 (antenas do radar primário e IFF solidárias, com emissão defasada em  $180^\circ$ ). Fonte: adaptado de Abdalla (2008).

Os Modos de Interrogação e as respostas dos sistemas IFF constam na Fig. 5.

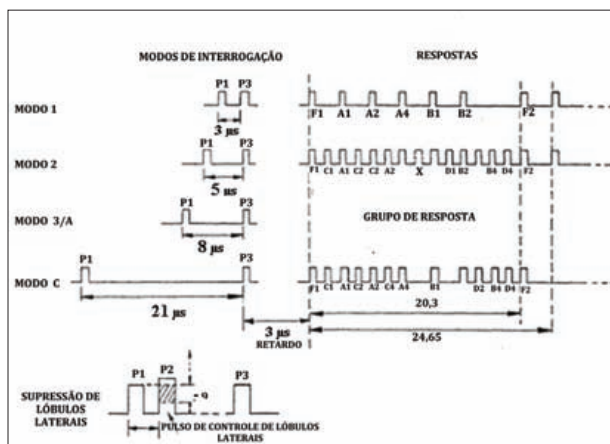


Figura 5: Modos de interrogação e resposta do IFF MARK X(A). Fonte: NATO (1990a) (adaptado).

## A Organização do Tratado do Atlântico Norte e suas normas de padronização

A Organização do Tratado do Atlântico Norte (OTAN), principal pacto militar de coligação de países na Europa Central e Ocidental, possui padrões para a produção dos seus sistemas de defesa.

O Sistema IFF da OTAN é um processo de reconhecimento entre plataformas de combate muito difundido nos países de cultura ocidental. Os padrões do IFF estão listados nas Normas de Padronização da OTAN 4193 (*Standardization Agreement – STANAG 4193*) nos fascículos a seguir:

- Parte I: Descrição Geral dos Sistemas IFF;
- Parte II: Performance do IFF na Presença de Contramedidas Eletrônicas;
- Parte III: Características Técnicas dos Equipamentos Instalados em Interrogadores e *Transponders* dos Sistemas IFF Mk X(A) e XII;
- Parte IV: Características Técnicas dos Interrogadores e *Transponders* dos Sistemas Militares de IFF Mk X(A) e Mk XII no Modo S;
- Parte V: Requisitos de Interoperabilidade no Modo 5;
- Parte VI: Especificações de Criptografia para a Interoperabilidade no Modo 5.

As Partes I e III foram publicadas em 12 de novembro de 1990 e a Parte IV, em 12 de abril de 1999. A Parte II das STANAG 4193 possui classificação sigilosa e seu acesso é restrito. As partes V e VI não estão acessíveis a consulta por países não signatários da OTAN, caso do Brasil.

Os modos civis do IFF são regulados pelo órgão encarregado da normatização para a segurança do desenvolvimento da aviação civil e do uso do espaço aéreo, a Organização Internacional de Aviação Civil (ICAO – *International Civil Aviation Organization*).

Os equipamentos IFF em uso atualmente no Brasil seguem os padrões da OTAN, apesar de o país não estar contido no bloco, ou seja, não é signatário da OTAN. Os padrões da OTAN devem ser mantidos no projeto ora em desenvolvimento, de acordo com o previsto pelo contrato que regula o Convênio (Brasil, 2008a) – será baseado nos requisitos operacionais descritos nas STANAG 4193 I e III (Brasil, 2008a).

## As versões do IFF e seus aperfeiçoamentos

O Mk I, primeiro Sistema IFF em uso, foi projetado em 1939 e entrou em serviço em 1940 (Carroll, 1999). Desde então, o IFF evolui com constância, destacando-se as seguintes versões (The United States of America, 2000b):

- Mk X, disponível em três variantes:
  - Mk X (BASIC): o sistema pode “responder” apenas por um Modo de Funcionamento, pois códigos não estão disponíveis no *transponder*. Apesar de ser considerado obsoleto, ainda está em uso por alguns países, inclusive o Brasil. O Mk X (BASIC) não é compatível com IFF Mk X (SIF), IFF Mk X(A) e IFF Mk XII;
  - Mk X (SIF – *Selective Identification Feature*): acresce ao Mk X (BASIC) a capacidade de interrogação com códigos de resposta, diferenciados em quantidade de acordo com os Modos de Funcionamento (Interrogação), que são o Modo Militar 1 (32 códigos), Modo Militar 2 (4096 códigos) e Modo Militar 3 (64 códigos). Funcionalidades para identificação especial de aeronaves e em situação de emergência também estão disponíveis, assim como a Supressão de Lóbulos Secundários no Pulso de Interrogação (ISLS – *Interrogation Sidelobe Supression*);
  - Mk X(A): incorpora ao Mk X (SIF) o Modo “C”, modo de vigilância adequado ao controle do tráfego aéreo, pois a altitude da aeronave, medida pela própria aeronave, é transmitida e recebida automaticamente pelo sistema. Também acresceu ao Modo Militar 3 a capacidade de operar com 4096 códigos. O Modo Militar 3 passou a ser compartilhado com o civil, sendo designado como 3/A, como exhibe a Fig. 5. A maioria dos IFF em uso no Brasil são Mk X(A), e os códigos sigilosos do Modo 2 têm o uso regulado nas Normas Operacionais do Sistema de Defesa Operacional Brasileiro (NOSDA) (Brasil, 2002).
- Mk XII, com duas versões:
  - Mk XII: equipamento compatível com o IFF Mk X (SIF) e Mk X(A), mas que pode operar também no Modo de Funcionamento (Operação) 4, Modo Militar com criptografia para maior segurança do sigilo da codificação. O Modo 4 é empregado com codificação “encriptada” por algoritmos próprios, podendo servir a um único país ou a coligação de países.



O IFF Mk XII também é conhecido nos Estados Unidos pela sigla AIMS:

ATCRBS – *Air Traffic Control Radar Beacon System*

IFF – *Identification Friend or Foe*

Mk XII – *Mark XII*

S – *System*

- Mk XII(A): o Mk XII(A) - Modo 5 é o último acréscimo ao IFF e seu maior aperfeiçoamento. Os níveis 1 e 2 do Modo 5 são criptografados, pois a informação possui codificação como no Modo 4 e a modulação é feita com “espalhamento espectral” do sinal, por variação de frequência da onda portadora, além de autenticação temporal de hora e dia.

Onível 1 do Modo 5 é semelhante ao Modo 4, mas acrescido da identificação do número exclusivo da aeronave (PIN – *Platform Identification Number*). O nível 2 do Modo 5 é o mesmo do nível 1, com a informação adicional da posição do vetor (GPS) e outros atributos (Fig. 6). Com o Modo 5, a identificação em combate (*Combat ID*) é obtida entre plataformas aéreas, navais e terrestres.



Figura 6: Níveis 1 e 2 do Modo 5 do IFF. Fonte: Trim (2007).

O nível 3 do Modo 5 pode operar com a “interrogação seletiva” de uma só plataforma e a resposta com os dados das questões feitas (como situação das armas). Todas as “perguntas” feitas à plataforma são por ela respondidas, e só por ela.

O nível 4 do Modo 5 é o mais completo de todos e contribui decisivamente para atingir a desejada “consciência situacional”<sup>1</sup> (*situation awareness*), tão necessária para esclarecer a “confusão” do combate moderno. Dados como PIN, proa, posição, nível de combustível, velocidade, identificação, estado das armas, entre outros, de todos os vetores, sejam aéreos, navais ou terrestres, podem ser trocados (Fig. 7).



Figura 7: Níveis 3 e 4 do Modo 5 do IFF. Fonte: Trim (2007).

Por isso, ao utilizar o Modo 5, duas deficiências do Sistema IFF das versões e modos anteriores são resolvidas:

- a facilidade de interferência intencional ou acidental, seja por parte de força adversa ou causada sem intenção deliberada, o que diminui a confiabilidade do sistema num ambiente de intenso

<sup>1</sup> A consciência situacional é a percepção dos elementos de um ambiente complexo, dentro de um volume de espaço e no tempo presente, a compreensão dos seus significados, a projeção do seu *status* para um futuro próximo e suas implicações para o processo decisório (Endsley *et al.*, 1998).



combate eletrônico ou próximo a grandes centros que não controlam as emissões eletromagnéticas proibidas pela ICAO, dado o estabelecimento de frequências padrão para interrogação e respostas dos *transponders*, respectivamente 1.030 e 1.090 MHz. O Modo 5, com espalhamento espectral, é menos suscetível às atividades de guerra eletrônica e emissões geradas sem licenças, tais como de rádios “piratas”;

- a impossibilidade de obter-se a “consciência situacional” por apenas indicar se a plataforma é amiga ou inimiga, com necessidade de processos adicionais de identificação (visual, procedimentos em voo e análise da situação, entre outros) e sem localizá-la com precisão; o Sistema IFF sem o Modo 5 não identifica de imediato a plataforma e não obtém acuidade na localização do vetor. Não é obtida a “consciência situacional”, resumida de uma maneira geral em três perguntas: “Onde estou?”, “Onde estão os inimigos?” e “Onde estão os amigos?”, referenciadas ao tempo presente e inseridas num sistema de comando e controle para a interpretação de seus operadores. Por intermédio do *combat ID*, o Modo 5 responde essas perguntas essenciais.

Em outubro de 2004, testes liderados pela Marinha Norte-Americana (*US Navy*), com a presença de plataformas da Força Aérea Norte-Americana (*US Air Force*), obtiveram sucesso em testes do Modo 5 do IFF, segundo artigo de Randy Geck, repórter do periódico *dcmilitary.com* para o Programa PMA-213:

*O Escritório do Programa de Identificação de Combate e Controle do Tráfego Aéreo - PMA 213 - gerencia os esforços para a aquisição pela Marinha do EUA desta nova capacitação. Planejamentos para este voo começaram aproximadamente três anos atrás e culminaram em outubro com o sucesso da aplicação do Modo 5 em três separadas plataformas aéreas, bem como em duas estações de superfície, de acordo com o líder de Testes de Voos da Marinha, Ken Senechal. Os outros membros de equipe foram o Capitão Maghan McNiff, da Força Aérea, e Andy Leone, da Administração Federal de Aviação (FAA). (Geck, 2004, tradução nossa).*

De acordo com os Termos de Referência (TOR – *Terms of Reference*) do Grupo de Estudo do Modo 5 do IFF da Organização de Simulação dos Padrões para a Interoperabilidade (SISO – *Simulation Interoperability Standards Organization*), a maioria das plataformas de combate e unidades estariam com equipamentos de IFF aperfeiçoados no Modo 5 num prazo de cinco anos, a contar de 2005 (Berry, Byers and Madison, 2004).

## O Modo S

O vertiginoso crescimento da circulação aérea civil e militar aumentou a necessidade de aperfeiçoamentos no desempenho do IFF nos Modos Cíveis A e C. Por isso, a Organização Internacional da Aviação Civil realizou estudos que resultaram no Modo S, ferramenta poderosa para facilitar o tráfego aéreo nos céus congestionados.

Os interrogadores e *transponders* do Modo S, como mostrado na Fig. 8, foram programados para serem compatíveis com os Modos A e C.



Figura 8: Interface homem-máquina do IFF AN/APX-100 Mark XII/Modo S IFF Transponder. Fonte: Raytheon (2008).

O Modo S incorpora melhorias na vigilância e nas comunicações para a automação do tráfego aéreo, com possibilidade de controle de um número muito maior de aeronaves, com uso de *datalink*. O Modo S, quando adotado pelos países ou bloco, marca o fim da divisão do controle do espaço aéreo por áreas. No Brasil, os Centros Integrados de Defesa Aeroespacial e Controle de Tráfego Aéreo (Cindacta) poderiam ser fundidos em uma só unidade, por exemplo.

O *datalink* do Modo S reduz a possibilidade de acidentes com choque aéreo devido à melhoria do Sistema para Evitar Colisão Aérea (ACAS – *Airborne Collision Avoidance System*).

Além dos incrementos do Modo S já citados, destacam-se também a sua técnica monopulso, que reduz o número de interrogações necessárias para identificação da aeronave, e o emprego do “código de endereço” (*Address Code*), como código único de uma aeronave em qualquer área de tráfego (PIN), permitindo interrogação direcionada para uma aeronave em particular e resposta recebida sem ambiguidade; no Modo S, não há interferência entre as respostas de *transponders* de aeronaves próximas.

## Veículos aéreos não tripulados

Uma nova vertente na defesa aeroespacial e no controle do tráfego aéreo surge com a desenfreada difusão dos veículos aéreos não tripulados (VANT), de tamanhos e pesos variados, operando com raios de ação cada vez maiores e cumprindo as mais diversas finalidades, desde ações de vigilância eletrônica em grandes centros até diversas ações de combate. Nos dois casos, os estudos crescem, seja para uso dos VANT em ações de combate ou para defender-se deles com a AAAe, seja para a sua inserção nos domínios dos centros de controle do tráfego aéreo, pois sua circulação ainda não está regulamentada. O problema dos VANT é complexo, pois envolve diversificados modelos com maneiras distintas de controle, desde veículos remotamente controlados até pré-programados, com autonomias diversas e cargas úteis (*payloads*) muito diferenciadas.

Como os custos dos VANT diferem muito e o seu emprego nem sempre requer um controle por centros de tráfego aéreo, permanece a dúvida sobre como dotá-los de IFF e regulamentar seu uso.

## O MODO 4

Para evitar uma intromissão não autorizada ou interferência nos equipamentos IFF, seja nos interrogadores ou *transponders*, incluindo o caso em que os dispositivos venham a cair em mãos hostis, o Modo 4 do IFF surgiu como solução ao empregar um código de chaves de difícil quebra e que devem ser periodicamente inseridas em cada equipamento, evitando a ação inimiga no comando e controle. Será, no caso do convênio em andamento (Brasil, 2008a), o diferencial para os IFF em uso no Brasil.

## O equipamento criptográfico

As interrogações codificadas são dependentes do modo de operação. As respostas codificadas recebidas a partir de um *transponder* cooperativo são processadas para verificar sua validade e fornecer indicações adequadas para o operador. No IFF Mk XII, Modo 4 do Sistema IFF, a codificação dos interrogadores e *transponders* é realizada por uma unidade de criptografia, existente somente se o Modo 4 está em operação.

A solução padrão normalmente adotada é o interrogador e o *transponder* (ou o equipamento com as duas finalidades) possuírem uma unidade criptográfica exclusiva para tal fim, projetada para realizar a formulação dos códigos de interrogação e a verificação das respostas, gerando a codificação de forma autônoma e independente (Fig. 9).



Figura 9: IFF 4760 com criptógrafo (direita) e sem criptógrafo (esquerda). Fonte: Jane's 1995-1996.

Observa-se que esse modelo de solução acarreta maior necessidade de componentes eletrônicos nos vetores, sejam aéreos, terrestres ou navais. Em plataformas de menor porte e com pouco espaço – como aeronaves dotadas de grande quantidade de visores e controles, casos de aviões de caça de interceptação, por exemplo – criptógrafos podem ser de difícil instalação em face das limitações físicas de espaço.

Se um equipamento de interrogação ou *transponder* não suporta tal unidade criptográfica por limitação física ou se deseja um equipamento mais simples e de menor volume e tamanho, pode-se criar uma facilidade ao instalar-se uma “unidade de armazenamento” de códigos do Modo 4. Nesse caso, a “unidade de armazenamento” estocará um bloco de informações que contém uma quantidade de interrogações no Modo 4 e os correspondentes atrasos das respostas dos *transponders*; a cada código armazenado corresponde uma combinação “código de interrogação do Modo 4/atraso do *transponder*”.

Quando há limitações no tamanho do armazenamento dos códigos do Modo 4, a interrogação poderá ser randomicamente ou pseudo-randomicamente selecionada da caixa de armazenamento (STANAG 4193-I). O código é derivado de uma unidade externa de criptografia do Modo 4 e “carregado” por pequenos dispositivos eletrônicos, e sugere-se que até *pen drives* ou diminutos cartões de dados possam ser utilizados pelo IFF nacional, dada a evolução dos meios eletrônicos e a facilidade de sua obtenção.

Uma acurada análise dos equipamentos IFF já existentes nas três Forças Armadas – e de amostras de SSR de plataformas civis, de diferentes origens, e das limitações físicas das plataformas – pode conduzir a soluções diferenciadas. Um exemplo de solução para o Brasil poderia ser a instalação de criptógrafos externos para plataformas aéreas e criptógrafos embutidos em navios da Marinha do Brasil.

Como uma saída possível, aponta-se que os aviões, e com mais ênfase os caças, podem possuir restrições

nas instalações físicas, porém mobilidade suficiente para “carregar” os códigos em aeroportos diversos. Em situação oposta está o caso dos navios, pois possuem amplas instalações e o longo isolamento da belonave no mar pode dificultar as cargas de códigos.

Indica-se que os padrões criptográficos e o número de códigos a ser armazenado nas plataformas, originados em criptógrafos externos, sejam determinados pela própria Força Aérea, por intermédio do Instituto Tecnológico da Aeronáutica (ITA), sob a coordenação do Ministério da Defesa, para manter a padronização.

Contudo, indica-se que a decisão da solução do tipo de criptógrafo (externo ou embutido) a ser instalado nas plataformas militares navais, terrestres ou aéreas deva caber a cada uma das Forças Armadas, por melhor conhecerem suas plataformas.

É adequado que plataformas de mesmo modelo, mas de Forças Armadas diferentes, possuam o mesmo padrão físico de Sistema IFF (interrogadores e *transponders*), por facilitar a logística, propiciando aquisições centralizadas pelo Ministério da Defesa, cabendo, portanto, a sua supervisão.

Recomenda-se, por fim, que os padrões físicos e criptográficos dos interrogadores e *transponders* do Sistema IFF devam ser mantidos pelas três Forças Armadas, em qualquer das soluções adotadas, por favorecerem as atividades logísticas e facilitarem a produção em série, adequada às vendas no Brasil pela indústria nacional de defesa.

## Os padrões de funcionamento do Modo 4

### A Interrogação do IFF no Modo 4

As STANAG 4193 preconizam que cada interrogação do IFF no Modo 4 seja composta de um grupo de pulsos sincronizados e uma informação do grupo de pulsos (P1, P2, P3 e P4), como mostra a Fig. 10.

De forma diferente dos demais Modos do IFF, no caso do Modo 4, a ISLS é feita pelo pulso P5, emitido 8  $\mu$ s após P1.

Uma “palavra-teste” não irradiada, designada “Palavra-Teste” A resulta em uma resposta posicionada no primeiro grupo, gerada pela unidade criptográfica e com chave de códigos de manutenção, quando o Código A é selecionado no painel de controle. Da mesma forma, quando o Código B é selecionado no painel de controle (Fig. 11), uma “palavra-teste” B é gerada no 16º grupo de respostas.

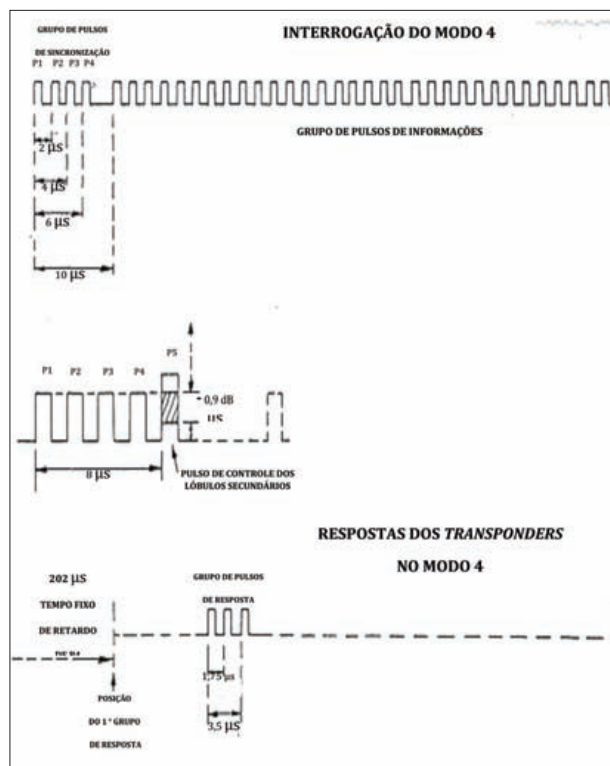


Figura 10: Interrogação e resposta do IFF MARK XII (Modo 4).  
Fonte: adaptado de NATO (1990a).



Figura 11: Interface homem-máquina do IFF AN/APX-100 (V) IFF Mark XII Transponder Set. Fonte: Raytheon (2008).

### Respostas de um transponder no Modo 4

A posição do primeiro grupo de respostas de um *transponder* no Modo 4, como descrito nas STANAG 4193, ocorre num tempo de retardo fixo de 202  $\mu$ s, após o pulso de interrogação P4 (Fig. 10).



Cada resposta do Sistema IFF no Modo 4 consiste de um grupo de três pulsos. O intervalo entre o primeiro e o segundo grupo é de  $1,75 \mu\text{s}$  ( $\pm 0,03 \mu\text{s}$ ), e o intervalo entre o primeiro e terceiro é de  $3,5 \mu\text{s}$  ( $\pm 0,03 \mu\text{s}$ ).

O primeiro pulso do Grupo de Respostas ocorre aleatoriamente em uma das 16 posições nominais múltiplas de  $4 \mu\text{s}$ , após o retardo fixo de  $202 \mu\text{s}$ .

O Grupo de Respostas é posicionado no Primeiro Grupo de Respostas, para a “Palavra-Teste” A, e no Décimo Sexto Grupo de Respostas, para a “Palavra-Teste” B. O Grupo é originado numa unidade criptográfica com chaves apropriadas, em resposta à “Palavra-Teste” do interrogador, mencionada na subseção anterior.

### Os controles da interface homem-máquina do Modo 4

Como previsto na STANAG 4193-I, os controles da interface homem-máquina do Modo 4 do Sistema IFF permitem a seleção do código de operação (*Code Select A/B*), o acionamento da alimentação autônoma (*Hold*), a função de “reinício” (*Zeroize*) e de seleção de supressão do alarme sonoro (*Override*).

#### Seleção de código (*Code Select A/B*)

A função de seleção no Modo 4 permite ao operador habilitar os dois grupos de códigos do Modo 4 pré-estabelecidos, A ou B (Fig. 12, item 16).

#### Alimentação autônoma

A função de alimentação autônoma (*Hold*) habilita a retenção dos códigos selecionados do Modo 4 nos computadores de interrogação (*Kit*) e dos *transponders* (*Kir*), se toda a energia é removida do sistema.

Para fornecer segurança física para as seleções feitas no Modo 4, considerações operacionais devem ditar o mais prudente método de prover a função *Hold*.

Nas plataformas aéreas, com os equipamentos reduzidos (ou sistemas funcionais equivalentes) e com fonte primária ou emergencial aplicada aos computadores *Kit/Kir*, a seleção da função *Hold* (automática ou manual) deve ser desabilitar a função *Zeroize*, se há uso da função *Hold* nos dispositivos *Kit/Kir*.

Nas aeronaves em que a alimentação de corrente contínua de emergência está disponível, o seu uso é preferível, ao invés da função *Hold*, para prevenir perda acidental dos

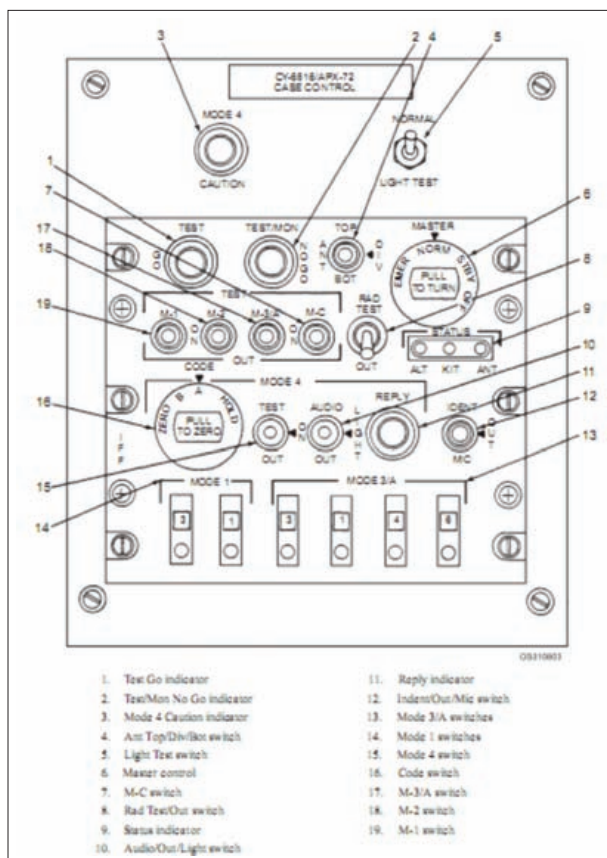


Figura 12: Interface homem-máquina do *Transponder Set Control C-6280A(P)/APX in Control Enclosure CY-6816/APX-72*. Fonte: The United States of America (2000b).

códigos do Modo 4, quando a energia primária é removida do sistema.

Nas aeronaves em que a alimentação de corrente contínua não é viável ou seu uso é impraticável, deve ser incorporada a função *Hold* automaticamente quando o equipamento de pouso tem energia reduzida. A retração do equipamento de pouso (ou equivalente funcional), com a fonte de energia primária aplicada, pode reiniciar as unidades de criptografia *Kit/Kir* e causar a perda da codificação e, por isso, manter o que propõe as Normas de Padronização da OTAN (STANAG 4193) é aconselhável.

Assim, considera-se correta a recomendação das STANAG 4193 de que o uso contínuo da função *Hold* em aeronaves não é aconselhável, sugerindo-se ser inadequada a sua utilização pelo Sistema IFF nacional do Modo 4.

Nos navios da Marinha do Brasil, em que a alimentação de corrente contínua não está disponível ou seu uso é impraticável, aconselha-se que deva ser fornecida a função *Hold* continuamente, como sugerem as STANAG 4193.



Para os sistemas de superfície, o uso da função *Hold* é desaconselhado pelas STANAG, também coerentemente.

#### *“Reinício” (Zeroize)*

A função *Zeroize* do Modo 4 consiste em fazer a unidade criptográfica apagar os Códigos A e B, quando o Modo 4 da unidade de criptografia é capaz de responder ao comando.

Como recomendam as STANAG 4193 para o Modo 4, no IFF nacional devem ser providenciados meios para impedir a seleção involuntária da função *Zeroize*, o que normalmente é feito por controle de pressão e giro (Fig. 12, item 16).

#### **Supressão do alarme sonoro (*Override*)**

A função *Override* permite ao operador anular os efeitos do ruído de alarme e restaurar a unidade de criptografia para a condição de “não alarme”.

Essa função existe, pois, por vezes, a repetição do alarme sonoro atrapalha a atenção do(s) operador(es) ou piloto(s), além de concorrer com outros sons, como dos receptores alerta-radar (RWR – *Radar Warning Receiver*), caso bastante comum nas plataformas aéreas de alta performance destinadas ao combate aeroespacial, os caças aéreos, mas que também ocorre com outros tipos de aviões.

Por isso, uma verificação dos equipamentos com alertas sonoros das plataformas aéreas nacionais deve preceder à adoção do Sistema IFF nacional com o Modo 4, de modo a evitar sons coincidentes que possam confundir os pilotos.

### **O FATOR POLÍTICO E A PRODUÇÃO DA INDÚSTRIA NACIONAL DE DEFESA**

Aumentar a eficiência dos armamentos, resolver os problemas de fraticídios e da possibilidade de “caos” aéreo são preocupações latentes no país, representado nesses preitos pelo Ministério da Defesa.

Soluções nacionais decorrem da Política de Defesa Nacional em vigor (decreto nº 5.484, de 30 de junho de 2005), que tem por diretriz, entre outras, “a busca de um nível de pesquisa científica, de desenvolvimento tecnológico e da capacidade de produção, de modo a minimizar a dependência externa do País quanto aos recursos de natureza estratégica de interesse para a sua defesa”.

No Brasil, a perspicaz e audaciosa decisão de agregar a defesa aeroespacial ao controle do tráfego aéreo é fator de peso para a escolha do modelo de desenvolvimento de sistemas de IFF militares, pois o seu fomento e solução podem atender às duas demandas simultaneamente. Sem dúvida alguma, o recebimento de recursos para o controle de tráfego beneficia o competente Comando de Defesa Aeroespacial Brasileiro (COMDABRA), um dos motivos que o torna tão eficiente.

Em ambos os casos – defesa aeroespacial e controle do tráfego aéreo – o desenvolvimento nacional dos sistemas de identificação e controle (IFF) tem importância vultosa.

Assim, o segmento científico-tecnológico do país voltado para a defesa aeroespacial, única área bélica do Brasil que possui um comando combinado das Forças Armadas ativo desde os tempos de paz, o COMDABRA, busca, com veemência, produzir e aprimorar seu poderio, coordenando os esforços e baseando-se na integração das indústrias de materiais de defesa com institutos tecnológicos, exercendo o seu papel de líder na área de monitoramento, como preconiza a Estratégia Nacional de Defesa (Brasil, 2008b, grifo nosso, p. 20):

*O Comando de Defesa Aeroespacial Brasileiro (COMDABRA) será fortalecido como núcleo da defesa aeroespacial, incumbido de liderar e de integrar todos os meios de monitoramento aeroespacial do país. A indústria nacional de material de defesa será orientada a dar a mais alta prioridade ao desenvolvimento das tecnologias necessárias, inclusive aquelas que viabilizem independência do sistema de sinal GPS ou de qualquer outro sistema de sinal estrangeiro.*

É compreensível a ideia de buscar tecnologias que minimizem a perda, em combate, das facilidades oferecidas pelo GPS; o fato de os Estados Unidos terem decidido retirar o erro de degradação intencional do sistema GPS (SA – *Selective Availability*) – entre o transcorrer dos anos de 2000 e 2006, gradativamente, conforme anúncio da Imprensa Oficial dos Estados Unidos, de 1º de maio de 2000 – não os impede de negar a disponibilidade do sinal, onde e quando entendam ser necessário (The United States of America, 2000a, grifo nosso):

*[...] My decision to discontinue SA was based upon a recommend by the Secretary of Defense in coordination with the Departments of State, Transportation, Commerce, the Director of Central Intelligence, and other Executive Branch Departments and Agencies. [...] Along with our commitment to enhance GPS for peaceful applications, my administration is committed to preserving fully the military utility of*

*GPS. The decision to discontinue SA is coupled with our continuing efforts to upgrade the military utility of our systems that use GPS, and is supported by threat assessments which conclude that setting SA to zero at this time have minimal impact on national security. Additionally, we have demonstrated the capability to selectively deny GPS signals on a regional basis when our national security is threatened[!].*

Surgem exemplos da produção de armamentos nacionais usados na defesa aeroespacial: o míssil Anti-irradiação MAR-1 (BVR) (Centro Tecnológico da Aeronáutica/Mectron) vem sendo incorporado ao poderio da Força Aérea Brasileira (Vitorino, 2000) e a linha dos Radares de Vigilância e Busca SABER tem projeto em andamento (M200) ou já está em fase de incorporação (M60) (Centro Tecnológico do Exército (CTEx)/Orbisat da Amazônia Indústria e Aerolevanteamento S.A.) (Jones and Pimentel, 2009). No caso do Radar SABER M200, a intenção é buscar a capacitação nacional para a produção de sensores a serem usados nos sistemas de artilharia antiaérea de média altura, ainda inexistentes no Brasil e, por extensão, no controle de tráfego aéreo, para cumprir o previsto na Estratégia Nacional de Defesa (Brasil, 2008b, p.16 grifo nosso):

*Nos centros estratégicos do país – políticos, industriais, tecnológicos e militares – a estratégia de presença do Exército concorrerá também para o objetivo de se assegurar a capacidade de defesa antiaérea, em quantidade e em qualidade, sobretudo por meio de artilharia antiaérea de média altura.*

A incorporação de uma artilharia antiaérea de média altura no país aumentará consideravelmente o nível de dissuasão, mas acrescentará necessidades extras de coordenação para evitar fraticídios, em exercícios de tempos de paz e, mais ainda, em combate.

Constata-se como estratégica a capacitação técnica e estrutural da Orbisat da Amazônia Indústria e Aerolevanteamento S.A. na produção de radares de busca (aquisição) e vigilância, fruto da parceria com o CTEx (Poggio, 2009), na linha de sensores radares (SABER), e que teve aproveitamento do êxito pelo Comando da Aeronáutica, por intermédio do ITA, executor do convênio (Brasil, 2008a), e do Instituto de Aeronáutica e Espaço (IAE), co-executor, suscitando o nascimento da produção nacional de antenas, interrogadores e *transponders* de IFF nos Modos 1, 2, 3/A e 4 (Projeto S200). Por isso, sugere-se que deva ter início um protocolo de entendimento do CTEx, com o Centro Tecnológico da Aeronáutica e, por extensão, entre o Exército Brasileiro e a Força Aérea Brasileira, sob a égide do Ministério da Defesa, para troca de informações.

Convém ressaltar a necessidade que surgirá de a Força Aérea rever as NOSDA, para atender à nova demanda de regular o emprego do Modo 4, quando estiver disponível.

Para o aproveitamento das informações geradas pelo radar secundário produzido no Brasil, seja na defesa aeroespacial ou no controle de tráfego aéreo do país, deve-se prever a camada de aplicação com o formato dos protocolos de transmissão de dados já adotado pela Força Aérea Brasileira, o ASTERIX (*All Purpose Structured Eurocontrol Radar Information Exchange Format*), como já prescreve o escopo do projeto em sua intenção (Brasil, 2008a). Nesse caso, as relações já existentes entre a Força Aérea e a Fundação ATECH Tecnologias Críticas suprem as demandas, existindo *softwares* autóctones disponíveis.

Outra avaliação necessária, no mais alto nível da Defesa, é a verificação da validade de ingresso do Brasil no Bloco da OTAN, o que facilitaria a produção de equipamentos em conjunto com integrantes desse bloco, de modo a facilitar a obtenção de tecnologia e também dos padrões já existentes, bem como a troca de experiências nos processos de produção.

O desenvolvimento de sistemas de armas e de comando e controle no Brasil, como mísseis e radares (primários e secundários), contribui para aumentar o poderio bélico do Brasil, mas ainda é preciso buscar, com muita ênfase, a escala industrial de produção e a criação de facilidades para a sobrevivência das indústrias de material de defesa.

Não se pode também deixar de atender à celeridade no desenvolvimento e produção nacionais de materiais de emprego militar, que pode ser obtida por aquisições pontuais de produtos bélicos com valor tecnológico agregado, de maneira a aumentar rapidamente o poder dissuasório do país em face de ameaças externas episódicas, posto que o desenvolvimento independente, por vezes, alonga-se no tempo.

## CONCLUSÕES

Os fraticídios representam uma preocupação durante as ações de combate aeroespacial no Brasil; é evidente a importância da produção de um Sistema de IFF nacional com o Modo 4, controle positivo em tempo real, para evitar e reduzir os riscos de fraticídios no país.

O emprego do IFF nacional deve atender às Forças Armadas e ser complementado pelas medidas de coordenação e controle do espaço aéreo, comuns às Forças irmãs, com a padronização de normas e procedimentos e a necessária integração das Forças Armadas no nível operacional, coordenada pelo Ministério da Defesa.

A existência de Normas de Padronização da OTAN – já utilizadas nos modelos atuais de IFF integrados às diversas plataformas brasileiras – é fator de muito peso na produção do Sistema de IFF autóctone.

A dotação de equipamentos de IFF distribuídos às Forças Armadas com controles na interface homem-máquina que seguem os padrões da OTAN contribui para a manutenção dos equipamentos nos moldes já existentes.

Também é de suma importância considerar a normatização da ICAO, pois, no Brasil, os sistemas de radares primários e secundários para o tráfego aéreo e a defesa aeroespacial são coincidentes e devem continuar, pela conveniência e economia de recursos.

Assim, a correta decisão de agregar a defesa aérea ao controle do tráfego aéreo é também fator a ser considerado para o desenvolvimento de sistemas de IFF militares, pois as necessidades dos equipamentos civis também podem ser contempladas com a produção de equipamentos de emprego dual.

Neste momento, buscar o estado da arte na produção de IFF, que seria a obtenção do Modo 5, não é o mais importante, tampouco imperativa a sua tempestividade, sob a pena de representar a estagnação do projeto. Contudo, o desenvolvimento de um IFF nacional com o Modo 4 deve suscitar a capacitação de pessoal e a previsão de incorporação, em momento posterior, do Modo 5. A compatibilização do IFF com uso civil e a extensão Modo S são importantes e devem ser consideradas no Projeto do IFF nacional.

Deve ser feita uma análise acurada dos sistemas IFF já disponíveis nas plataformas das três Forças Armadas para verificar a viabilidade de incrementá-los com o Modo 4, e até em vetores civis, para padronização dos *transponders* civis e militares, se cabível, otimizando o uso dos recursos orçamentários disponíveis para o convênio. Por isso, é necessária a coordenação do Ministério da Defesa.

Outro fator importante é a previsão de facilidades para a indústria nacional realizar a posterior produção em série dos equipamentos. Para tanto, as aquisições em escala terão maior amplitude se a produção do IFF nacional atender às três Forças e também aos órgãos civis de tráfego aéreo.

O caminho da produção nacional de equipamentos de defesa, sem dúvida, foi acertadamente escolhido para o poder dissuasório atingir a estatura política do Brasil e, até mesmo, para contrabalançar a importação crescente de

materiais bélicos de ponta por países diversos, inclusive da América do Sul, mas ainda carece de maiores investimentos para sair da prospecção tecnológica e alcançar a produção em escala, que depende de encomendas regulares.

A produção dos armamentos e meios de detecção utilizados na defesa aeroespacial do Brasil passou a ser acompanhada pelo desenvolvimento de sistemas de identificação, graças ao convênio para a produção de IFF nacional entre o CTA e a Orbisat (Brasil, 2008a), e surge como uma forte luz no fim do túnel para clarear a escuridão dos fratricídios, além de contribuir para aumentar o poder dissuasório do país, pois a coordenação e o controle proporcionados pelo IFF são fatores multiplicadores do poder bélico de uma nação.

Por fim, a reconhecida competência dos envolvidos no desenvolvimento é vital para que se obtenha a solução que ofereça a melhor relação custo-benefício ao país no projeto do IFF nacional com o Modo 4, a fim de evitar que os militares brasileiros provem o mais amargo dos remédios em combate: o fratricídio.

## REFERÊNCIAS

Abdalla, J., 2008, “Operação do Radar SABER M60 pelos Fuzileiros Navais”, *Jornal CTEx Notícias*, Ano III, Nº 10, pp. 6, Disponível em: <[http://www.ctex.eb.br/jornal\\_ctex/jornal\\_010\\_ctex.pdf](http://www.ctex.eb.br/jornal_ctex/jornal_010_ctex.pdf)>, Acesso em: 1º de outubro de 2010.

Bennet Avionics, 2010, “ARC (Cessna) RT-359A Transponder”, Disponível em: <<http://www.bennettavionics.com/rt359a.html>>, Acesso em: 1 out. 2010.

Berry, A., Byers, R., Madison, K., 2004, “Terms of Reference for the SISO Study Group on: Mode 5 IFF”, *Simulation Interoperability Standards Organization*, Disponível em: <[www.sisostds.org/index.php?tg=fileman&idx=get&id=31&gr=Y&path=&file=SISO-SG-OR-Mode5](http://www.sisostds.org/index.php?tg=fileman&idx=get&id=31&gr=Y&path=&file=SISO-SG-OR-Mode5)>, Acesso em: 7 de dezembro de 2007.

Brasil, 2008a, “Extrato de Convênio Encomenda Vertical de Projetos de Pesquisa Ref. 0402/08: Projeto do IFF e Transponder Compatível com o IFF”, Ministério da Ciência e Tecnologia. Financiadora de Estudos e Projetos. Diário Oficial da República Federativa do Brasil, N. 253, pp. 25.

Brasil, 2008b, “Estratégia Nacional de Defesa”. Ministério da Defesa, pp. 17-20.

Brasil, 2008c, “Política de Defesa Nacional”. Presidência da República.

Brasil, 2002, “Normas Operacionais do Sistema de Defesa Aeroespacial Brasileiro”. Ministério da Defesa. Comando de Defesa Aeroespacial Brasileiro.

Brasil, 2001, “C 44-1: Emprego da Artilharia Antiaérea”, 4. Ed., Ministério da Defesa. Estado-Maior do Exército.

Carroll, S., 1999, “The mark of Cain: avoiding fratricide”, *Journal of Electronic Defense*, Vol. 22, N. 1, pp. 40, Disponível em: <<http://www.jedonline.com/default.asp?func=articles&year=1999&month=1&page=9901j13&doct=cover%20story>>, Acesso em: 26 de junho de 2002.

Endsley, M.R. *et al.*, 1998, “A comparative analysis of SAGAT and SART for evaluations of situation awareness”, *Proceedings of the 42nd Annual Meeting of the Human Factors and Ergonomics Society*, Chicago, IL, USA, pp. 1, Disponível em: <<http://www.satechnologies.com/Papers/pdf/HFES98-SAGATvSART.pdf>>, Acesso em: 1º de outubro de 2010.

Geck, R., 2004, “New IFF passes the test”. *dcmilitary.com*. Disponível em: <[http://www.dcmilitary.com/navy/tester/9\\_49/national\\_news/32555-1.html](http://www.dcmilitary.com/navy/tester/9_49/national_news/32555-1.html)>. Acesso em: 30 de maio de 2010.

Hess, P., 2003, “Feature: The Patriot’s fratricide record”, Disponível em: <<http://www.washtimes.com/upi-breaking/20030424-042117-6399r.htm>>, Acesso em: 11 de junho de 2004.

Jane’s, 1995-1996, “IFF 4700 SERIES TRANSPONDERS”, *Radar and Electronic Warfare Systems*, pp. 337 e p. 334.

Jones, L., Pimenta, V., 2009, “Radar BRASILEIRO SABER M60 é um dos destaques da LAAD”. Disponível em: <[http://defesabrasil.com/laad2009/index.php?option=com\\_content&view=article&id=73:radar-brasileiro-saber-m60-e-um-dos-destaques-da-laad&catid=39:noticias&Itemid=78](http://defesabrasil.com/laad2009/index.php?option=com_content&view=article&id=73:radar-brasileiro-saber-m60-e-um-dos-destaques-da-laad&catid=39:noticias&Itemid=78)>. Acesso em: 20 de junho de 2010.

Jorge, R.C.B., Wurts, E., 2006, “Radar SABER X60 – Um radar do Exército destinado à defesa aeroespacial brasileira”, *Revista CTEEx P&D*, Ano I, Nº. 1, pp. 3-9, Disponível em: <[http://www.ctex.eb.br/revista\\_ctex/edicao\\_01\\_2006/sumario\\_2.htm](http://www.ctex.eb.br/revista_ctex/edicao_01_2006/sumario_2.htm)>, Acesso em: 31 de setembro de 2010.

Lum, Z.A., 1995, “Friend? ...Foe? ... Fire !!!”, *Journal of Electronic Defense*, Vol. 18, Nº 5, p. 35-38.

Lum, 1990b, “STANAG 4193. Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders

- Part III: IFF Installed System Characteristics”, IHS, Englewood, CO, USA.

Lum, 1999, “STANAG 4193. Technical Characteristics of IFF Mk Xa and Mk XII Interrogators and Transponders - Part IV: Technical Characteristics of Mode S in Military Interrogators and Transponders”, IHS, Englewood, CO, USA.

Poggio, G., 2009, “Radar de defesa antiaérea é destaque na LAAD 2009”, *Jornal Poder Aéreo*, Disponível em: <<http://www.aereo.jor.br/2009/04/15/radar-de-defesa-antiaerea-e-destaque-na-laad-2009/>>, Acesso em: 31 de setembro de 2010.

Primeira Brigada de Artilharia Antiaérea (1ª Bda AAAe), 2007, “Experimentação Doutrinária de Comando e Controle de Artilharia Antiaérea com o Radar SABER M60”.

Raytheon, 2006, “AN/TPX-57(V) Common MK XIIA/ Mode 4/5 IFF Interrogator”. Disponível em: <[http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn\\_ncs\\_products\\_tpx57\\_pdf.pdf](http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn_ncs_products_tpx57_pdf.pdf)>. Acesso em: 11 de junho de 2010.

Raytheon, 2007, “AN/TPX-56 IFF Interrogator Set”, Disponível em: <[http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn\\_ncs\\_products\\_tpx56\\_pdf.pdf](http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn_ncs_products_tpx56_pdf.pdf)>, Acesso em: 11 de junho de 2010.

Raytheon, 2008, “AN/APX-100 (V) IFF Mark XII Transponder Set”, Disponível em: <[http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn\\_ncs\\_products\\_apx100v.pdf](http://www.raytheon.com/capabilities/rtnwcm/groups/ncs/documents/content/rtn_ncs_products_apx100v.pdf)>, Acesso em: 11 de junho de 2010.

Riggs, R., 2004, “Blue On Blue. How did an Army patriot missile battery shoot down a navy F-18?”. Disponível em: <<http://www.globalsecurity.org/org/news/2004/040205-patriot-shootdown.htm>>, Acesso em: 31 de maio de 2010.

Souza, C.A.M., 1983, “Major Puga e LT CMDR Francis W. G. O’Shaughnessy”, *Revista Aeronáutica*, N. 142, pp. 27-40.

The United States of America, 2000a, “Statement by the president regarding the United States decision to stop degrading Global Positioning System”, White House, Office of the Press, Secretary, Disponível em: <<http://www.whitehouse.gov/library/PressReleases.cgi?date=3&briefing=0>>, Acesso em: 5 de maio de 2000.

The United States of America, 2000b, “Non Resident Training Course”, *Operations Specialist. United States Navy*, Vol. 1.



Trim, R.M., 2007, "Identification Friend or Foe", Presentation in IET Sussex Centre, Hawth Theatre Crawley. Disponível em: <<http://www.theiet.org/local/uk/southeast/sussex/docs/iff.cfm>>, Acesso em: 10 de novembro de 2010.

Universidade Estadual de Campinas (Unicamp), 2008, "Parceria com indústria resulta no primeiro radar brasileiro", Jornal da Unicamp, Disponível em: <[http://www.unicamp.br/unicamp/unicamp\\_hoje/jornalPDF/ju392pag07.pdf](http://www.unicamp.br/unicamp/unicamp_hoje/jornalPDF/ju392pag07.pdf)>, Acesso em: 31 de setembro de 2010.

Vitorino, R., 2000, "Mectron faz míssil anti-radiação", Disponível em: <<http://jornal.valeparaibano.com.br/2000/07/29/sjc/mectron.html>>, Acesso em: 21 de junho de 2010.

Wurts, E., 2001, "Identificação amigo ou inimigo: perguntas e respostas...", Revista da Escola de Artilharia de Costa e Antiaérea, Nº 7, pp. 44-47.