ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3/2022

JOZIAS **DEL RIOS** VIEIRA GRANADO SANTOS, Cap Eng

Emprego da Identificação Segura com IFF Modo 4 nas Regras de Engajamento

Rio de Janeiro

2022

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3/2022

JOZIAS **DEL RIOS** VIEIRA GRANADO SANTOS, Cap Eng

Emprego da Identificação Segura com IFF Modo 4 nas Regras de Engajamento

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Emprego da Força Aérea
Orientador: Israel Cordeiro dos Santos Rocha, Maj Eng

Rio de Janeiro
2022

JOZIAS **DEL RIOS** VIEIRA GRANADO SANTOS, Cap Eng

Emprego da Identificação Segura com IFF Modo 4 nas Regras de Engajamento

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Jaqueline de Azevedo Bruno, Ten Cel Int
EAOAR

_____

Israel Cordeiro dos Santos Rocha, Maj Eng
EAOAR

Rio de Janeiro

2022

RESUMO

A necessidade de mitigação de fratricídio (fogo amigo) é um importante modulador do emprego de armamentos em razão dos danos morais e financeiros que esses eventos podem provocar. Neste contexto, as regras de engajamento de armamentos aéreos e antiaéreos num Teatro de Operações (TO) devem adotar a capacidade de identificação segura oferecida pelo Sistema IFF (*Identification Friend or Foe*) Modo 4 Nacional (IFFM4BR), visando melhores resultados operacionais simultaneamente à redução de fratricídio. A identificação de alvos com IFF Modo 4 preenche requisitos operacionais de alcance, rapidez e disponibilidade quando comparada com métodos baseados em imageamento visual e infravermelho, alerta antecipado de radar, assinatura radar do alvo, enlaces táticos de dados e visão a olho nu. Além disso, o IFF Modo 4 também é seguro em razão do uso de criptografia, enquanto que reconhecimento de voz, corredores de segurança e IFF Modos 1 e 2 são métodos que não impedem que um inimigo engane a identificação de alvos e cause inibição ou atraso da reação das defesas. Devido a adequabilidade operacional e segurança, a adoção do IFF Modo 4 nas Forças Armadas viabiliza o emprego adequado e seguro desses armamentos em toda sua potencialidade, com especial relevância em cenários de interoperabilidade e no combate além do alcance visual. As características do IFF Modo 4 ainda permitem que seja empregado como fator prioritário de identificação em combate e que seja expandido para exercícios e operações combinadas, seja por empréstimo ou exportação aos países vizinhos em coalização.

Palavras-chave: identificação amigo-inimigo; regras de engajamento; IFF modo 4; fratricídio; identificação segura.

1 **INTRODUÇÃO**

A incorporação pelas Forças Armadas de modernos mísseis ar-ar, antinavios e antiaéreos operando além do alcance visual (BVR, do inglês *Beyond Visual Range*) habilita o combate com maior afastamento (*stand off*), diminuindo a exposição do atacante aos riscos de ser detectado e abatido.

Contudo, o incremento de alcance também propicia maior incerteza acerca do alvo engajado, acarretando erros de classificação que ampliam as possibilidades de fratricídio (fogo amigo). Os eventos de fratricídio causam extremo prejuízo operacional, impactam a moral da tropa e provocam hesitação nos comandantes (HART, 2004). Portanto, os procedimentos para o emprego desses armamentos asseguram que o alvo não é amigo no início do engajamento letal (*kill chain*).

A capacidade de identificação remota baseada em sistemas IFF (do inglês *Identification Friend or Foe*) usando protocolos de comunicação seguros Modo 4 ou Modo 5 permite a localização de plataformas amigas (ou aliadas) com um nível de confiança muito superior aos meios atualmente disponíveis para uso pelo Sistema de Defesa Aeroespacial Brasileiro (SISDABRA).

A comunicação de rádio cooperativa em IFF inicia-se com um interrogador transmitindo códigos (em um Modo) direcionados a aeronaves e embarcações militares munidas de um transpônder. Esse transpônder, então, emite respostas que permitem ao interrogador deduzir a localização e identificação da plataforma.

O interrogador IFF está geralmente associado a um radar primário em solo do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB). Todavia, também pode equipar os lançadores de mísseis de ombro, ser instalado em embarcações navais, ou ainda ser aeroembarcado, como no caça F-39 Gripen, no avião de patrulha marítima P-3AM Orion e na aeronave de alerta aéreo antecipado e controle E-99M.

Considerando a necessidade de meios adequados para se evitarem fratricídios, este ensaio defende que as regras de engajamento de armamentos aéreos e antiaéreos num Teatro de Operações (TO) devem adotar a identificação segura com IFF Modo 4, especialmente para Operações Conjuntas.

Isto porque o IFF Modo 4 é um meio de identificação aeroespacial com características adequadas de disponibilidade, imediatismo e alcance, o que mitiga o fratricídio em combate quando utilizado nas regras de engajamento (ROE, do inglês *Rules of Engagement*) de mísseis, especialmente com alcance BVR.

Ademais, o mecanismo de identificação em o IFF Modo 4 utiliza criptografia, o que protege contra vulnerabilidades de segurança que permitiriam que um inimigo engane a classificação por conseguir se passar como impostor, com a intenção de adentrar o território sem estimular a reação da defesa aérea, antiaérea e naval.

2 **FATORES PARA A ADOÇÃO DO IFF MODO 4**

Sistemas de navegação e de comunicação mais avançados, sensores aprimorados, táticas robustas, etc. ampliam a capacidade de combate por meio da melhoria da consciência situacional. Deve-se reconhecer que isso também se traduz em redução da taxa de fratricídio em combate, porém um sistema de identificação dedicado é necessário para complementar a redução de fratricídio (OTA, 1993).

Assim, o Plano Estratégico Militar da Aeronáutica (PEMAER) prevê o Projeto Sistema IFF Modo 4 Nacional (IFFM4BR) para o desenvolvimento de uma solução de identificação segura (BRASIL, 2018). Todavia, sua adoção ainda demandará doutrinação, avaliações operacionais e conscientização aos pilotos, operadores e autoridades de que os atuais meios de identificação são inadequados e inseguros.

Segundo Oliveira (2004), estão disponíveis os seguintes meios de identificação: visual (a olho nu), imageamento visual eletróptico (EO) ou no espectro infravermelho (IR), reconhecimento de voz na fonia de comunicação, enlaces táticos de dados (TDL, do inglês *Tactical Data Links*), Medidas de Coordenação e Controle de Espaço Aéreo (MCCEA), assinatura radar do alvo, receptor de alerta radar (RWR, do inglês *Radar Warning Receiver*) e sistema IFF nos Modos militares 1, 2.

Será visto que apenas os IFF Modos 1, 2, 4 e 5 são adequados para as ROE de armamentos, enquanto que apenas TDL e IFF Modos 4 e 5 são seguros. Outrossim, a adoção do IFF Modo 4 assegura a soberania estratégica e tecnológica ao Brasil, em detrimento à mera implantação do IFF Modo 5, cujos equipamentos e as chaves criptográficas são de fornecimento estrangeiro.

Logo, pela interseção das soluções elencadas, apenas o IFF Modo 4 satisfaz aos requisitos de adequabilidade operacional, segurança e soberania. Cabe salientar que há somente um projeto de desenvolvimento dessa capacidade no Brasil, o que facilita a interoperabilidade sem competitividade dentre as Forças Singulares. Uma concorrência de projetos seria prejudicial, pois causa redundância de esforços e dificuldades de aceitação por aquele que teve o projeto desfavorecido.

2.1 **Adequabilidade dos Meios de Identificação de Alvos**

Os meios de identificação visual ocular (opcionalmente com auxílio de binóculo para aumento de alcance) ou com auxílio de câmeras e lentes EO/IR são afetados pela atenuação atmosférica, fumaça e condição meteorológica, o que limita o alcance para até 25 km (OLIVEIRA, 2004). Tal limitação é incompatível com as ROE do míssil BVR ar-ar Meteor, cujo alcance é superior a 100 km e equipa o caça F-39 Gripen recém adquirido pela Força Aérea Brasileira (BORGES, 2018).

Aeronaves com capacidade de inteligência de sinais (SIGINT, do inglês *Signals Intelligence*) têm sensores RWR que captam e localizam emissões de rádios e radares. Os sinais são comparados com uma biblioteca de emissões que permite classificar o emissor como amigo ou suspeito. Contudo, o RWR não está sempre disponível para identificação, pois não detecta alvos cujo transmissor está desligado.

Radares primários avançados sugerem o tipo de aeronave ao correlacionar vários fatores: frequência Doppler dos sinais refletidos; intensidade do sinal recebido; seção reta radar (RCS, do inglês *Radar Cross Section*) esperada pelo tipo de alvo; e a modulação produzida por hélices do alvo. Tais dados, em conjunto, produzem para o radar uma assinatura única do tipo de alvo. Entretanto, esse meio de identificação torna-se inaplicável quando o inimigo opera o mesmo modelo de aeronave, e ainda depende de um banco-de-dados empírico de difícil obtenção.

Os enlaces táticos de dados (TDL) são seguros e habilitam a consciência situacional pelo compartilhamento da posição dos amigos, entre outras informações. O *Multifunctional Information Distribution System* (MIDS) Link-16 será escolhido nesta análise, pois é o TDL mais comum em uso na Organização do Tratado do Atlântico Norte (OTAN) e forças de coalizão, além de ser um dos mais modernos.

Todos os rádios TDL Link-16 participantes da rede precisam sincronizar seus relógios entre si com precisão de microssegundos para viabilizar a comunicação. Essa precisão é necessária para que todos façam 77 mil saltos em frequência por segundo ao mesmo tempo, causando um espalhamento espectral. Esse recurso confere aos rádios maior resistência ao ataque de *jamming*, que é a interdição de determinadas bandas de frequências com sinais ruidosos transmitidos por inimigos com a intenção de negar o uso do espectro de radiofrequência.

Contudo, a sincronização de relógio é um processo de múltiplos estágios (aquisição, grosso e fino). Para que uma plataforma ingresse na rede, primeiro deve

escutar e se sincronizar com mensagens de convite ou anúncio. Após o sincronismo, ainda será requerido negociar um canal de comunicação seguro, pelo qual a plataforma ingressante então poderá disponibilizar a sua informação de posição e identificação (NORTHROP GRUMMAN, 2014). Somente após receber essa informação é que os outros participantes da rede saberão a localização da nova plataforma amiga, permitindo evitá-la num eventual engajamento.

Esses processos causam um atraso considerável para informar toda a rede sobre a localização do novo participante, e ainda dificultam a manutenção do enlace durante o combate na presença de interferências, obstáculos, distanciamentos, etc. A disponibilidade da rede também é fortemente afetada pelo tráfego de dados de voz, *streaming* de vídeo e quantidade de participantes. As redes TDL ainda podem estar fragmentadas, ao invés de serem únicas. Essa combinação de fatores tornam o TDL pouco confiável para identificar amigos visando as ROE. Consequentemente, a OTAN requer tanto o TDL Link-16, quanto a capacidade IFF Modo 5 instaladas nas plataformas para haver a mínima interoperabilidade em combate (CADY, 2020).

Em contraste, o IFF Modo 4 usa o conceito de interrogações e respostas sem prévia negociação de canal e sincronismo. As interrogações são repetidas cerca de duas dúzias de vezes para tolerar eventuais interferências de rádio, conflitos por simultaneidade com outras interrogações IFF e ainda para garantir maior margem de segurança criptográfica. O alcance também só é limitado pela linha de visada direta (LOS, do inglês *Line-of-Sight*), sendo aproximadamente 500 km (NATO, 1990).

Cada interrogação em IFF Modo 4 demora até 4 milissegundos devido ao tempo de propagação da onda eletromagnética no trajeto de ida e volta até um alvo. Assim, o processo completo de uma tentativa de identificação com duas dúzias de interrogações numa certa direção é finalizado em até 100 milissegundos. (FAHMY; MOUSTAFA, 2006). Esse intervalo temporal, limitado e garantido, é suficiente para que um piloto de aeronave de caça ou um operador de bateria antiaérea tenham subsídios rapidamente que embasem suas ROE de armamentos letais.

Sumarizando, o uso da identificação remota com IFF Modo 4 satisfaz as qualidades de confiabilidade, disponibilidade, imediatismo e alcance requeridos para as regras de engajamento (ROE) de armamentos. Por outro lado, os procedimentos que se apoiam em TDL, RWR, assinatura radar do alvo, imageamento EO/IR e visual olho nu não se mostraram adequados para essa finalidade e ensejam um aumento de casos de fratricídio se forem empregados.

2.2 **Segurança dos Meios de Identificação de Alvos**

Os meios de identificação devem ser seguros para impedir que um inimigo engane as defesas com ações de inteligência. No combate aeroespacial, uma dessas ações é a imitação (*spoofing*), quando um atacante faz suas unidades se confundirem com as defesas, a fim de inibir ou atrasar a reação delas.

Dentre os meios de identificação susceptíveis ao *spoofing*, o Controle por Procedimentos é uma MCCEA que estabelece Corredores de Segurança (especificando rota, altitude, velocidade, códigos IFF, etc.) destinados a identificação de aeronaves. Todavia, aeronaves que passam pelos corredores podem ser observadas por radares inimigos, viabilizando sua réplica posterior. E ainda, o inimigo pode ter tido acesso às MCCEA vazadas por ação de espionagem. O Manual de Defesa Antiaérea exige que esses corredores precisam “variar constantemente, a fim de se evitar que o mesmo possa ser utilizado por ameaças aeroespaciais para ludibriar e comprometer a Defesa Antiaérea” (BRASIL, 2017, p. 69). Portanto, essas MCCEA devem ser usadas apenas em casos excepcionais.

Já o reconhecimento do idioma e timbre de voz de um aliado na comunicação de rádio também não é um meio seguro de identificação, haja vista que recentes avanços em inteligência artificial produziram o recurso do *deepfake*. Essa tecnologia de aprendizagem de máquina é capaz de recriar frases com conteúdo diverso da intenção do locutor, se apropriando da sua voz e linguagem de forma impostora humanamente indistinguível (KIETZMANN *et al*., 2020).

Por fim, a identificação com IFF Modos 1 e 2 utilizam interrogações fixas e respostas sem proteção criptográfica, sendo trivial para o inimigo estimular, escutar e copiar os códigos das respostas para suas próprias plataformas, assim ludibriando a identificação no lado defensor (WURTS, 2010).

Por outro lado, o IFF Modo 4 permite bilhões de alternativas de interrogações, habilitando ao transpônder rejeitar interrogações inimigas. O IFF Modo 4 também impede que a localização da plataforma seja facilmente compreendida por interrogadores inimigos que estejam escutando as respostas (NEEMAT, 2010). Somando-se a isso, a segurança contra um inimigo de elevado poder computacional é garantida no IFF Modo 4 com o uso de técnica de criptografia nos algoritmos matemáticos usados para gerar interrogações e calcular as respectivas respostas.

Portanto, o reconhecimento de voz, a identificação com IFF nos Modos 1 e 2 e corredores nas MCCEA são meios inseguros de identificação. Se forem confiados para essa tarefa, permitem que um inimigo atacante seja um impostor e cause inibição do engajamento oportuno de armamentos para repelir o ataque. Em contrapartida, a identificação segura com IFF Modo 4 impede essa vulnerabilidade.

3 **CONSIDERAÇÕES FINAIS**

Os eventos de fratricídio causam grande prejuízo e dano moral, de forma que a sua mitigação determina as etapas das regras de engajamento (ROE) para o emprego de armamentos aéreos e antiaéreos, especialmente com alcance BVR.

Observou-se que os meios de identificação por visão ocular, imageamento EO/IR, rádio TDL, assinatura radar do alvo e RWR apresentaram deficiências operacionais nos quesitos de disponibilidade, alcance ou imediatismo para o adequado suporte às ROE de armamentos BVR, assim propiciando fratricídio.

Paralelamente, a identificação em combate empregando reconhecimento de voz, corredores das MCCEA ou IFF Modos 1 e 2 são meios vulneráveis quanto à segurança por não adotar criptografia, permitindo que o inimigo engane a identificação e cause indesejável inibição das defesas aéreas, segundo as ROE.

Como visto neste ensaio, somente a adoção do IFF Modo 4 Nacional (IFFM4BR) nas Forças Armadas é capaz de entregar um meio de identificação adequado, seguro, soberano e interoperável para as regras de engajamento de armamentos aéreos e antiaéreos, especialmente em operações conjuntas e BVR.

Ademais, a doutrina e a avaliação operacional podem revelar que a identificação em combate com IFF Modo 4 permite receber prioridade e confiança absolutas pelas ROE, sobrepujando todos os outros meios de identificação. Nessa concepção de operação, normalmente adotada para a proteção de navios porta-aviões, a identificação positiva em IFF Modo 4 é uma *conditio sine qua non* para permitir a aproximação de aeronaves e embarcações ao território ou aos meios.

Além da sua aplicabilidade em um Teatro de Operações Conjuntos, a capacidade IFFM4BR também permite ser exportada ou emprestada aos países amigos e vizinhos na América Latina, vislumbrando-se, assim, possibilidades de mitigação de fratricídio em Operações Combinadas de coalizão em nosso continente.

REFERÊNCIAS

BORGES, R. C. C. **Aeronave Gripen NG equipado com míssil BVR Meteor**: eficiência no cumprimento da missão. 2018. Monografia (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, 2018.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 2.102/GC3, de 18 de dezembro de 2018. Aprova a reedição do Plano Estratégico Militar da Aeronáutica 2018 – 2027. (PCA 11-47). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 222, f. 14766, 20 dez. 2018.

BRASIL, Comando da Aeronáutica. Primeira Brigada de Defesa Antiaérea. Portaria nº 10/A-3, de 22 de junho de 2017. Aprova a reedição do Manual de Defesa Antiaérea. (MCA 355-1). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 109, f. 6317, 28 jun. 2017.

CADY, J. M. Combat Identificaton Branch. Joint Fires Division J6 Staff. **Link 16 is different than Mode 5**. US DoD AIMS User Working Group. 2020. 1 vídeo (36 min).

FAHMY, A.; MOUSTAFA, K. H. A Survey of IFF Systems. *In:* International Conference on Electrical Engineering (ICEENG), 5., v. 5, 2006, Cairo. **Anais eletrônicos** [...]. Piscataway: IEEE, 2006. p. 1-11. Disponível em: https://iceeng.journals.ekb.eg/article_33679_3bdc8a99bf6f694902a4ff80ce4747c0.pdf. Acesso em: 28 set. 2022.

HART, R. J. **Fratricide: A Dilemma which is Manageable at Best**. Newport, 2004. Disponível em: http://apps.dtic.mil/sti/citations/ADA422788. Acesso em: 22 set. 2022.

KIETZMANN, J.; LEE, L. W.; MCCARTHY, I. P.; KIETZMANN, T. C. Deepfakes: Trick or Treat? **Business Horizons**, v. 63, n. 2, p. 135-146, mar./abr. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0007681319301600. Acesso em: 10 out. 2022.

NATO – NORTH ATLANTIC TREATY ORGANIZATION. **STANAG 4193:** Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders. 2nd ed. NATO, 1990.

NEEMAT, S. **Design and Implementation of a Digital Real-Time Secondary Surveillance Radar/Interrogation Friend or Foe Target Emulator**. Dissertação (Mestrado em Engenharia Elétrica) – Universidade da Cidade do Cabo, Cidade do Cabo, 2010.

NORTHROP GRUMMAN. **Understanding Voice and Data Link Networking**. 2014. Northrop Grumman, Estados Unidos da América, San Diego. 320 p. Disponível em: https://dl.icdst.org/pdfs/files/e90d37a9b93e2 e607206320ea07d7ad2.pdf. Acesso em: 30 set. 2022.

OLIVEIRA, H. E. S. M. **Modernização na Identificação de Combate**: fator de rapidez e precisão. Monografia (Curso de Aperfeiçoamento de Oficiais) – Escola de Aperfeiçoamento de Oficiais da Aeronáutica, Universidade da Força Aérea, Rio de Janeiro, 2004.

OTA – OFFICE OF TECHNOLOGY ASSESSMENT. U.S. Congress. **Who Goes There:** Friend of Foe? OTA-ISC-537. Washington, DC: U.S. Goverment Printing Office, jun. 1993. Disponível em: https://ota.fas.org/reports/9351.pdf. Acesso em: 28 set. 2022.

WURTS, E. J. A identificação amigo-inimigo nativa do Brasil: perguntas e respostas. **Journal of Aerospace Technology and Management**, São José dos Campos, v. 2, n. 3, p. 371-386, 2010. Disponível em: https://www.scielo.br/j/jatm/a/HH9XgmryqZf7P9nnhwkP6Qw. Acesso em: 27 set. 2022.