ORIGINAL

Análise de risco de pequenas aeronaves remotamente pilotadas na presença de incerteza

Risk analysis of small unmanned aircraft in uncertainty presence

Análisis de riesgo de pequeñas aeronaves remotamente pilotadas delante de situaciones de incertidumbre

Cel Av André Luiz Pierre Mattei, Mestre
Instituto Tecnológico de Aeronáutica - ITA
São José dos Campos/SP - Brasil
mattei@ita.br

Cap Esp Elói Fonseca, Doutorando
Instituto Tecnológico de Aeronáutica - ITA
São José dos Campos/SP - Brasil
eloif@ita.br

Cap EB Nina Machado Figueira, Mestre
13º Regimento de Cavalaria Mecanizada - 13º RCMec
Pirassununga/SP - Brasil
nina_figueira@hotmail.com

Onofre Trindade Júnior, Doutor
Universidade de São Paulo - USP
São Carlos/SP - Brasil
otj@icmc.usp.br

Felipe Figueira Vaz
Fine Instrument Technology - FIT
São Carlos/SP - Brasil
fvztdk@gmail.com

RESUMO

A integração definitiva de Aeronaves Remotamente Pilotadas (ARP) ou Veículo Aéreo Não Tripulado (VANT) no espaço aéreo depende da comprovação do risco associado à sua operação ser igual ou menor ao valor aceito para as aeronaves com pilotos a bordo. O mercado militar e civil tem amplas aplicações para ARP, mas a dificuldade de certificação dificulta a sua disseminação nas operações, principalmente nas de pequeno porte (menor que 25 kg) devido ao uso de dispositivos e componentes COTS *(Commercial Off-The Shelf)*, sem valor de confiabilidade definido ou confiável, muitas vezes provenientes de aeromodelos recreativos. Neste trabalho se apresenta uma revisão acerca das publicações realizadas sobre os principais temas necessários à avaliação de risco de um sistema e inova com a aplicação de uso de incertezas advindas da árvore de falhas na avaliação de risco. O artigo também demonstra a necessidade de aumento da consciência situacional em voo das aeronaves por meio de enlaces de dados eficientes. Duas aeronaves remotamente pilotadas, desenvolvidas pelo grupo de pesquisa do INCT-SEC, são usadas como exemplos de aplicação dos conceitos.

Palavras-chave: Veículo Aéreo Não Tripulado (VANT). Aeronaves Remotamente Pilotadas (ARP). Árvore de falha. Avaliação de risco.

Recebido / Received / Recibido
12/08/13

Aceito / Accepted / Aceptado
29/04/14

ABSTRACT

The final integration of the Remotely Piloted Aircraft (RPA) or Unmanned Aerial Vehicle (UAV) into controlled airspace depends on the evidence of risk related to its operation be equal or less than the accepted value for aircraft with pilots on board. The military and civilian market has broad applications for RPA, but the difficulty of accreditation hinder its dissemination in operations, primarily for small aircraft (less than 25 kg) due to the use of devices and COTS (Commercial Off-The Shelf) without value or exact set of reliability, often originating from recreational flying models. This paper presents a review of the publications made on key issues that are necessary for the risk assessment of a system and innovates with the application of uncertainties usage deriving from the fault tree analysis at the risk assessment. The article also demonstrates the need for increased situational awareness in flight by means of efficient data link. Two remotely piloted aircraft, developed by the research group of INCT-SEC, are used as examples of concepts application.

Keywords: *Unmanned Aerial Vehicle (UAV). Remotely Piloted Aircraft (RPA). Fault Tree Analysis. Risk Analysis.*

RESUMEN

La integración definitiva de Aeronaves Remotamente Pilotadas (ARP) o Vehículo Aéreo sinTripulación (VANT) enelespacio aéreo depende de lacomprovacióndelriesgoasociado al hecho de suoperación ser igual o menor que el valor acepto para las aeronaves con pilotos al borde. El mercado militar y civil tiene amplias aplicaciones para ARP, pero ladificultad de certificaciónimpidesudiseminaciónenlasoperaciones, principalmente para las aeronaves de pequeño porte (menor que 25 kg) devido al uso de dispositivos y componentes COTS (Commercial Off-The Shelf), sin valor de confiabilidaddefinido o exacto, muchas veces provenientes de aeromodelos recreativos. Este trabajo presenta unrepaso acerca de laspublicaciones realizadas sobre losprincipales temas necesarios a laevaluación de riesgo de un sistema e innovaconlaaplicación de uso de incertidumbres oriundas del "árbol de fallas" enlaevaluación de riesgo. El artículo también de muestra la necesidad de aumento de la consciencia situacional en vuelo de aeronaves a través de enlaces de datos eficientes. Dos aeronaves remotamente pilotadas, desarrolladas por el grupo de pesquisa del INCT-SEC, son utilizadas como ejemplos de aplicación dos conceptos.

Palabras-clave: *Vehículo Aéreo Sin Tripulación (VANT). Aeronaves Remotamente Pilotadas (ARP). Árbol de falla. Evaluación de riesgo.*

1 INTRODUÇÃO

A integração de Aeronaves Remotamente Pilotadas (ARP) no espaço aéreo depende da comprovação do risco associado à sua operação ser igual ou menor ao valor aceito para as aeronaves com pilotos a bordo. O mercado militar e civil tem amplas aplicações para ARP, mas dificuldades de certificação dificultam a sua disseminação nas operações. Ao contrário das ARP de grande porte, que possuem valor elevado e sua operação exige certificação semelhante a aeronaves com piloto, as de pequeno porte (menor que 25kg) comumente usam dispositivos e componentes *Commercial Off-The Shelf* (COTS), sem valor de confiabilidade definido ou fidedigno, muitas vezes provenientes de aeromodelos recreativos.

Esse cenário tornou-se palco de atrito, pois, de um lado, há empresas e consumidores ávidos pela operação de pequenas aeronaves e, de outro, autoridades aeronáuticas responsáveis pela segurança de voo. Em uma tentativa de colaborar na solução dessa questão, este trabalho propõe uma metodologia inovadora para avaliação quantitativa de risco, assumindo a incerteza sobre a probabilidade de falha dos elementos e componentes usados em pequenas ARP.

A segurança é resultado de uma série de procedimentos e testes necessários para assegurar a aeronavegabilidade do sistema (BRASIL, 2013). A confiabilidade de um sistema, contudo, é resultado da combinação e da arquitetura de seus diversos subsistemas. Uma empresa integradora exige certo nível de confiabilidade de seus fornecedores de subsistemas para poder atingir os níveis aceitos pela Autoridade Aeronáutica Certificadora, ANAC (Agência Nacional de Aviação Civil) para aeronaves civis, ou IFI (Instituto de Fomento e Coordenação Industrial) para aeronaves militares. Normalmente, esses subsistemas podem ser sequencialmente divididos em outros subsistemas, até que seja atingido o nível de componente. Cada nível atingido possui uma confiabilidade associada, resultante dos valores de confiabilidade dos subsistemas e/ou componentes de que é formado. Entidades que fabricam ou desenvolvem sistemas ou subsistemas aeronáuticos estão interessadas somente na confiabilidade daqueles

elementos de *hardware* ou *software* que estão integrados e são utilizados em sua linha de montagem ou laboratório.

A confiabilidade do sistema aeronáutico, ou sua probabilidade de falha (PdF), pode ser usada para avaliar o risco de uma missão ou o risco para a segurança de voo, tendo em conta cenários operacionais. Derivado da Concepção de Operação, CONOPS, no que se refere à segurança de voo, esse cenário fornece os elementos necessários para se compor uma análise de risco para uma colisão em voo ou um pouso de emergência descontrolado. Essa análise leva em conta os elementos mais relevantes, tais como: o volume usado na missão (área sobrevoada vezes o teto de voo), a densidade de aeronaves no setor, o ângulo de planeio para pouso de emergência, a densidade populacional e de construções na região, a presença de controle de tráfego (elemento mitigador de acidentes), a área frontal das aeronaves, a velocidade etc.

O recente ingresso de pequenas ARP, ou VANT, como também são chamadas no Brasil, traz um elemento novo para a avaliação de risco: a probabilidade de falha (PdF) de diversos (ou todos os) componentes e subsistemas é incerta ou mesmo desconhecida. Quase que como regra, Universidades e empresas, para poderem manter os custos baixos, desenvolvem suas pequenas ARP com componentes COTS, algumas vezes os mesmos usados em aeromodelos recreativos. Para avaliar a probabilidade de falha, duas abordagens são possíveis: ou as diversas opções são testadas para verificação da mais confiável ou é solicitada a opinião de um especialista experiente para a escolha ser mais rápida e com menor custo, presumindo-se que esse especialista já tenha testado e amplamente usado em campo as diversas alternativas. Essa abordagem viabiliza o produto, mas, sem um valor para a probabilidade de falha do sistema, também fica praticamente impossível fornecer um número exato para o risco à segurança, associado ao uso dessa plataforma.

Para suplantar essa dificuldade, a abordagem de estimativa de risco à segurança de voo é apresentada neste trabalho, considerando-se não números bem definidos para a PdF de subsistemas e componentes, mas faixas baseadas em limites mínimo e máximo, fornecidos por especialistas, no nível de credibilidade na opinião dos mesmos.

Há diversas referências no texto, algumas delas empregadas como base para este trabalho. O estudo de Murtha (2009) tem sido referência no uso de incertezas epistêmicas para avaliação de probabilidade de falha e uso da Teoria de Dempster-Shafer no caso de pequenas ARP (menos de 25 kg). Para conhecimento dos aspectos gerais de avaliação de risco, recomenda-se a leitura dos trabalhos de Weibel e Hansman (2004), Grimsley (2004) e Lum e Waggoner (2011).

Este trabalho apresenta uma revisão das publicações realizadas sobre os principais temas necessários à avaliação de risco de um sistema e inova com a aplicação de uso de incertezas advindas da árvore de falhas na avaliação de risco e no desenvolvimento de elementos mitigadores, sem entrar em detalhes acerca desses elementos por extrapolarem o escopo deste trabalho. O desenvolvimento de tecnologias para aumento de consciência situacional em voo e mitigadoras para a avaliação de risco pode ser encontrado nos trabalhos de Figueira *et al.* (2013), Fonseca, Mattei e Cunha (2013) e Mattei *et al.* (2013).

2 CÁLCULO DE PROBABILIDADE DE FALHA NA PRESENÇA DE INCERTEZA

Considerando a parcial ou total ignorância acerca das probabilidades de falha dos diversos componentes presentes em pequenas ARP, torna-se necessário buscar uma ferramenta adequada para avaliação desses sistemas.

2.1 Análise de Árvore de Falhas

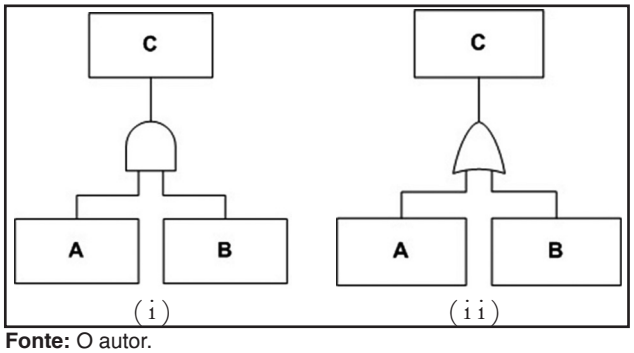
A falha de sistemas complexos pode ser inferida por meio da sua árvore de falhas TFA *(Tree Fault Analysis)*. Partindo do sistema como um todo, faz-se a divisão de seus sistemas e subsistemas até que sejam atingidos os componentes para os quais o analista possa associar falhas e suas respectivas probabilidades de ocorrência. Os diversos componentes agregam-se para a formação de subsistemas e esses para a formação de outros subsistemas, criando um tronco convergente para o sistema completo e, no sentido contrário, galhos e ramificações cada vez mais numerosos à medida que se dirige para o nível de componentes (ERICSON, 1999).

A TFA tem sido adotada, pois, partindo de valores de probabilidade de falha de componentes, simples álgebra booleana pode ser usada para avaliar a probabilidade do sistema. Adicionalmente, ela permite avaliar elementos mais críticos para a ocorrência de uma falha em voo e para a adição de elementos mitigadores ou redundantes. Os diversos elementos da TFA estão relacionados por portas OU (OR) ou E (AND). Normalmente, elementos se combinam para formar um outro acima, com o uso de portas OU. Por outro lado, a presença de portas E indica que a falha de um nível necessita da falha de todos os níveis abaixo, sendo assim, identifica-se a presença de redundância no sistema ou de um sistema supervisor.

Uma análise de álgebra booleana permite ao leitor inferir as diferenças entre portas E e OU na formação de uma TFA e a PdF do sistema. Em termos práticos, a falha de um componente é suficiente para a falha do nível

acima, se ele está relacionado a outros elementos por meio de uma porta OU. No caso de uma porta E, é necessário que todos os elementos associados falhem para que haja falha do sistema do nível acima. Como exemplo, pode-se considerar que dois elementos, A e B, com PdF associadas p_A e p_B, associem-se para formar um elemento C, um nível acima, por meio de portas E e OU (veja Figura 1). As equações (1) e (2) apresentam as relações matemáticas para os casos E e OU, respectivamente. Digamos que, conforme informado pelo fabricante, o elemento A não falhe em um período de 500 horas e o B não falhe em um período de 200 horas, neste caso, $p_A = 1/500 = 0,002$ e $p_B = 1/200 = 0,005$. Assim, nesse caso específico, a probabilidade de falha do sistema C será $p_C = 0,00001$, se a porta for E, e será $p_C = 0,00699$ se a porta for OU. Nota-se que a probabilidade de falha do sistema C é quase 700 vezes maior se a porta usada for OU. Sob outro ponto de vista, o uso de uma porta E permitiu um decréscimo significativo na probabilidade de falha do sistema C (A e B devem falhar para que C falhe) e, por essa razão, redundâncias são comumente usadas em sistemas críticos, entendendo-se por sistema crítico aquele cuja falha resulta em falha catastrófica do sistema ou em perda de vidas.

Figura 1: Em uma FTA, dois elementos A e B podem relacionar por meio de portas E (figura i) ou de portas OU (figura ii).



Fonte: O autor.

$$p_A \text{ E } p_B = p_A * p_B \quad (1)$$

$$p_A \text{ OU } p_B = p_A + p_B - p_A * p_B \quad (2)$$

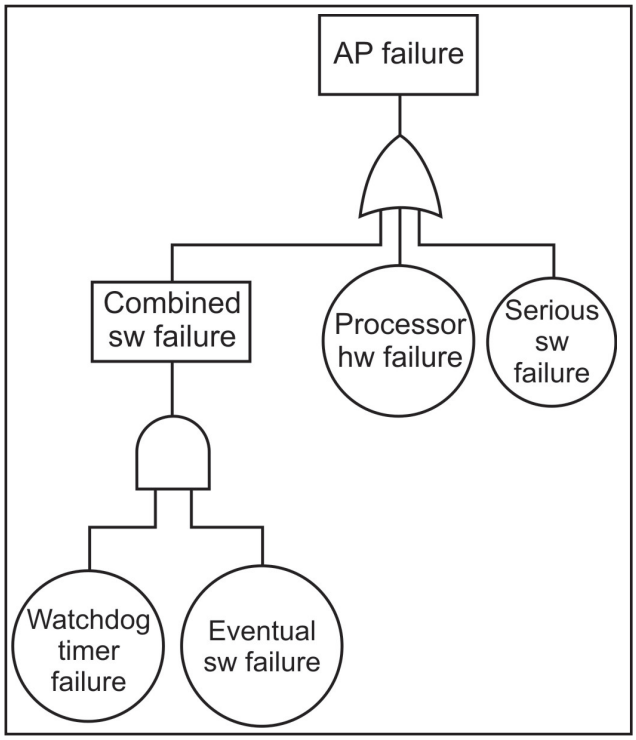
A partir desse exemplo, pode-se apresentar outro mais concreto. Murtha (2009) apresenta (Figura 2) um exemplo de árvore de falhas de uma ARP hipotética. Nela, três situações foram consideradas para a perda do piloto automático: falha de *hardware* do processador da placa eletrônica, uma falha séria do *software* embarcado ou uma falha combinada de software. Uma falha combinada pode ser detectada e corrigida por meio de um sistema de segurança chamado *watchdog timer*. Esse sistema de segurança é posicionado como redundante às falhas eventuais, significando que falhas menores de *software* somente poderão comprometer o funcionamento do piloto automático da aeronave se houver também a falha do *watchdog timer*. Para sistemas mais complexos, uma análise de viabilidade econômica e de sensibilidade poderia levar à conclusão de que são necessários dois ou mais pilotos automáticos trabalhando de forma redundante para que haja a necessária confiabilidade ou, em outras palavras, para que a PdF seja baixa o suficiente.

No caso apresentado na Figura 2, tem-se uma porta E com dois componentes, resultando em um elemento que se compõe com outros dois para formar o elemento "falha do piloto automático", por meio de uma porta OU. Digamos que uma falha eventual menor de *software* ocorra a cada 200 horas de voo ($p_S = 5,0.10^{-3}$) e que uma falha no *watchdog timer* ocorra a cada 1000 horas de voo ($p_W = 1,0.10^{-3}$), então uma falha combinada de *software* terá $p_{SC} = 5,0.10^{-6}$. Se uma falha de *hardware* do processador e uma falha séria de *software* ocorrerem a cada 4000 horas, então, respectivamente, terão $p_{hw} = p_{SW} = 2,5.10^{-4}$. Para que ocorra uma falha no piloto automático, significando a perda de controle da aeronave, basta que apenas um desses eventos ocorra (falha combinada de *software*, falha no processador ou falha séria de *software*), pois eles relacionam-se por uma porta OU. A Equação (3) pode ser usada na obtenção da probabilidade de falha do piloto automático, $p_{PA} = 5,05.10^{-4}$.

$$p_{PA} = p_{sc} + p_{hw} + p_{sw} - p_{sc} * p_{hw} - p_{sc} * p_{sw} - p_{hw} * p_{sw} + p_{sc} * p_{hw} * p_{sw} \quad (3)$$

A árvore de falhas tem sido amplamente usada como meio de propagação das probabilidades de falhas dos componentes por meio de subsistemas, subindo o nível de integração até que se obtenha um valor para o sistema, no caso, uma aeronave. Mas uma forma de fornecer um valor para a autoridade aeronáutica, sem valores de *Mean Time Between Failure*, (MTBF) de componentes e subsistemas, é fornecer somente a árvore de falhas como forma de permitir à autoridade avaliar qualitativamente se a arquitetura adotada está coerente com as regras gerais de segurança. Por outro lado, que componente do sistema deve receber redundância ou ser trocado por outro mais confiável, sem um número definido? Qual o risco associado à operação de uma aeronave em um certo contexto? No universo das pequenas ARP, é comum o uso de componentes indicados por especialistas que os identificaram por experiências anteriores e por meio de muitas horas de testes em campo, pois raramente é encontrado um número de MTBF na especificação. Murtha (2009) sugere o uso da Teoria da Evidência como melhor forma possível de estimar um valor de confiabilidade mais próprio para sistemas de aeronaves pequenas remotamente pilotadas.

Figura 2: Exemplo hipotético de árvore de falhas de um piloto automático de uma ARP.



Fonte: Murtha (2009).

2.2 Teoria da Evidência de Dempster-Shafer

Conforme visto até o momento, são suficientes as informações relacionadas ao MTBF de componentes comumente empregados em pequenas ARP que dificultam a análise quantitativa de confiabilidade do sistema e seu consequente risco à segurança. Usualmente, a incerteza é encontrada na análise de sistemas, e ferramentas estatísticas estão disponíveis para a melhor estimativa possível a partir dos dados disponíveis. Na indústria aeronáutica, peças são ensaiadas de forma sistemática para que se possa estimar o tempo necessário de falha. Assim, apesar de ser possível a determinação do tempo exato para que uma falha ocorra, uma estimativa estatística permite uma suficiente aproximação para que se cumpram as exigências e os limites de segurança. No entanto, como inexistem, no universo das pequenas ARP, informações suficientes para que haja uma estimativa estatística nos padrões usualmente desejados, a incerteza é chamada de epistêmica. Agarwal *et al.* (2004) demonstram o uso de ferramentas computacionais para tratar a avaliação quantitativa de risco e mantém, assim como este trabalho, as definições de incertezas, epistêmica e estatística, realizadas por Oberkampf *et al.* (1998, 1999, 2001). Cabe ressaltar que Murtha (2009) também utiliza as mesmas definições na aplicação desses conceitos em pequenas ARP e salienta diversos aspectos interessantes, como os meios para a obtenção de dados mais acurados e necessários à diminuição da incerteza epistêmica.

Uma metodologia de abordagem de incertezas epistêmicas é fornecida pela Teoria da Evidência, ou de Dempster-Shafer, como também é conhecida. Essa teoria foi, de início, desenvolvida por Arthur P. Dempster (1968) e Glenn Shafer (1976), na década de 60, como uma alternativa para o cálculo probabilístico tradicional e, de fato, encontrou, recentemente, boa receptividade com o incremento das capacidades computacionais, como citado por Agarwal *et al.* (2004).

Conforme já citado neste trabalho, a árvore de falhas é útil à propagação das PdF incertezas aleatórias de componentes (MTBF). No entanto, no caso de incertezas epistêmicas, o uso de álgebra booleana propagaria um valor inerentemente desconhecido ou incerto. Nesse caso, a Teoria da Evidência é uma saída para a superação dessa dificuldade e para a obtenção de um valor quantitativo de probabilidade de falha para a aeronave. De acordo com Jacob, Dubois e Cardoso (2012), há poucas aplicações da Teoria da Evidência para árvore de falhas. Outra possibilidade no caso de incerteza epistêmica é o uso de simulação Monte-Carlo, porém este trabalho não analisa esse caso, por considerar a Teoria da Evidência mais interessante pelo uso da árvore de falhas. O leitor pode, não obstante, encontrar clara descrição dessa abordagem no artigo de Murtha (2009).

Em vez de usar números precisos, Murtha faz uso de funções de confiança, Equações 4, 5 e 6, para avaliar dados imprecisos de dispositivos (incerteza epistêmica). Nessa abordagem, como inexistem dados experimentais confiáveis, usam-se informações derivadas de experiências pessoais para se estabelecer um intervalo em vez de um único número e uma massa *m* (credibilidade) derivada do nível de *credibilidade* sobre a faixa fornecida pelo(s) especialista(s). De Murtha (2009):

$$m: X \rightarrow [0,1] \tag{4}$$

$$\sum_{x \in X} m(x) = 1 \tag{5}$$

$$\sum_{A \subseteq X} m(A) = 1 \quad , \tag{6}$$

onde X é a variável desconhecida que usa a variável aleatória X como estimativa de valor.

O conjunto A é composto por todos os valores possíveis de X e a massa m é um valor atribuído a todos os possíveis X. A massa m é a incerteza do valor da variável x, A. A Equação (4) informa que m está no intervalo entre 0 e 1 e as Equações (5) e (6) mostram que a soma de todos os possíveis valores de m resulta sempre em 1. A Equação (5) mostra que todos os

valores possíveis da variável *x* estão contidos pelo conjunto das variáveis aleatórias *X*, modelo probabilístico portanto. Por outro lado, a Equação (6) mostra que a Teoria de Dempster-Shafer assume que a soma de todas as probabilidades da variável *x* estar em um certo intervalo é 1. Nem sempre a Teoria de Dempster-Shafer atenderá a Equação (5) portanto.

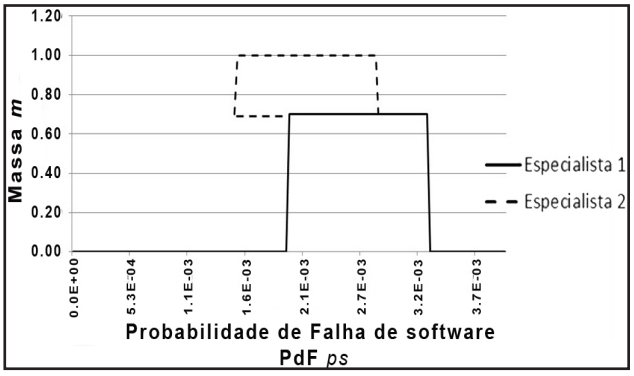
Em caso de um especialista atribuir que uma eventual falha do *software* pode ocorrer entre 300 e 500 horas de voo e que o *watchdog* empregado nessa hipotética ARP pode falhar entre 1000 e 2000 horas de voo, o limite inferior e superior dos limites PdFs para eventual falha de *software* são 0,0020 e 0,0033, respectivamente, e, para o *watchdog*, 0,0005 e 0,0010. Uma vez que existe somente a opinião de um único especialista, a massa é definida como 1. Fazendo cálculos PdF, os novos limites, inferior e superior, tornam-se $1{,}0E^{-6}$ e $3{,}3E^{-6}$(eram $2{,}0E^{-3}$e $3{,}3E^{-3}$). Nesse caso, há uma faixa de confiabilidade e não mais um valor único. Nesse cenário, tem-se um valor otimista, um valor pessimista e uma crença associada a essa faixa de valores. Na teoria de evidência, denomina-se o pior cenário de plausibilidade (*P*), o melhor de crença (*B*, do inglês *belief*) e a confiança nesses limites de massa *m*. Como a soma de todas as massas deve ser 1, havendo apenas um especialista, a massa m terá sempre o valor unitário; havendo dois ou mais especialistas, a soma das massas atribuídas a cada um deles deve somar 1 (um) (0,7 e 0,3, por exemplo). Nesse sentido, a cada elemento são necessários 3 números, conforme a Equação (7).

$$Elemento = \{P, B, m\} \tag{7}$$

A Equação (7) mostra que a taxa de falhas de um certo componente ou sistema é expressa em forma de faixa de valores (*P* e *B*), e não de um valor único, e que existe uma incerteza associada a esta faixa (representada por *m*). Assim, no caso de interesse específico deste artigo, são estabelecidos os limites mínimo e máximo da probabilidade de falha de um certo elemento e o quanto se acredita nesta faixa. Como o fabricante não fornece o valor da taxa de falhas do componente ou sistema, os valores de *P*, *B* e *m* devem ser estabelecidos por especialistas diversos. Cada especialista consultado fornecerá os limites mínimo (plausibilidade, *P*) e máximo (crença, *B*) em que ele acredita está a probabilidade de falha de um certo sistema e a nossa confiança na opinião do mesmo é representada pela massa *m*. Ou seja, acredita-se com *m* de certeza de que a probabilidade de falha de um certo componente ou sistema (PdF) está entre os valores *P* e *B*.

Como exemplo prático, faz-se a atribuição de valores hipotéticos aos elementos da Figura 2 e a representação gráfica de p_S é apresentada na Figura 3. A Figura 3 mostra que dois especialistas foram consultados e que cada um forneceu faixas diferentes para a probabilidade de falha de *software* (p_S) de uma aeronave, valores limites no eixo das abscissas. A Figura mostra também que a crença na opinião destes especialistas difere e esta é representada através da altura da figura entre os valores limites.

Figura 3: Representação gráfica dos limites inferior e superior para a falha do tipo eventual de *software* p_S, sendo plausibilidade *(P)* o inferior e a crença *(B)* o superior.



Fonte: O autor.

No grupo de Equações (8), tem-se a visualização dos valores mínimos (plausibilidade, *P*) e máximos (crença, *B*) e a confiança nesses dados (massa *m*). A partir desses dados, pode-se levantar a PdF para o sistema representado por meio da árvore de falhas, propagando a faixa de incerteza (plausibilidade *P* e crença *B*) e a crença na opinião dos especialistas (massa *m*) por meio de portas E ou OU.

$$\begin{aligned}
p_s &= \begin{cases} 0{,}0020; 0{,}0033; 0{,}7 \\ 0{,}0015; 0{,}0028; 0{,}3 \end{cases} = \begin{cases} p11; b11; ms1 \\ p12; b12; ms2 \end{cases} \\
p_w &= \begin{cases} 0{,}0005; 0{,}0010; 0{,}7 \\ 0{,}0007; 0{,}0013; 0{,}3 \end{cases} = \begin{cases} p21; b21; mw1 \\ p22; b22; mw2 \end{cases} \\
p_{hw} &= \begin{cases} 0{,}00015; 0{,}00025; 0{,}7 \\ 0{,}00010; 0{,}00035; 0{,}3 \end{cases} = \begin{cases} p31; b31; mhw1 \\ p32; b32; mhw2 \end{cases} \\
p_{sw} &= \begin{cases} 0{,}00025; 0{,}00030; 0{,}7 \\ 0{,}00015; 0{,}00030; 0{,}3 \end{cases} = \begin{cases} p41; b41; msw1 \\ p42; b42; msw2 \end{cases}
\end{aligned} \tag{8}$$

Conforme apresentado na Figura 2, os elementos constituintes do piloto automático relacionam-se por meio de portas E e OU. Tendo faixas de valores de confiabilidade e crenças associadas aos elementos, a propagação por meio das portas da árvore exige considerar esses limites e crenças. A falha eventual de *software* possui dois elementos relacionados por meio de porta E. Assim, faz a operação p_S E $p_W = p_S * p_W$. Contudo, se a relação fosse por meio de porta OU, a operação correta seria p_S OU $p_W = p_S + p_W - p_S * p_W$. No grupo de Equações (9), apresenta-se p_{SC} como resultado da incerteza de confiabilidade em seus elementos componentes, p_S e p_W, relacionados por meio de uma porta E e com valores identificados no grupo de Equações (8). Nota-se ainda que a soma das massas permanece 1 para p_{Tsc}.

$$p_{TLsc} = \begin{cases} p_{TL1sc} = p11 * p21 = 1{,}00E-6; \\ p_{TL2sc} = p11 * p22 = 1{,}40E-6; \\ p_{TL3sc} = p12 * p21 = 7{,}50E-7; \\ p_{TL4sc} = p12 * p22 = 1{,}05E-6; \end{cases}$$

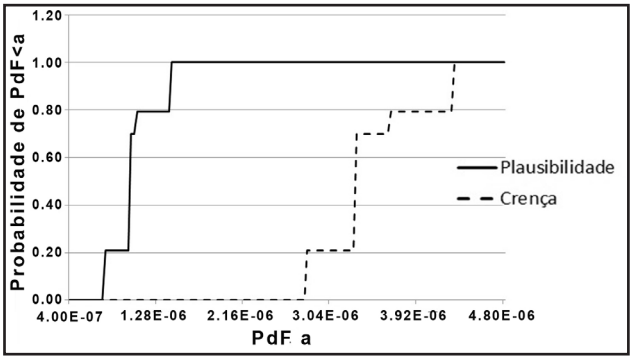
$$p_{TUsc} = \begin{cases} p_{TU1sc} = b11 * b21 = 3{,}30E-6; \\ p_{TU2sc} = b11 * b22 = 4{,}29E-6; \\ p_{TU3sc} = b12 * b21 = 2{,}80E-6; \\ p_{TU4sc} = b12 * b22 = 3{,}64E-6; \end{cases} \Rightarrow p_{Tsc} = \begin{cases} 1{,}00E-6 & 3{,}30E-6 & 0{,}49; \\ 1{,}40E-6 & 4{,}29E-6 & 0{,}21; \\ 7{,}50E-7 & 2{,}80E-6 & 0{,}21; \\ 1{,}05E-6 & 3{,}64E-6 & 0{,}09; \end{cases} \quad (9)$$

$$m_{Tsc} = \begin{cases} m_{T1sc} = ms1 * mw1 = 0{,}49; \\ m_{T2sc} = ms1 * mw2 = 0{,}21; \\ m_{T3sc} = ms2 * mw1 = 0{,}21; \\ m_{T4sc} = ms2 * mw2 = 0{,}49. \end{cases}$$

A partir dos valores obtidos no grupo de Equações (9), pode-se traçar o gráfico de Atribuição de Probabilidade Básica (APB), ou *Basic Probability Assignment* (BPA) em inglês. A APB, apresentada graficamente, permite perceber, de forma intuitiva, a faixa de confiabilidade do sistema. A Figura 4 mostra a distribuição cumulativa da probabilidade de falha (PdF) de um elemento isolado, isto é, permite determinar que a probabilidade de que este elemento tenha taxa de falhas menores do que um certo valor *a* (PdF *a*) está na faixa de valores entre a Plausibilidade e a Crença (PdF < *a*). Lembrando que pequenos valores de PdF implicam em sistemas mais confiáveis e que maiores valores em menos confiáveis, pode-se afirmar que, com os dados disponíveis, a probabilidade de falha deste exemplo é maior do que $7{,}5.10^{-7}$ (grupo de Equações (9) e Figura 4) e menor do que $4{,}29.10^{-6}$, com 100% de certeza. Se valores menores de certeza forem aceitáveis, 80%, por exemplo, pode-se afirmar que a probabilidade de falha desse sistema está entre $7{,}5.10^{-7}$e $3{,}64.10^{-6}$. Fora desses limites, nada é passível de afirmação. Resta, nesse caso, estabelecerem-se requisitos de confiabilidade para que seja aceito o sistema em análise ou que se busquem formas de melhorá-lo, seja por meio de troca por um mais confiável, seja por meio de uso de redundância.

A partir do valor de confiabilidade do sistema, pode-se avaliar de forma quantitativa o risco oferecido à segurança de voo. A análise quantitativa de confiabilidade é necessária como um dos fatores que podem provocar um pouso sem controle e eventuais choques com pessoas e edifícios, com possibilidade de fatalidades.

Figura 4: Representação gráfica dos limites inferior e superior da plausibilidade (*P*) o inferior e a crença (*B*) o superior para a falha do tipo eventual de *software* p_{SC}.



Fonte: O autor.

2.3 Análise de risco na Presença de incerteza

A análise de risco de uma aeronave deve levar em conta diversos parâmetros da aeronave e dos externos a ela para que se possa avaliar a probabilidade de uma falha catastrófica e de uma fatalidade dela decorrente. Essa é uma questão de suma importância para a definitiva inserção de ARP no espaço aéreo controlado. A análise de risco pode levar em conta diversos elementos, como um conceito particular de operações (CONOPS), sistema e subsistemas das aeronaves, meio ambiente, presença de outras aeronaves da frota ou não, elementos mitigadores de colisão em voo, prioridades no cumprimento da missão e outros. A avaliação da segurança é obrigatória para inserção de ARP no espaço aéreo nacional, assim como para realizar avaliação de risco associado às missões (relé de comunicação, sensoriamento remoto, monitoramento etc.).

Weibel e Hansman (2004), Grimsley (2004) e Lum e Waggoner (2011) fazem referência a diferentes modelos de impacto no solo, a fim de estabelecerem níveis de segurança para uma dada situação. No entanto, além de impacto com o solo, Lum e Waggoner (2011) também consideram colisões no ar por meio do choque hipotético entre um avião intruso e um ARP. Importante ressaltar que, em caso de uma colisão no ar, resíduos ARP e da aeronave intrusa são esperados, caindo verticalmente no chão, impondo assim riscos adicionais à população. Este trabalho considera as duas hipóteses de acidentes (pouso de emergência e choque no ar). Assim, o modelo de Lum e Waggoner (2011) foi utilizado como base neste trabalho, equações 10 a 15. No entanto, ao contrário de Lum e Waggoner (2011), neste artigo considera-se a incerteza no valor de confiabilidade das ARP e uma faixa de valores é considerada em vez de um valor único. Como os autores citados, o objetivo é fornecer ferramentas para demonstrar que os níveis de risco de ARP são menores ou iguais àqueles aceitos pela aviação em geral.

Como abordagem inicial, somente uma aeronave foi considerada em voo de baixa altitude (menos que 1000 pés), em áreas segregadas, para executar missão de sensoriamento

remoto, sendo F_{ped} o número total de colisões por hora com pedestres e F_{bldg} o número total de colisões por hora com edifícios, devido a uma combinação de falha catastrófica do sistema e colisões no ar (LUM; WAGGONER, 2011).

$$F_{ped} = F_{ped,p} + F_{ped,midair} \quad (10)$$

$$F_{bldg} = F_{bldg,p} + F_{bldg,midair} \quad (11)$$

$$F_{ped,p} = N_{ua}\lambda\sigma_p A_{L_{Hp}} \quad (12)$$

$$F_{ped,midair} = C_{midair}\sigma_p A_{L_{Vp}} \quad (13)$$

$$F_{bldg,p} = N_{ua}\lambda\sigma_b A_{L_{Hb}} \quad (14)$$

$$F_{bldg,midair} = C_{midair}\sigma_b A_{L_{Vb}} \quad (15)$$

onde:

Fped, p	Taxa de colisão com pedestres, devido a falha da aeronave (sistema), (colisão / hora);
Fped, midair	Taxa de colisão com pedestres, devido a colisões em voo, (colisão / hora);
Fbldg, p	Taxa de colisão com construções, devido a falha da aeronave (colisão / hora);
Fbldg, midair	Taxa de colisão com construções, devido a colisões em voo, (colisão / hora);
$A_{L_{Hp}}$, $A_{L_{Hb}}$	Área letal para pedestres e edifícios em um acidente horizontal (devido à falha do sistema) (m^2);
$A_{L_{Vp}}$, $A_{L_{Vb}}$	Área letal para pedestres e edifícios em um acidente vertical (devido à colisão no ar) (m^2);
C midair	Taxa de colisões de aeronaves no ar (transitório e em frota) (acidentes / hora);
Nua	Número de ARP na frota;
λ	Taxa de falhas em voo para uma única ARP (falhas / hora), derivada da análise da árvore de falhas; e
σ_b, σ_p	Respectivamente, densidade de construções e de pedestres na área (itens/m^2).

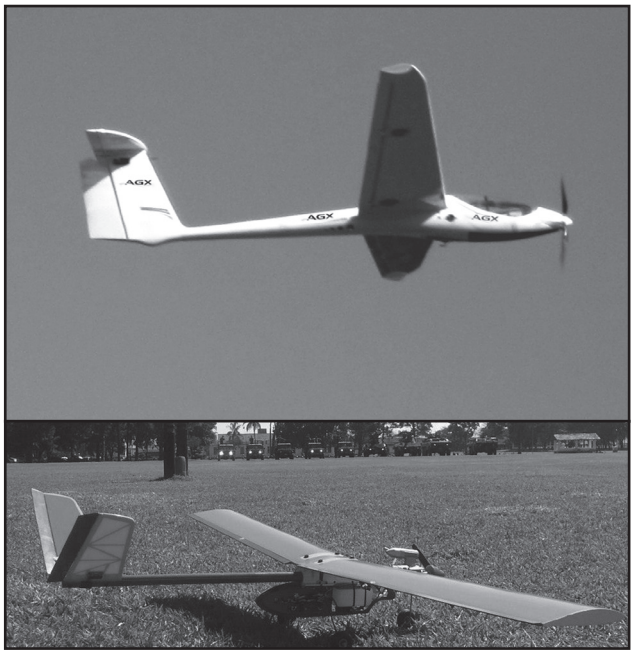
No trabalho de Lum e Waggoner (2011), o leitor pode encontrar uma descrição completa e clara para a avaliação de risco utilizada nesta sessão. Aqui, apenas as funções principais são apresentadas para permitir uma compreensão da metodologia utilizada.

Dadas as incertezas associadas à taxa de falhas da aeronave (λ), este trabalho propõe o uso dos valores máximo e mínimo obtidos com o uso da teoria da evidência em vez de um valor único. Para exemplificar o uso dessa metodologia, este trabalho usa as aeronaves desenvolvidas pela empresa AGX em parceria com o Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos (INCT-SEC), de que é parte o Instituto Tecnológico de Aeronáutica (ITA).

2.4 Exemplo de aplicação

O grupo de pesquisas do INCT-SEC é formado principalmente por professores e alunos do ITA, do Instituto de Ciências Matemáticas e de Computação / Universidade de São Paulo (ICMC/USP) e da empresa AGX Tecnologia. O grupo possui diversas ARP desenvolvidas e algumas em desenvolvimento com tecnologia 100% nacional. Para este trabalho, tem-se como exemplo o Tiriba (sensoriamento remoto) e o Ararinha (treinador de baixo custo de código aberto), conforme Figura 5. O Tiriba acumula um total de mais de 2.000 horas de voo para o Exército Brasileiro, a agricultura, o meio ambiente. O Ararinha é uma ferramenta valiosa não apenas para treinamento de novas tripulações, mas também como um banco de ensaio para novas soluções tecnológicas e algoritmos. Cabe ressaltar que boa parte do sucesso do Ararinha resulta dos esforços de alunos e professores de um grupo de pesquisas do ICMC, denominado Grupo de Interesse em SisVANTs e Aplicações (GISA)[1]. O Tiriba tem piloto automático complexo e, portanto, novas soluções são inicialmente testadas e amadurecidas com o Ararinha.

Figura 5: ARPs Tiriba® acima e Ararinha® abaixo. Ambas desenvolvidas em parceria entre a empresa AGX Tecnologia e INCT-SEC.



Fonte: O autor.

[1]Disponível em: <http://gisa.icmc.usp.br>.

Trabalhos experimentais foram realizados para testar soluções teóricas no campo. Apesar de valores reais das aeronaves terem sido alterados devido à confidencialidade associada ao produto, esses resultados continuam válidos como exemplo de aplicação da metodologia proposta.

A árvore de falhas fornece a confiabilidade total do sistema (λ) e permite identificar os elementos que mais impactam seu valor total. Caso a confiabilidade esteja acima do valor aceitável, uma análise de custo-benefício de um elemento determinado permite a decisão sobre o uso de sistema de supervisão para atuar como um ponteiro precoce de falha, por meio de uma porta E, ou a sua troca por outro sistema mais confiável, diminuindo a PdF do sistema. O uso da teoria da evidência permite uma análise qualitativa e quantitativa na presença de incertezas sobre a probabilidade de falha dos elementos componentes do sistema em análise e produz faixas de confiabilidade na sua propagação na árvore de falhas. O uso de uma faixa de confiabilidade λ na avaliação de risco resulta também em uma faixa na avaliação de risco, com um valor otimista (menor) e outro pessimista (maior).

Para um cálculo de exemplo da avaliação de risco, será usada a árvore de falhas da aeronave Tiriba (valores fictícios), operação em uma área segregada em baixa altura (1000 pés) e a presença de uma aeronave intrusa pilotada. Levando em conta a incerteza de MTBF do sistema e sem qualquer sistema de mitigação, a taxa de colisão, por hora, de pedestres (F_{ped}) atingidos durante um ano de operação, devido a choques em voo e pousos de emergência sem controle, varia de $7{,}5.10^{-06}$e $3{,}5.10^{-05}$e para edifícios (F_{bldg}) entre $1{,}4.10^{-04}$ e $6{,}6.10^{-04}$.

Dados quantitativos na árvore de decisão são úteis para a verificação do impacto ou da necessidade de redundâncias ou troca de componentes. Por exemplo, no caso analisado, a adição de um processador redundante reduz o F_{ped} entre 2 e 3%. Pode não parecer muito, mas em operações e condições de voo diferentes, esse número pode ser decisivo para a escolha da plataforma. Como já foi explanado, a escolha entre um sistema redundante e um sistema supervisor deriva de uma análise técnico-econômica.

Os dados necessários a este exemplo estão apresentados nas Tabelas 1, 2 e 3. A Tabela 1 apresenta os parâmetros de aeronaves tripuladas na área de missão do VANT em análise. A Tabela 2 mostra as características específicas do VANT Tiriba, considerado no exemplo. A Tabela 3 descreve os elementos de interesse sobre a área de operação do VANT. Os dados contidos nestas Tabelas permitem a avaliação de risco tendo em conta o VANT, o ambiente e o tipo de operação realizada.

Vale a pena notar que, se houver somente a presença de uma aeronave ARP e uma intrusa pilotada, as taxas de colisão em voo ficam improváveis e podem ser desconsideradas, devido ao seu baixo valor em comparação com as vítimas potenciais encontradas por um pouso de emergência, $5{,}5.10^{-09} \leq F_{ped,h} \leq 2{,}6.10^{-08}$ (taxa de colisão com pedestres, devido a falha do sistema, colisão / hora) e $F_{ped,midair} = 5{,}4.10^{-19}$ (taxa de colisão com pedestres, devido a colisões em voo, colisão / hora). Os parâmetros utilizados estão condensados na Tabela 1 e a CONOPS envolve voos sobre áreas com fraca densidade populacional (campos agrícolas) e sem ações comuns de mitigação, como observadores ao redor da área e contato direto com o controlador de tráfego aéreo local e agricultores.

No primeiro exemplo, o risco às pessoas está basicamente situado na eventual falha das ARP e num pouso descontrolado de emergência, visto a existência de poucas aeronaves no ar. Há de se supor uma outra situação de tragédia na mesma área, em que uma busca mais rápida seja necessária, porque vidas estão em risco e o tempo é fator importante na localização. Uma opção plausível seria o aumento do número de ARP com sensores apropriados em missão de busca (visual, termal, multiespectral, etc.). Mas, se, em vez de apenas uma, sejam utilizadas 10 ARP e que haja duas aeronaves tripuladas no local, sem possibilidade alguma de coordenação de posição com as não tripuladas, nesse caso, a taxa de colisão com pedestres, devido à falha do sistema (colisão / hora), aumenta dez vezes, pois dez vezes mais aeronaves estão no ar. A taxa de colisão com pedestres, devido a colisões em voo (colisão / hora), passa, no entanto, de um valor desprezível, da ordem de 10^{-19}para $3{,}1.10^{-06}$, tornando-se, superior à falha do sistema em voo e o maior fator de risco.

É evidente que o uso de múltiplas plataformas ARP em voo é desejável em aplicações civis e militares e a demanda atual deve aumentar. Uma solução técnica possível para diminuir o risco de colisões aéreas é tornar as aeronaves cientes da posição umas das outras e de procedimentos de desvio e posição relativa. Se cada uma das aeronaves Tiriba estiver sempre ciente das outras ARP e das aeronaves tripuladas, mantendo distância segura ou relativa, assim como da posição das casas na área sobrevoada, pode-se esperar diminuição significativa do risco (significa aumento dos fatores de mitigação $\varepsilon_{ua/ua}$ e de $\varepsilon_{ua/acft}$, na Tabela 2). O modelo de risco, todavia, demonstra que um aumento significativo de aeronaves exige valores de mitigação próximos de 1 para tornar o espaço aéreo novamente seguro, o que implica sistemas de comunicação entre aeronaves eficientes e confiáveis. Portanto, mesmo sem intervenção humana, é possível evitar, de forma simples e com baixo custo, situações de colisão no ar (utilizando algoritmos pré-armazenados) e no solo (no caso de uma aterragem de emergência), se somente forem usados algoritmos e sistemas de comunicação eficientes.

Tabela 1: Parâmetros das aeronaves na área de missão do VANT em análise utilizados para a avaliação de risco, conforme o modelo descrito em Lumand e Waggoner (2011).

Parâmetro	Valor	Unidade	Comentário
V_{acft}=	150	km/h	Velocidade cruzeiro da aeronave intrusa
ρ_0=	$2{,}19.10^{-19}$	m^{-3}	Densidade de intrusos
Φ_{acft}=	5,00	m^2	Área frontal das aeronaves intrusas
R_{acft}=	1,26	m	Raio das aeronaves intrusas
P_0=	2		Passageiros dentro das aeronaves intrusas
ε_0=	0		Fator de mitigação: considerado que intruso não está sob o controle do tráfego aéreo

Fonte: O autor.

Tabela 2: Dados sobre o VANT em análise para avaliação de risco.

Parâmetro	Valor	Unidade	Comentário
V_{ua}=	100	km/h	Velocidade cruzeiro
ω_{ua}=	2,24	m	Envergadura
γ =	0,083	rad	Ângulo de planeio em emergência
Φ_{ua}=	0,37	m^2	Área Frontal
R_{ua}=	$3{,}42.10^{-01}$	m	Raio
L_{ua}=	1	m	Comprimento
λ=	$2{,}31.10^{-04}$ – $1{,}08.10^{-03}$		Faixa de incerteza da PdF da ARP (obtida da árvore de falhas)
$\varepsilon_{ua/acft}$=	0		Mitigação aplicada para evitar colisão entre a ARP e o intruso
$\varepsilon_{ua/ua}$=	0		Mitigação aplicada para evitar colisão entre duas ARP
Φ_{col}=	5,37	m^2	Área de colisão

Fonte: O autor.

Tabela 3: Características da área de operação do VANT.

Parâmetro	Valor	Unidade	Comentário
VOL_{voo}=	$4{,}57.10^{+09}$	m^3	Volume da área de voo
N_{ua}=	1		Número de ARP no ar
N_{acft}=	1		Número de intrusos no ar
M_l=	1344	h	Número de horas de operação por ano
A_{opr}=	$1{,}5.10^{+07}$	m^2	Área de Operação
Ceiling=	1000	ft	Altitude máxima
σ_b=	$1{,}0.10^{-06}$	bldg/m^2	Densidade de construções
A_b=	50	m^2	Área média das construções
H_b=	3	m	Altura média das construções
D_b=	0,42		Densidade de colisões fatais
σ_p=	$2{,}6.10^{-07}$	pedestre/m^2	Densidade de pedestres
R_p=	0,25	m	Raio dos pedestres
H_p=	1,75	m	Altura dos pedestres
D_{ped}=	1	fatalidade/colisão	Expectativa de fatalidades devido à colisão de uma ARP com um pedestre (assumido que todo choque resulta em fatalidade).

Fonte: O autor.

Além disso, caso uma aeronave perceba a presença de uma tempestade repentina ou de um incêndio florestal, ela pode compartilhar esse dado com sua frota e, se necessário, uma ou mais delas realizar uma mudança automática de rota durante o voo (informando a base no solo sobre a alteração), para aumentar a segurança de voo sem abortar a missão em andamento.

Cabe citar, sem aprofundar o tema, que o INCT-SEC, por meio do grupo GISA/USP e do ITA, vem realizando experimentos de voo em formação de ARP, com a utilização da aeronave Ararinha e com o desenvolvimento de sistemas de comunicação de dados digital por meio de rádio definido por *software*, conforme Figura 6.

3 CONCLUSÃO

Este trabalho apresenta uma abordagem que permite a avaliação quantitativa de risco para pequenas aeronaves, remotamente pilotadas com valores incertos de confiabilidade em seus componentes. Partindo da árvore de falhas de uma aeronave usou-se a teoria da evidência de Dempster-Shafer para avaliação da sua probabilidade de falha e a faixa de valores encontrada foi usada na avaliação de risco associada a uma operação. Duas aeronaves desenvolvidas pelo grupo do INCT-SEC, Tiriba e Ararinha, são exemplos práticos da aplicação dos resultados.

Os resultados do estudo realizado neste trabalho podem servir para avaliação qualitativa e quantitativa do risco associado à operação de ARP e como auxílio à decisão para mudança dos subsistemas embarcados na aeronave não tripulada. A avaliação levou em conta as características e a arquitetura da aeronave, a área sobrevoada, a presença de outras aeronaves não previstas, a existência de mais de uma aeronave ARP e elementos que permitem o voo coordenado ou em formação, que evitam colisões aéreas e aumentam a eficiência no cumprimento da missão.

Figura 6: Experimentos de *"Hardware-in-the-loop"*, com o Ararinha, utilizando o *software* aberto e *hardware* Arduino e simuladores de voo.

Fonte: O autor.

REFERÊNCIAS

AGARWAL, Harish et al. Uncertainty quantification using evidence theory design optimization. **Reliability Engineering & System Safety**, v. 85, p. 281-294, 2004.

BRASIL. Secretaria de Aviação Civil.Agência Nacional de Aviação Civil. **Regulamentos Brasileiros.** Disponível em: <http://www2.anac.gov.br/biblioteca/rbha.asp>. Acesso em: 07 de jun. 2013.

DEMPSTER, Arthur P. A generalization of Bayesian inference. **Journal of the Royal Statistical Society:** series B, n. 30, p. 205-247, 1968.

ERICSON, C. Fault tree analysis : a history. In: PROCEEDINGS OF THE 17TH INTERNATIONAL SYSTEM SAFETY CONFERENCE, 17., 1999, Fórida. **Proceedings**... Flórida, 1999.

FIGUEIRA, Nina et al. Mission oriented sensor arrays: an approach towards UAS Usability Improvement in Practical Applications. In: EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES,5., 2013, Munich. **Proceedings**... Munich: EUCASS, 2013.

FONSECA, Eloi; MATTEI, Andre P; CUNHA, Wagner C. Adaptative integration systems using FPGA COTS devices. In: EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES, 5., 2013, Munich. **Proceedings**... Munich: EUCASS, 2013.

GRIMSLEY, Frank M. Equivalent Safety using Casualty Expection Approuch. In: UNMANNED UNLIMITED: TECHNICAL CONFERENCE, 3., 2004, Chicago, Illinois. **Proceedings**... Chicago, Illinois: AAIA, 2004. Disponível em: <www.ifi.cta.br>. Acesso em: 07 jun. 2013.

JACOB, Christelle; DUBOIS, Didier; CARDOSO, Janette. Evaluating the Uncertainty of a Boolean Formula with Beleif Functions. In: International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, 14., 2012, Catania, Italy. **Proceedings**... Catania, Italy: IPMU, 2012. p. 521-531. Part III.

LUM, Christopher; WAGGONER, Blake. A risk based paradigm and model for unmanned aerial systems in the national airspace. In: INFOTECH@AEROSPACE, 2011, St Louis, Missouri. **Proceedings**... St Louis, Missouri: AAIA, 2011.

MATTEI, Andre P. et al. UAV In-Flight Awareness: a tool to improve safety. In: EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES, 5., 2013, Munich. **Proceedings**... Munich: EUCASS, 2013.

MURTHA, Justin F. **Evidence Theory and Fault Tree Analysis to Cost-Effectively Improve Reliability in Small UAV Design**. Virginia: Virginia Polytechnic, 2009.

OBERKAMPF, W. et al. A new methodology for the estimation of total uncertainty in computational simulation. In: NON-DETERMINISTIC APPROACHES FORUM, 1999. **Proceedings**... AAIA, 1999.

OBERKAMPF, W. et al. Variability, uncertainty, and error in computational simulation. In: 7TH AIAA/ASME JOINT THERMOPHYSICS AND HEAT TRANSFER CONFERENCE, 7., 1998, Albuquerque, NM, USA. **Proceedings**... Albuquerque, NM, USA: AAIA, 1998. 357-2, p. 259–72, 1998.

OBERKAMPF, W.; HELTON, J.; SENTZ, K. Mathematical representation of uncertainty. In: NON-DETERMINISTIC APPROACHES FORUM, 2001, Seattle. **Proceedings**... Seattle: AIAA, 2001.

SHAFER, Glenn. **A Mathematical Theory of Evidence**. Princeton: Princeton University Press, 1976.

WEIBEL, Roland E.; HANSMAN, John. Safety considerations for operation of different classes of UAVs in the NAS. In: AVIATION TECHNOLOGY, INTEGRATION AND OPERATIONS, ATIO Forum, 4., 2004, Chicago, Illinois. **Proceedings**... Chicago, Illinois: AAIA, 2004.