APIS: Método para Desenvolvimento de Interfaces Homem-Computador em Sistemas de Segurança Visando a Confiabilidade Humana

Lúcia Vilela Leite Filgueiras

lfilguei@usp.br
Escola Politécnica da Universidade de São Paulo - Departamento. de Engenharia de Computação e Sistemas Digitais; IEEE Reliability Society Human Reliability Committee
Av. Prof. Luciano Gulaberto, tv 3 no. 158 CEP 05508-900 São Paulo SP

Resumo

Este trabalho apresenta o método APIS: Análise e Projeto de Interfaces de Segurança, para desenvolvimento de interfaces homem-computador para sistemas de risco, nos quais o erro humano pode levar a catástrofes. O método proposto tem por base a aplicação das técnicas de Análise da Confiabilidade Humana em um ciclo de desenvolvimento, considerando os aspectos específicos da interação homem-computador.

Palavras Chave: confiabilidade humana, erro humano, interfaces homem-computador, metodologia

1. INTRODUÇÃO

Os erros humanos são responsáveis por um número estarrecedor de incidentes na indústria e na aeronáutica[1]. Algumas pesquisas indicam uma média de 60% de incidentes que podem ser atribuídos à ação humana. Em alguns casos, este número pode chegar a 90%[2]. Por outro lado, são incontáveis as situações em que a intervenção humana evitou um acidente ou mesmo reduziu seu impacto, o que faz com que mesmo sistemas de alto risco sejam muito dependentes da ação humana.

Sempre que a análise de um acidente conclui por um erro humano, a tendência é reduzir a probabilidade desta ocorrência pela substituição do homem por equipamentos extremamente confiáveis, aumentando-se o grau de automação, até um limite não totalmente utópico da automação total das atividades humanas. O alto investimento com a confiabilidade de hardware e software visa garantir que, nas mais diversas condições de operação, estes equipamentos deverão atuar corretamente. Mesmo assim, o homem ainda se insere no processo para compensar as eventuais falhas de projeto – agindo com sua criatividade e sua capacidade de solução de problemas quando a automação não tiver sido suficiente.

O resultado desta política, que ficou evidente nos mais recentes estudos da FAA sobre Fatores Humanos [3], é de que embora os sistemas automáticos cumpram as funções programadas, os erros humanos continuam acontecendo, desta vez associados ao desconhecimento das situação real do processo e à incompatibilidade entre os comandos humanos e o estado do sistema automático.

A questão que se coloca como de vital importância no projeto de sistemas críticos é como integrar a ação humana e os sistemas automáticos, desenvolvendo uma interface homem-computador que aumente a confiabilidade humana. A resposta, acredita-se, está em um método de desenvolvimento de interfaces que considere as características do erro humano e mantenha estas considerações em foco durante o processo de desenvolvimento pela aplicação de técnicas de Análise da Confiabilidade Humana.

Os motivos para o desenvolvimento de tal método não se resume, atualmente, a sistemas de controle de processos: na legislação americana, o projetista de um equipamento ou sistema pode ser responsabilizado civil e criminalmente se o uso deste equipamento causar algum dano ao usuário. Assim, a busca pela redução dos erros humanos atinge, atualmente, a interface homem-computador de produtos comerciais tais como equipamentos biomédicos, veículos, eletrodomésticos e outros.

Este trabalho apresenta o método APIS: Análise e Projeto de Interfaces de Segurança, uma proposta para o desenvolvimento de interfaces homem-computador visando a confiabilidade humana. Para apresentar o método proposto, inicialmente, a seção 2 apresenta as técnicas atualmente utilizadas para Avaliação da Confiabilidade Humana, bem como as características específicas do erro humano na operação de interfaces homem-computador. Em seguida, a seção 3 expõe o método para desenvolvimento de interfaces homem-computador visando a Confiabilidade Humana.

2. TÉCNICAS DE AVALIAÇÃO DA CONFIABILIDADE HUMANA

As raízes das técnicas de Avaliação da Confiabilidade Humana remontam à Segunda Guerra, quando a complexidade dos equipamentos trouxe pela primeira vez a preocupação com a capacidade humana de operá-los. Como disciplina formal, a Confiabilidade Humana nasceu logo após o surgimento da Teoria da Confiabilidade, sendo aplicada principalmente a sistemas militares. O grande impulso desta área veio como acidente nuclear de Three Mile-Island, quando se reconheceu que a ação humana, condicionada por um ambiente desfavorável, poderia levar sistemas de risco a situações indesejáveis.

Podem ser definidos dois grandes objetivos para a Avaliação da Confiabilidade Humana:

- Reduzir os erros humanos, a partir de sua identificação e da avaliação do impacto destes erros no sistema como um todo;
- Quantificar a probabilidade de ocorrência destes erros e consequentemente, o sucesso das tarefas, permitindo a avaliação numérica do impacto dos erros na confiabilidade do sistema;

Não é objetivo deste trabalho descrever com detalhes as técnicas de avaliação da confiabilidade humana, porém, destaca-se um processo básico, necessário a todas:

- Definição do problema, em que são determinadas as situações em que a avaliação do erro humano é importante; esta definição pode surgir tanto dos estudos usados para avaliar modos de falha e seus efeitos, tradicionalmente empregados na avaliação de confiabilidade de sistemas, tais como HAZOP (Hazard and Operability Study), e FMEA (Failure Mode and Effect Analysis) ou ainda, em plantas em operação, de erros humanos observados na prática;
- Análise de tarefas, em que as funções humanas são detalhadas, compreendendo-se não só as atividades humanas mas também o contexto - ambiente físico, psicológico e organizacional – no qual as atividades são executadas;
- Análise do erro humano, em que são identificadas situações de erro, suas conseqüências e possibilidade de recuperação, com base nos mecanismos psico-fisiológicos do ser humano e nas características das tarefas;
- Quantificação, em que se estima a probabilidade de insucesso da tarefa, a partir de dados coletados historicamente, relativos a tarefas semelhantes, sendo que as probabilidades são compostas para cobrir os vários tipos de erro identificados. Dentre os métodos quantitativos, o mais conhecido é o THERP (Technique for Human Error Rate Prediction), acompanhado de técnicas complementares como o SLIM (Success Likelihood Index Method) e as curvas de correlação tempo-confiabilidade [4].
- Redução dos erros, em que são propostas medidas para evitar os erros quantificados como mais críticos.

Percebe-se que a aplicação destes métodos é complexa, pelo simples exame da seqüência de atividades. Mais ainda, a aplicação de métodos quantitativos nem sempre é possível, pela escassez de dados históricos. Dada a forte relação entre o contexto da atividade humana e o erro humano, nem sempre os dados existentes na literatura podem ser transportados para uma outra situação. Apesar disto, existem ferramentas para automatizar estes cálculos. Em geral, apenas a análise qualitativa é efetuada. A análise quantitativa é feita quando o número que expressa a confiabilidade é um requisito relevante para o projeto (como no caso de plantas nucleares), ou quando se deseja um parâmetro de comparação entre alternativas de projeto.

No caso de interfaces com computadores, o cenário é mais complexo. Os dados são efetivamente escassos, e por mais que existissem, dificilmente poderiam ser aproveitados, dada a grande variação de uma interface para outra. As técnicas de análise da confiabilidade humana usadas para avaliar interfaces homem-máquina podem ser usadas para analisar a interação com computadores, desde que alguns cuidados sejam considerados:

- enquanto a interface homem-máquina geralmente suporta apenas atividades motoras e de percepção, a interface homem-computador pode ser usada como auxílio à decisão, agindo, portanto, nos níveis mais altos do processamento cognitivo.
- a interface homem-computador manipula também conceitos abstratos, enquanto as interfaces homem-máquina relacionam-se com objetos concretos;
- enquanto o ser humano é sempre o agente da interação com uma máquina, no caso de interfaces homem-computador o computador é um agente também - muitas vezes, o ser humano é apenas supervisor das ações automáticas.

A natureza da interação homem-computador é responsável pela natureza dos erros humanos: nestas interfaces, os erros mais críticos tendem a ser do tipo equívocos ("mistakes"), provocados pela complexidade cognitiva da interface, ao invés de deslizes ("slips") e lapsos no nível sintático da interface. Listam-se a seguir alguns tipos de erros humanos prováveis:

O conhecimento embutido no software – que Hollnagel chama de "cognição artificial" [5] – faz o papel de um agente cujo comportamento pode ser desconhecido do usuário. Neste caso, os erros humanos vão estar associados com previsões erradas feitas a respeito do comportamento automático. Um segundo tipo de erro decorre da navegação através do espaço virtual, para encontrar um informação necessária para se concluir uma tarefa. Dada a disponibilidade crescente de informação, há um grande consumo da atenção do usuário em localizar o que se deseja, e nem sempre o processo de separar o que interessa se dá com sucesso. Um terceiro tipo de erro está associada à automação das tarefas humanas, que substituiu o trabalho manual e contínuo por trabalho intelectual e intermitente. Este erro se manifesta das seguintes formas:

- erro na percepção de eventos importantes, que deveriam disparar as ações humanas; em geral, a falta de atenção é devida ao tédio de longos períodos de supervisão sem nenhuma ação física;
- perda da habilidade de ação rápida, pela falta de prática.

Na próxima seção, apresenta-se um método para a consideração sistemática dos erros humanos no ciclo de desenvolvimento de interfaces homem-computador.

3. DESENVOLVIMENTO DE INTERFACES VISANDO CONFIABILIDADE HUMANA

O método APIS visa a redução da incidência dos erros humanos na operação de um sistema pela consideração sistemática destes erros e de suas conseqüências durante todo o projeto. A aplicação deste método permite ainda estabelecer cenários de treinamento e a identificação das soluções tecnológicas específicas, quando estas se fizerem necessárias. APIS apóia-se no ciclo de Engenharia de Usabilidade [6] e em técnicas de identificação de objetos.

Uma interface homem-computador visando a confiabilidade humana deve ter as seguintes características:

- deve apresentar informações adequadas, qualquer que seja a tarefa executada pelo usuário; deve ainda garantir que o processo cognitivo do usuário seja disparado quando necessário e que o modelo mental do usuário seja adequadamente alimentado;
- deve apresentar recursos de manipulação adequados, de forma que o usuário não seja induzido a erros na ação sobre os objetos da interface;
- deve ser capaz de rejeitar ou pelo menos indicar um erro humano, se ele acontecer.

O método APIS tem por base duas premissas:

- a confiabilidade da interface homem-máquina depende do transporte adequado dos objetivos da operação para o processo de especificação das funções da interface; isto implica que deve haver uma fase de identificação de erros humanos, suas causas e mecanismos de recuperação;
- a medida da eficiência deste transporte deve ser feita de forma iterativa, ao longo do ciclo de desenvolvimento da interface, sendo a confiabilidade humana o parâmetro de controle da repetição dos ciclos.

3.1. Fases do APIS

O método APIS possui duas fases, que diferem no nível de granularidade com que se representa a interação com o operador. As fases estão representadas na Figura 1

O **APIS-Fase de Análise** corresponde à fase de análise de requisitos do ciclo de desenvolvimento de software. O principal objetivo do método, nesta fase, é o estabelecimento do *modelo conceitual da operação*, que têm nos RMOs - Resumos de Metas Operacionais - a principal representação. Os RMOs são produzidos a partir da identificação dos cenários de operação. Técnicas de balanceamento são usadas para garantir que os limites do desempenho humano não sejam ultrapassados, e são propostas as metas de confiabilidade humana para a operação do sistema.

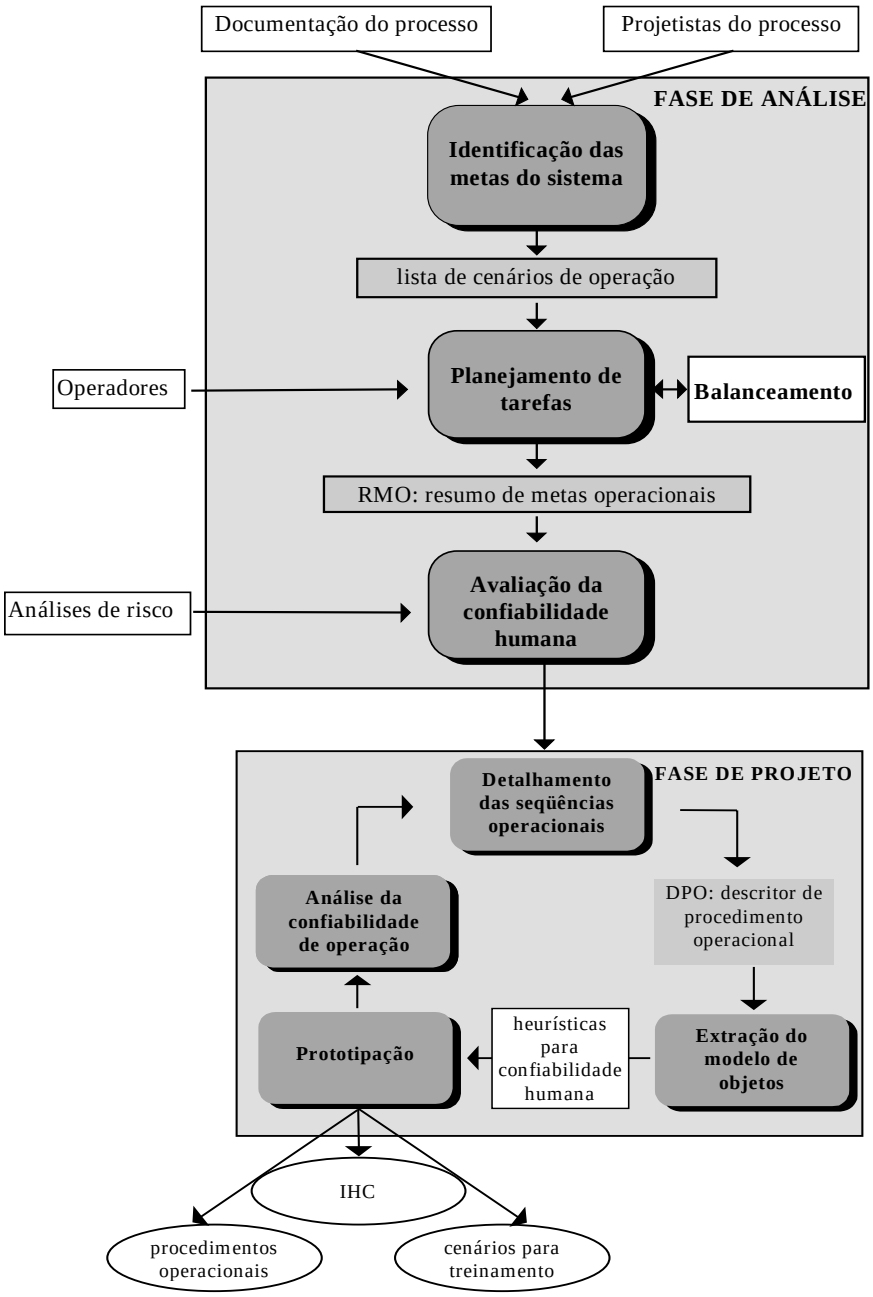

Figura 1 - Fases do APIS

Estando definidas as seqüências operacionais sobre o processo, o objetivo passa a ser o de mapear na IHC o modelo conceitual da operação, enquanto se garantem os requisitos de desempenho e confiabilidade da fase anterior. Desta forma, o **APIS-Fase de Projeto** corresponde ao projeto da IHC. Esta fase apóia-se em um ciclo de prototipação. O detalhamento das seqüências operacionais dá origem ao modelo de objetos da IHC, que é implementado em vários níveis de prototipação e avaliado do ponto de vista da confiabilidade humana. Além da interface homem-computador, resultam da aplicação do APIS o conjunto de procedimentos operacionais e os cenários para o treinamento dos operadores.

Em ambas as fases do APIS, a análise da confiabilidade humana exerce um papel fundamental. Na fase de análise, acontece a alocação da confiabilidade humana, através do projeto das variáveis de contexto. Na fase de projeto, as avaliações da confiabilidade humana são feitas sobre um protótipo cada vez mais detalhado. É importante salientar, porém, que o APIS não é um método de análise da confiabilidade humana, mas um método para garantir, por construção, a confiabilidade da interface homem-computador.

3.2. APIS - Fase de Análise

O desenvolvimento de uma interface confiável requer um planejamento das tarefas operacionais, para permitir ao operador, em qualquer circunstância, manter uma representação mental adequada e o controle sobre o processo. No APIS - Fase de Análise, a atividade de planejamento de tarefas é a formalização do processo de transferência de informações, dos projetistas e operadores do processo para a IHC, identificando as metas de operação.

Para isto, no APIS - Fase de Análise executa-se uma série de atividades, enumeradas a seguir:

- identificação das metas do sistema, produzindo uma lista de cenários de operação;
- planejamento de tarefas, em que as operações sobre a IHC são identificadas e documentadas na forma de Resumos de Metas Operacionais;
- balanceamento da interface homem-computador, para garantir que os limites do desempenho humano não sejam ultrapassados;
- avaliação de confiabilidade, quando se identificam os erros humanos e as formas de evitá-los.

3.2.1. Identificação das metas do sistema

O objetivo desta atividade é produzir uma lista de cenários de operação em que fiquem claras as metas a serem atingidas pelo operador. Identificando-se os propósitos do sistema, pode-se dizer que eles serão também as metas de cada usuário. Para compreender a forma de atingi-las, deve-se decompor estes propósitos nas sub-metas essenciais do sistema, isto é, naquelas metas que, se não atingidas por qualquer motivo, acarretam perda do propósito principal.

3.2.2. Planejamento de tarefas

A atividade de planejamento de tarefas consiste no detalhamento das metas operacionais identificadas na atividade anterior. Este detalhamento é documentado no RMO - Resumo de Metas Operacionais, apresentado na Figura 2. Os dados do RMO são coletados através de entrevistas com especialistas, sejam usuários ou projetistas do processo e da instrumentação. A etapa de coleta de dados é crítica no método APIS e, sem dúvida, particularmente difícil de ser executada na prática. Os projetistas da IHC não devem perder o objetivo do trabalho da coleta de dados, que é a definição das **metas** de operação, e por isto não devem se restringir às operações realizadas sobre o sistema de controle. A observação de operadores em salas de controle permite concluir que eles utilizam o sistema de controle como **ferramenta** para cumprir suas metas que, na maioria dos casos, não estão diretamente implementadas como funções no sistema de controle.

Quando a coleta é feita sobre um sistema em operação, é comum que os usuários não conheçam as metas, mas apenas as funções do sistema. Assim, pode-se dizer que a etapa de planejamento de tarefas é “top-down” no c aso de um projeto totalmente novo, pois se parte das metas para obter as operações, mas é “bottom-up” no caso de revisões de projetos, já que se parte das operações para obter as metas e daí, um novo projeto das operações.

Identificador:

Meta a atingir:

Cenário:

Prioridade: ☐ crítica ☐ importante ☐ regular ☐ baixa

Interrupção: ☐ possível ☐ indevida ☐ impossível

Atividade: ☐ supervisão ☐ manutenção ☐ recuperação ☐ calibração ☐ testes

Tempo máximo permitido:

para início: para conclusão:

Condições iniciais:

Gatilho:

Seqüência de Execução

Identificador	Meta

Condições de finalização:

Alternativas:

Figura 2 - Resumo de Metas de Operação (RMO)

3.2.3. Balanceamento entre operação humana e controle automático

O balanceamento entre a operação humana e a automação define-se como a atividade de atribuição criteriosa de funções de operação do processo entre a equipe de operação e o controle automático, de forma a garantir, em qualquer circunstância, a operação segura e eficiente do processo de risco. O balanceamento deve ser feito para explorar ao máximo as diferenças de comportamento entre homem e máquina, atribuindo a cada um as tarefas que lhes forem mais adequadas. Métodos quantitativos podem ser usados, tais como análises de linha de tempo e carga cognitiva, dependendo do grau de conhecimento sobre as tarefas nesta fase.

3.2.4. Avaliação da confiabilidade humana

A atividade de avaliação da confiabilidade humana deverá analisar os RMOs em função dos modos de erro humano, para determinar, em cada caso:

- quais as formas de erro humano que podem levar o cenário a não se cumprir;
- a influência do contexto na probabilidade destes erros acontecerem.

É importante ressaltar que, nesta fase, não existem dados suficientemente precisos para realizar um **cálculo** da confiabilidade humana como um número absoluto. As técnicas de análise da confiabilidade humana são aplicadas sobre sistemas em fase operacional ou sobre simuladores. Por isto, qualquer análise da confiabilidade humana realizada apenas sobre o protótipo da IHC deverá levar a resultados parciais. Por ser apenas uma indicação relativa, o número associado à confiabilidade humana estará fortemente associado à operação do sistema particular, e não deverá ser transportado diretamente para outros sistemas semelhantes. Sugere-se o uso de ferramentas automatizadas para suportar este cálculo, que nesta fase do APIS, é feita através da seguinte estratégia, comum aos métodos de avaliação da confiabilidade humana:

- pesquisa do erro humano, que consiste na análise qualitativa dos RMO em função dos vários modos de erro humano, identificando quais erros que podem levar a meta a não ser atingida;
- análise de sensibilidade do erro humano às condições de contexto, para refletir condições desfavoráveis e reavaliar a probabilidade de erro.

3.3. APIS - Fase de Projeto

As metas em cada cenário, descritas pelos RMOs, trazem requisitos de informação, a qual deve se tornar disponível oportunamente, através da IHC, para alimentar o modelo mental do operador sobre o processo. Da mesma forma, os RMOs descrevem as ações do operador sobre o sistema, em cada cenário, as quais cumprem o papel de levar o processo até o estado desejado.

O objetivo do APIS - Fase de Projeto é realizar o detalhamento das seqüências operacionais, através:

- da extração sistemática dos requisitos de informação e atuação dos RMOs;
- do transporte destes requisitos para um protótipo da IHC.

Sobre este protótipo, deverão ser ensaiados os diversos cenários e verificados os requisitos de desempenho do operador, definidos nos RMOs pelo tempo máximo para realização de cada operação. O ciclo de prototipação é feito sobre cada um dos cenários identificados na Fase de Análise, devidamente priorizados em função de sua relevância. Os erros humanos identificados na Fase de Análise, bem como as formas de evitá-los, deverão também fazer parte destes ensaios. Para isto, no APIS - Fase de Projeto executa-se uma série de atividades, enumeradas a seguir:

- detalhamento das seqüências operacionais;
- extração do modelo de objetos;
- prototipação;
- avaliação do protótipo;
- avaliação de confiabilidade humana.

3.3.1. Detalhamento das seqüências operacionais

O detalhamento das seqüências operacionais é a continuação do refinamento dos RMOs, planejando cada seqüência operacional e documentando estas seqüências em Descritores de Procedimento Operacional (DPO). As operações consideradas mais freqüentes ou mais relevantes em termos de risco deverão receber prioridade nesta atividade.

O DPO é uma descrição do comportamento esperado do operador. Para isto, o DPO representa a seqüência operacional por uma regra de execução de tarefas elementares, isto é, em unidades de comportamento humano que alteram ou verificam o estado do sistema. O formato do DPO é apresentado através de um exemplo na figura 3. O DPO tem por origem os formulários de análise de tarefas propostos por Burgy [7], Swain e Guttman [8] e Embrey [9], devidamente modificados pelo fato do procedimento destinar-se ao projeto da IHC.

3.3.2. Extração do modelo de objetos

Várias tentativas de se realizar uma IHC adequada à operação humana fracassaram principalmente porque a decisão dos objetos a representar na IHC foi arbitrária. O método APIS procura evitar esta inadequação ao extrair, da documentação da operação, representada pelos RMOs e DPOs, o conjunto de objetos que efetivamente represente o modelo conceitual do operador. Os objetos necessários a cada seqüência operacional são extraídos do campo *objeto* do DPO. Para cada objeto, os campos *atributo* e *valor* informam, respectivamente, sobre os atributos e seus domínios de validade. A extração dos métodos se faz a partir da análise do uso do objeto em cada operação. Esta análise implica

na classificação dos atributos em relação à sua função na seqüência operacional. Para isto, algumas definições, específicas do método APIS, se fazem necessárias.

Identificador: SI-0034

Seqüência Operacional: Injeção de polímero

Dificuldade: ☐ muito fácil ☐ fácil ☒ regular ☐ difícil ☐ muito difícil

Tempo estimado: 12,5min

	sujeito	*tarefa*	*objeto*	*atributo*	*valor*	*exceção*	*rotina de exceção*
	OP1	identifica	bomba de injeção 215PIPA e 215PIPB	estado de manutenção	em serviço	nenhuma bomba disponível	procedimento de manutenção de bombas
	OP1	decide	bomba de injeção	estado de manutenção	fora de serviço		
		com base em	bomba de injeção	tempo máximo recomendado de operação			
		e	bomba de injeção	tempo total em serviço			
	OP1	posiciona	bomba de injeção	estado de manutenção	fora de serviço		
	OP1	verifica	receita	volume de injeção		inventário de polímero insuficiente	procedimento de receita básica
	OP1	calcula	bomba de injeção	tempo no estado ligado		cálculo errado	repetir passo
		com base em	receita	volume de injeção			
	OP1	ajusta	temporizador	tempo no estado ligado		valor errado	ajusta novo valor
se bomba de injeção ativa for 215PIPA							
então	OP1	posiciona	HV1401	estado de operação	aberto	válvula não abre	usar reserva
	OP1	posiciona	HV1411	estado de operação	aberto	válvula não abre	usar reserva
	OP1	posiciona	215PIPA	estado de operação	ligado	bomba não liga	usar reserva
senão	OP1	posiciona	HV1402	estado de operação	aberto	válvula não abre	usar reserva
	OP1	posiciona	HV1412	estado de operação	aberto	válvula não abre	usar reserva
	OP1	posiciona	215PIPB	estado de operação	ligado	bomba não liga	usar reserva
fim							
	OP1	ajusta	temporizador	tempo_restante	início		
	OP1	monitora	temporizador	tempo restante	> 0	temporizador não responde	interromper seqüência
	OP1	monitora	tanque	nível		nível alto	interromper seqüência
	OP1	detecta	temporizador	tempo restante	=0	erro de deteção de final	procedimento calcular excesso de polímero
se bomba de injeção ativa for 215PIPA							
then	OP1	posiciona	HV1401	estado de operação	fechado	válvula não fecha	fechar válvula auxiliar
	OP1	posiciona	HV1411	estado de operação	fechado	válvula não fecha	fechar válvula auxiliar
	OP1	posiciona	215PIPA	estado de operação	desligado	bomba não desliga	procedimento de recuperação da injeção
else	OP1	posiciona	HV1402	estado de operação	fechado	válvula não fecha	fechar válvula auxiliar
	OP1	posiciona	HV1412	estado de operação	fechado	válvula não fecha	fechar válvula auxiliar
	OP1	posiciona	215PIPB	estado de operação	desligado	bomba não desliga	procedimento de recuperação injeção
end							
	OP1	informa	Supervisor	conclusão da tarefa			

Figura 3 - Descritor de Procedimento Operacional

Os **atributos observáveis** são definidos como aqueles atributos que carregam alguma informação que deve ser **compreendida** pelo operador para a realização de alguma tarefa. Os **atributos controláveis** são características de objetos que devem ser **modificadas** pelo operador em alguma tarefa. Dada a importância da realimentação na IHC, todos os atributos controláveis são também observáveis, por definição. Observe-se ainda que os atributos observáveis podem ser **dinâmicos**, isto é, sujeitos a mudanças, como por exemplo o estado de uma bomba, ou podem ser **estáticos**, se mantêm sempre o mesmo valor, por exemplo, características de fabricação desta mesma bomba. Logicamente, atributos controláveis são sempre dinâmicos.

A classificação em atributos observáveis e controláveis é feita, para cada atributo, a partir da análise dos comportamentos. Como os atributos observáveis são percebidos pelo operador, eles estão associados aos

comportamentos de percepção e cognitivos, bem como a comportamentos de comunicação. Os atributos controláveis exigem ação do operador e estão associados aos comportamentos motores. Esta classificação define o conjunto de métodos para cada objeto: os atributos observáveis estáticos dão origem a **métodos de exibição do atributo**; os atributos observáveis dinâmicos dão origem a métodos de exibição do atributo, distintos dos anteriores porque exigem consulta aos dados dinâmicos do processo; atributos controláveis resultam em **métodos de alteração do atributo**, que se traduzem em comandos do operador.

Os RMOs também devem ser inspecionados com o intuito de se extraírem objetos. Neste caso, a extração não é tão simples como no caso dos DPOs, porque a documentação está em um nível mais alto de abstração. Os objetos em um RMO estão principalmente nos campos de condição inicial, gatilho e condições finais. Os objetos extraídos dos RMOs deverão ser usados para compor as telas de nível mais alto, sobre as quais os operadores deverão fazer as operações de diagnóstico e a seleção das operações a executar.

Ressalte-se que os objetos utilizados na documentação da operação nos DPOs refletem balanços de massa e energia, leis físico-químicas específicas, tabelas de valores e parâmetros de estratégias de operaçã, o que permite, muitas vezes, a identificação de recursos não-convencionais da IHC que contribuem para aliviar as funções do operador e conseqüentemente otimizar o desempenho.

3.3.3. Prototipação

Uma vez definido o modelo de objetos da IHC, a etapa seguinte corresponde à prototipação da IHC. A prototipação corresponde à implementação:

- de cada objeto, com todos seus atributos e controles;
- de telas de suporte a cada operação, com a representação dos atributos visíveis de cada objeto;
- de telas de suporte à decisão;
- da apresentação dos alarmes do sistema.

A IHC produzida pelo método APIS estrutura-se de forma hierárquica. Rasmussen [10] considera que o operador tende a solucionar problemas a partir da visão mais abstrata dos conceitos do processo, tais como balanço de massa e energia, e prosseguir para a solução nos níveis mais próximos dos elementos físicos disponíveis do processo, tais como válvulas e bombas. Para se adequar à estrutura decisória do operador, a IHC deve poder atender todos os níveis de abstração:

- a monitoração do estado do processo é feita sobre o conjunto de informações que representa o **estado global** do processo: pela observação de um painel mímico ou, na falta deste, pela seleção da tela de maior visão geral sobre o processo que contenha o conjunto desejado de informações;
- na ocorrência de alguma anormalidade, o operador realiza o diagnóstico através da combinação de listas de alarmes e pela monitoração das informações que ele julga pertinentes aos alarmes em questão;
- a ação sobre o processo é feita através da seleção das telas onde são representados os elementos físicos do processo que implementam a ação desejada.

Desta forma, uma IHC adequada ao processamento mental do operador deverá reunir, em uma tela principal, o conjunto de informações que permite a seleção da meta apropriada para a situação. Cada meta operacional deverá, por sua vez, estar associada a uma tela que reúna as informações importantes para as decisões que devam ser tomadas neste contexto. Todas as possíveis ações sobre o processo, decorrentes das decisões tomadas pelo operador deverão estar disponíveis a ele no contexto da meta operacional selecionada. Acrescente-se a estes requisitos o fato de que o operador pode estar, em um mesmo instante de tempo, em estágios diferentes do mecanismo de diagnóstico e ação para várias metas simultâneas.

3.3.4. Avaliação do protótipo

A avaliação do protótipo é feita através de ensaios sobre o protótipo, com os seguintes objetivos:

- avaliar as condições gerais de usabilidade;
- verificar se os recursos oferecidos pela IHC são realmente suficientes para o cumprimento de cada tarefa;
- verificar se cada operação pode ser cumprida no tempo especificado nos RMOs;
- realizar avaliação sobre os erros cometidos sobre a interface;
- simular as várias condições de erro humano previstas durante a pesquisa de erros humanos.

3.3.5. Avaliação da confiabilidade humana

Na fase de projeto, o detalhamento da seqüência operacional permitirá obter a probabilidade intrínseca de falhas, dependente da ação em si e de fatores como a qualidade da interface naquela função específica. A quantificação da probabilidade de erro humano deverá ser feita pela aplicação das técnicas de análise da confiabilidade humana descritas na Seção 2. Desta forma, considera-se que confiabilidade humana, relacionada com um determinado cenário, tem duas componentes:

- a confiabilidade da cognição humana, relacionada à probabilidade de o operador identificar com sucesso a meta de operação; esta probabilidade está relacionada com os processos cognitivos de percepção, diagnóstico e tomada de decisão;
- a confiabilidade da ação humana, relacionada à implementação de uma solução sobre a IHC.

A confiabilidade da cognição humana deverá ser calculada, para cada cenário, como a probabilidade de o operador diagnosticar corretamente o cenário e fazê-lo no tempo correto. Para o cálculo da probabilidade de o operador diagnosticar corretamente a situação, deverá ser usado sistematicamente o julgamento de especialistas, ancorado em alguns (poucos) dados existentes na literatura. Para o cálculo da probabilidade de o diagnóstico se dar no tempo determinado, utilizam-se as curvas de correlação tempo-confiabilidade A confiabilidade da ação humana, após a seleção da meta, deverá ser calculada como a probabilidade de finalizar com sucesso a seqüência operacional. Para este cálculo, deverá ser usado o THERP.·

4. CONCLUSÃO

O método APIS destina-se ao desenvolvimento da IHC de sistemas críticos do ponto de vista de segurança, isto é, sistemas em que falhas causam perdas de vidas, danos materiais e danos ao meio ambiente. Nestes sistemas, muitas vezes, as ações humanas são essenciais para a segurança do processo. A utilização do APIS no desenvolvimento da IHC permite a aplicação de técnicas de avaliação da confiabilidade humana, importantes para as análises de risco destes processos.

Este trabalho foi desenvolvido com pesquisa de doutoramento no Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica e foi aplicado, parcialmente, em projetos de consultoria junto ao Centro Tecnológico da Marinha, em São Paulo.

REFERÊNCIAS

[1] LaSala, K.P; Filgueiras, L.V.L; Gigley, H.; Ullman, R. Designing Systems for Reliable Human Performance, IEEE Tutorial Video, 1997.
[2] Lee, K.W.; Tillman, F.A.; Higgins, J.J.; A Literature Survey of the Human Reliability Component in a Man-Machine System; IEEE Transactions on Reliability, vol. R-37, no. 1, april 1988, p.24-34
[3] Evans, B. Cockpit automation: The Good, the Bad, and the Ugly; Avionics Magazine, May 1998, pg 34-38.
[4] Dougherty, E. M.; Fragola, J. R. Human reliability analysis - a system engineering approach with nuclear power plant applications. John Wiley& Sons, 1988.
[5] Hollnagel, E. Human Reliability Analysis - Context and Control; Academic Press, 1993, 336 p.
[6] Nielsen, J. Usability Engineering, Academic Press, 1993
[7] Burgy, D. et al. Task analysis of nuclear power plant control room crews. United States Nuclear Regulatory Commission. 1983. (NUREG/CR-3371)
[8] Swain, A.D.; Guttmann, H.E. Handbook of human reliability analysis with emphasis on nuclear power plant applications. United States Nuclear Regulatory Commission. 1983. (NUREG/CR-1278)
[9] Embrey, D.E.. Human reliability. In: Serra, A.; Barlow, R.E. Teoria dell'Affidabilità. 1986. p.465-490.
[10] Rasmussen, J.; The role of hierarchical representation in decision making and system management. IEEE Transactions on Systems, Man and Cybernetics. v. SMC(15), p. 234-243, 1985