INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Departamento de Engenharia Mecânica

ISEL

Conceito, Classificação e Quantificação da Fiabilidade Humana na Relação Homem-Máquina

EDGAR JORGE MONIZ SERRANO
(Licenciado em Engenharia Mecânica)

Trabalho Final de Mestrado para obtenção do grau de Mestre
em Engenharia Mecânica

Orientador:
Prof. Mestre José Augusto da Silva Sobral

Júri:
Prof. Doutor João Carlos Quaresma Dias
Profª. Doutora Anabela Simões
Prof. Mestre José Augusto da Silva Sobral

Setembro de 2009

"The only man who makes no mistake is the man who does nothing."

Theodore Roosevelt

Dedicatória

à minha avó Judite, que sempre me apoiou,
acarinhou e depositou em mim uma confiança inabalável

Resumo

O estudo da fiabilidade humana é um tema imprescindível para qualquer sistema homem-máquina que pretenda adquirir os melhores índices de segurança e rendimento. Se a fiabilidade dos equipamentos é um campo onde já muito foi estudado, debatido e provado no terreno e onde os novos desenvolvimentos irão apenas acontecer devido aos avanços tecnológicos que permitam melhor predizer as potenciais falhas dos equipamentos, já a fiabiliade humana é uma área de estudo relativamente nova e onde muito há a desenvolver, particularmente devido às características inatas do ser humano. Ao contrário da evolução tecnológica, onde a melhoria dos materiais e processos obedece a um aperfeiçoamento relativamente gradual e crescente e que pode ser avaliado e melhorado, o comportamento e o aperfeiçoamento do ser humano apresentam dificuldades e complexidades variadas porque o mesmo é único e sofre influências adversas e imprevisíveis do meio em que vive, as quais têm influência directa no seu comportamento.

Assim, este trabalho académico propõe-se estudar e identificar as principais causas de erros humanos, através do conhecimento adquirido acerca dos processos cognitivos mais comuns do Homem, bem como definir os conceitos e procedimentos adjacentes à fiabilidade humana e às suas principais ferramentas de avaliação.

Palavras-chave: Fiabilidade Humana, Erros Humanos, Avaliação da Fiabilidade Humana, ATHEANA, THERP, ASEP, HEART, SPAR-H, CREAM, Relação Homem-máquina

Abstract

The study of human reliability is an essential subject for any human-machine system where the best safety and efficiency parameters are needed. While equipment reliability is a matter where much has been studied, debated and field-proven, and where new developments are only going to happen due to technological advances that will improve the prediction of potential equipment failures, human reliability is a relatively new field of study, where there is much more to develop, mostly due to human innate characteristics. In contrast to technological evolution, where materials' and processes' improvements obey to a relatively gradual and increased perfectioning and which can be evaluate and even more improved, human behavior and his constant perfectioning present a varied group of difficulties and complexities because each human being is unique and suffers adverse and unexpected influences from his own habitat, which have direct influence on his behavior.

This academic work is about the study and identification of the main causes of the human errors, through the knowledge of the most common human cognitive processes, as well as, to define the adjacent concepts and procedures to the human reliability and its main tools of assessment.

Key words: Human Reliability, Human Error, Human Reliability Analysis (HRA), ATHEANA. THERP, ASEP, HEART, SPAR-H, CREAM, Human-Machine interaction

Agradecimentos

A realização deste trabalho académico só foi possível graças à ajuda e colaboração de várias pessoas que, com o seu maior ou menor contributo, permitiram a sua prossecução com o detalhe científico que se exigia.

Antes de mais cumpre-me expressar desde já o meu franco agradecimento ao Sr. Eng. José Sobral do Departamento de Engenharia Mecânica do Instituto Superior de Engenharia de Lisboa, orientador desta tese de mestrado, pela sua enorme, abnegada e pronta disponibilidade com que sempre me recebeu, assim como pelas orientações gerais, dicas e sugestões que tornaram este trabalho possível. Destaco ainda a prévia organização das reuniões que teve comigo, sempre dotadas de resumos muito esclarecedores e que muito ajudaram na preparação e abordagem dos diversos temas, assim como a sua competência técnica nas matérias abordadas, que se revelaram extremamente úteis na compreensão das mesmas.

A pesquisa de fontes foi dos processos mais exaustivos e detalhados desta tese. Deste modo, segue o meu profundo agradecimento à Sra. Dra. Paula Serrano do Laboratório Nacional de Energia e Geologia, do Ministério da Economia e da Inovação, pelo seu papel essencial na realização deste trabalho, consubstanciado pela permanente e incansável disponibilidade com que sempre acedeu aos meus pedidos, nomeadamente na pesquisa e aquisição de fontes, assim como na normalização e no apoio geral concedido à elaboração desta dissertação.

Pelas revisões gerais, sugestões importantes e carinho com que acompanharam este trabalho, o meu grande agradecimento à Sra. Dra. Sofia Braz da Siemens S.A. e ao Sr. Dr. Eduardo Serrano, duas pessoas sempre disponíveis e cuja ajuda e compreensão foram extremamente preciosas.

Pretendo ainda agradecer à Sra. D. Fátima Firmino do Centro de Informação e Documentação do Gabinete de Estratégia e Planeamento do Ministério do Trabalho e da Solidariedade Social, por ter permitido o acesso a determinadas fontes que se revelaram extremamente difíceis de obter e cuja utilidade deveras importante não posso deixar de destacar.

Aos mencionados e a todos os outros que, de algum modo, contribuiram para a realização deste trabalho académico, o meu sincero agradecimento.

Edgar Serrano

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

APOA – *Assessed Proportion of Affect* (avaliação proporcional de afectação)

ASEP - *Accident Sequence Evaluation Program* (método de HRA)

ATHEANA - *A Technique for Human Error Analysis* (método de HRA)

COCOM - *Contextual Control Model* (modelo cognitivo dependente do contexto)[9]

CPC - *Common Performance Conditions* (condições comuns de desempenho)

CREAM - *Cognitive Reliability and Error Analysis Method* (método de HRA)

EF - *Error Factor* (factor de erro)

EFC - *Error-Forcing Context* (contexto forçador de erro)

EOC – *Error of Commission* (erro de comissionamento)

EOO – *Error of Omission* (erro de omissão)

EPC – *Error Producing Condition* (condição geradora de erro)

HAZOP - *Hazard And Operability Technique* (método de avaliação de risco)

HEART - *Human Error Assessment and Reduction Technique* (método de HRA)

HEP - *Human Error Probability* (probabilidade de erro humano)

HFE - *Human Failure Event* (evento de falha humana)

HMI – *Human-Machine Interface* (interface homem-máquina)

HRA – *Human Reliability Analysis* (avaliação/análise da fiabilidade humana)

PIF – *Performance Influencing Factors* (factores que influenciam o desempenho)

PRA - *Probabilistic Risk Assessment* (avaliação probabilística de risco)

PSA - *Probabilistic Safety Assessment* (avaliação probabilística de segurança)

PSF - *Performance Shaping Factor* (factor que define o desempenho)

SPAR-H - *Simplified Plant Analysis Risk Human Reliability Assessment* (método de HRA)

THERP - *Technique for Human Error Rate Prediction* (método de HRA)

UA - *Unsecured Action* (acção insegura)

Glossário

Acção insegura (UA) - acção indevidamente realizada, ou não realizada quando necessário pelos operadores, e que resulta numa degradação das condições de segurança do sistema.

Árvore de eventos – é uma rede lógica que pode ser quantificável e que inicia com um acidente ou evento iniciador e progride através de uma série de ramos que representam possíveis desempenhos de sistemas, acções humanas ou fenómenos que podem levar a um estado seguro, estável ou indesejável.

Árvore de falhas – é uma representação gráfica que mostra a relação lógica entre falhas, fornecendo uma descrição concisa e ordenada de várias combinações de possíveis eventos de falhas dentro de um sistema, os quais podem resultar em eventos predefinidos e indesejáveis de um sistema.

Cenário de acidente – é cada uma das várias possibilidades de evolução de um acidente, a partir do evento iniciador, ou seja, é a sequência de eventos e condições que podem resultar em consequências totalmente distintas.

Erro de comissionamento (ECO) – é um evento de falha humana resultante de uma acção insegura que leva à mudança na configuração e eventual degradação do sistema.

Erro de omissão (EEO) – é um evento de falha humana resultante da falha em realizar uma acção requerida e que leva a uma mudança, ou não, inadequada, da configuração do sistema, tendo como consequência a sua degradação.

Evento de falha humana (HFE) – é um evento básico que é modelado nos modelos lógicos das PSAs (árvore de eventos e árvore de falhas) e que representa a falha de uma função, sistema ou componente, que é o resultado de uma ou mais acções inseguras.

Evento iniciador – é o primeiro evento de uma sequência eventos que culmina na ocorrência de um acidente, podendo dar origem a vários cenários de acidente.

Factores que formatam o desempenho (PSF) - é um conjunto de influências no desempenho de uma equipa de operadores, resultante das características das instalações, da própria equipa e de cada operador, relacionadas com a *performance* humana. Estas características incluem procedimento, aprendizagem, treino e aspectos de factores humanos dos dispositivos de indicação e controlo do sistema.

Mecanismo de erro – é um mecanismo psicológico que pode causar uma determinada acção insegura que é gerada por uma combinação particular de factores que formatam o desempenho (PSFs) e as condições das instalações. Não são necessariamente maus comportamentos, mas sim mecanismos pelos quais as pessoas frequentemente executam, eficientemente, trabalhos com competência. Entretanto, em contextos errados, estes mecanismos podem levar a acções inadequadas que poderão culminar em consequências graves a nível da segurança.

1. INTRODUÇÃO

1.1.Motivação

A escolha deste tema para realização da Dissertação para obtenção do grau de Mestre em Engenharia Mecânica, adveio da vontade, por mim expressa, de conhecer os factores que condicionam a Fiabilidade Humana, bem como o modo como o fazem, a importância que podem ter na realização de uma determinada tarefa e ainda os métodos, técnicas e ferramentas para a determinar.

Dada a minha formação em Engenharia Mecânica, que inevitavelmente passa por algum estudo no campo da fiabilidade de equipamentos e, atendendo a que muitas das falhas que ocorrem, por exemplo na produção de um determinado componente, devem-se muitas vezes a erros humanos e nem sempre à fiabilidade dos equipamentos em questão, decidi explorar esta área de estudo que creio ser de extrema importância em todos sectores da indústria.

A nível académico, a realização deste trabalho motiva-me no sentido em que o mesmo poderá ser objecto de estudo e/ou um "ponto de partida" para desenvolver trabalhos científicos nesta e noutras áreas adjacentes.

Por último, acresce o facto de considerar que o conhecimento adquirido aquando da realização deste trabalho científico será para mim uma mais-valia a nível profissional, ainda que possa não vir a ter possibilidade de explorar mais profundamente este tema. Inevitavelmente, estarei mais apto para identificar os meus erros e os dos outros, assim como para avaliar as causas de algumas falhas e determinar a fiabilidade humana relativa a certas acções/tarefas. Serei certamente um profissional mais esclarecido nesta área, o que indiscutivelmente aumentará os meus índices de produtividade, independentemente da função profissional que desempenho e que possa vir a desempenhar futuramente.

1.2. Objectivos

Esta dissertação para a obtenção do grau de Mestre em Engenharia Mecânica pretende definir e identificar os factores que condicionam a fiabilidade humana e o modo como o fazem.

Para tal, serão abordados e explicados conceitos básicos de probabilidade e fiabilidade de equipamentos que, no decorrer da dissertação, irão ser utilizados para melhor enquadrar e explicar a fiabilidade humana e temas adjacentes, como é o caso da interacção homem-máquina. Serão frequentemente estabelecidas analogias entre a fiabilidade de equipamentos e a fiabilidade humana que, desse modo, permitem melhor perceber e identificar as principais fontes de erro humano dos operadores na sua relação com os equipamentos. Quando devidamente estudadas e aplicadas em simultâneo, a fiabilidade de equipamentos e a fiabilidade humana, permitem obter sistemas homem-máquina com menor número de erros e, consequentemente, com maior rendimento.

Será ainda feito um levantamento das principais metodologias, técnicas e ferramentas de avaliação da fiabilidade humana, das quais se irá resumir as mais relevantes, tendo em conta critérios como a sua aplicabilidade e importância no desenvolvimento de novas metodologias. Pretende-se com este passo melhor conhecer as metodologias de HRA, de modo a desenvolver comparações entre os vários métodos.

Posteriormente, será realizado um estudo aprofundado de uma dessas metodologias, cuja escolha terá em consideração a sua aplicabilidade no actual panorama da indústria de produção de energia nuclear a nível mundial e, ainda, as suas características específicas que fazem desta uma das mais abrangentes e conceituadas metodologias de avaliação da fiabilidade humana. Será objecto de estudo a descrição pormenorizada desta metodologia, assim como a comparação com outras metodologias de HRA.

1.3. Estrutura da Dissertação

A dissertação começa com um capítulo introdutório, onde é explicada a motivação do autor para a realização deste trabalho, assim como os objectivos a que se propõe. No mesmo capítulo, nomeadamente neste sub-capítulo, é definida a estrutura da tese, onde são explicados os temas

abordados em cada capítulo e sub-capítulos, culminando com um sub-capítulo em que se explica a metodologia adoptada para a realização do referido trabalho académico.

No segundo capítulo, "Definição dos conceitos básicos", é elaborado o levantamento e explicação dos conceitos considerados fundamentais para os temas que serão desenvolvidos nos capítulos sequentes. Neste capítulo, conceitos como a probabilidade, fiabilidade e falhas, serão abordados no contexto dos equipamentos e não no contexto dos operadores humanos, embora mais à frente sejam realizadas analogias e até utilizados alguns conceitos que são os mesmos, quer para máquinas quer para seres humanos. É ainda abordado o conceito de Ergonomia, que será fundamental na compreensão das interfaces homem-máquina.

O terceiro capítulo é inteiramente dedicado à fiabilidade humana, realizando-se uma breve introdução e evolução histórica para criar um *backgroud* do passado e actual panorama da fiabilidade humana a nível internacional. Realizar-se-á uma revisão da literatura científica, definindo o *state-of-the-art* da fiabilidade humana e metodologias da avaliação desta. Ainda neste capítulo, serão definidos conceitos relativos à fiabilidade humana, traçando-se analogias com a fiabilidade de equipamentos. Será ainda resumido o *modus operandi* do comportamento humano, nomeadamente o processamento da informação através de actividades sensoriais e cognitivas. Por último, é realizado um estudo da relação homem-máquina, onde serão definidos os conceitos mais relevantes, assim como os componentes constituintes e o modo de funcionamento do sistema homem-máquina. De igual modo, serão abordados temas como a fiabilidade e o melhoramento do referido sistema, recorrendo para tal à fiabilidade humana/equipamentos e conceitos de ergonomia, respectivamente.

No capítulo 4 será realizada uma breve introdução com o objectivo de definir e enquadrar na dissertação as metodologias de avaliação da fiabilidade humana e ainda de explicar a escolha das metodologias de HRA que o autor se propõe desenvolver no seu trabalho. Posteriormente, será feito um resumo das metodologias mais relevantes de avaliação da fiabilidade humana (THERP, ASEP, HEART, SPAR-H e CREAM), onde serão descritos alguns procedimentos genéricos, assim como as técnicas para determinação das probabilidades de ocorrência de erros humanos.

O quinto capítulo é inteiramente dedicado à metodologia ATHEANA, no qual se realiza um estudo aprofundado da referida metodologia, abordando tópicos como a constituição de equipas para a aplicação dessa metodologia, assim como técnicas de identificação de cenários e de contextos forçadores de erros, tipos de análises e procedimentos diversos.

Por último, no capítulo 6, procede-se à conclusão deste trabalho académico, onde serão tiradas algumas conclusões do estudo efectuado que permitiu a sua realização, assim como serão tecidos comentários acerca dos temas abordados e dificuldades sentidas.

No final desta dissertação surge um grupo de anexos que estão devidamente identificados ao longo do trabalho e que apenas pretendem contextualizar os seus leitores, assim como fornecer exemplos úteis para a percepção dos temas desenvolvidos.

1.4.Metodologia

A realização deste trabalho académico resultou de uma pesquisa exaustiva de fontes em vários locais e utilizando diferentes métodos: pesquisa geral na *internet*, bibliotecas *online*, bibliotecas físicas, bases de dados *online* de referências bibliográficas, teses científicas, entre outros.

A nível das bases de dados *online* de referências bibliográficas, foram consultadas as seguintes: *Web of Science, Current Contents* e *ISI Proceedings*. Basicamente, estas bases de dados contêm referências de artigos publicados em revistas científicas, assim como *proceedings* de conferências, simpósios, seminários e colóquios de diferentes áreas científicas. A consulta destas bases de dados permitiu não só conhecer o estado da arte dos assuntos abordados neste trabalho, assim como desenvolver uma pesquisa mais detalhada dos temas propostos.

Foram igualmente consultadas três editoras *online*: *Elsevier-Science Direct, Springer/Kluwer* e *Taylor & Francis*. Através das páginas da *internet* da *Springer/Kluwer* e da *Taylor & Francis*, foram consultados vários *ebooks* relativos ao âmbito deste trabalho e que culminaram na elaboração dum *background* da temática central, assim como no desenvolvimento dos vários temas adjacentes.

Da página da *internet* da *Elsevier-Science* (foi escolhida por ser a maior editora de periódicos científicos a nível mundial), foram consultados bastantes artigos científicos que permitiram não só conhecer o estado da arte, assim como aprofundar os temas propostos.

A pesquisa geral efectuada na *internet* foi realizada por intermédio de palavras-chave, maioritariamente em inglês e recorrendo a motores de pesquisa *online,* o que gerou bastantes resultados. Contudo, a selecção dos conteúdos destes foi bastante criteriosa, uma vez que muitos deles são de origem duvidosa, o que não se compadece com a natureza científica deste trabalho.

Outra grande fonte de conteúdos científicos relacionados com a temática tratada, talvez até a maior, foi a página da *internet* da *U.S. Nuclear Regulatory Commission* (http://www.nrc.gov), que permitiu uma extensa consulta da literatura específica de praticamente todos os temas abordados neste trabalho. Destaco particularmente os diversos relatórios elaborados para esta comissão, cujos conteúdos científicos são de extrema importância para todas as áreas relativas à Fiabilidade Humana.

Paralelamente, foram consultadas bibliotecas gerais, de universidades e de entidades estatais, as quais permitiram o acesso a vários e importantes conteúdos relativos aos temas abordados.

Por último e, para a elaboração da redacção, formatação e descrição dos vários temas, fontes e índices, foi consultado um guia (Sousa, 2005), que propõe uma metodologia de elaboração de trabalhos científicos com base em normas portuguesas e internacionais.

2. DEFINIÇÃO DE CONCEITOS BÁSICOS

2.1. Probabilidade

O termo "Probabilidade" expressa a razão entre o número de casos favoráveis a determinado evento e o número total de casos possíveis. O modo tradicional de se expressar essa razão é através da seguinte equação:

$$Probabilidade = \frac{número\ de\ casos\ favoráveis}{número\ total\ de\ casos\ possíveis}$$

Tendo em vista que a quantidade de eventos favoráveis pode variar apenas entre "nenhum evento" e "todos os eventos", a probabilidade de um dado evento é sempre um número entre 0 e 1, ou seja, pode variar somente entre 0 e 100%.

Seguem-se dois exemplos básicos que melhor explicam este conceito:

a) Probabilidade de sair "Cara" no lançamento de uma moeda
   Casos Favoráveis: Cara
   Casos Possíveis: Cara ou Coroa
   Probabilidade: Um caso favorável (Cara) dividido por dois casos possíveis (Cara ou Coroa), ou seja, 1/2, que é 0,50 ou 50%.

b) Probabilidade de sair um "Quatro" no lançamento de um dado
   Casos Favoráveis: Quatro
   Casos Possíveis: Um, Dois, Três, Quatro, Cinco ou Seis.
   Probabilidade: Um caso favorável (Quatro) dividido por seis casos possíveis (Um, Dois, Três, Quatro, Cinco ou Seis), ou seja, 1/6, que é 0,1666... ou 16,666...%.

O conceito de probabilidade está ainda sujeito a algumas propriedades, teoremas e axiomas. Assim, a probabilidade de um evento A, P(A), tem as seguintes propriedades:

$$0 \leq P(A) \leq 1$$
$$P(A) = 1 - P(\overline{A})$$
$$P(\varnothing) = 0$$
$$P(S) = 1$$

Por outras palavras, quando é garantido que um evento vai acontecer, a sua probabilidade é igual a 1 e quando a sua ocorrência é de todo impossível, então a probabilidade será 0 (zero).

A probabilidade da união de dois eventos A e B, é:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Do mesmo modo, a probabilidade de união de três eventos A, B e C, é dada por:

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

Quanto à exclusividade, dois eventos A e B dizem-se mutuamente exclusivos se for impossível a ocorrência simultânea de ambos, ou seja, $A \cap B = \varnothing$. Nestes casos, a expressão de união destes dois eventos, resume-se a:

$$P(A \cup B) = P(A) + P(B)$$

A probabilidade de intersecção dos dois eventos é, logicamente, zero.

A probabilidade condicional de dois eventos, A e B, é definida como a probabilidade de um evento ocorrer, sabendo que o outro evento já ocorreu. A expressão seguinte permite determinar a probabilidade de ocorrência do evento A, sabendo que o evento B já ocorreu:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Nota: ao saber-se que o evento B já ocorreu, reduz-se a amostra.

Se o conhecimento da ocorrência do evento B não gerar informação sobre o evento A, então os eventos dizem-se independentes e a expressão de probabilidade condicional reduz-se a:

$$P(A|B) = P(A)$$

Da definição de probabilidade condicional, pode concluir-se que a primeira equação pode ser escrita da seguinte forma:

$$P(A \cap B) = P(A|B)P(B)$$

Uma vez que os eventos A e B são independentes, a expressão reduz-se a:

$$P(A \cap B) = P(A)P(B)$$

2.2. Fiabilidade

2.2.1. Definição e características

A fiabilidade é a probabilidade de um bem (equipamento, sistema ou componente) cumprir uma determinada função, em condições de utilização e por um período de tempo específicos[1]. Assim, a fiabilidade exprime o grau de confiança que se pode depositar na acção de objectos falíveis, sendo um equipamento fiável e num sentido lato, aquele "em que se pode confiar".

Por exemplo, ao afirmar-se que a probabilidade de um equipamento operar sem falhas é de 75% em 1000 horas, está a prever-se que esse equipamento possa funcionar sem falhas 75 vezes em cada 100 horas (ou durante 750 horas), ou que possa falhar 25 vezes em cada 100 horas (ou durante 250 horas). O mesmo será dizer que durante 1000 horas a fiabilidade (R) é igual a 0.75 (ou 75%), e que a probabilidade de falha (F) é igual a 0.25 (ou 25%).

[1] Definição segundo a AFNOR (Association Française de Normalisation)

Contudo, o conhecimento da fiabilidade não nos garante que um determinado equipamento funcionará sem falhar durante um determinado intervalo de tempo, mas unicamente a probabilidade do equipamento não falhar nesse intervalo de tempo ou até que, em média, um certo número de avarias ocorrerá durante esse intervalo. Por outras palavras, o conhecimento da fiabilidade permite obter o número de avarias que em média ocorrerá durante um intervalo de tempo.

Para determinar a fiabilidade, importa antes conhecer as características das quais resulta:

- características intrínsecas, como é o caso das que advêm da concepção e da qualidade de fabrico do equipamento;
- características extrínsecas, ou seja, das condições de serviço (condições sob as quais o equipamento é previsto funcionar, dividindo-se em condições de carga e condições ambientais) em que decorre a sua operação.

Do mesmo modo e, de acordo com a origem das suas fontes, podem definir-se dois tipos diferentes de fiabilidade:

- Fiabilidade intrínseca (também designada de fiabilidade inerente ou fiabilidade à saída da fábrica). Os fabricantes podem determinar a fiabilidade de um equipamento a partir de ensaios normalizados, sendo o resultado obtido independente da aplicação real. Esta fiabilidade resulta da qualidade intrínseca do projecto (determinante para o nível de desempenho da função objectivada).

- Fiabilidade extrínseca (também designada de fiabilidade demonstrada). Os utilizadores podem determinar a fiabilidade de um equipamento a partir da experiência da sua aplicação (ou fornecer os dados ao fabricante, que os tratará estatisticamente), sendo que o resultado assim obtido depende inteiramente da aplicação real. Esta fiabiliade reveste-se de grande importância prática, uma vez que constitui uma média obtida a partir de grande número de aplicações diferentes e durante um longo período.

A competitividade obriga a que se concebam e produzam equipamentos com *performances* crescentes. Tal facto conduz, frequentemente, à exigência de que os equipamentos que suportem

cargas maiores, forcem os sistemas a funcionar perto dos limites de resistência. Paralelamente, os equipamentos que comportam maior número de funções implicam maior número de componentes (e consequente aumento do nível de complexidade). Qualquer uma destas exigências resulta num maior número provável de avarias, a menos que se possam adoptar medidas de prevenção adequadas.

A melhoria da *performance* e da fiabilidade têm assim de ser conciliadas, tal como a redução de custos, uma vez que quanto maior for a fiabilidade desejada, maiores serão os custos para a obter. A forma de conseguir os compromissos necessários depende da aplicação em causa e dos requisitos da fiabilidade apropriados.

Como exemplos distintos destes compromissos, atente-se num carro de competição, em que os requisitos de fiabilidade são naturalmente secundários face aos requisitos de desempenho, e num avião comercial, em que os requisitos de fiabilidade são naturalmente predominantes sobre quaisquer outros.

Em situações intermédias, os requisitos de fiabilidade colocam-se mais em termos económicos, uma vez que interessa encontrar o melhor compromisso entre o custo de obtenção de uma fiabilidade elevada e o custo resultante das potenciais paragens por avarias.

Se admitirmos o princípio de que qualquer equipamento deve funcionar em condições que proporcionem o maior rendimento, segurança e economia de meios torna-se, então, necessário percorrer três etapas:

- MEDIR – dedução da expressão de fiabilidade adequada a cada tipologia de equipamento e posterior investigação do seu resultado;
- MELHORAR - procurar as formas mais adequadas conducentes à melhoria da fiabilidade global, limitadas por compromissos de custo e de segurança;
- OPTIMIZAR - maximizar a fiabilidade do equipamento, considerando-se como adquiridos determinados factores para verificar que condições melhor optimizam o sistema.

2.2.2. Medição da Fiabilidade

Para deduzir as várias expressões matemáticas relativas à fiabilidade, há que ter em consideração as seguintes variáveis:

N_0 - número de equipamento todos iguais, nas mesmas condições, no momento *t=0*;
N_S - número de equipamentos sobreviventes no momento t;
N_F - número de equipamentos falhados no momento t;
R(t) - probabilidade de sobrevivência;
F(t) – probabilidade de falhar.

Assim, num dado momento *t*, a probabilidade de sobrevivência de um determinado componente é dada por:

$$R(t) = \frac{N_S(t)}{N_0}$$

A probabilidade de falhar será calculada de forma semelhante:

$$F(t) = \frac{N_F(t)}{N_0}$$

Como as situações de sobrevivência e de falha são mutuamente exclusivas, isto é, a intersecção dos elementos de sobrevivência com os elementos de falha formam um conjunto vazio, as duas probabilidades são efectivamente complementares. Deste modo, fica:

$$R(t) + F(t) = 1$$

A função de mortalidade *f(t)* é a função densidade de probabilidade de falha que traduz a percentagem de equipamentos que estão a falhar por unidade de tempo, relativamente à população N_0, no momento *t* (ou no intervalo de tempo *dt*). Deste modo, a função de mortalidade será calculada por:

$$f(t) = \frac{dF(t)}{dt} \qquad f(t) = \frac{1}{N_0} \times \frac{dN_f(f)}{dt}$$

Se se admitir a existência de um único equipamento em funcionamento, a função *f(t)* permite determinar a probabilidade de o equipamento falhar exactamente no momento *t*.

Se a função *f(t)* for integrada entre o momento 0 (zero) em que se inicia o funcionamento dos N_0 equipamentos e o momento genérico *t*, obtem-se a chamada função densidade de probabilidade acumulada de falhas. O seu cálculo é realizado através da seguinte fórmula:

$$F(t) = \int_0^t f(t)dt$$

A função de fiabilidade ou função de sobrevivência *R(t)*, é determinada a partir da probabilidade de um equipamento (ou de um sistema composto por N_0 equipamentos) sobreviver sem falhas durante um período de tempo pré-determinado *t*, sob condições de utilização específicas. Assim, a sua fórmula de cálculo será:

$$R(t) = 1 - \int_0^t f(t)dt$$

Por exemplo, se $R(t_1) = 0,85$, significa que 85 % dos equipamentos são previstos estarem ainda em funcionamento no instante t_1.

A função λ(t) é frequentemente designada de taxa de avarias, sendo calculada através da seguinte expressão:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

A expressão que permite o cálculo da fiabilidade de um dado componente em função da sua equação de taxa de avarias é a descrição matemática mais geral da função de fiabilidade sendo,

portanto, independente de qualquer que seja a distribuição de probabilidade de falha. Assim, a função de fiabilidade geral vem expressa da seguinte forma:

$$R(t) = e^{-\int_0^t \lambda(t).dt}$$

2.3.Curvas de mortalidade

As funções de distribuição de probabilidade de falha, de taxa de avarias e de fiabilidade (ou da sua função complementar, probabilidade de falha), são frequentemente utilizadas para determinar o tempo de vida expectável dos componentes, ou seja, as "leis da vida" dos componentes. Deste modo, surgem as curvas de mortalidade que são representações gráficas, qualitativas, das "leis da vida" de um componente em geral.

A curva correspondente à taxa de avarias, *λ(t)*, assume frequentemente a designação popular de "curva da banheira", dada a sua forma geométrica.

Na Fig. 1 encontram-se representadas as três curvas: fiabilidade *R(t)*, taxa de avarias *λ(t)* e probabilidade de falha *f(t)* para um componente genérico.

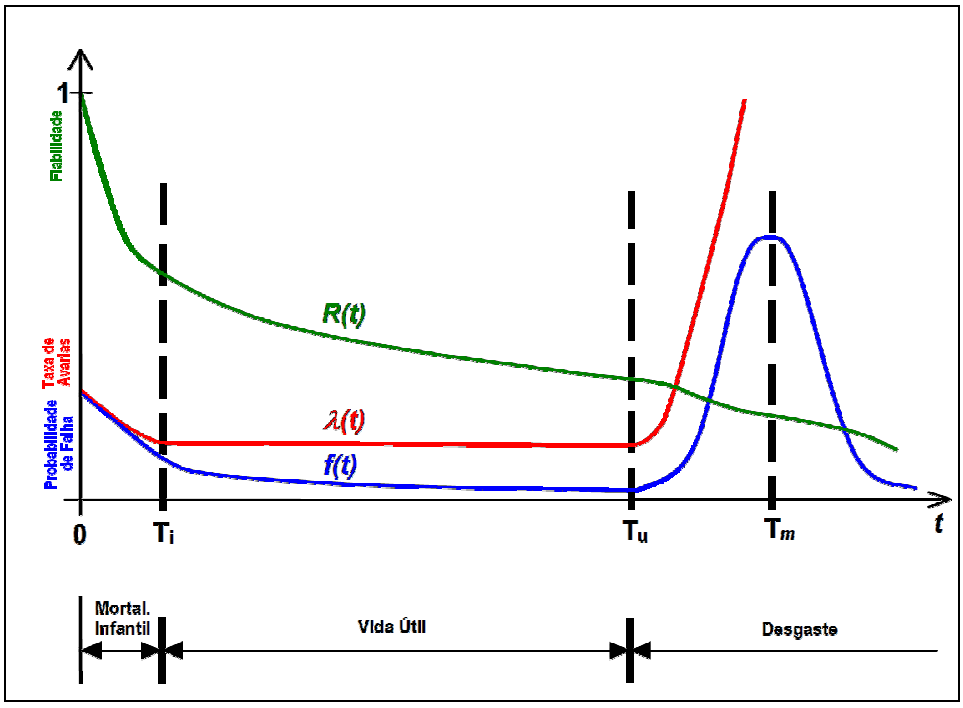

Fig. 1 - Curvas de Mortalidade

Da simples observação da "curva da banheira", resulta a identificação de três períodos característicos do comportamento do componente genérico: mortalidade infantil, vida útil e desgaste.

No primeiro período (mortalidade infantil ou infância), todos os equipamentos de uma amostra são novos e são postos em funcionamento, apresentando assim uma taxa elevada de falhas - $\lambda(t)$ - devido à existência de defeitos (erros de concepção, defeitos de fabrico, controlo de qualidade deficiente, instalação incorrecta ou rodagem deficiente /insuficiente). Esta taxa decresce rapidamente até os equipamentos atingirem a idade T_i, ou seja, o tempo em que todos os equipamentos originalmente deficientes já falharam.

No período de vida útil só funcionam os equipamentos originalmente não deficientes, apresentando uma taxa de avaria constante e que se estende por parte significativa da vida em serviço de um equipamento. Neste período as falhas são frequentemente devidas a solicitações de operação superiores às projectadas ou a avarias acidentais, ocorrendo de forma aleatória, uma vez que não obedecem a qualquer lógica de ocorrência. Esta fase termina em T_u, ou seja, na idade que define a duração ou vida nominal do componente e que se designa frequentemente por período de maturidade ou de vida útil.

Ao ser atingida a idade T_u, entra-se no período de desgaste ou envelhecimento. Nesta fase, a taxa de avarias do componente tenderá a crescer acentuadamente como consequência do aparecimento de modos de falha relevantes, influenciados ou controlados pela relativa longevidade do item em serviço. São exemplos desses modos de falhas a fadiga, a corrosão ou o desgaste propriamente dito.

2.4.Falha

Compreende-se por falha a cessação de funcionamento de um sistema (equipamento, componente e/ou ser humano), causada pelo defeito ou condição anormal de um parâmetro de funcionamento até um nível considerado insatisfatório.

Ao conceito de falha está normalmente associado um problema de classificação, uma vez que esta é muito subjectiva, dependendo de diferentes critérios e autores, considerando que estes têm frequentemente diferentes expectativas relativamente ao desempenho do equipamento. Poderá também haver uma diversidade entre utilizador e fabricante em relação ao que é exactamente um mau desempenho ou falha (Blashe, Shrivastava, 1994).

Embora os termos ”falha” e “avaria” sejam muitas vezes utilizados indistintamente, de acordo com a recente Norma Portuguesa NP-EN 13306:2007, sobre Terminologia em Manutenção, a diferença entre estes dois conceitos define-se referindo que o primeiro diz respeito a um “acontecimento”, enquanto o último caracteriza um “estado”.

Relativamente a um produto final (equipamento, componente ou sistema), defeitos como mudanças da aparência ou uma menor degradação que não afectem a função (desempenho) para o qual foi concebido, não são relevantes para a fiabilidade. Contudo, por vezes a degradação pode ser interpretada como uma indicação de que uma falha poderá vir a ocorrer, sendo tais incidentes classificados como falhas. Os defeitos, a nível da fiabilidade, são considerados como características que não afectam o desempenho, bem ao contrário das falhas que afectam directamente o desempenho.

Assim e, após uma pesquisa abrangente sobre o tema, o critério de classificação de falhas utilizado por Blashe e Shrivastava (1994) é o que reúne maior consenso na literatura científica consultada. A Fig. 2 ilustra bem essa mesma classificação:

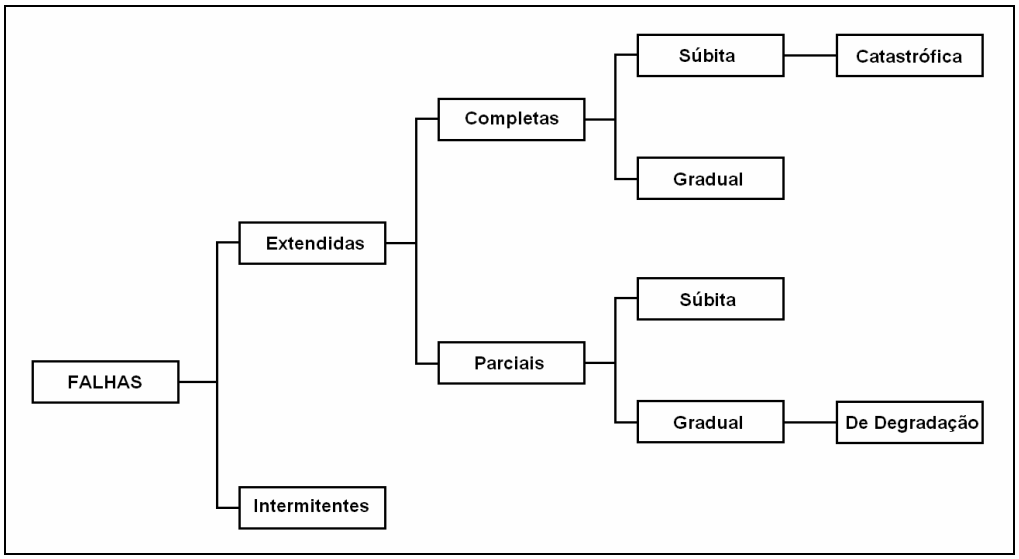

Fig. 2 - Tipos de Falhas

Detalhando, seguem as descrições dos diferentes tipos de falhas, segundo a classificação dos mesmos autores:

- Falhas Intermitentes - resultam na falta de alguma função do produto, apenas por um curto período de tempo. O componente volta completamente ao seu estado funcional imediatamente após a falha;
- Falhas Extendidas - resultam na falta de algumas funções que continuarão em falta até que os componentes em falha sejam substituídos ou reparados, dividindo-se em dois tipos:

  – *Falhas Completas***:** causam faltas completas de funções exigidas;

  – *Falhas Parciais***:** conduzem à falta de algumas funções, embora não como as falhas completas, uma vez que podem utilizar-se redundâncias para contornar o problema até que a falha seja corrigida.

Ambas as falhas, completas e parciais, podem ainda ser classificadas de acordo com a velocidade com que ocorrem podendo, por sua vez, serem divididas em:

- Falhas Súbitas: não poderiam ser prevenidas através de testes e inspecção;
- Falhas Graduais: poderiam ser previstas através de teste e inspecção.

As falhas ainda podem ser combinadas para gerar a seguinte classificação:

- Falhas Catastróficas: são simultaneamente súbitas e completas;
- Falhas de Degradação: são simultaneamente parciais e graduais.

Além do mais e ainda segundo Blashe e Shrivastava (1994), as falhas podem ser classificadas como:

- Falhas de Desgaste: atribuídas ao processo normal de desgaste de um equipamento;
- Falhas de Mau Uso: atribuídas à incorrecta aplicação do produto, contra as funções para as quais foi concebido;
- Falhas Inerentes à Fragilidade: acontecem devido a erros de projecto, produção ou montagem, que faz com que o produto falhe, quando sujeito a aplicações para as quais foi concebido e dentro das capacidades especificadas.

2.5. Ergonomia

Segundo a Associação Portuguesa de Ergonomia (APERGO), a Ergonomia é a disciplina científica relacionada com a compreensão das interacções entre os seres humanos e os outros elementos de um sistema, podendo igualmente definir-se como a profissão que aplica os princípios teóricos, dados e métodos pertinentes para a concepção, com vista a optimizar o bem-estar humano e o desempenho global do sistema.

Para melhor explicar o conceito de Ergonomia, seguem-se algumas definições igualmente válidas e que, quando conjugadas, melhor a definem:

"*A Ergonomia é o estudo científico da relação entre o homem, os seus meios, métodos e espaços de trabalho. O seu objectivo é elaborar, mediante a contribuição de diversas disciplinas científicas que a compõem, um corpo de conhecimentos que, dentro de uma perspectiva de aplicação, deve resultar numa melhor adaptação ao homem dos meios tecnológicos e dos ambientes de trabalho e de vida*". (definição segundo a *International Ergonomics Association*)

"*Ergonomia define-se como a aplicação das ciências biológicas conjuntamente com as ciências da engenharia para conseguir um óptimo ajustamento do ser humano ao seu trabalho e assegurar, simultaneamente, a eficiência e o bem-estar*". (definição segundo a *International Labour Organization*)

Ainda segundo a Associação Portuguesa de Ergonomia, dentro da disciplina, os domínios de especialização representam competências mais profundas em atributos específicos humanos ou características de interacção humana:

- Ergonomia Física diz respeito às características humanas anatómicas, antropométricas, fisiológicas e biomecânicas que se relacionam com a actividade física. Os tópicos relativos incluem posturas de trabalho, manipulação de materiais, movimentos repetitivos, lesões músculo-esqueléticas relacionadas com o trabalho, *layout* do posto de trabalho, segurança e saúde.
- Ergonomia Cognitiva diz respeito aos processos mentais, como a percepção, memória, raciocínio e resposta motora, que afectam as interacções entre humanos e outros elementos de um sistema. Os tópicos relevantes incluem a carga de trabalho mental, tomada de decisão, desempenho especializado, interacção homem-computador, fiabilidade humana, *stress* do trabalho e formação, relacionados com a concepção homem-sistema.
- Ergonomia Organizacional diz respeito à optimização de sistemas socio-técnicos, incluindo as suas estruturas organizacionais, políticas e processos. Os tópicos relevantes incluem comunicação, gestão de recursos de equipas, concepção do trabalho, organização do tempo de trabalho, trabalho em equipa, concepção participativa, "*community ergonomics*", trabalho cooperativo, novos paradigmas do trabalho, cultura organizacional, organizações virtuais, teletrabalho e gestão da qualidade.

A Ergonomia é, assim, uma forma de focar as capacidades e necessidades dos seres humanos no *design* dos sistemas tecnológicos. O objectivo é assegurar que tanto os seres humanos como a tecnologia funcionem em completa harmonia com o equipamento e as tarefas adequadas às características humanas. A Ergonomia pode ser aplicada em várias situações do dia-a-dia para

melhorar significativamente a eficiência, produtividade, segurança e saúde nos postos de trabalho. Seguem-se alguns exemplos onde pode ser aplicada a Ergonomia:

- Na definição de tarefas, de modo a que sejam eficientes e tenham em conta as necessidades humanas tais como pausas para descanso e turnos de trabalho sensíveis ou factores como as recompensas intrínsecas do trabalho em si;
- No desenho de equipamentos e organização do trabalho, de modo a melhorar a postura e aliviar a carga de trabalho no corpo, reduzindo assim as lesões músculo-esqueléticas dos membros superiores e as lesões resultantes de trabalho repetitivo;
- No desenho de equipamentos e sistemas computorizados, de modo a que sejam mais fáceis de utilizar e que haja menor probabilidade de ocorrência de erros durante a sua operação;
- Na criação de acções de formação para que todos os aspectos do trabalho sejam compreendidos pelos trabalhadores;
- Na arquitectura da informação, de modo a que a interpretação e o uso de guias, sinais, e ecrãs seja mais fácil e sem ocorrência de erros;
- No desenho de equipamento militar e espacial, casos extremos de resistência do corpo humano;
- Na concepção de ambientes de trabalho, incluindo a iluminação e a temperatura ambiente, de modo a satisfazer as necessidades dos utilizadores e das tarefas executadas.

Contudo e, em muitos casos, os seres humanos adaptam-se a condições desfavoráveis, levando a que haja frequentemente casos de ineficácia, erros, *stress* e carga física e/ou mental excessiva.

Posto isto e, dada a sua natureza multi-disciplinar, a Ergonomia tem também por objectivo assegurar que o conhecimento das características humanas é utilizado para resolver os problemas práticos das pessoas no trabalho e no lazer.

3. FIABILIDADE HUMANA

3.1.Introdução

O termo "Fiabilidade Humana" é frequentemente descrito como uma disciplina abrangente que procura determinar a probabilidade de ocorrência do erro humano num qualquer ambiente de trabalho, independentemente das ferramentas utilizadas e durante um determinado período de tempo, caso este seja um factor limitativo.

O seu princípio básico, no qual assenta esta disciplina, baseia-se no facto de não existirem pessoas à prova de falhas. Ao contrário dos equipamentos que se degradam ao longo do tempo, a fiabilidade humana é directamente influenciada por determinados factores, tais como a aptidão (inata), o treino (aprendizagem), a experiência, a idoneidade das pessoas e até mesmo as falhas etárias relacionadas com a natural diminuição das capacidades das pessoas.

Seguem-se algumas definições de diversos autores que, de um modo geral, se completam, dando origem à definição da "Fiabilidade Humana" propriamente dita:

"*A Fiabilidade Humana está relacionada com a probabilidade de que um trabalho ou tarefa seja completado com sucesso num tempo determinado"* (Meister, 1993);

"*A Fiabilidade Humana é uma subdisciplina da Ergonomia, baseando-se em conhecimentos da Fiabilidade e da Análise de Risco"* (Kirwan, 1999);

"*A Fiabilidade Humana é a probabilidade de que uma pessoa não falhe no cumprimento de uma tarefa (acção) requerida, quando exigida, num determinado período de tempo, em condições ambientais apropriadas e com recursos disponíveis para executá-la"* (Pallerosi, 2008).

A partir destas e de outras definições, conclui-se que o objectivo desta disciplina é o estudo do "factor" humano existente na realização de uma qualquer tarefa por parte de um operador criando, para tal, técnicas que permitem determinar os erros humanos que, uma vez identificados e corrigidos, irão aumentar a fiabilidade geral de um sistema.

Surge então o conceito de **Análise da Fiabilidade Humana**, frequentemente descrito na literatura científica como *Human Reliability Analysis* (HRA) e que, de forma predictiva se preocupa com a identificação do erro antes de este acontecer.

Em síntese, pode afirmar-se que esta análise se baseia em três funções intrinsecamente ligadas:

- identificar o erro (determinação do que "pode correr mal");
- quantificar a fiabilidade humana (quantificação das probabilidades de erro);
- analisar a redução de erros (redução da possibilidade de erro) (Kirwan, 1999).

3.2. Evolução Histórica

A Segunda Guerra Mundial levou a um incessante e acelerado desenvolvimento técnico do equipamento militar, com vista a ganhar mais valias nos campos de batalha. Este acontecimento teve como uma das muitas consequências o interesse pelo estudo de disciplinas até então inexistentes, como é o caso da Fiabilidade, Manutenção, Ergonomia, Análise de Risco, entre outras, que viriam (e vêm cada vez mais) a assumir um papel preponderante na concepção e prolongamento da vida útil de diversos tipos de equipamentos.

Do mesmo modo, a Fiabilidade Humana surge naturalmente como uma subdisciplina da Ergonomia, baseando-se em conhecimentos da Fiabilidade e da Análise de Risco (Kirwan, 1999). Assim e, resultante do emergente avanço tecnológico ocorrido no pós-guerra e, sobretudo nos EUA[2], surge o primeiro estudo probabilístico sobre a Fiabilidade Humana, nomeadamente em 1952 no Sandia National Laboratories (EUA), para descobrir a exequibilidade de um sistema de armamento defensivo (Swain, 1990). As análises simples do erro humano, cujo objectivo era aumentar a fiabilidade e desempenho humanos, iniciaram-se na década de 60. Estas análises centravam-se principalmente nas tarefas realizadas pelos operadores, apesar de algumas destas metodologias,

[2] Época em que os EUA beneficiaram, acima de tudo, de um vasto leque de recursos naturais e de um incomparável crescimento económico, resultante do aumento da sua produção destinada maioritariamente à Europa em guerra e destruída.

como é o caso das *Task Analysis*, já existirem desde há alguns anos sob a forma de "instruções de operação" (Lees, 2005).

Com a continuidade dos avanços tecnológicos ocorridos desde então, os grandes desenvolvimentos investigados nesta área de estudo têm sido geralmente realizados nos EUA pelas indústrias nuclear e aeroespacial, dados os avultados prejuizos inerentes às falhas e erros que nelas possam ocorrer. Assim, a emergente necessidade da criação de um ou mais métodos de análise e avaliação das falhas humanas, surgiu após o acidente nuclear de *Three Mile Island* (ver Anexo C1), objecto de estudo dos primeiros investigadores na área da Fiabilidade Humana. O marco mais importante deste campo de estudo despontou com o primeiro método de avaliação da Fiabilidade Humana - THERP, *Technique for Human Error Rate Prediction* (ver 4.2) - que começou a ser desenvolvido nos anos 60 por Alan Swain, tendo-se intensificado o seu uso com a publicação, em 1983, do procedimento do método (Swain, Guttmann, 1983).

Desde essa época e tendo muitas vezes como base o método THERP, foram surgindo outros métodos destacando-se, pela sua aplicabilidade, os seguintes: SLIM (*Success Likelihood Index Method*), HEART (*Human Error Assessment and Reduction Technique*), ASEP (*Accident Sequence Evaluation Program*), CREAM (*Cognitive Reliability and Error Analysis Method*), SPAR-H (*Standardized Plant Analysis Risk-Human*), ATHEANA (*A Technique for Human Event Analysis*), entre outros. Os primeiros métodos eram baseados essencialmente em abordagens meramente comportamentais e não cognitivas, considerando-se métodos de "primeira geração". Assim sendo, a visão comportamentalista do homem enquanto "mecanismo" ou componente de uma máquina (abordagem mecanicista) dominou os diversos estudos realizados até então, começando apenas a ser contestada com a publicação e respectiva influência do trabalho de Rasmussen em 1987 (Rasmussen, 1987). Começaram então a ser tomados em consideração factores cognitivos como a perícia, o conhecimento e as regras, permitindo que o seu modelo do "controlo cognitivo" se tornasse o segundo grande marco nesta área de estudo, abrindo o caminho à aclamada "segunda geração" das técnicas de avaliação das falhas humanas.

Paralelamente, os conceitos e avanços desenvolvidos até então foram adaptados a aplicações civis, mais concretamente no design de sistemas homem-máquina. Um exemplo desses avanços é o

estudo *"An Index of Electronic Equipment Operability"* levado a cabo pelo *American Institute for Research*, no qual a *performance* humana foi analisada através da decomposição em pequenas sub-acções e a probabilidade total de falha humana foi obtida pela combinação das várias probabilidades individuais. (Topmiller, Eckel, Kozinsk, 1982). As probabilidades de falha das sub-acções formaram, posteriormente, a denominada *AIR Data Store*, cujo objectivo é utilizar os mais recentes dados da *performance* humana para determinar as probabilidades associadas ao erro humano, tendo como base factores ergonómicos. Outras bases de dados foram então criadas para permitirem estimar a probabilidade de falha humana nas mais variadas aplicações (ver Anexo A), sendo inclusivamente utilizadas, directa ou indirectamente, por alguns dos métodos de avaliação da Fiabilidade Humana.

Actualmente, muito embora as metodologias de "2ª geração" ainda se encontrem em plena utilização e até em desenvolvimento, novos estudos apontam para a criação de ferramentas que tendem a incorporar metodologias de primeira geração, como é o caso da NARA (*Nuclear Action Reliability Assessment*), sendo já frequentemente referidos como métodos de "3ª geração".

3.3. Estado da Arte

O tema "Fiabilidade Humana", conforme exposto em 3.2, começou a ser abordado na década de 60 do século XX, embora só na década de 80 se tenha começado efectivamente a desenvolver metodologias, técnicas e ferramentas de quantificação probabilística da fiabilidade humana.

Surgiu então uma primeira "vaga" de ferramentas designada de "1ª geração", como é o caso de THERP (Swain, Guttmann, 1983), ASEP (Swain, 1987), HEART (Williams, 1986, 1988, 1992), SPAR-H (Gertman et al., 2004), entre outras, que se baseavam essencialmente em abordagens meramente comportamentais e não cognitivas, nas quais o ser humano, enquanto parte integrante do sistema homem-máquina, era visto como um "mecanismo" ou componente de uma máquina. Após o trabalho de Rasmussen em 1987 (Rasmussen, 1987), começaram a ser tidos em consideração factores cognitivos como a perícia, o conhecimento e as regras, abrindo o caminho à segunda "vaga" de ferramentas de avaliação da fiabilidade humana, designada de "2ª geração". Deste grupo destacam-se metodologias como a CREAM (Hollnagel, 1998), que ainda se encontra em desenvolvimento, e a ATHEANA (Cooper et al., 1996; US NRC, 2000).

Desde então têm sido publicados inúmeros artigos científicos e relatórios técnicos que expõem não só os procedimentos como também fornecem tabelas de suporte ao cálculo probabilístico, assim como realizam validações independentes e geram novos pontos de vista dos métodos até então desenvolvidos.

No que respeita a considerações gerais e validações das metodologias expostas, Kirwan, Kennedy, Taylor-Adams e Lambert (1997) realizaram uma validação independente de três metodologias: THERP, HEART e JHEDI (*Justified Human Error Data Information*), tendo concluído que nenhuma delas se distanciava excessivamente das outras em termos de resultados e verificando ainda que qualquer uma das três atingiu níveis razoáveis de precisão.

A metodologia ASEP, por ser uma ferramenta que deriva da THERP, é validada na sua própria literatura de referência (Swain, 1987). Assim, Swain expõe os resultados de pequenos testes e ensaios, destacando-se a concordância que este encontrou entre valores de HEPs determinados usando a metodologia ASEP e utilizando a THERP. É certo que não se pode considerar uma validação independente, uma vez que foi o próprio autor que a realizou, mas também é um facto que não surgiram mais validações, provavelmente por ser uma ferramenta muito específica e desenvolvida para determinados contextos (ver 4.3), e ainda por depender directamente da metodologia THERP. Contudo e, embora não sendo uma validação, ao efectuar uma comparação entre as metodologias THERP e ASEP, Kirwan (1994) descreveu a ASEP como uma metodologia mais rápida de se realizar do que a THERP, podendo inclusivamente ser utilizada com computadores. Verificou ainda que a ASEP é uma excelente ferramenta para identificação de tarefas que requerem análises muito detalhadas e exaustivas através da metodologia THERP, servindo de complemento a esta.

A metodologia HEART foi validada de forma independente por Kirwan (1988), Kirwan et al. (1997) e por Kennedy et al. (2000), tendo-se sempre obtido resultados semelhantes aos da primeira validação (exposta anteriormente – ver validação de THERP).

No que respeita à metodologia SPAR-H, e conforme se verá em 4.5, é das metodologias que mais tem sofrido alterações, de que constituem exemplo as múltiplas validações indirectas levadas a cabo por vários grupos da *U.S. Nuclear Regulatory Commission* ao longo dos anos. Estes *reviewers* têm indicado diferentes áreas de melhoramento e clarificação que vão sendo incorporadas em sucessivas revisões do método, culminando na actual versão do mesmo (Gertman, et al., 2004). É

ainda de salientar o trabalho de Forester, Kolaczkowski, Lois e Kelly (Forester et al., 2006) ao verificarem que os tipos de tarefas e os PSFs foram adaptados de metodologias disponíveis na época em que foram criadas (exemplos: THERP, ASEP, HEART e CREAM), o que dá uma ideia de validação da metodologia. Contudo e, os autores alertam para o facto, nem sempre são claras as formas como os HEPs são escolhidos, efectuando uma espécie de crítica construtiva no sentido de melhorar o método, através da inclusão de informação mais detalhada sobre este assunto, numa futura revisão do mesmo. Mais recentemente, Cĕpin (2008a) publicou um artigo onde efectua a comparação entre os métodos IJS-HRA (*Institute Jožef Stefan Human Reliability Analysis*) e SPAR-H, visando as dependências existentes entre os HFEs. No mesmo ano, O'Hara, Higgins, Brown, Fink, Persensky, Lewis, Kramer e Szabo (O'Hara et al., 2008) elaboram para o *Idaho National Laboratory* – EUA um relatório onde, através da metodologia SPAR-H, pretendem quantificar os erros humanos através de PSFs.

A metodologia CREAM, conforme referido, encontra-se ainda em desenvolvimento havendo, contudo, já alguns trabalhos de validação sobre a mesma. Assim, destaca-se o trabalho de Collier (2003) que encontrou diversos problemas na utilização desta metodologia, particularmente com a aquisição de dados necessários à conclusão das análises. Segundo o mesmo, será necessário mais desenvolvimento antes de considerar este tipo de análises válido e fiável. Anos mais tarde, Marseguerra, Zio e Librizzi (2007), aplicaram a metodologia tradicional CREAM juntamente com a apelidada "Fuzzy CREAM" (metodologia CREAM baseada na lógica *Fuzzy*, ou seja, através de uma forma de Álgebra que emprega uma gama de valores do "verdadeiro" ao "falso", que é utilizada na tomada de decisões com dados pouco precisos) a um cenário de um acidente ferroviário real. Deste modo, encontraram distintas vantagens na aplicação da lógica *Fuzzy* em relação à metodologia CREAM, uma vez que verificaram que assim conseguiam não só uma definição mais sistemática e transparente do modelo, bem como um tratamento mais explícito da ambiguidade envolvida na sua avaliação. Pouco tempo depois, Hollnagel veio confirmar através de um comunicado pessoal na página da *Internet* da *University of Illinois at Urbana-Champaign* (http://www.ews.uiuc.edu) que a sua ferramenta era relativamente limitada em certos aspectos, propondo-se continuar a desenvolvê-la. Paralelamente e, com o apoio do autor, Roger D. Serwy e Esa Rantanen da *University of Illinois at Urbana-Champaign*, têm vindo a desenvolver um *software* que integra a metodologia CREAM numa ferramenta relativamente fácil de utilizar, poupando tempo e realizando análises detalhadas com um menor número de erros. Esta ferramenta continua em desenvolvimento, não havendo

progressos desde Setembro de 2007. Ainda mais recentemente, Everdij e Blom (2008) começaram em 2008 a desenvolver um estudo sobre a validação e fiabilidade da metodologia CREAM.

Relativamente à metodologia ATHEANA, não foi realizada qualquer validação empírica, embora Forester, Kiper e Ramey-Smith (1998), tenham testado a aplicação desta metodologia num reactor de água pressurizado. As conclusões deste ensaio apontam para o sucesso da metodologia em termos dos objectivos propostos, embora tenham também sido identificados vários pontos que careciam de melhoria, quer a nível de ferramentas, quer a nível de processos. No mesmo ano, foi também efectuada uma revisão à documentação por um conjunto de cerca de 20 *reviewers*, dos quais se destacam Hollnagel, Cacciabue, Straeter e Lewis e que culminou na publicação do *Appendix F* da obra de referência NUREG-1624 (US NRC, 2000). Esta revisão resultou numa opinião unânime de que o método representava melhorias e vantagens significativas quando comparado com outras metodologias de HRA, sendo "uma boa alternativa às abordagens de primeira geração". Contudo e, segundo os próprios, "o método não vai longe o suficiente e, como tal, precisa de ser melhorado e expandido".

No que respeita às aplicações das metodologias, têm sido realizados vários trabalhos científicos para algumas indústrias onde a segurança, tal como na nuclear, é igualmente importante, como é o caso da aeronáutica, ferroviária, química, entre outras. Assim, destaca-se o trabalho de Matoba (1999) que explora os métodos de HRA do ponto de vista da indústria naval, investigando as formas de "introduzir os elementos humanos nas análises de fiabilidade das atracagens e colisões".

Também na medicina, por ser um sector onde o erro humano pode implicar graves prejuízos aos pacientes, a fiabilidade humana é frequentemente utilizada, como é o caso do trabalho de Montague, Lee e Hussain (2004). Neste trabalho científico, os autores recorreram a uma metodologia de avaliação da fiabilidade humana (THERP), para analisar uma Miringotomia[3] e a inserção de um tubo de ventilação, obtendo resultados bastante satisfatórios. Concluiram, inclusivamente, que "a identificação de erros humanos é crucial para evitar futuros erros na maioria dos procedimentos otológicos".

No mesmo ano, Shappell e Wiegmann (2004) elaboraram um estudo onde realizaram uma comparação das causas dos erros humanos em acidentes de diferentes tipos de operações na aviação

[3] Miringotomia é um procedimento cirúrgico no qual uma pequena incisão é criada no tímpano, de maneira que haja alívio da pressão causada pelo acumular de fluido ou para drenar pus.

norte-americana (geral, comercial e militar), alertando as autoridades dos EUA para a necessidade de se investir na modificação dos modelos de análise e sistemas de classificação dos factores humanos (HFACS - *Human Factors Analysis and Classification System*).

A nível académico, começam igualmente a surgir trabalhos interessantes na aplicação de ferramentas da fiabilidade humana, como é o caso da monografia de Jorge Luís Benedetti, apresentada na Faculdade de Jaguariúna – Brasil (Benedetti, 2006), onde é realizado um estudo focado na área dos interfaces homem-computador, efectuando-se uma revisão geral da literatura e culminando com o desenvolvimento de ferramentas no cenário de uma indústria específica.

Na indústria nuclear muitos trabalhos têm sido realizados, principalmente no que concerne a considerações sobre alterações que certos autores sugerem realizar nos métodos já conhecidos. No entanto e, por ser de carácter bastante diferente, é de salientar o artigo de Boring para o *Idaho National Laboratory* (Boring, 2006), que estabelece uma ponte entre a ferramenta de HRA SPAR-H e um simulador desenvolvido pela *NASA* que modela o cenário, tendo como objectivo principal a simulação e modelação da contribuição humana no risco que envolve as operações realizadas nas salas de controlo das centrais de produção de energia nuclear.

Em 2007, Dhillon publica uma obra (Dhillon, 2007) onde compila bastante informação relativa à aplicação da fiabilidade humana em indústrias de transporte de passageiros e mercadorias, fornecendo os conceitos básicos necessários e percorrendo sectores como os transportes rodoviários, ferroviários, marítimos e aviação, especificando neste último caso, a manutenção aeronáutica.

Na indústria petrolífera, surge um trabalho bastante interessante de López Droguett, Moura, Jacinto e Silva Jr. (López Droguett et al., 2008), onde as HEPs são estudadas em operações de manutenção, com o propósito de se desenvolver um modelo baseado parcialmente em Cadeias de Markov[4], aplicando-se a inferência Bayesiana[5] para determinar a ligação entre a probabilidade de erro humano e a disponibilidade dos equipamentos de perfuração. O objectivo último deste trabalho será a aplicação do modelo em sistemas de monitorização de plataformas petrolíferas de meia idade, dadas as maiores necessidades de manutenção que estas instalações exigem.

[4] Cadeia de Markov é um caso particular de um processo estocástico com estados discretos (o parâmetro, em geral o tempo, pode ser discreto ou contínuo) e que apresenta a propriedade Markoviana, chamada assim em homenagem ao matemático Andrei Andreyevich Markov. A definição desta propriedade, também chamada de memória markoviana, parte do princípio de que os estados anteriores são irrelevantes para a predicção dos estados seguintes, desde que o estado actual seja conhecido.

[5] A inferência Bayesiana é um tipo de inferência estatística que descreve as incertezas sobre quantidades invisíveis de forma probabilística. Incertezas essas que são modificadas periodicamente após observações de novos dados ou resultados.

Como último exemplo de aplicações da fiabilidade humana surge um trabalho interessante no sector dos transportes ferroviários (Baysari et al., 2009), no sentido em que utiliza duas técnicas de identificação de erros humanos: HFACS (já aqui referida neste sub-capítulo) e a TRACE (*Technique for the Retrospective and predictive Analysis of Cognitive Errors*. Este trabalho procura determinar a consistência das duas ferramentas, concluindo com a recomendação de que as "mesmas devem ser modificadas, ou deverá ser desenvolvida uma nova ferramenta para uma classificação completa e consistente dos erros".

O tema "Fiabilidade Humana" não se esgota nas metodologias para a sua identificação e avaliação. Assim sendo, existe uma série de trabalhos (artigos científicos, relatórios, teses e até monograsfias) que fornecem dados essenciais para o desenvolvimento deste tema e que, de algum modo, servem de suporte às metodologias de avaliação da fiabilidade humana.

Desta forma e, concretamente no que se refere a relatórios técnicos, realça-se o trabalho de pesquisa levado a cabo pela *International Atomic Energy Agency* que culminou num relatório (IAEA, 1998) onde se desenvolve a estrutura de uma base de dados comum para registo dos HFEs que sejam considerados importantes nas análises de risco de diferentes tipos de sistemas de reactores nucleares.

De salientar ainda os trabalhos realizados para a *U.S. Nuclear Regulatory Commission* que, como é sabido, é tida como uma entidade de referência no que respeita à área de estudo da fiabilidade humana. Destaca-se, assim, o relatório elaborado por Higgins e O'Hara (2000) onde é proposta uma revisão de alterações nas acções humanas consideradas importantes para o risco das operações realizadas na indústria de produção de energia nuclear. Também os trabalhos de O'Hara, Higgins, Persensky, Lewis e Bongarra (2002b) e de O'Hara, Brown, Lewis e Persensky (2002a) merecem destaque por investigarem e definirem as *guidelines* que garantem *interfaces* homem-máquina que proporcionam menores probabilidades de erro humano. Kolaczkowski, Forester, Lois e Cooper (2005) apresentam um relatório onde definem as boas práticas para a implementação de metodologias de HRA. Em 2007, Hallbert e Kolaczkowski (2007) elaboraram um estudo sobre a aplicação de dados empíricos e métodos de inferência Bayesiana em ferramentas de HRA. Já no ano de 2008, surge um trabalho bastante importante por O'Hara, Higgins, Brown, Fink, Persensky, Lewis, Kramer e Szabo (2008) que revê e estabelece novas considerações sobre os factores humanos no que respeita às novas e emergentes tecnologias utilizadas nas centrais de produção de energia

nuclear. É ainda importante destacar o relatório realizado por Drouin, Parry, Lehner, Martinez-Guridi, LaChance e Wheeler (2009) que fornece os procedimentos necessários ao tratamento das incertezas associadas às PRAs nas tomadas de decisão que envolvem risco.

No respeitante a artigos científicos, realçam-se os diversos trabalhos de Embrey, nomeadamente *Preventing Human Error: Developing a Consensus Led Safety Culture based on Best Practice* (2000c), *Performance Influencing Factors (PIFs)* (2000b), *Task Analysis Techniques* (2000d), *Understanding Human Behaviour and Error* (2000e), *Data Collection Systems* (2000a), entre outros, onde são abordados tecnicamente vários aspectos adjacentes ao tema "Fiablidade Humana", conseguindo atingir um nível de pormenor bastante elevado, especialmente no que toca a procedimentos e técnicas utilizados em metodologias de avaliação da fiabilidade humana (exemplos: *Task Analysis*, PIFs e *Data Collection Systems*).

Também os trabalhos de Erik Hollnagel (autor da metodologia CREAM) merecem destaque, particularmente o estudo *Human reliability assessment in context* (Hollnagel, 2005) que conclui que as metodologias HRA, por si só, não são suficientes para gerarem todos os dados necessários às PSAs, havendo "caminhos melhores e mais realistas para analisar os riscos, quer qualitativamente, quer quantitativamente".

No ano de 2004 surge um artigo extremamente interessante por Hallbert, Gertman, Marble, Lois e Siu (2004) que sugere a utilização frequente de informação proveniente do campo operacional e da experiência dos operadores nas metodologias de HRA.

Também bastante interessante é a comparação entre as abordagens atomistas e holísticas aos métodos de HRA, realizada por Boring, Gertman, Joe e Marble (2005), a qual, segundo os autores, é "importante para perceber a natureza da quantificação das HRAs e a utilidade dos atalhos associados a cada abordagem".

Os trabalhos de Cĕpin (2008a, 2008b, 2008c) também merecem particular destaque, nomeadamente no que diz respeito ao desenvolvimento de uma nova metodologia de HRA (a também já referida IJS-HRA) e ainda no que concerne ao estudo das dependências entre HFEs.

Mais recentemente, destaca-se o trabalho de Pallerosi (2008), onde é abordada uma nova metodologia de análise qualitativa e quantitativa da fiabilidade humana.

Também os trabalhos de Reer (2008a, 2008b) e de Zio (2009) são importantes na medida em que realizam uma revisão e levantamento dos principais avanços da fiabilidade humana, assim como vaticinam os novos desafios nesta área de estudo.

Em termos de artigos científicos realça-se ainda o trabalho de H. Liu, Hwang e T. H. Liu (2009), onde é realizada uma abordagem económica do impacto dos erros humanos nos sistemas de produção.

A nível académico começam igualmente a surgir trabalhos muito interessantes, destacando-se a tese de doutoramento de Pekka Pyy da *Lappeenranta University of Technology* – Finlândia (Pyy, 2000), onde o autor desenvolve algumas considerações sobre as metodologias HRA para, através da extensão das suas aplicabilidades, criar bases sólidas de suporte às PSAs. Destaca-se também a tese de doutoramento de Robert Fields da *University of York* - Reino Unido (Fields, 2001) que investiga técnicas através das quais engenheiros e *designers* de sistemas computacionais interactivos consigam antecipar problemas relacionados com falhas humanas. Realça-se ainda a tese de mestrado de Katherine Kohlhepp da *Texas A&M University* – EUA (Kohlhepp, 2005), onde são avaliados os julgamentos da engenharia quando aplicados à quantificação de eventos pós-iniciadores utilizados pelas metodologias de HRA.

Quanto a monografias, destaca-se a obra de Waldemar Karwowski: *International Encyclopedia of Ergonomics and Human Factors* (Karwowski, 2001) que aborda, de um modo geral, todos os assuntos relacionados com Ergonomia e Factores Humanos a ela adjacentes. Embora não entre em excessivos pormenores, constitui uma referência na literatura científica destas áreas de estudo.

Destaca-se ainda o livro de Hollnagel e Woods (2005), que explora as origens dos sistemas cognitivos aplicados à engenharia.

No panorama nacional pouco se tem desenvolvido no campo da fiabilidade humana, embora haja dois trabalhos que mereçam particular destaque. Assim, José Sampaio (Sampaio, 2002) realizou um ensaio sobre o processo de tomada de decisão em ambientes operacionais, abordando temas como a automatização cognitiva e o erro humano. Em 2003, Isabel Nunes e Celeste Jacinto (Nunes, Jacinto, 2003) efectuaram uma revisão do estado da arte da fiabilidade humana. É certo que não é

um documento actual, remetendo para o estado da arte do ano em que foi feito, mas é sem dúvida uma boa base de trabalho para futuros estudos, como é o caso desta dissertação.

3.4.Falhas Humanas

3.4.1. Classificação das Falhas Humanas

Todo e qualquer componente pode estar sujeito a vários tipos de falhas, derivadas na maioria das vezes de problemas mecânicos, eléctricos ou simplesmente de falhas humanas.

Deste modo e, tal como se pode observar na Fig. 3, as falhas humanas podem ser classificadas em Erros e Transgressões, sendo os Erros classificados, por sua vez, em Deslizes e Enganos e as Transgressões em Intencionais ou Não Intencionais (Pallerosi, 2008).

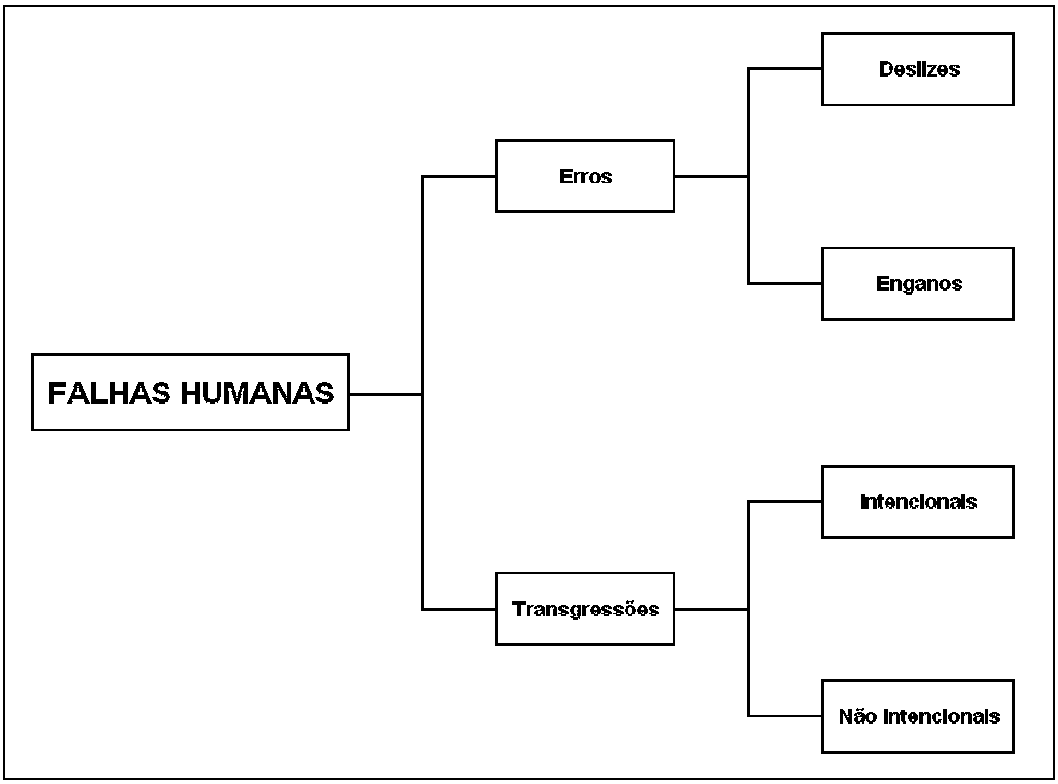

Fig. 3 - Classificação das falhas humanas

Os erros, por dependerem essencialmente da capacidade por parte do operador para executar uma determinada tarefa, do *stress* a que este está sujeito, da motivação, das condições ambientais do

local, entre outros, constituem a principal causa das falhas humanas. Por estes e outros motivos, estas falhas são muitas vezes associadas à falta de conhecimento e de lógica do operador.

Partindo do pressuposto de que o ser humano nunca consegue atingir a sua própria capacidade total para desempenhar determinadas e complexas funções, é fácil explicar a ocorrência de deslizes. Estes podem acontecer mesmo quando o executante tem bastante prática e uma correcta aprendizagem, uma vez que pode ser influenciado por certos factores que determinam a sua prestação. O cansaço surge como um factor natural quando o operador está sujeito a sessões laborais prolongadas, funções específicas contínuas e ininterruptas por tempo excessivo ou em condições ambientais inadequadas. O *stress* é outra das grandes causas dos deslizes e que muitas vezes se confunde com o cansaço. Contudo e, apesar de resultar quase sempre em cansaço, o mesmo pode não depender exclusivamente de acções prolongadas, mas também de toda a envolvência a que o operador está sujeito (situação no emprego, situação familiar, rotinas, etc). O executante pode até ter descansado, repousado fisicamente, mas se se encontrar numa situação de *stress*, inevitavelmente terá cansaço mental, o que muitas vezes se traduz também em cansaço físico. Outra causa dos deslizes é a senilidade mental dos operadores, ou seja, é a natural e contínua redução da capacidade neuronal que ocorre pelo envelhecimento da pessoa ou pela existência de determinada patologia.

Paralelamente aos factores já expostos surge a inaptidão física ou mental para realizar uma tarefa, ou seja, a incapacidade, por parte do operador de realizar determinadas operações. Por exemplo, se a tarefa de um operador é colocar caixas numa prateleira a 2 m de altura, um operador baixo (1,5 m, por exemplo) muito dificilmente realizará com sucesso a mesma função que um operador de 1,90 m - este é um exemplo de incapacidade física. Quanto à incapacidade mental temos, por exemplo, um operador de caixa de uma loja, com pouca agilidade e cálculo mental. Pode até ter tido formação e aprendizagem para a função em causa, mas a falta de agilidade mental para realizar rapidamente operações matemáticas sem recurso a calculadora e/ou papel, confere-lhe inaptidão mental para desempenhar a referida função.

Os enganos ocorrem quando uma função não é desempenhada segundo determinadas normas ou padrões previamente estabelecidos. Estes têm como principais causas factores como as falhas na aprendizagem/treino (que permitem enganos nas decisões a tomar), falhas de julgamento na tomada de decisões (são as chamadas falhas de diagnóstico que derivam de aspectos cognitivos) e,

paralelamente, a falta de aptidão dos operadores (característica inata à pessoa que conduz a erros frequentes de procedimento nas funções a desempenhar).

As transgressões, subdivididas em intencionais e não-intencionais, têm a sua origem em falhas (premeditadas ou não) de cariz comportamental. Estas devem separar-se dos erros aquando da realização de análises quantitativas, uma vez que dependem de factores particularmente difíceis de ser identificados, não tendo qualquer relação com as capacidades físicas e mentais do operador para a execução da função.

Relativamente às transgressões intencionais, estas ocorrem por haver certeza da impunidade do acto praticado, ou até mesmo uma sanção ligeira da acção indevidamente praticada por parte do executante da função. Este tem plena consciência do seu acto e tal pode ser explicado pela sua sagacidade ou mesmo esperteza, uma vez que toma como garantido, ou quase, que a acção indevidamente realizada irá passar despercebida. Outra explicação será, por exemplo, a ausência de responsabilidade, uma vez que acredita que a consequência do acto erradamente realizado poderá ser imputado a outra pessoa ou conjunto de pessoas. Paralelamente, outra das principais causas das transgressões intencionais é a ambição do operador, uma vez que o mesmo tenciona lucrar de algum modo (na maioria dos casos financeiramente) com a transgressão.

Por último e, sendo uma transgressão completamente intencional, surge a sabotagem. Este tipo de transgressão tem como único propósito impedir o normal funcionamento de um ou vários mecanismos/processos, com os mais variados tipos de intuito (normalmente advém da vontade de desacreditar a marca no mercado e consequente ganho de vantagem competitiva de outra empresa). Assim, dado o carácter comportamental e a diferença substancial das causas expostas, percebe-se o quão difícil se torna, por vezes, a tarefa de determinar que factores poderão estar na origem de uma transgressão intencional.

Já as transgressões não intencionais ocorrem por falta de conhecimento e das regras/normas pré-estabelecidas e inerentes à função ou ao comportamento esperado no decorrer da mesma. Estas têm normalmente por base motivos sociais ou até culturais, em que o operador sai de um ambiente em que está acostumado a uma determinada maneira de estar no trabalho e passa a enfrentar um

novo ambiente, com novas regras, outras culturas, etc. Assim, será fácil entender que para o operador uma determinada postura no emprego está certa porque numa vivência anterior assim o era, mas no panorama actual do seu emprego, essa mesma postura poderá ser perfeitamente errada, resultando numa transgressão não intencional e que certamente, de algum modo, trará prejuízo para a sua organização.

3.4.2. Analogia com a "Curva da Banheira"

Tal como acontece com os componentes de um determinado sistema, o comportamento genérico da vida laboral de um operador também pode ser representado graficamente por uma curva semelhante à "curva da banheira", representada na Fig. 1. Deste modo e após a obervação da Fig. 4, consegue definir-se igualmente três períodos durante a realização de determinada tarefa ou conjunto de várias acções.

Assim e, no período inicial, o operador encontra-se ainda numa fase de aprendizagem, onde surgem com facilidade falhas humanas, uma vez que ainda não consolidou os ensinamentos adquiridos e/ou não adquiriu experiência necessária para laborar com o mínimo de falhas.

No segundo período, o funcionamento do operador pode considerar-se normal, uma vez que detem a formação e experiência necessárias para realizar as acções requeridas, correndo um menor número de riscos. Neste período, as falhas que podem surgir são normalmente de carácter aleatório, uma vez que dependem essencialmente de factores que não são inerentes ao operador.

No último período e por estar sujeito a um *stress* prolongado e/ou por adquirir uma incapacidade progressiva (exemplo: senilidade) o operador, mesmo devidamente formado e experienciado, tende a cometer falhas, o que se traduz num aumento gradual da curva, intensificando-se a partir de certa idade/estado de *stress*.

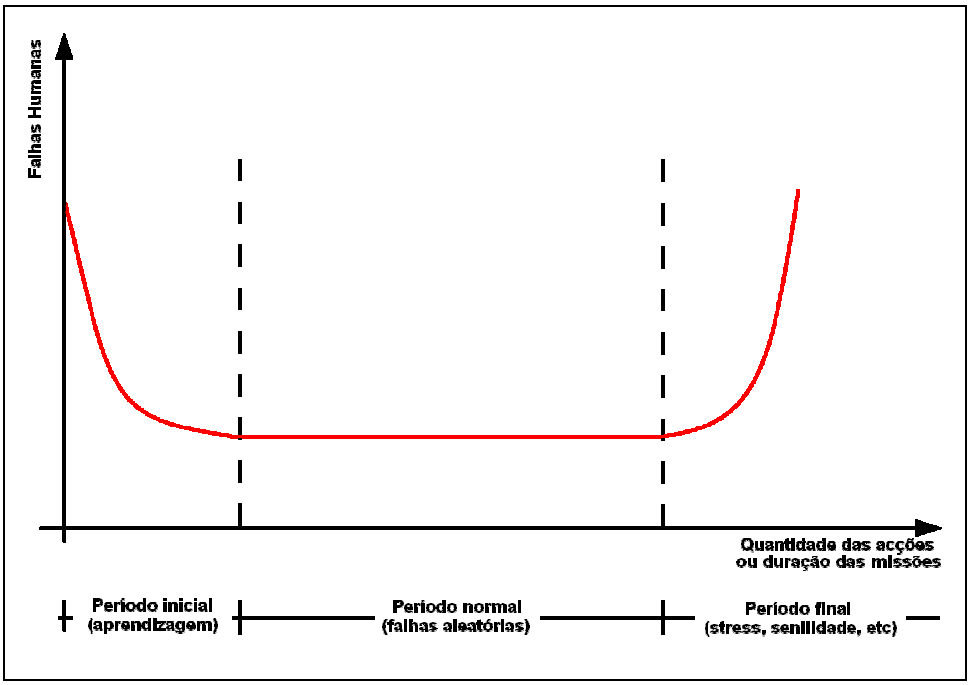

Fig. 4 - Analogia com a "curva da banheira"

Conforme se verificou, a actividade laboral dos operadores pode ser comparada à vida de um componente e/ou sistema, embora com as devidas diferenças ao nível das causas das falhas.

Enquanto o componente no primeiro período falha devido a defeitos que podem advir de erros de concepção, defeitos de fabrico, etc., o ser humano falha por falta de experiência e/ou de formação completa.

No segundo período, tanto o componente como o ser humano apresentam o menor número de falhas, sendo as suas causas, para ambos os casos, devidas a erros aleatórios.

No terceiro período, o componente começa a estar sujeito a fenómenos de fadiga, corrosão ou desgaste, enquanto que o operador falha igualmente devido a outros fenómenos como o *stress*, a senilidade, etc.

3.5.Actividades Sensoriais e Actividades Cognitivas

Tal como qualquer outro ser vivo, o ser humano também dispõe de estímulos sensoriais que lhe permitiram não só sobreviver como também obter um desenvolvimento relativamente rápido na história recente do nosso planeta. Durante o processo de desenvolvimento da espécie, este definiu um encadeamento lógico de acções que, sem ter conhecimento imediato, passou a marcar toda a sua

história, assim como toda a sua vivência (só há relativamente poucos séculos é que se começaram a estudar os comportamentos humanos). Deste modo e, recorrendo ao encadeamento lógico anteriormente referido, as actividades humanas, das quais dependem as falhas humanas, baseiam-se em estímulos sensoriais e recursos cerebrais.

Relativamente aos estímulos sensoriais e, tal como é sabido e universalmente aceite, o ser humano dispõe de cinco "sentidos":

- Visão – cores, formas, brilhos, tamanhos, espectros, etc.;
- Audição – todas as gamas de frequência que vão de 20 a 20000 Hz;
- Tacto – formas, vibrações, choques, temperaturas, etc.;
- Olfacto – odores;
- Paladar – sabores.

Estes estímulos sensoriais são também eles utilizados por outras espécies tanto a nível evolutivo como, simplesmente, a nível de sobrevivência, chegando inclusivamente a ser bastante mais apurados (exemplo: os cães normalmente têm um olfacto muito apurado).

Contudo e, pese embora o facto dos estímulos sensoriais do ser humano serem muitas vezes inferiores aos de outros animais, as suas actividades são compensadas pela inteligência que lhe é inerente, permitindo-lhe criar dispositivos que as complementem (exemplo: sensores).

Quanto aos recursos cerebrais, destaca-se a capacidade de memória que pode ser dividida em duas características principais:

- Lógica – capacidade de armazenar e processar encadeadamente um vasto número de informações, assim como emitir julgamentos;
- Percepção – capacidade de coordenar movimentos, realizar sequências, considerar posições, etc.

A memória pode assim armazenar e reactivar uma enorme quantidade de informações e até sensações, por intermédio de três sub-sistemas básicos:

- Memória Sensorial – resulta dos estímulos sensoriais obtidos e tem normalmente uma duração bastante reduzida (intervalos de tempo inferiores a 1 segundo), podendo em situações de perigo iminente tornarem-se praticamente imediatos;
- Memória Transitória – retem as informações por um determinado período de tempo bastante variável e dependente da sua importância e capaciade neural do sujeito, sendo apenas eliminadas quando as mesmas se tornam irrelevantes ou quando é atingido o limite da capacidade neural do mesmo;
- Memória Permanente – retem informações importantes e/ou marcantes por longos períodos de tempo, podendo estas inclusivamente acompanhar a pessoa durante todo o seu período de vida.

Contudo e, proporcionalmente ao avanço da idade (depende, como é óbvio, de pessoa para pessoa), o ser humano começa a ter dificuldade na retenção de novas informações, nomeadamente na já referida Memória Transitória. Por outro lado, factos muito distantes e até detalhados já "enraizados" na sua memória, como seja o caso de algumas recordações de infância, são facilmente relembrados.

A eliminação de informações ou falta de retenção das mesmas é, por si só, um factor gerador de falhas humanas. Este pode estar presente em alguns dos já referidos tipos de falhas, como é o caso dos erros por deslizes e/ou enganos e das transgressões não intencionais.

A nível cognitivo a resposta aos estímulos sensoriais é realizada tal como se apresenta na Fig. 5:

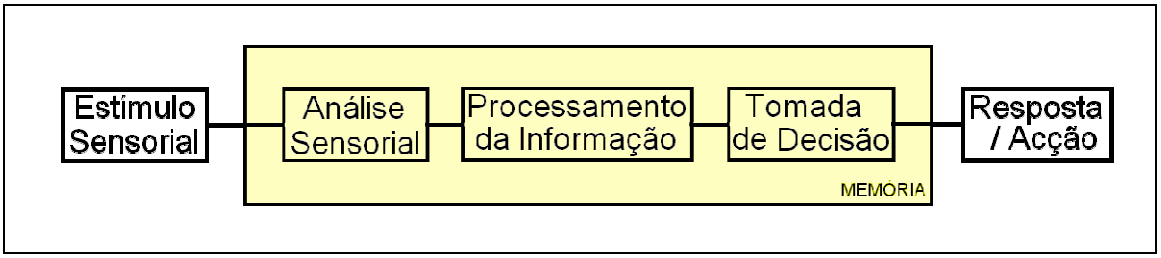

Fig. 5 - Resposta a estímulos do ponto de vista cognitivo

Deste modo, uma falha humana pode ocorrer por uma ou mais das seguintes razões:

- Desconhecimento da resposta ao estímulo;
- Interpretação errada do estímulo;

- Incapacidade para uma correcta discriminação do estímulo;
- Inaptidão para decidir a melhor resposta/acção;
- Realização da acção fora da sequência lógica.

3.6.Relação Homem-Máquina

3.6.1.Conceito, Constituição e Funcionamento do Sistema Homem-Máquina

As máquinas são frequentemente definidas como instrumentos de trabalho projectados e construídos pelo homem, visando ajudá-lo na execução de determinados trabalhos. Estas podem ser entendidas como prolongamentos do organismo humano, proporcionando ao homem melhores condições na execução de certas tarefas.

Um sistema Homem-Máquina é uma combinação operativa entre o homem e a máquina que se complementam para executar uma determinada função, partindo de estímulos de entrada sujeitos às condições de um dado ambiente. Assim, na operação de uma máquina, o homem recebe informações desta (estímulos de entrada), processa-as e transforma-as em acções de comando.

Deste modo, pode definir-se que o sistema Homem-Máquina é constituído pelos seguintes componentes básicos:

- Máquina – componente operador (executor) das acções;
- Homem – criador e supervisor dos sistemas;
- Visualizadores – fazem a "ponte" entre os sinais da máquina e o homem;
- Controlos – fazem a "ponte" entre os sinais do homem e a máquina.

Estes componentes são, por sua vez, afectados por factores ambientais tais como a humidade, temperatura, ruídos, iluminação, radiações, entre outros, satisfazendo os seguintes princípios-base:

- As máquinas devem ser adaptadas ao homem e não o contrário;
- O homem, ao contrário das máquinas que podem realizar milhões de operações sem erros e ainda serem adaptadas a factores ambientais adversos ao ser humano, falha pelos mais diversos motivos (ver 3.4);

- Os controlos devem ser adaptados ao homem, dentro das suas capacidaddes físicas, mentais e sensoriais;
- Os visualizadores devem permitir ao homem uma fácil e rápida leitura dos sinais da máquina;
- Não existe um sistema sem falhas dado que, em última instância, estas serão originadas pela degradação ao longo do tempo de todos os componentes do sistema;
- Os factores ambientais anteriormente referidos afectam significativamente a fiabilidade do sistema homem-máquina.

A Fig. 6 ilustra a sequência das acções que ocorrem num sistema homem-máquina. Vejamos: o homem através de estímulos cerebrais actua nos controlos que, por sua vez, irão actuar na máquina de modo a que esta realize as tarefas desejadas. Desta saem sinais para os visualizadores que, por outro lado e através dos estímulos cerebrais do homem, são captados por este, permitindo o processamento da informação e o início de um novo ciclo.

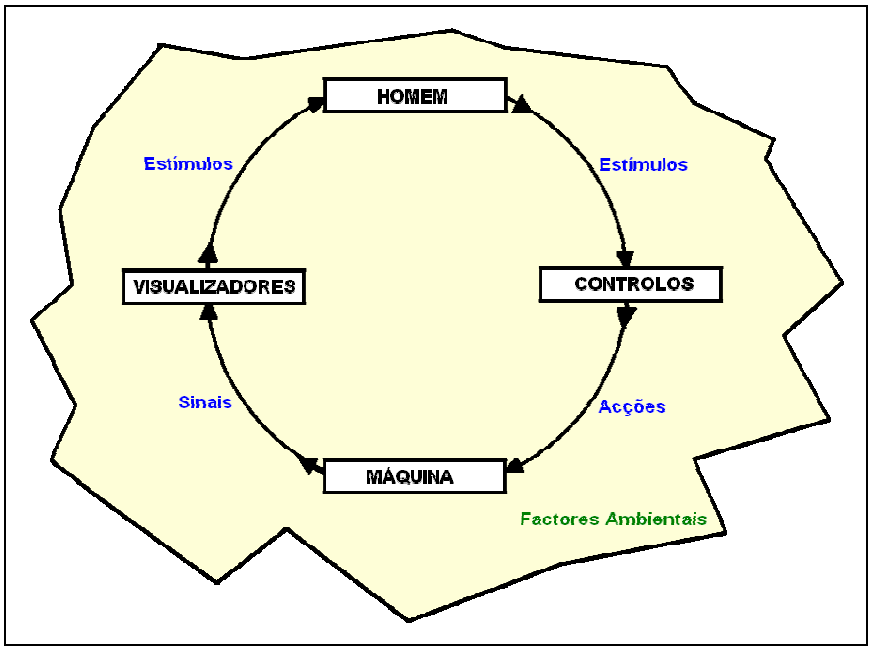

Fig. 6 - Sistema Homem-Máquina

Para o devido cumprimento dos referidos princípios-base deverão ser tidas em consideração algumas características básicas aquando da fase de concepção (projecto) e utilização do sistema Homem-Máquina, tais como:

- O operador do sistema deverá ter a aptidão (vocação) para a tarefa, experiência anterior, formação adequada, personalidade, interesse e características físicas adequadas, assim como bons níveis de resistência ao stress, entre outros;
- A nível da máquina, deverá haver um projecto adequado dos controlos, painéis, ferramentas de apoio, *layout* da máquina e do local de trabalho, capacidade produtiva, manutenção do sistema, canais de acesso às informações/comunicações, supervisão, planeamento da produção/manutenção, entre outros;
- Quanto às condições ambientais, as mesmas deverão ser supervisionadas frequentemente, assim como deverão ser realizados procedimentos administrativos que definam as cargas de trabalho, rotatividade nas missões e modificação de parâmetros alteráveis (exemplo: temperatura na oficina, através do comando do ar condicionado) de modo a proporcionar as melhores condições de trabalho.

3.6.2.Fiabilidade Humana no Sistema Homem-Máquina

O conceito, técnicas e estudos relativos ao tema fiabilidade humana, conforme já descrito em 3.2, só se desenvolveram para melhorar dois aspectos fundamentais em qualquer indústria/serviço que utilize sistemas homem-máquina:

- Segurança
- Produção

A nível da segurança, os desenvolvimentos realizados foram feitos no âmbito das operações em centrais nucleares, onde um simples erro humano pode gerar uma cadeia de acontecimentos que poderá resultar na morte/invalidez de milhares de pessoas. Outra grande indústria onde também foram desenvolvidos estudos e técnicas na área da fiabilidade humana e em que as falhas humanas podem, uma vez mais, gerar fatalidades na relação homem-máquina, é a indústria aeronáutica. Contudo, o perigo de ocorrência de erros humanos que possam gerar falhas graves de segurança, encontra-se em todo o tipo de indústrias, principalmente quando se dá a referida interacção homem-máquina.

Quanto à produção, a fiabilidade humana também é estudada para garantir melhorias na segurança dos trabalhadores, embora o seu objectivo essencial seja melhorar os processos de modo a rentabilizar os esforços dos operadores e, consequentemente, aumentar a produtividade/qualidade dos seus produtos.

Mesmo sendo a segurança um aspecto adjacente a qualquer sistema homem-máquina e que "caminha" com este onde quer que seja aplicado, o facto é que a produção é uma função directa do referido sistema. Assim, podem definir-se os dois tipos de erros que mais afectam a produção:

- Erros de execução – podem ser cometidos por qualquer indivíduo que se encontre no percurso produtivo (fabrico e montagem) e pós-produtivo (testes, transporte e armazenamento) de cuja acção errónea resulte, directa ou indirectamente, numa ou mais falhas no produto final. Exemplos: utilização de ferramentas inadequadas, ligação incorrecta de circuitos, queda de componentes, falhas de inspecção, entre outros.

- Erros de processo – são erros inerentes às máquinas e que não dependem directamente dos operadores, resultando de deficiências no projecto inicial ou na manutenção. Exemplos: transporte e/ou armazenamento incorrectos, condições ambientais inadequadas (temperatura, pressão, etc.), *layout* da oficina inadequado, ausência de instruções de montagem, entre outros.

3.6.3.Melhoria do Sistema Homem-Máquina

Com vista a minimizar as falhas e, consequentemente, aumentar a produtividade, o sistema Homem-Máquina pode ser significativamente melhorado por acções e procedimentos. Deste modo, referem-se de seguida as principais condições que possiblitam uma melhor eficiência do processo produtivo do sistema Homem-Máquina.

Relativamente às condições ambientais, estas deverão aproximar-se das ideais, tanto para o homem como para a máquina. Neste aspecto, ambos apresentam um rol de factores que afectam directamente a sua capacidade de produção. Para o homem, factores como a temperatura, humidade do ar (ver Fig. 7), iluminação, entre outros, são os que mais directamente influenciam a sua

produtividade, pelo que deverão ser tidos em consideração quando são definidas as condições de trabalho dos operadores.

Quanto à máquina e, dependendo do destino para o qual foi concebida (aqui pode haver bastantes alterações na fase de projecto que, como se verá adiante, poderão proporcionar condições que permitam a máquina funcionar em ambientes adversos), deverão ser respeitados os limites de funcionamento da mesma (definidos na fase de concepção) para temperaturas, humidades, vibrações, entre outras condições.

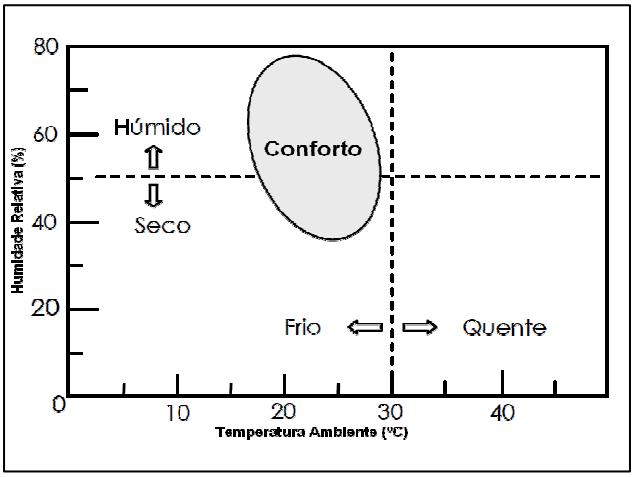

Fig. 7 - Condições ambientais para conforto humano

Fig. 8 - Condições sonoras para conforto humano

Ainda relativamente à concepção da máquina deverão ser evitadas as repetições de posições, formas e cores dos comandos que, de algum modo, possam confundir o operador nas suas acções. A forma considerada mais correcta de conseguir estes objectivos é através de normas e padrões aplicáveis na fase de projecto.

Por exemplo, na Fig. 9 apresenta-se um interruptor simples que foi concebido para funcionar de uma forma que é universalmente aceite, ou seja, a função "ligar" deve ficar sempre na parte superior quando montado na vertical e no lado direito quando montado na horizontal.

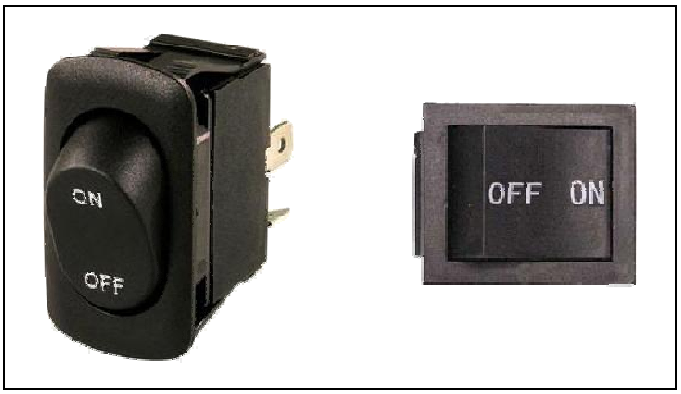

Fig. 9 - Disposição-padrão para montagem de interruptores

A adopção e utilização de normas e padrões por parte das entidades responsáveis pelos operadores, suas acções e equipamentos evitam assim e, de um modo geral, muitos dos erros humanos que normalmente ocorrem. Esta situação deve-se ao facto de se gerar uma "inércia" mental nos operadores associada a comandos e acções que tornam extremamente improvável a ocorrência dos referidos erros. Exemplificando, sempre que o operador está perante um botão vermelho, identifica o mesmo como sinal de parado, enquanto que o sinal verde será identificado como sinal de "OK" ou de avanço. O mesmo se passa com comandos associados a movimentos. Noutra situação, como no movimento de um elevador, o sinal que desencadeará o movimento de subida será facilmente identificado pelo operador como o botão que está por cima do de descida.

Um factor importante no processo produtivo é a monitorização do mesmo. Desta forma, o homem não deverá ser utilizado sistematicamente como monitor do sistema, mas sim de forma bastante moderada e activa, evitando sempre rotinas excessivas, monótonas e passivas. A monotonia e a passividade das acções induzem normalmente à ocorrência de falhas por omissão, enquanto que a continuidade e excesso das mesmas gera frequentemente falhas por fadiga.

Para reduzir este tipo de falhas deverão ser utilizados sensores que substituam as acções humanas, sempre que tal seja possível. Ao contrário do homem, o sensor não falha por realizar tarefas monótonas ou passivas, actuando sempre com maior fiabilidade, inclusivamente em ambientes desfavoráveis. Um exemplo prático desta situação é o caso de uma fábrica onde é necessário contar o número de unidades que passa num determinado tapete rolante. Como é de fácil percepção, um ser humano muito provavelmente irá enganar-se na contagem, principalmente se se tratarem de muitas unidades. Por esse motivo, são frequentemente utilizados sensores ligados a

autómatos ou outros controladores lógicos que recebam os sinais destes e façam o seu processamento (neste caso, a contagem).

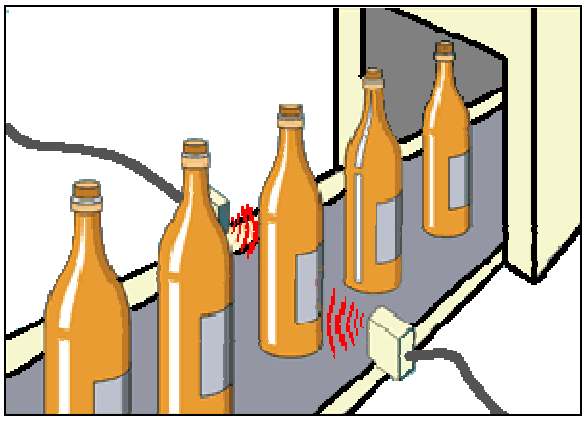

Fig. 10 - Sensores para contagem de unidades

Outro factor importante será a escolha correcta do operador para a execução de determinada tarefa. Por vezes e, no caso concreto de tarefas mais monótonas e repetitivas, é preferível a utilização de pessoas com menor QI[6] do que indivíduos com QIs superiores. Esta escolha deve-se ao facto de, quando bem treinadas, estas pessoas conseguirem atingir níveis de eficiência bastante superiores aos de pessoas consideradas "normais", uma vez que conseguem abstrair-se com mais facilidade do meio envolvente. Por outro lado, pessoas consideradas inteligentes, têm uma maior tendência para se alienarem e dispersarem a atenção quando confrontadas com tarefas mais monótonas e repetitivas. Este tipo de pessoas são mais indicadas para funções que envolvam maior responsabilidade e/ou tomada de decisões.

A nível do projecto propriamente dito (componentes, equipamentos e sistemas), este deverá ser concebido de forma a permitir uma rápida e correcta manutenção, evitando deste modo a ocorrência de um maior número de falhas humanas. Assim sendo, o projecto deverá ter em consideração aspectos como a boa visibilidade dos comandos a actuar e dos alertas a visualizar, bem como dispor de códigos de cores, tomadas, tipos de pinos, entre outros, de modo a facilitar as operações de manutenção, reduzindo assim os erros humanos. Um exemplo prático desta situação e que ocorre muito frequentemente é a substituição dum simples *led* num qualquer painel eléctrico. Considerado como uma situação com consequências muito negativas a nível de manutenção, a

[6] QI (Quociente de Inteligência) é uma medida obtida por meio de testes desenvolvidos para avaliar as capacidades cognitivas de um sujeito, quando em comparação com a sua faixa etária.

substituição do *led* pode ser condicionada pela remoção de um vasto número de outros componentes até chegar à referida luz. Se inicialmente tivesse sido projectada a inclusão de um *led* de remoção externa em vez da desmontagem de inúmeros componentes, os *downtimes* seriam menores, uma vez que a desmontagem e montagem de componentes já não seria necessária.

Factores igualmente importantes para gerar melhorias no sistema Homem-Máquina são, ainda, entre outros, a supervisão e a gestão.

Toda e qualquer tarefa realizada por um ser humano, por muito bem executada que seja, estará sempre sujeita a erros e falhas. Uma supervisão atenta, cuidada e com controlo sobre todo o processo produtivo, funcionará como um filtro de eventuais falhas que ocorram, de modo a que o produto final (entenda-se por produto, o resultado do trabalho realizado) seja o mais perfeito possível.

A gestão é importante a um nível superior, no sentido de dividir tarefas de acordo com as potencialidades dos operadores e a disponibilidade dos equipamentos. Actua ainda no campo da gestão de *stocks* e na criação de regras fundamentais para o bom funcionamento e melhor eficiência do sistema Homem-Máquina.

4. Metodologias de Avaliação da Fiabilidade Humana

4.1. Introdução

A avaliação da fiabilidade humana (HRA) é, de um modo genérico, um conjunto de metodologias, técnicas e ferramentas, através das quais a probabilidade de uma determinada acção ou tarefa levada a cabo por um operador humano é realizada com sucesso, dentro de um intervalo de tempo requerido e sem a existência de acções humanas que, de algum modo, deteriorem a *performance* do sistema[7]. Segundo Kirwan et al. (1997), as metodologias de avaliação da fiabilidade humana são ferramentas analíticas primárias para gestão de risco, em particular para predizer e prevenir os impactos negativos do erro humano na segurança de sistemas complexos.

Os resultados das HRAs são frequentemente utilizados como *inputs* para as avaliações probabilísticas de risco (PRA), que analisam a fiabilidade dos sistemas como um todo, através da decomposição de cada sistema nos seus componentes constituintes, desde *hardware*, *software* e operadores humanos.

Os benefícios gerais da realização de HRAs são:

- Geram estimativas quantitativas dos potenciais de erro humano;
- Identificam as fraquezas existentes nos interfaces dos operadores com o sistema;
- Demonstram quantitativamente os melhoramentos nos interfaces humanos;
- Melhoram as avaliações dos sistemas, através da inclusão de elementos humanos;
- Demonstram quantitativamente a predição do comportamento humano.

Após uma exaustiva pesquisa em artigos científicos, livros, relatórios e pesquisa na *Internet*, foram encontradas 36 metodologias, técnicas e ferramentas de HRA. A Tabela 1 apresenta um quadro-resumo com todas as referências encontradas.

[7] Definição segundo *Sandia National Laboratories*

Tabela 1 - Metodologias, técnicas e ferramentas HRA encontradas

ASEP	*Accident Sequence Evaluation Program*
AIPA	*Accident Initiation and Progression Analysis*
APJ	*Absolute Probability Judgement*
ASHRAM	*Aviation Safety Human Reliability Analysis Method*
ATHEANA	*A Technique for Human Error Analysis*
CAHR	*Connectionism Assessment of Human Reliability*
CARA	*Controller Action Reliability Assessment*
CES	*Cognitive Environmental Simulation*
CESA	*Commission Errors Search and Assessment*
CM	*Confusion Matrix*
CODA	*Conclusions from occurrences by descriptions of actions*
COGENT	*COGnitive EveNt Tree*
COSIMO	*Cognitive Simulation Model*
CREAM	*Cognitive Reliability and Error Analysis Method*
DNE	*Direct Numerical Estimation*
DREAMS	*Dynamic Reliability Technique for Error Assessment in Man-machine Systems*
FACE	*Framework for Analysing Commission Errors*
HCR	*Human Cognitive Reliability*
HEART	*Human Error Assessment and Reduction Technique*
HORAAM	*Human and Organisational Reliability Analysis in Accident Management*
HRMS	*Human Reliability Management System*
IJS-HRA	*Institute Jožef Stefan Human Reliability Analysis*
JHEDI	*Justified Human Error Data Information*
MAPPS	*Maintenance Personnel Performance Simulation*
MERMOS	*Method d'Evaluation de la Realisation des Missions Operateur pour la Surete*
NARA	*Nuclear Action Reliability Assessment*
OATS	*Operator Action Tree System*
OHPRA	*Operational Human Performance Reliability Analysis*
PC	*Paired comparisons*
PHRA	*Probabilistic Human Reliability Assessment*
SHARP	*Systematic Human Action Reliability Procedure*
SLIM	*Success likelihood index methodology*
SPAR-H	*Simplified Plant Analysis Risk Human Reliability Assessment*
STAHR	*Socio-Technical Assessment of Human Reliability*
TESEO	*Tecnica empirica stima errori operatori*
THERP	*Technique for Human Error Rate Prediction*

Destas 36 metodologias, técnicas e ferramentas, foram seleccionadas as 5 mais relevantes (THERP, ASEP, HEART, SPAR-H e CREAM), para se proceder aos seus resumos, com o intuito de

conferir um *background* mais abrangente do tema. Esta escolha deveu-se não só ao facto de serem as mais utilizadas como também por serem as que, de algum modo, marcaram positivamente os desenvolvimentos futuros de novas metodologias de HRA. Uma sexta metodologia será desenvolvida mais detalhadamente (ATHEANA), por ser uma das mais utilizadas no actual panorama da indústria de produção de energia nuclear a nível mundial, uma vez que tem em consideração não só os cenários de potenciais acidentes, como também os mais recentes avanços das ciências cognitivas.

4.2. Technique for Human Error Rate Prediction (THERP)

Os primeiros estudos e princípios-base que estão na origem da metodologia THERP começaram a ser desenvolvidos ainda na década de 50 do século XX com propósitos militares, nomeadamente no controlo da qualidade para estimar erros existentes na assemblagem de ogivas nucleares. Com base nestes princípios e, já na década de 60, Swain e Guttmann começaram a desenvolver no *Sandia National Laboratories* a metodologia THERP, cujo objectivo era diagnosticar as probabilidades de ocorrência de erros humanos e avaliar a degradação dos sistemas homem-máquina causada por erros humanos, fossem eles solitários ou em conjunto com o funcionamento de equipamentos, procedimentos operacionais ou características específicas do ser humano ou do sistema, que pudessem condicionar o comportamento do sistema em sectores de elevado risco como é o caso das centrais de produção de energia nuclear.

Após a publicação de uma versão preliminar ("*draft report*") do método em 1980 (Swain, Guttmann, 1980), a versão final surgiu em 1983 numa publicação realizada pelos mesmos autores para a *U.S. Nuclear Regulatory Commission* com o título: *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (Swain, Guttmann, 1983).

A aplicação da metodologia compreende normalmente a seguinte sequência de passos:

1 - Decomposição das tarefas em elementos;
2 - Atribuição de HEPs nominais a cada elemento;
3 - Determinação dos efeitos dos PSFs em cada elemento;
4 - Cálculo dos efeitos das dependências entre tarefas;
5 - Modelação numa árvore de eventos de HRA;
6 - Quantificação do HEP global da tarefa.

Duas das características fundamentais deste método e que o distinguem de muitos outros, assentam no facto de ser o primeiro método que considera o erro do operador como uma falha do equipamento e ainda o pioneirismo na criação de uma árvore de eventos como ferramenta de analítica.

A árvore de eventos é uma estrutura lógica que é utilizada para identificar os eventos possíveis que podem ter origem numa situação inicial. Cada extremidade da árvore (também designada de tarefa), representa um ponto de decisão binário, isto é, a decisão só pode ser correcta ou incorrecta, sendo associada a uma probabilidade de erro humano (HEP – *Human Error Probability*) específica. Há algumas bases de dados e tabelas de onde é possível retirar os valores, como é o caso da Tabela 2.

Para ter em conta as características específicas de cada análise, torna-se necessário modificar os HEPs, recorrendo à utilização de factores que definem o desempenho (PSF – *Performance Shaping Factors*). De acordo com Kirwan et al. (1997), é possível escolher um valor de HEP num raio fixado por limites superior e inferior, que são respectivamente:

$$HEP \times EF \quad \text{e} \quad HEP / EF$$

Tabela 2 – HEPs de erros de comissionamento

Item	Potential Errors	HEP	EF
(1)	Inadvertent activation of a control	see text	
	Select wrong control on a panel from an array of similar-appearing controls**:		
(2)	identified by labels only	.003	3
(3)	arranged in well-delineated functional groups	.001	3
(4)	which are part of a well-defined mimic layout	.0005	10
	Turn rotary control in wrong direction (for two-position switches, see item 8):		
(5)	when there is no violation of populational stereotypes	.0005	10
(6)	when design violates a strong populational stereotype and operating conditions are normal	.05	5
(7)	when design violates a strong populational stereotype and operation is under high stress	.5	5
(8)	Turn a two-position switch in wrong direction or leave it in the wrong setting	†	
(9)	Set a rotary control in an incorrect setting (for two-position switches, see item 8)	.001	10††
(10)	Failure to complete change of state of a component if switch must be held until change is completed	.003	3
	Select wrong circuit breaker in a group of circuit breakers**:		
(11)	densely grouped and identified by labels only	.005	3
(12)	in which the PSFs are more favorable (see text)	.003	3
(13)	Improperly mate a connector (this includes failures to seat connectors completely and failure to test locking features of connectors for engagement)	.003	3

* The HEPs are for errors of commission only and do not include any errors of decision as to which controls to activate.

** If controls or circuit breakers are to be restored and are tagged, adjust the tabled HEPs according to Table 16-2.

† Divide HEPs for rotary controls (items 5-7) by 5 (use same EFs).

†† This error is a function of the clarity with which indicator position can be determined: designs of switch knobs and their position indications vary greatly. For plant-specific analyses, an EF of 3 may be used.

fonte: Swain, A. D., Guttmann, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. Washington, DC, U.S. Nuclear Regulatory Commission.

Define-se EF como sendo o factor de erro (EF – *Error Factor*) associado a cada HEP retirado das tabelas referidas anteriormente. A HEP considerada será um valor médio do intervalo cujos extremos são HEP x EF e HEP / EF. Assim, será lógico concluir-se que a HEP aumenta quando as

condições forem piores que as consideradas (logo maiores HEPs) e diminui quando as condições forem melhores que as consideradas (logo menores HEPs).

Quando a cada extremidade da árvore está associado um valor de HEP e quando o evento final da árvore é identificado como um evento de sucesso (S) ou de falha (F), a probabilidade de cada sequência de eventos é então calculada multiplicando os valores dos ramos que fazem parte da sequência. Na Fig. 11 está ilustrada uma árvore de eventos, na qual os ramos com letras minúsculas representam acções bem sucedidas, enquanto que os ramos com letras maiúsculas representam as falhas das mesmas acções.

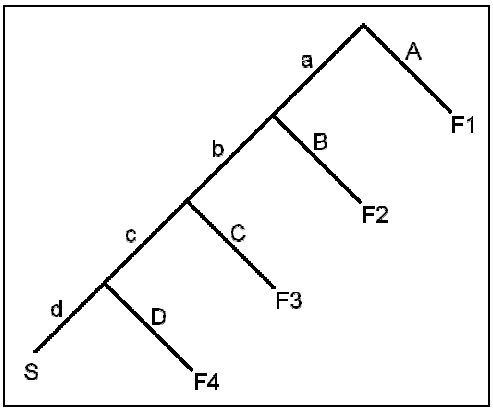

Fig. 11 - Exemplo de árvore de eventos

A determinação da probabilidade geral de falha implica que a equação das falhas envolva a soma de todas as probabilidades existentes nas ramificações da árvore de eventos. Quando todas as HEPs foram menores ou iguais a 0,01, a equação de falha pode ser aproximada à soma das ramificações de falha principais, ignorando as ramificações correspondentes a acções bem sucedidas. A precisão desta aproximação diminui com o aumento do número de termos e/ou com o aumento dos valores das HEPs (Swain, Guttmann, 1983).

Quanto à sua utilização, a metodologia THERP é bastante utilizada em várias indústrias, apesar de ter sido concebida para a aplicação na indústria nuclear. A sua larga utilização advém do facto de apresentar resultados bastante credíveis, sendo mesmo considerada uma ferramenta bastante poderosa e com a vantagem de poder ser auditada (Kirwan, 1994). Outra grande vantagem desta

metodologia é o facto da mesma se basear numa extensa e bem documentada base de dados, incluída na literatura de referência (Swain, Guttmann, 1983).

Por outro lado esta metodologia exige elevados recursos de tempo e económicos, tornando o nível de detalhe bastante excessivo em algumas avaliações. Contudo, não fornece suficientes instruções para a modelação de cenários, bem como para a determinação do impacto dos PSFs na *performance* dos operadores.

4.3. Accident Sequence Evaluation Program (ASEP)

O método ASEP foi desenvolvido em 1987 pelo mesmo autor da metodologia THERP, Alan D. Swain, para a *U.S. Nuclear Regulatory Commission* do *Office of Nuclear Regulatory Research*, que expressou a necessidade da existência de um método que promovesse estimativas das probabilidades de ocorrência de erros humanos, assim como de tempos de resposta para tarefas desempenhadas sob condições normais de operação e condições de pós-acidente, devendo para tal ser suficientemente exacto e recorrendo a um mínimo de tempo e de recursos (Swain, 1987).

Este método surge pois como uma versão resumida e ligeiramente modificada da metodologia THERP, enquadrando os pré e pós-acidentes na análise nominal da fiabilidade humana. Deste modo, esta metodologia permite um percurso mais curto nessa mesma análise quando comparada com a THERP, uma vez que requer menos formação para utilização da ferramenta, menos perícia/experiência no enquadramento das estimativas e, consequentemente, menos tempo para completar as análises (Everdij, Blom, 2008). Segundo Kirwan (1994), o método ASEP é mais rápido de realizar comparativamente ao THERP, podendo inclusivamente ser computorizado. Refere ainda que este método tem tendência a ser utilizado como uma primeira abordagem de enquadramento que permite desde logo identificar as tarefas que requerem análises mais detalhadas aquando da utilização da metodologia THERP.

Resumidamente, apresentam-se os procedimentos básicos em que assenta a metodologia ASEP:

- tarefas pré-acidentais: são tarefas que, quando realizadas incorrectamente, podem resultar na indisponibilidade de sistemas necessários ou componentes num complexo industrial (por exemplo, uma central nuclear), para responder eficazmente em caso de acidente;

- tarefas pós-acidentais: estas tarefas têm o objectivo de garantir que o complexo industrial lida com sucesso aquando da ocorrência de um evento anormal, conduzindo os seus vários sistemas a um estado de segurança;

- enquadramento das análises da fiabilidade humana: as probabilidades de teste assim como os tempos de resposta são atribuídos a cada tarefa realizada pelo operador como um tipo inicial de análise sensível. Se um valor amostral deste enquadramento não tem efeito material na análise do sistema, poderá ser abandonado após investigação detalhada sobre o mesmo. Dessa forma, o enquadramento permite a redução da quantidade de análises detalhadas a serem realizadas. Assim e, neste ponto, verifica-se que as análises da fiabilidade humana usam deliberadamente estimativas conservativas do potencial de erro humano de cada acção, bem como dos tempos de resposta, dos níveis de dependência e de outras características da *performance* humana.

- análises nominais da fiabilidade humana: a avaliação probabilística do risco, realizada nas acções identificadas durante o processo de enquadramento, usa o que a equipa responsável pela avaliação da fiabilidade humana decide como sendo os valores mais realísticos, ou seja, os valores que mais se aproximam da situação real. Contudo, estes valores são ainda assim um pouco conservativos ou até mesmo pessimistas, de modo a ter em consideração a natural inaptidão da equipa para considerar todas as potenciais fontes de erro, assim como todas as possíveis interacções comportamentais.

O relatório de Swain (1987) relata detalhadamente cada um destes procedimentos aqui resumidos.

Ao contrário da metodologia THERP, esta ferramenta foi desenvolvida especificamente para a indústria nuclear, pelo que não é aplicável a outros sectores industriais.

4.4. Human Error Assessment and Reduction Technique (HEART)

A metodologia HEART foi inicialmente apresentada num artigo de uma conferência por J. C. Williams (1985), tendo sido posteriormente desenvolvida e detalhada em artigos subsequentes e do mesmo autor (Williams, 1986, 1988, 1992).

O HEART foi desenvolvido para ser um método simples e rápido de quantificar o risco da existência de erro humano, "dando" sugestões ao utilizador de como proceder para reduzir este tipo de erro. Sendo um método geral, poderá ser aplicado a qualquer situação ou indústria onde a fiabilidade humana seja importante, não se especializando numa indústria particular como acontece, por exemplo, com muitos métodos relativamente à indústria nuclear.

A metodologia assenta no princípio de que toda e qualquer tarefa realizada tem a si associada a possibilidade de ocorrência de uma falha, pelo que a probabilidade de esta ocorrer é afectada pelas denominadas condições geradoras de erros (EPCs – *Error Producing Conditions*). Estas condições, como é o caso do cansaço, da distracção e da senilidade, entre outras, podem ser aplicadas a cenários teoricamente perfeitos para estimar a probabilidade de falha sob condições ideais. Esta informação irá ser muito útil na determinação da probabilidade de ocorrência de erros numa análise de risco mais alargada, onde os EPCs serão forçosamente introduzidos de modo a gerarem indirectamente um conjunto de sugestões relativas ao aumento da fiabilidade e, consequentemente, minimização do risco.

Resumidamente, o método tem em consideração todos os factores que possam ser negativos e que, de algum modo, afectem a *performance* de tarefas dependentes da Fiabilidade Humana. Cada um destes factores é distintamente quantificado para obter uma probabilidade geral de erro humano (HEP – *Human Error Probability*), que será o produto de todos os factores reunidos.

Segundo Williams (1986), há nove tipos de tarefas genéricas, tendo associada a cada uma delas uma HEP (probabilidade de erro humano de cada tarefa) e trinta e oito EPCs que poderão afectar a fiabilidade da tarefa. Posteriormente e, dependendo do grau de afectação de cada EPC, irá surgir mais uma variável que resultará da avaliação proporcional de afectação (APOA – *Assessed Proportion of Affect*) e que, por sua vez, irá entrar no cálculo geral para determinar a HEP da tarefa.

Assim, o procedimento para a determinação da HEP, segundo a metodologia HEART, é:

- Classificação da tarefa a analisar, de acordo com os nove tipos de tarefas genéricas;
- Associar à tarefa a respectiva HEP;
- Decidir que EPCs poderão afectar a fiabilidade da tarefa;
- Considerar a APOA de cada EPC;
- Calcular a HEP.

No Anexo C poderão ser consultadas tabelas auxiliares que permitem uma melhor visualização dos tipos de tarefas genéricas, assim como os EPCs e respectivos factores multiplicativos, utilizados no cálculo da HEP segundo a metodologia HEART.

Este método é frequentemente utilizado recorrendo a aplicações informáticas[8], que permitem uma maior flexibilidade, rapidez e aplicabilidade do mesmo, granjeando assim e ainda mais a sua popularidade. A juntar a estes factores, acresce ainda que este é um método de baixo custo, uma vez que requer recursos relativamente limitados para completar a avaliação e permite ainda ao agente coordenador da sua aplicação obter sugestões relativas à redução dos erros humanos.

Contudo, este método requer grande clareza nas várias descrições efectuadas, uma vez que dois agentes envolvidos na aplicação do mesmo podem calcular diferentes HEPs para a mesma tarefa, o que se traduzirá de imediato em resultados diferentes.

Apesar de terem sido realizadas algumas validações empíricas e independentes do método (exemplo: Kirwan et al., 1997), nunca foi de todo possível chegar a um consenso relativamente à

[8] HEART Online Calculator: http://tricenote.com/safety/heart-calculator

curta lista de EPCs e de tipos de tarefas genéricas, uma vez que tanto as nove EPCs como as trinta e oito tarefas genéricas existentes não expressam a totalidade das condições geradoras de erros e tarefas existentes no mundo industrial, sendo para tal necessário mais validação teórica sobre o mesmo (Kirwan, 1994).

4.5.Simplified Plant Analysis Risk Human Reliability Assessment (SPAR-H)

A metodologia SPAR-H começou a ser desenvolvida em 1994 pelo *Idaho National Laboratory* para a *U.S. Nuclear Research Commission* do *Office of Nuclear Regulatory Research*, com o objectivo de ser uma abordagem fácil de utilizar e que permitisse o desenvolvimento de modelos probabilísticos de avaliação da fiabilidade humana em centrais nucleares. Numa fase inicial foi designada de *Accident Sequence Precursor Standardized Plant Analysis Risk Model* (ASP/SPAR) no desenvolvimento das referidas centrais, tendo sido actualizada em 1999, fruto da experiência adquirida no trabalho de campo e renomeada com o nome actual. Estas e outras alterações culminaram na produção de mais um relatório do *Idaho National Laboratory* para a *U.S. Nuclear Research Commission* do *Office of Nuclear Regulatory Research* com o título *NUREG CR-6883 - The SPAR-H Human Reliability Analysis Method* (Gertman et al., 2004) e que é considerada a obra de referência para a aplicação da metodologia SPAR-H.

Mais recentemente e, por ser de fácil utilização, este método tem sido aplicado para gerar dados necessários ao software de análise probabilística de risco e fiabilidade, utilizado nas centrais nucleares – SAPHIRE (*Systems Analysis Programs for Hands-on Integrated Reliability Evaluation*) (Boring et al., 2005).

Segundo Gertman et al. (2004), esta metodologia decompõe a probabilidade de falha numa de duas categorias: falhas de diagnóstico e falhas de acções; cria HEPs-tipo, baseando-se em casos estudados de ocorrências de falhas humanas (*HFE- Human Failure Event*) conjugadas com os PSFs; utiliza as HEPs e os PSFs anteriormente referidos, juntamente com regulamentação criada para o caso, para atribuir/definir o valor mais correcto a aplicar a cada PSF; emprega a distribuição beta para análises duvidosas, gerando dados que permitem emular a distribuição normal; utiliza ainda

ferramentas informáticas como determinadas folhas de cálculo para garantir a consistência das análises.

Este método, conforme referido anteriormente, atribui as actividades humanas a uma de duas categorias gerais:

- Tarefas de diagnóstico (taxa de erro genérica: 0,01) – representam a componente de processamento/planeamento e baseiam-se no conhecimento e na experiência para compreender as condições existentes e assim planear e melhor definir as actividades e procedimentos das acções, assim como as prioridades a serem tidas em conta.

- Tarefas de acção (taxa de erro genérica: 0,001) – representam a componente de resposta, onde são levadas a cabo uma ou mais actividades indicadas pelos diagnósticos, regras de operação ou procedimentos escritos, como por exemplo: equipamento de operação a utilizar, arranque de bombas, realização de alinhamentos/calibrações/testes, execução de tarefas em resposta a alarmes e outras actividades realizadas durante o decorrer dos procedimentos de operação e/ou ordens dos operadores.

De acordo com os mesmos autores, existem oito PSFs com a capacidade de influenciarem a *performance* humana, que são tidos em consideração no processo de quantificação da metodologia SPAR-H. São eles:

- Tempo disponível;
- Complexidade;
- Experiência e formação;
- Condição física;
- *Stress*;
- Ergonomia/HMI;
- Procedimentos;
- Processos de trabalho.

O SPAR-H distribui os HFEs em falhas de diagnóstico e falhas de acção, quantificando os dois tipos de falhas separadamente. As HEPs nominais são atribuídas a ambos e ajustadas para reflectir o impacto de cada um dos oito PSFs. Posto isto e, tal como se faz em muitos outos métodos de avaliação da Fiabilidade Humana, cada PSF é examinado de acordo com regulamentação específica fornecida para determinar a influência de cada PSF (por exemplo: complexidade elevada, moderada ou normal), sendo posteriormente a ele (PSF) associado um factor multiplicativo que permita ajustar a HEP nominal baseada na avaliação do PSF. Os PSFs e respectivos factores multiplicativos utilizados neste método surgem da exaustiva pesquisa levada a cabo pelos seus autores em literatura científica, aquando do seu desenvolvimento, aplicando muitas vezes variadíssima informação de outros métodos de avaliação da Fiabilidade Humana. O SPAR-H permite ainda a modelação das dependências entre HFEs, recorrendo ao modelo de dependência da metodologia THERP.

Em suma, o SPAR-H surge como um método relativamente fácil de utilizar, em que os oito PSFs incluídos conseguem cobrir imensas situações onde não são necessárias análises mais detalhadas (Forester et al., 2006). Contudo, este método não fornece os procedimentos necessários aquando da necessidade de um raio mais alargado de PSFs, embora a realização de pesquisas aprofundadas em métodos mais recentes e em desenvolvimento seja encorajada no caso de ser necessário mais detalhe nas suas aplicações, mais concretamente em erros de diagnóstico.

Apesar dos seus princípios-base, assim como as informações relativas às HEPs poderem ser aplicados a outros domínios, o facto é que a metodologia SPAR-H não só foi desenvolvida para o sector nuclear, como também é neste mesmo sector que se conhece a sua aplicação.

4.6.Cognitive Reliability and Error Analysis Method (CREAM)

A metodologia CREAM foi desenvolvida por Erik Hollnagel no inicio da década de 90 do século XX, tendo sido formalmente apresentada em 1998 num artigo científico do mesmo autor com o título *Cognitive Reliability and Error Analysis Method* (Hollnagel, 1998), encontrando-se presentemente ainda em desenvolvimento.

Hollnagel descreve a metodologia CREAM como sendo bidireccional, isto é, os princípios podem ser aplicados tanto em análises retrospectivas como na predição da *performance* dos operadores. O modelo é então baseado fundamentalmente na distinção entre competência e controlo que, por sua vez, se baseia no modelo COCOM[9], desenvolvido pelo mesmo autor e que inclui na competência as características e conhecimentos pessoais dos operadores. Já o controlo é visto como uma série de acções que se podem desenvolver desde uma posição em que o operador tem pouco ou nenhum controlo até uma posição de controlo total. Através deste modelo identificam-se alguns aspectos do contexto que se designam na literatura científica por *Common Performance Conditions* (CPC).

O esquema de classificação separa claramente as causas (genótipos) das manifestações (fenótipos) e propõe ainda uma organização não hierárquica das categorias ligadas por intermédio das sub-categorias designadas por antecedentes e consequentes. No que respeita às causas, as mesmas classificam-se em três categorias distintas:

- Causas com ligação directa ou indirecta ao comportamento (exemplos: personalidade, estado emocional, entre outros);
- Factores relativos à interacção/interface homem-máquina;
- Factores ambientais relativos ao local (exemplos: temperatura, ruído, etc.)

As manifestações são as consequências das acções dos operadores ou omissões destas sendo, na maioria das vezes, o ponto de partida para as análises. Estes fenótipos, ou modos de erro, são frequentemente divididos em quatro sub-grupos:

- Acção do tipo errado;
- Acção no tempo errado;
- Acção no objecto errado;
- Acção no local errado.

Para cada consequência deve existir uma lista de antecedentes prováveis (possíveis explicações). Cada um desses antecedentes são também considerados consequências para a causa

[9] COCOM (*Contextual Control Model*), é um modelo cognitivo dependente do contexto, desenvolvido por Erik Hollnagel em 1993 na obra *Human reliability analysis: Context and control*. Mais informação disponível na página da *Internet* do próprio autor: http://www.ida.liu.se/~eriho/COCOM_M.htm

raiz. Tal procedimento apresenta a extensão que o método pode obter até se alcançar uma explicação ou enquanto ainda fizer sentido.

Assim, tanto as causas como as manifestações, são classificadas em consequências gerais e para cada uma dessas consequências há inúmeros antecedentes gerais e específicos. Por exemplo, para o genótipo "comunicação" a consequência geral pode ser a "falha de comunicação", como antecedente geral pode definir-se a "distracção", assim como os antecedentes específicos podem ser "ruído" ou até "incapacidadde temporária".

O primeiro passo na aplicação da metodologia CREAM é a análise de tarefas, produzido-se para tal uma lista das actividades dos operadores, para a qual são efectuadas análises aos CPCs. Hollnagel definiu a existência de nove CPCs:

- Adequação da organização;
- Condições de trabalho;
- Adequação do interface homem-máquina e do suporte operacional;
- Disponibilidade de procedimentos, manuais e planos;
- Número de objectivos simultâneos;
- Disponibilidade de tempo;
- Hora do dia;
- Formação e experiência adequadas;
- Colaboração dos vários elementos da equipa.

Para cada actividade é determinado o nível do CPC, por exemplo: a experiência pode ser considerada como "elevada experiência", "baixa experiência" ou "experiência inadequada". Os efeitos esperados destes níveis de experiência na *performance* são, respectivamente: "melhorada", "insignificante" e "reduzida". A metodologia CREAM chega, inclusivamente, a descrever regras para a quantificação destes identificadores/descritores.

O passo seguinte envolve a descrição de cada actividade cognitiva em termos de observação, interpretação, planificação e execução (funções desenvolvidas no modelo COCOM), assim como representar graficamente estas funções.

Tendo como base a classificação fenótipo-genótipo, é possível criar uma lista completa das falhas de funções cognitivas, subdividindo-as em vários sub-conjuntos. Para um dado sub-conjunto, cada função cognitiva (erros de observação, interpretação, planificação e execução), terá falhas potenciais identificadas. Estas falhas serão também representadas graficamente, assim como será calculada a probabilidade de falha cognitiva para cada uma das funções cognitivas. A esta probabilidade será aplicado um factor que depende das influências contextuais determinadas, nomeadamente os CPCs.

Quanto à aplicabilidade da metodologia CREAM e, apesar da mesma ter sido desenvolvida para a indústria de produção de energia nuclear e ser nela que se encontra a maioria das suas aplicações, o facto é que se trata de uma metodologia genérica que permite a utilização em vários tipos de indústria. São conhecidas adaptações da metodologia CREAM em indústrias químicas e em cenários de acidentes ferroviários.

5. Estudo Aprofundado da Metodologia ATHEANA

5.1. Introdução

A metodologia ATHEANA é uma ferramenta de avaliação de fiabilidade humana de segunda geração (ver 3.2 e 3.3) que começou a ser desenvolvida em meados da década de 90 do século XX por um consórcio de especialistas em Avaliação da Fiabilidade Humana para a *U.S. Nuclear Research Commission* do *Office of Nuclear Regulatory Research*. Os estudos culminaram em dois trabalhos de referência, sendo o primeiro o *NUREG/CR-6350* (Cooper et al., 1996), que descreve os princípios-base do método, e o segundo - *NUREG-1624* (US NRC, 2000), um manual detalhado e completo sobre a aplicação prática da metodologia.

A partir da análise de vários e sérios acidentes ocorridos (exemplos: *Three Mile Island*, *Chernobyl*, entre outros – ver Anexo B), e para atender às novas directrizes de regulação e fiscalização da *U.S. Nuclear Research Commission*, esta patrocionou um estudo para a criação de uma nova metodologia de avaliação da fiabilidade humana, tendo como principais factores impulsionadores do seu desenvolvimento, os seguintes factos:

- Os eventos humanos modelados em anteriores metodologias de avaliação da fiabilidade humana e de risco não eram considerados consistentes uma vez que, em geral, não eram tidos em conta ambientes e/ou condições extremamente adversos, como é o caso das falhas de diversos equipamentos em simultâneo;
- O registo de acidentes e os avanços nas ciências comportamentais, ambos suportados por um forte ênfase em factores contextuais, nomeadamente nas condições ambientais das instalações e na percepção do erro humano;
- Avanços na área da psicologia foram integrados com disciplinas de engenharia, factores humanos e avaliação probabilística de risco, na modelação de falhas humanas.

Através das referidas análises efectuadas após os grandes acidentes ocorridos em centrais nucleares constatou-se que existe um conjunto de factores que, sendo inerentes ao operador, não são qualificáveis nem se consideram para efeitos de análise probabilística de segurança, uma vez que podem surgir aleatoriamente nas mais variadas situações. São os designados factores complicadores

de eventos e que apenas a experiência do operador pode influir na redução de acidentes por eles gerados. Seguem-se alguns exemplos dos referidos factores:

- Exposição do operador a cenários diferentes daqueles para os quais foi treinado ou que adquiriu através da experiência;
- Várias falhas e indisponibilidade simultânea de equipamentos que, mesmo estando o operador familiarizado com cada uma individualmente, em conjunto geram situações que vão além das suas capacidades, adquiridas pela sua experiência, formação ou análises de segurança;
- Procedimentos que não são aplicados à situação existente;
- Interpretações erradas de eventos por parte dos operadores que não foram totalmente preparados para o efeito.

A conjugação destes factores com as condições das instalações, juntamente com os PSFs, geram ambientes físicos e psicológicos que propiciam a ocorrência de erros, os chamados *EFC*s. A associação destes factores induzem a mecanismos psicológicos que podem levar o operador a realizar uma determinada acção, designada de acção insegura (*UA – Unsecured Action*), a qual pode degradar as condições de segurança das tarefas do operador. Muitas das vezes estes mecanismos não podem ser considerados, por si só, maus comportamentos, embora sejam mecanismos que permitem ao operador realizar acções rápidas e que requerem grande perícia. Por exemplo, é frequente os operadores diagnosticarem uma dada ocorrência pela comparação com um padrão já conhecido, sendo mesmo, na maioria das vezes, um modo rápido e eficiente de responder a um determinado evento. Perante alguma diferença que possa surgir entre a ocorrência e o evento já conhecido e rotinado, há tendência por parte do operador de utilizar um padrão que mais se aproxime, agindo tal e qual como se de um evento rotineiro se tratasse. Se no evento conhecido a rápida identificação e consequente acção levam a respostas eficientes e dentro do tempo desejado, no caso de um evento diferente o mesmo processo pode levar a respostas inadequadas.

Esta medodologia difere dos restantes métodos tradicionais que procuravam, de um modo geral, quantificar os erros humanos de uma forma aleatória e em condições previstas de acidente. Assim, esta visa a identificação e determinação das probabilidades de ocorrência de certas situações que, quando sujeitas a condições pouco usuais e até mesmo desconhecidas, podem induzir o

operador a realizar acções que, de algum modo, propiciem insegurança no contexto geral das acções a realizar.

De um modo geral, a metodologia fornece orientações para analisar (retrospectiva e prospectivamente), o tipo de desempenho humano inadequado (o designado erro de comissionamento), que contribui para o risco e que pode ser totalmente integrado com a análise probabilística de segurança. Gera ainda planos estruturados de pesquisa para encontrar os referidos EFCs, através da integração do conhecimento e da experiência em avaliação probabilística de risco, engenharia, factores humanos e psicologia, juntamente com informação específica dos locais e ainda com a análise de acidentes anteriormente ocorridos. A integração é realizada através de uma plataforma de trabalho multidisciplinar que serve de base organizacional à metodologia e é aplicada directamente às análises retrospectivas de eventos operacionais, fornecendo também uma base para as análises prospectivas.

Relativamente à aplicação deste método e apesar de ter sido desenvolvido para a indústria nuclear poderá ser aplicado noutros ramos, uma vez que os seus procedimentos não dependem do tipo de indústria a aplicar. Contudo e, atendendo a que a literatura científica que serve de suporte à metodologia é toda ela voltada para a produção de energia nuclear, o desenvolvimento deste tema, quer a nível de exemplos, sequências de operação e verificação, constituição de equipas especializadas, simuladores, entre outros, é feito no âmbito das instalações nucleares.

5.2.Plataforma de trabalho multidisciplinar

A plataforma multidisciplinar começou a ser desenvolvida através de mais um estudo levado a cabo pela *U.S. Nuclear Research Commission* do *Office of Nuclear Regulatory Research*, tendo-se iniciado em 1992 e culminado em 1995 com o relatório *NUREG – CR-6265* (Barriere, 1995) que serviu de base para o desenvolvimento da metodologia ATHEANA. Esta plataforma pressupõe a criação de uma equipa que compreende várias áreas, desde a engenharia e operação dos reactores atómicos, aos factores humanos, passando pelas ciências comportamentais, especialistas em análise probabilística de segurança, entre outros.

O objectivo desta plataforma é integrar todo o conhecimento que advém das várias disciplinas e que é relevante para a análise do desempenho humano significativo para o risco em centrais nucleares.

A plataforma de trabalho multidisciplinar encontra-se representada graficamente na Fig. 12, onde do lado esquerdo se encontram localizados os elementos relacionados com o desempenho humano, nomeadamente os que dizem respeito às ciências comportamentais, disciplinas de factores humanos e engenharias.

Os PSFs, as condições das instalações e os mecanismos de erro, representam as informações necessárias para descrever as influências fundamentais na acção insegura conseguindo-se, desse modo, estabelecer as causas que levam determinada pessoa a realizar uma acção insegura.

Do lado direito encontram-se as falhas humanas que advêm das acções inseguras e ainda da definição do cenário específico do acidente. Juntos representam o modelo da análise probabilística de segurança (PSA).

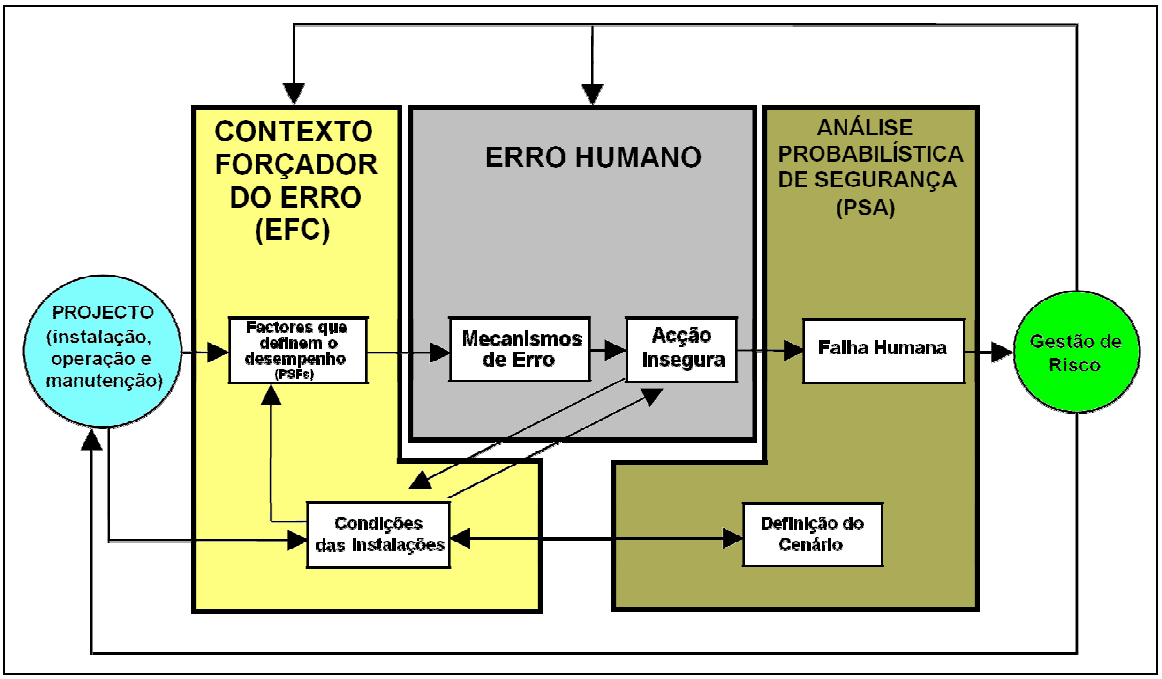

Fig. 12 - Plataforma de trabalho multidisciplinar

5.2.1. Contextos Forçadores de Erro (EFCs)

Os contextos forçadores de erros (EFCs), tal como representado na Fig. 12, resultam da combinação dos PSFs com as condições das instalações, gerando situações onde o erro humano surge com maior probabilidade de ocorrer (Forester, Kiper, Ramey-Smith, 1998).

As condições das instalações incluem a configuração física do espaço de trabalho, assim como as condições de disponibilidade e fiabilidade dos componentes e equipamentos dos sistemas homem-máquina (máquinas, instrumentos de medida, sistemas de monitorização e controlo, etc.), parâmetros dos processos (pressão, temperatura, etc.) e outros factores de características dinâmicas que induzem a comportamentos menos frequentes das instalações e seus sistemas (homens, máquinas, componentes, etc).

Relativamente aos PSFs, estes representam as influências centradas no homem e que podem afectar o seu desempenho, relacionadas com factores organizacionais, condições ambientais, procedimentos, formação, carga de trabalho, *stress*, supervisão, comunicação, tempo, interface homem-máquina, entre outros.

Um exemplo frequente de um PSF são os erros em procedimentos. No caso de um procedimento cujo conteúdo está incorrecto, incompleto ou confuso, pode o mesmo contribuir para uma falha de avaliação da situação e consequente planeamento errado da resposta.

5.2.2.Erro Humano

O erro humano, entre outras particularidades e definições, pode ser caracterizado por uma divergência entre uma acção realizada e uma acção que deveria ter sido realizada, tendo consequências fora da tolerância requerida pelo sistema homem-máquina. De acordo com o âmbito do seu estudo, o erro humano assume diferentes interesses por parte dos analistas. Assim e para a PSA, o significado de erro humano é definido como sendo a falha provocada pelo homem, ou seja, o interesse está na consequência do erro, enquanto que para as ciências comportamentais o interesse no estudo do erro humano está mais relacionado com as causas dos erros.

No que diz respeito à metodologia ATHEANA, o erro humano compreende as duas vertentes ou seja, o mecanismo do erro e as consequências do mesmo, isto é, as acções inseguras.

Quanto aos mecanismos de erro, estes são utilizados para descrever os mecanismos psicológicos que contribuem para o erro humano e que podem, a qualquer momento, ser disparados quer por um ou mais PSFs, assim como por uma ou mais condições das instalações. Por exemplo a carga excessiva de trabalho pode causar cansaço e, através de um mecanismo psicológico, o operador pode fazer uma avaliação inadequada de uma determinada situação que, como consequência, pode culminar num acidente grave.

Relativamente às acções inseguras (UA), podem definir-se como aquelas que são realizadas inadequadamente pelos operadores, ou até que não são realizadas quando necessário, resultando na degradação das condições de segurança das instalações. Contudo, os operadores nem sempre são apontados como a causa do problema, uma vez que podem ter sido influenciados pelas condições presentes aquando do acidente. Ou seja, um operador face às condições existentes pode executar uma tarefa de forma incorrecta não por falta de conhecimento mas por, num dado momento, lhe parecer ser a mais correcta.

5.2.3.Modelo da PSA

A avaliação probabilística de segurança utilizada aquando da aplicação da metodologia ATHEANA é em tudo semelhante à existente noutras metodologias, assumindo um comportamento de "cliente final" no processo de avaliação da fiabilidade humana. A PSA é então utilizada para estimar a frequência de um determinado cenário que pode levar a condições extremas de falta de segurança. Para tal o modelo lógico é convertido em modelo probabilístico obtendo-se, para o efeito, a probabilidade de cada evento existente no modelo, nos quais se incluem os eventos de falha humana. Estes são modelados na PSA para um determinado cenário específico de acidente, de forma a representar falhas de funções, componentes ou sistemas, como resultado de acções humanas que degradam as condições de segurança das instalações.

Cada HFE representa uma mudança incorrecta no estado do equipamento afectado, dentro do contexto das definições de eventos no modelo da árvore de eventos. Dado que o estado geral das instalações não muda instantaneamente aquando da ocorrência de uma falha humana, os HFEs são definidos para representar o erro cometido e também a falha dos operadores e supervisores em reconhecer esse mesmo erro e, desse modo, não realizarem quaisquer acções correctivas antes de ocorrer uma mudança do estado das instalações. Assim e dependendo do que se deseja que o HFE represente, este pode estar associado a uma sequência completa de uma árvore de eventos ou apenas a um corte mínimo gerado pela solução do modelo da PSA. O nível de decomposição adequado do cenário é o necessário para satisfazer a definição única de um HFE, respeitando o impacto das condições da planta na probabilidade do HFE.

As definições dos cenários da PSA fornecem assim uma descrição mínima das condições das instalações, requeridas não só para o desenvolvimento da PSA, como também para a definição dos HFEs adequados. Deste modo, o nível de detalhes para a definição dos cenários varia de acordo com os seguintes níveis: funcional, de sistema e do estado dos componentes (falha ou sucesso de componentes).

5.3.Actividades Cognitivas no Desempenho Humano

Conforme descrito em 5.2, uma das partes da plataforma multidisciplinar de trabalho que serve de base à metodologia ATHEANA é a relação entre as UAs, os mecanismos de erro e os PSFs. Esta relação obtém-se de duas fontes distintas e simultaneamente complementares:

- Análise dos eventos operacionais;
- Conhecimento das falhas humanas derivadas dos modelos de comportamento humano, adquirido com os especialistas de ciências comportamentais da plataforma.

5.3.1.Análise ao Desempenho Humano Cognitivo

De acordo com *NUREG-1624, Rev.1* (US NRC, 2000), as conclusões dos estudos das causas dos erros humanos nas últimas três décadas apontam para o facto da maioria dos erros humanos serem explicados pelo modo como o homem processa a informação em situações complexas. Desta forma a compreensão das bases do processo cognitivo, associadas à monitorização, tomada de

decisão e controlo das condições das instalações, assim como o modo como estes podem induzir ao erro humano, são fundamentais para a sua análise.

Para tal criou-se um modelo básico de representação que descreve as actividades humanas requeridas para fazer face às condições anormais de funcionamento do sistema homem-máquina, assim como de acidentes. Pode pois resumir-se o modelo em quatro passos cognitivos:

1 - avaliação da situação

2 - monitorização e detecção

3 - planeamento da resposta

4 - implementação da resposta

Para melhor interpretação e compreensão do modelo, a Fig. 13 ilustra as principais actividades cognitivas que influenciam o desempenho humano:

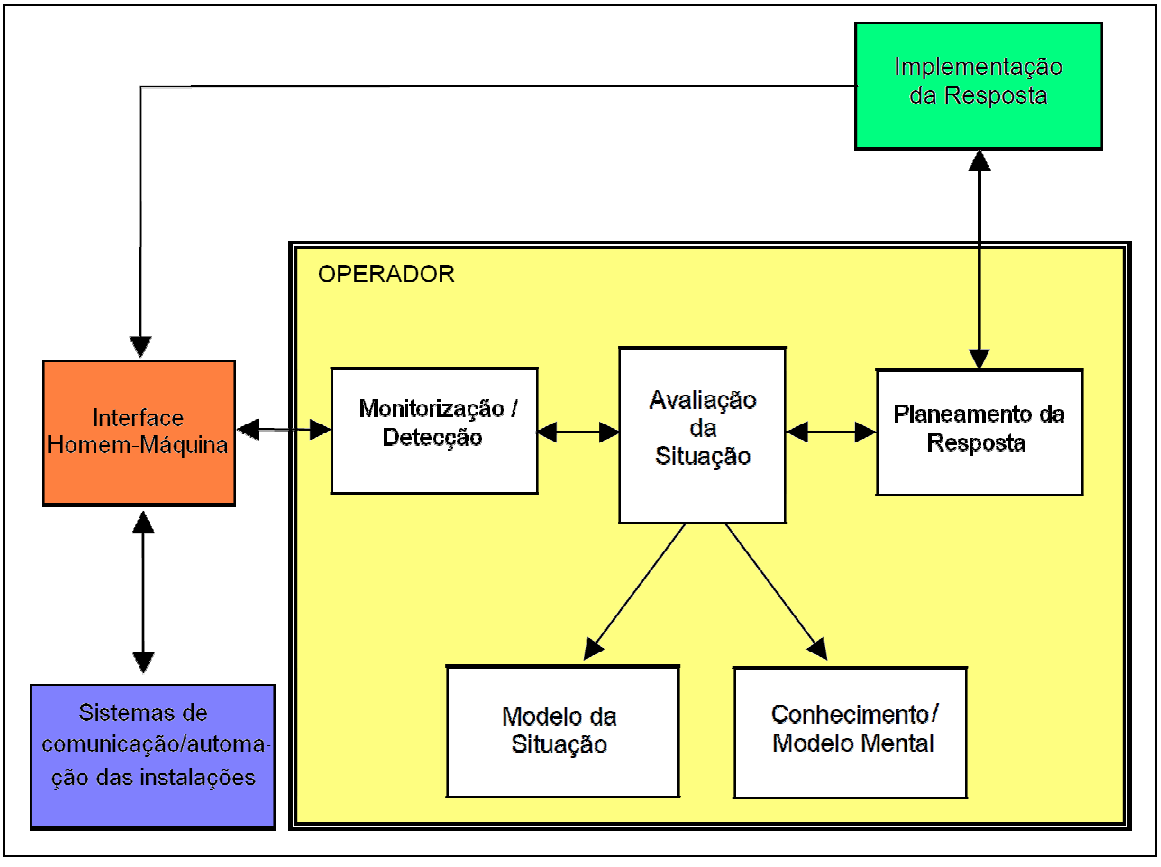

Fig. 13 - Principais actividades cognitivas que influenciam o desempenho humano

A avaliação lógica é o processo que ocorre naturalmente sempre que uma pessoa se depara com uma situação anormal, tendendo rapidamente a construir uma explicação lógica para tal. Esta avaliação envolve o desenvolvimento e actualização constantes da representação mental dos factores conhecidos e/ou das hipóteses criadas, podendo afectar directamente o estado dos sistema homem-máquina, assim como das condições envolventes. Esta representação, que resulta da avaliação, é referida como um modelo da situação que não é mais do que a percepção que a pessoa tem de uma determinada situação corrente, sendo constantemente actualizada a cada nova informação recebida. A avaliação da situação é semelhante em significado e com um aspecto mais amplo a nível de diagnóstico, uma vez que se refere à pesquisa das causas de sintomas de funcionamento anormal dos sistemas. Deste modo, essa avaliação envolve explicações que são geradas para justificar condições normais e anormais de funcionamento.

O conhecimento dos operadores é obtido através de formação e pode variar desde detalhes específicos de conhecimento até princípios genéricos abstractos que são aplicáveis a uma vasta classe de situações. Através deste conhecimento e da experiência que têm do local, das operações e das condições de laboração existentes, avaliam a sitação para gerar um modelo. A metodologia ATHEANA considera quatro tipos diferentes de conhecimentos que geram e permitem manter actualizado o modelo da situação:

- Episódios;
- Estereótipos;
- Modelo mental;
- Procedimento.

Este modelo da situação, que inclui os eventos que estão a decorrer no momento, assim como o modo como eles se comportam com o tempo e as consequências que deles podem surgir, gera uma expectativa que é utilizada para procurar por evidências que confirmam o modelo da situação criado. Esta expectativa procura ainda explicar os sintomas observados, como a seguir se exemplifica. Assim, se um novo sintoma coincidir com a sua expectativa, os operadores têm uma pronta explicação para a situação, reforçando a sua confiança no modelo da situação criado. No caso do sintoma não coincidir com a sua expectativa podem ocorrer duas situações: ou é ignorado ou é interpretado de forma diferente, de modo a torná-lo coincidente com a sua expectativa. Se entretanto

o novo sintoma for devidamente reconhecido como um comportamento inesperado do sistema, surge a necessidade de rever o modelo da situação existente. Deste modo, a avaliação da situação pode envolver o desenvolvimento de uma hipótese para o que está a ocorrer, relançando a procura por evidências.

A avaliação da situação permite assim detectar alguma não conformidade no comportamento do sistema que ainda não tivesse sido registada, além de poder detectar sintomas e alarmes que não tenham sido observados no momento, bem como como identificar falhas de sensores e mau funcionamento dos sistemas.

A monitorização e detecção referem-se às actividades de extracção das informações do meio ambiente e são influenciadas essencialmente por três factores:

- Características do ambiente;
- Conhecimento e expectativa da pessoa;
- Procedimento específico.

A nível das características do ambiente a monitorização por elas orientada é frequentemente denominada de monitorização orientada por dados (*data-driven monitoring*), sendo afectada pelo formato da informação, isto é, o seu formato físico (exemplos: tamanho, cor, som, etc.) e ainda pelo comportamento da informação (exemplo: velocidade). Para destacar informações mais importantes são utilizadas características especiais, tais como o tipo de cores, a intensidade do som, entre outros.

A monitorização também pode ser iniciada pelo operador, tendo como base o seu conhecimento e expectativa, ou ainda por um procedimento específico como acontece, por exemplo, quando se dá a troca de turnos onde se faz uma verificação de todo o painel de controlo. Este tipo de monitorização é frequentemente denominado de monitorização activa ou de monitorização orientada pelo conhecimento (*knowledge-driven*).

O planeamento da resposta refere-se a todo o processo de tomada de decisão acerca da acção a executar. Para tal envolve o modelo da situação previamente descrito, de modo a identificar objectivos, gerar planos de resposta alternativos, avaliar planos de resposta e seleccionar o mais adequado para o modelo da situação que está a ocorrer. Contudo e, dependendo das situações e da

existência de procedimentos escritos e julgados adequados para a ocorrência, nem sempre será necessário gerar planos de resposta em tempo real. Entretanto e mesmo com a existência destes procedimentos, alguns dos aspectos do planeamento da resposta precisam ainda de ser realizados, tais como identificar os objectivos adequados de acordo com a avaliação da situação, seleccionar o procedimento adequado, avaliar se as acções definidas no procedimento são suficientes para atingir os objectivos e ainda adaptar o procedimento à situação sempre que necessário.

Outro passo importante é a monitorização. Esta inclui a avaliação de competências de uma determinada acção executada e que conste dos procedimentos e também a realização de uma avaliação no sentido de perceber se o procedimento está a ser seguido de forma adequada. A realização desta monitorização permite assim ao operador detectar quando o procedimento não está a atingir os objectivos para os quais foi proposto e ainda quando contém erros (nos quais se incluem os erros na realização dos passos).

A adaptação do plano é outra actividade cognitiva incluída no planeamento da resposta e inclui acções específicas como o preenchimento de alguma deficiência/lacuna no procedimento, assim como a adaptação do procedimento a situações específicas, sendo por vezes necessário redireccionar o andamento do procedimento.

Por último e após planeada a resposta, segue a implentação da mesma, que mais não é do que executar as acções planeadas para realizar a tarefa requerida.

5.3.2. Factores Cognitivos que Afectam o Desempenho Humano

Existem três tipos de factores que influenciam directamente o desempenho humano, através da qualidade das respostas das actividades cognitivas. São eles:

- Factores de conhecimento;
- Factores de processamento cognitivo;
- Factores estratégicos.

Relativamente aos factores de conhecimento, podem ser divididos em dois grupos no que respeita à influência que incutem no desempenho humano: conteúdo e acesso. O conteúdo reúne todas as informações que o operador dispõe para realizar determinada tarefa, que foram adquiridas através de formação e experiência. Por exemplo, uma informação essencial que não conste do conhecimento do operador tem influência determinante no desempenho do mesmo. O acesso, por seu lado, refere-se à recuperação da memória, dependendo directamente do contexto. Isto é, as particularidades do contexto facilitam a recuperação das informações da memória e quanto mais particularidades houver maior será a probabilidade da informação ser acedida. Existem ainda outros factores que influenciam a recuperação da memória, permitindo que determinadas informações sejam mais facilmente recuperáveis que outras: factos que aconteceram recentemente, factos que ocorrem com maior frequência e ainda factos semelhantes. Nalgumas situações estes factores podem permitir a recuperação de informações que não são totalmente adequadas para a situação. Por exemplo, numa determinada situação cujos factos são semelhantes aos de um evento ocorrido recentemente, os operadores podem recuperar as informações desse evento, interpretando como se a situação presente fosse a mesma. Por outro lado, informações relevantes que o operador possa ter, podem nunca vir a ser recuperadas. Vejamos o caso duma situação que muito raramente ocorre em que há factos em comum com um evento que é mais familiar ao operador, este pode falhar no reconhecimento do evento raro, interpretanto a informação como se se tratasse de um evento familiar.

Quanto aos factores de processamento cognitivo, são recursos internos dos operadores, tais como a atenção ou a memória. Estes recursos, como é reconhecido, não existem numa quantidade infinita, pelo que a quantidade limitada existente deve ser distribuída pelas tarefas que estão a decorrer. Uma vez que há quase sempre diferenças a nível da exigência dos processos cognitivos a distribuição deverá ser efectuada de acordo com as necessidades. Por exemplo, se uma determinada tarefa requer grandes quantidades de recursos cognitivos, como a atenção e memória, então haverá pouca disponibilidade destes recursos para a execução de outras actividades. Consequentemente e caso essa tarefa utilize quase todos os recursos de processamento cognitivo disponíveis, novas tarefas serão atrasadas até que os recursos estejam novamente disponíveis. Caso a tarefa requeira mais recursos do que os disponíveis a execução da mesma poderá ficar atrasada e sujeita a erros.

A realização de tarefas familiares e devidamente treinadas por parte dos operadores necessita de poucos recursos cognitivos, sendo realizadas de modo quase automático, ou seja, é como se se tratasse de uma máquina que realiza vários ciclos consecutivos, sem qualquer tipo de processamento cognitivo associado (ver melhorias na fiabilidade com a utilização deste *modus operandi* em 3.6.3). Contudo e caso a tarefa não seja familiar ao operador, este deixa de trabalhar em modo "automático" e começa a realizar o processamento cognitivo da informação, o que se traduz em acções realizadas de forma mais cautelosa e lenta. Conforme referido, estes processos consomem recursos cognitivos que são superados pela tendência natural e cuidadosa do operador em criar uma espécie de atalhos (denominados de "heurísticos) que lhe permitem, sem efectuar uma análise completa da situação, reduzir os esforços, os recursos cognitivos e a incerteza de situações não familiares. Todavia e, por não ser realizada uma análise completa, o modelo da situação pode tornar-se impreciso, assim como pode ocorrer um planeamento inadequado da resposta.

Os factores estratégicos, por sua vez, influenciam as escolhas efectuadas pelos operadores em situações de dúvida e de riscos potencialmente elevados. Este tipo de factores surge, geralmente, em situações onde existem múltiplos conflitos de objectivos, escassez de recursos, *timings* apertados, entre outros, estando normalmente associados a conflitos entre o custo e a produtividade. Um exemplo prático desta situação, aplicado à produção de energia nuclear, é o balanço entre o desligar desnecessariamente um reactor e o custo do *downtime* inerente à realização de uma acção preventiva.

Existem ainda situações críticas de decisões relacionadas com o momento em que se deve realizar determinada acção. Por exemplo, um operador tem de decidir realizar uma acção correctiva, logo no início de uma tarefa, baseando-se em informações limitadas ou ainda atrasar a resposta até que estejam disponíveis outras informações que lhe permitam realizar uma melhor análise da situação e, consequentemente, tomar a melhor decisão. Neste ponto, surgem duas situações complicadas de resolver e que têm de ser verificadas caso a caso, medindo-se os prós e os contras de cada decisão. Por um lado, em situações dinâmicas de potenciais consequências (quer a nível de risco, quer também no que se refere a produtividade), o custo de esperar pela existência de novas informações pode ser bastante elevado. Por outro lado, o custo de tomar uma decisão imediata e incorrecta pode também acarretar custos de igual ordem.

Assim, nas decisões que o operador está prestes a tomar, importa considerar os factores estratégicos que são mais prováveis de afectar o desempenho, nos quais se incluem a presença de múltiplos objectivos que interagem entre si e as vantagens e desvantagens de um em relação ao outro, de modo a ser tomada a melhor decisão.

5.3.3.Falhas nas Actividades Cognitivas Humanas

As falhas humanas podem ocorrer em qualquer uma das principais actividades cognitivas descritas em 5.3.1 e quando são requeridos processos cognitivos em qualquer uma delas, a sequência geralmente utilizada pelos operadores para a solução dos problemas tende a assumir os seguintes passos:

1 - Revisão geral iniciada após o disparo de alarmes, sinalizadores ou outros indicadores, dividindo-se a sua atenção entre várias actividades e aquisição de dados;
2 - Escolha de um grupo específico de indicadores e sequente avaliação inicial da situação;
3 - Estruturação dos recursos relativos à atenção para a pesquisa de dados que confirmem a sua hipótese.

No último ponto pode surgir o problema do operador ficar retido na hipótese e assim falhar na observação de mudanças no estado geral do ambiente em que se está a realizar a tarefa ou novos desenvolvimentos. O operador pode inclusivamente tomar conhecimento de mudanças sequentes, embora o processo fique logo dificultado pela atenção que é direccionada para a hipótese inicial e também pelas limitações gerais do processo.

As falhas derivadas de erros cognitivos têm origem nos factores descritos em 3.5, podendo ocorrer em qualquer uma das quatro principais actividades cognitivas.

Deste modo e a nível da monitorização e detecção, o erro mais comum surge da falha em detectar ou observar as indicações das instalações. Este tipo de falha depende da relevância e destaque físico da indicação, da disponibilidade dos recursos da atenção, da prioridade da monitorização em relação a outras actividades, da frequência com que a monitorização da indicação é realizada, entre outros.

A informação escolhida pelo operador para monitorizar é determinada pelo seu modelo da situação, onde a necessidade de uma influência de confirmação o direcciona para a pesquisa de evidências que confirmem a sua hipótese, ao invés das que a negam.

Quanto à avaliação da situação, a falha mais comum é a interpretação incorrecta das observações. Assim, ao observar as indicações, o operador identifica a qualidade da informação, nomeadamente no que diz respeito ao entendimento que ele próprio tem das condições de operação (ambientais, físicas, etc.) e ainda se a informação é a esperada, ou seja, se explica a situação existente. Deste modo, se o operador determinar que a observação é válida e não esperada, inicia uma avaliação da situação até encontrar explicação para as observações. No entanto estas observações podem ter explicações incorrectas da parte dos operadores, uma vez que as avaliações iniciais estão sujeitas a erros que dependem de processos como a recuperação da memória e da avaliação da situação.

Os operadores, em geral, estão mais propensos a procurar por informações consistentes com os seus modelos da situação corrente. Assim, quando se cria uma hipótese para explicar um grupo de indicações, serão explicadas novas indicações em termos de hipótese inicial, ou então serão ignoradas. Uma falha de revisão da avaliação da situação, quando uma nova evidência é introduzida, é designada de erro de fixação.

Relativamente ao planeamento da resposta, a falha que ocorre com maior frequência é o estabelecimento de planos de resposta incorrectos. Para evitar tal facto, o planeamento da resposta deve envolver uma sequência de acções, tais como: estabelecer objectivos e desenvolver um plano de resposta que, por sua vez, deverá permitir identificar e executar os procedimentos predefinidos, assim como verificar se estes estão a atingir os seus objectivos e em caso negativo, deverão ser feitas modificações e adaptações.

As falhas no planeamento da resposta envolvem erros que podem ocorrer em todas as etapas, tais como: percepção inadequada do risco, modelos de situação inadequados, decisões incorrectas, acções fora do tempo, deficiências no conhecimento e outros.

Na implementação da resposta, as falhas que geralmente ocorrem são a nível da execução das acções necessárias à realização das tarefas. Deste modo e, considerando erros casuais de

implementação, assume-se que o operador pretende sempre realizar correctamente as acções, embora devido a um qualquer factor (exemplos: omissões, lapsos de memória, etc.), possa falhar na execução da acção requerida.

5.4. Preparação para Aplicação da Metodologia

A aplicação da metodologia ATHEANA pressupõe a realização de determinadas actividades preliminares, tais como:

- selecção do tipo de análise (retrospectiva, prospectiva ou ambas);
- selecção, formação e treino da equipa multidisciplinar;
- reunir informações básicas;
- planear o uso de simuladores e simulacros.

A metodologia ATHEANA pode ser usada em três tipos de análise: retrospectiva, prospectiva ou a conjugação de ambas.

A análise retrospectiva refere-se à análise de um evento real que ocorreu no sistema, devendo o cenário escolhido para tal conter pelo menos um evento pós-iniciador[10]. Este pode, por sua vez, ter ou não sido modelado na PSA, como um evento de falha humana, embora se não for corrigido possa resultar numa falha funcional e com potencial de risco para o sistema. O objectivo deste tipo de análise é a actualização das bases de dados das PSAs ou das HRAs, assim como descobrir acções correctivas que evitem a sua repetição.

Relativamente à análise prospectiva, o objectivo será dar suporte às análises de eventos pós-iniciadores de falhas humanas, dado que foram esses mesmos eventos que, aquando da realização das análises aos mesmos, representaram as falhas funcionais com maior potencial de risco.

No que concerne à equipa multidisciplinar, a mesma deverá ser formada por indivíduos que possuam um vasto conhecimento e experiência do sistema, devendo ser liderada por um analista de HRA. Deste modo é recomendado na literatura técnica que serve de suporte à metodologia que a equipa inclua, no mínimo, os seguintes membros:

[10] Evento pós-iniciador: evento que contém omissões nas respostas à sequência de eventos após a ocorrência do evento iniciador.

- analista de HRA (será o líder da equipa);
- analista de PSA;
- instrutor dos operadores (com formação em simuladores);
- operador experiente a nível de processos e operação do reactor;
- especialista na área termodinâmica;
- especialista na área de hidráulica.

Esta equipa pode ser completada por outros especialistas, sempre que necessário, podendo mesmo ocorrer a troca de alguns especialistas no caso de se estar a aplicar a metodologia ATHEANA a outro tipo de indústria que não a nuclear.

A formação da equipa envolve a explicação e desenvolvimento dos princípios básicos e processos da metodologia ATHEANA, assim como a familiarização com características comuns dos acidentes mais graves já ocorridos e ainda abordagens ao nível das ciências comportamentais e cognitivas ou outras.

Outro dos pontos fundamentais no processo de preparação para a aplicação da metodologia ATHEANA, tal como acontece noutros métodos de HRA, é a reunião das informações básicas do sistema que possam ser relevantes para a análise, tais como: projecto das instalações/maquinaria, desenhos técnicos, procedimentos, experiência operacional (aqui inclui-se as informações adquiridas pelos operadores e que não costumam ser registadas formalmente), histórico de falhas humanas, de equipamento e de instrumentação, etc. Deverão ainda ser reunidas todas as informações importantes relativas à tarefa e ao objecto da análise, assim como a documentação e os resultados da PSA. Os objectivos desta actividade visam obter a melhor compreensão possível do ambiente de laboração do trabalhador, assim como detectar *a priori* eventuais erros que possam ocorrer (numa visão meramente lata e desprovida de focagem na detecção de erros).

O planeamento e criação de simuladores e simulacros é outra actividade bastante importante na preparação da aplicação da metodologia, uma vez que permite reproduzir eventos e alternativas operacionais que facilitem a identificação de acções inseguras, assim como de mecanismos de erros e PSFs. A observação atenta dos operadores, a sua forma de trabalhar e eventuais considerações que

elaborem, aquando da laboração em simulação, permite tirar informações relevantes para o processo de análise, contendo expectativas, dificuldades, facilidades, riscos, entre outros.

5.5. Análise Retrospectiva

A utilização da análise retrospectiva na metodologia ATHEANA representa uma mudança marcante nas demais metodologias de HRA, uma vez que esta foi projectada para identificar os eventos de falha humana, tal como acontece nas PSAs, além de aferir as suas causas principais.

No processo de desenvolvimento da metodologia (que inicialmente apenas identificava e quantificava acções humanas representadas inadequadamente em análises prospectivas tais como as PSAs), foram analisados vários eventos operacionais de forma padronizada, criando-se para o efeito bancos de dados onde se registavam as informações destas análises. Este procedimento passou a ser incorporado na metodologia, uma vez que se tornou evidente a sua utilidade no desenvolvimento da abordagem prospectiva da ATHEANA.

Como tal, o objectivo deste tipo de análise é a compreensão das causas das falhas humanas em eventos operacionais, que sejam significativas para o risco. Para o efeito o analista deverá fazer o levantamento e registo dos seguintes dados do evento:

- Explicação do sucedido;
- Consequências;
- Causas.

De acordo com os autores do *ATHEANA User's Guide* (Forester et al., 2007), as características mais importantes na análise retrospectiva, aquando da ocorrência de um evento, são:

- Resumo do sucedido;
- Identificação das falhas funcionais;
- *Timeline* dos eventos;
- Resumo das acções humanas mais relevantes e suas causas aparentes;
- Resumo dos PSFs assim como das condições de laboração antes, durante e após o evento;
- Registo dos diagnósticos do evento, representando as condições do sistema e as respostas dadas pelos operadores em função do tempo.

Os resultados destas análises podem ser incluídos nas referidas bases de dados para futura utilização noutras análises, assim como para servir de base à compreensão dos PSFs ou até mesmo para propor medidas correctivas para a redução da probabilidade de ocorrências semelhantes no futuro.

A análise da fiabilidade humana, aquando da realização da análise retrospectiva, deverá ser capaz de identificar os EFCs onde ocorrem as acções inseguras, de modo a estimar a probabilidade de se conjugarem essas condições, assim como as prováveis consequências, quer a nível das acções humanas inadequadas quer na ausência destas. Este processo é interactivo e simultaneamente subjectivo, por se basear em registos reais do evento assim como em possíveis suposições sobre o mesmo e sobre as suas causas.

A análise retrospectiva inicia-se em pleno cenário real, com o intuito de identificar as causas funcionais que se deveram aos comportamentos humanos, examinando todos os dados do evento para descobrir os EFCs. Para o efeito, deverá seguir o seguinte procedimento:

- Identificar o evento;
- Identificar as falhas funcionais, as UAs e os HFEs;
- Identificar as causas das UAs bem como os PSF's e condições das instalações;
- Compilar, documentar e concluir os resultados.

A identificação do evento, perante os vários eventos que decorreram simultaneamente, pressupõe o interesse para o estudo da falha humana. Por essa razão, os eventos de interesse escolhidos para análise possuem, geralmente, as seguintes características:

- Consequências graves ou com potencial de risco bastante elevado;
- A realização da tarefa foi além dos limites desejáveis;
- Houve a necessidade de grandes intervenções dos operadores para o controlo das tarefas.

O agente analista efectuará então uma descrição completa do evento, onde descreverá não só os principais parâmetros do sistema antes e depois do acidente, como ainda deverá identificar problemas e deficiências pré-existentes e os factores inesperados que possam ter surgido.

As falhas funcionais são normalmente modeladas nas PSAs, podendo subdividir-se em falhas de sistema, falhas de função ou falhas de componentes. Um HFE não é mais do que uma falha funcional que resulta de uma ou mais acções inseguras. Estas, por sua vez, são acções que são realizadas indevidamente pelos operadores ou não realizadas quando necessárias, degradando as condições de segurança do sistema. O analista deverá então examinar as informações de modo a identificar as acções humanas realizadas que levaram à ocorrência do HFE. Para tal deverá elaborar uma lista sequencial dos eventos, que não é mais do que uma representação cronológica das condições do sistema, assim como das acções dos operadores, ocorridas desde o início do evento até ao seu fim (estabilização do sistema). As acções dos operadores e, de igual modo, as falhas dos equipamentos que possam de alguma forma ter contribuído para o agravamento ou atenuação das consequências do evento indesejado deverão ser incluídas em tabelas e representados graficamente, sob o formato de uma relação cronológica de acções e falhas ocorridos durante o evento. As acções e os eventos dependentes são extremamente importantes porquanto possuem uma forte influência no EFC, pelo que as dependências entre acções e eventos deverão também ser identificadas e registadas numa tabela própria.

A identificação das causas das UAs, base da análise fundamental da metodologia ATHEANA, é realizada através da identificação das falhas do processamento da informação assim como dos EFCs que, por sua vez, são compostos pelos PSFs e outros factores relacionados com as condições de laboração do sistema.

No que respeita às falhas de processamento da informação torna-se bastante complexo para o analista determinar concretamente o que o operador estava a pensar no momento em que realizou a acção insegura. O analista poderá eventualmente acertar na causa da UA, baseando-se apenas nas condições do sistema no momento da acção insegura, declarações dos restantes trabalhadores ou noutras informações. Assim sendo só as falhas de processamento que sejam evidenciadas pelo comportamento dos operadores é que, em geral, permitem a determinação das causas as UAs.

O analista deverá ainda procurar factores que possam, de algum modo, induzir o operador a cometer um erro. Para o efeito deverá examinar cuidadosamente as informações colhidas sobre o

evento, identificando os PSFs que, quando combinados com as condições do sistema, podem causar mecanismos de erro que permitam a realização de acções inseguras por parte dos operadores. Os PSFs, conforme anteriormente referido, podem ser causados por má/incompleta formação dos operadores, factores organizacionais, procedimentos errados/incompletos, entre outras causas, devendo o analista resumir qual destas teve uma influência mais negativa e mais positiva nas acções mencionadas pelos operadores. Como parte integrante do EFC o analista deverá ainda identificar a condição do sistema que se revele mais significativa, como por exemplo: condições extremas e pouco frequentes de funcionamento, falhas em vários equipamentos em simultâneo ou outras consideradas relevantes.

Na preparação das conclusões o analista deverá agrupar para cada UA as condições do sistema assim como os PSFs que, no seu julgamento, possam ter causado a falha no processamento da informação e que culminaram na realização de uma UA. Deverão ainda ser devidamente documentadas as suas observações, pontos de vista e discussões com os operadores e restantes membros da equipa multidisciplinar, bem como as deficiências encontradas.

5.6. Análise Prospectiva

O objectivo principal da análise prospectiva da metodologia ATHEANA é a identificação dos potenciais erros de comissionamento que possam vir a ocorrer. Este tipo de erros não são analisados pelas restantes metodologias de HRA que se dedicam a quantificar as probabilidades de ocorrência de erros humanos em condições nominais de acidente.

A análise dos eventos ocorridos que serviu de base à metodologia ATHEANA identificou serem os erros humanos mais significativos para o risco fortemente influenciados pelos EFCs, ou seja, pelas condições das instalações e pelos PSFs, razão por que estes contextos são, em geral, diferentes das condições operacionais assumidas pelas PSAs. Assim, a ATHEANA requer um novo modelo de quantificação para tratar dos elementos dos EFCs que vão além do tipo e objectivo do contexto, considerados pelos métodos de HRA anteriores. Mais particularmente, a quantificação das probabilidades dos HFEs correspondentes está baseada em estimativas relativas à maior probabilidade das causas se deverem às condições das instalações e/ou aos PSFs, em vez de estimativas de ocorrência aleatórias de falha humana. Como tal esta abordagem engloba uma

combinação de técnicas de análise que envolvem o julgamento de analistas e operadores experientes, de modo a quantificar a probabilidade de uma classe específica de EFC, assim como a probabilidade da UA, dentro de determinado contexto.

Pelo que este tipo de análise é composto pelas seguintes tarefas essenciais:

- Integração da tarefa na perspectiva da PSA e da metodologia ATHEANA;
- Identificação dos HFEs e das UAs que são relevantes para a tarefa;
- Identificação, através de uma abordagem bem estruturada e controlada para cada HFE ou UA, das razões que determinaram a ocorrência de tais eventos, ou seja, as condições das instalações e os PSFs;
- Quantificação dos EFCs, assim como da probabilidade de cada UA, dado o seu contexto;
- Avaliação do resultado da análise relativamente à tarefa para a qual a análise foi realizada.

A metodologia ATHEANA assume que as UAs mais significativas devem-se à combinação de influências associadas com as condições das instalações assim como a factores específicos centrados no homem e que disparam os mecanismos de erro. Para o efeito, foi desenvolvido um processo de pesquisa e quantificação de EFCs que permite procurar, entre outras coisas, as condições das instalações que possam confundir o operador, levando a que este desenvolva uma avaliação incorrecta da conjuntura, seguindo-se de um planeamento errado da situação e culminando na realização de uma acção insegura. Este processo prospectivo consiste na realização de 10 passos fundamentais, conforme a representação gráfica da Fig. 14.

O objectivo do primeiro passo é definir e interpretar a tarefa devendo para tal proceder à sua descrição, recorrendo a uma linguagem técnica que contenha indicações dos limites e objectivos gerais da análise, assim como a relação com o risco e a PSA, sempre que possível.

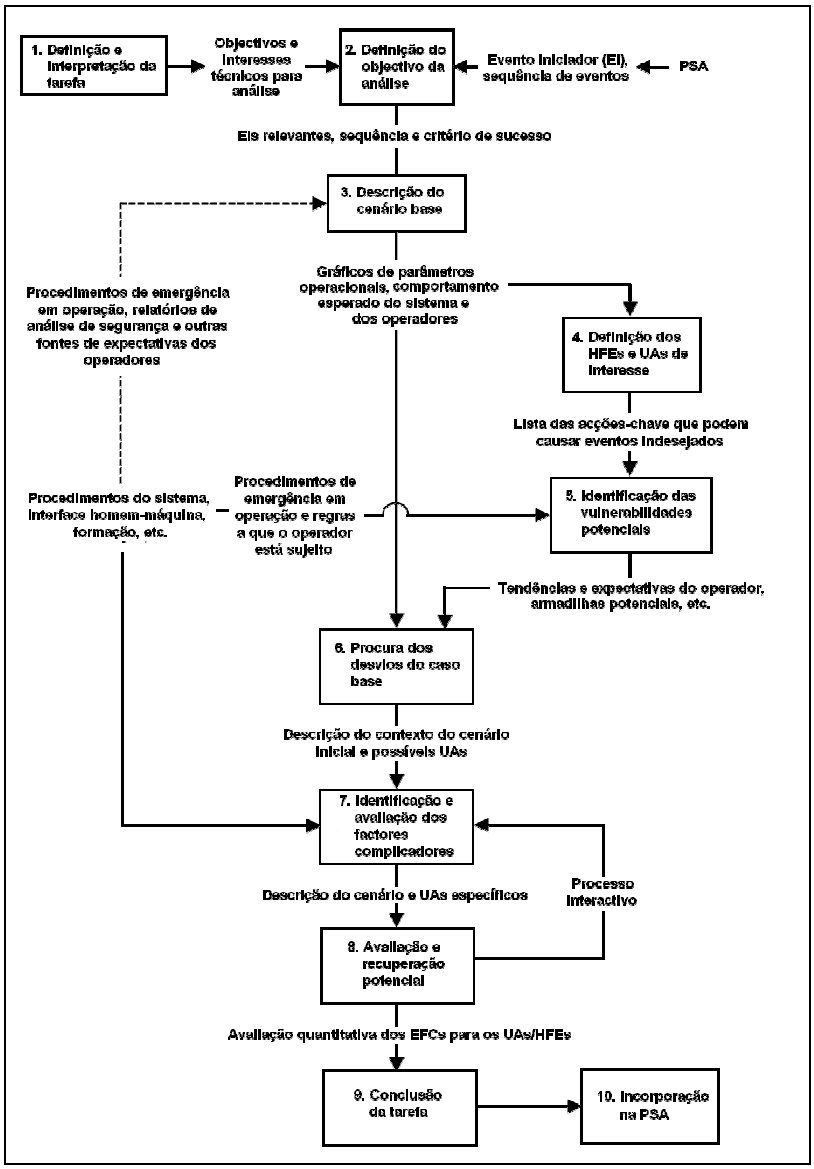

Fig. 14 - Análise Prospectiva da metodologia ATHEANA (fonte: NUREG-1624, Rev. I)

Relativamente ao segundo passo a sua finalidade é limitar o objectivo da análise, através da aplicação da tarefa definida no passo 1 e, se necessário, por razões práticas, definir limites adicionais aos objectivos da análise, recorrendo ao estabelecimento de prioridades das características da sequência do evento. Por sua vez estas prioridades são utilizadas para restringir adicionalmente o objectivo da análise e dirigi-la para os eventos de risco elevado. Embora a metodologia ATHEANA possa ser utilizada noutras aplicações que vão além das PSAs, o processo de estabelecimento de prioridades está baseado nos modelos de PSA específicos da actividade, assim como nos conceitos gerais relevantes para o risco. Portanto, a primeira limitação a considerar deverá ser a selecção da

classe do evento iniciador, assim como o respectivo iniciador associado que se pretende analisar (poderá ser consultado o Anexo D, onde se encontra uma lista genérica das classes de eventos iniciadores e os respectivos iniciadores associados que mais frequentemente podem ocorrer na indústria da produção de energia nuclear). As prioridades dos objectivos serão então consideradas posteriormente para cada evento iniciador seleccionado equilibrando, desse modo, os recursos de análise com as necessidades específicas do projecto.

Deste segundo passo resulta um grupo de eventos iniciadores seleccionados para o qual a tarefa definida no primeiro passo será analisada, fornecendo uma limitação para a análise e delimitando, portanto, um contexto global. Em simultâneo estabelece um relacionamento com a PSA, cujo desenvolvimento das prioridades dos cenários e das funções do sistema serão utilizados nos passos seguintes para orientação da análise.

No terceiro passo e, para o evento iniciador escolhido, será definido e caracterizado o cenário que deverá ter uma descrição realista do comportamento do sistema assim como dos seus intervenientes, em relação à tarefa e ao evento iniciador. Este comportamento irá fornecer uma base de dados de onde serão posteriormente (no sexto passo) identificados e definidos os desvios de tais expectativas. O cenário ideal deverá ser definido de acordo com a árvore de decisão representada na Fig. 15.

Desta forma, o cenário ideal deverá ser bem entendido pelos operadores e reunir o consenso destes, devendo para tal ser bem definido e regulado por procedimentos, formação técnica especializada e treino operacional (real ou através de simuladores). Será também importante fazer uma boa documentação do cenário e de eventuais problemas deste, através da realização de descrições amplas baseadas em relatórios de, por exemplo, PSAs. Deverão estar igualmente bem definidos e documentados princípios físico-químicos tais como física quântica, física nuclear, termodinâmica, hidráulica ou outros que se deva considerar.

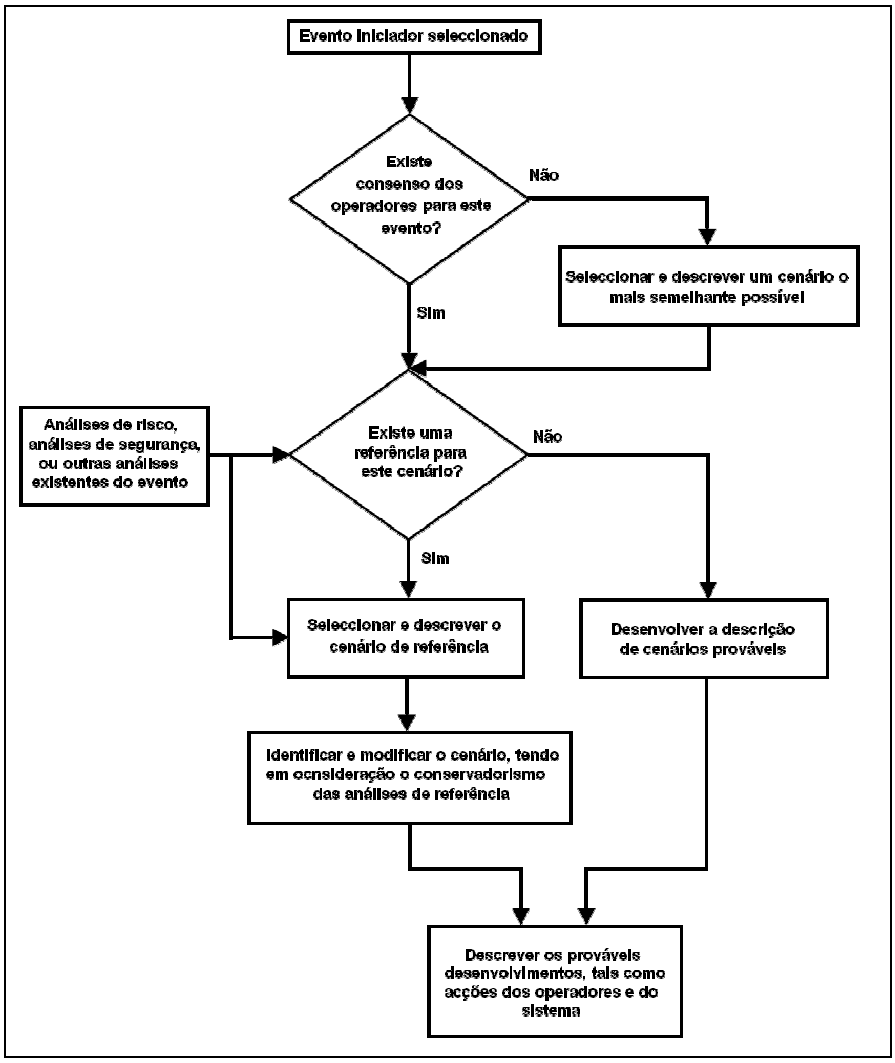

Fig. 15 - Árvore de decisão para definição do cenário ideal (fonte: NUREG-1624, Rev. I)

Deste terceiro passo resulta portanto uma descrição completa do cenário a ser analisado, baseado num modelo de consenso dos operadores, juntamente com informação recolhida de análises relevantes. Posto isto, a descrição do cenário ideal deverá incluir:

- Condições iniciais assumidas das instalações;
- Descrição geral da sequência de eventos esperada;
- Lista das causas previamente assumidas do evento iniciador;
- Descrição detalhada da sequência cronológica esperada;
- Descrição detalhada dos principais parâmetros funcionais do sistema, assim como da resposta dos vários sistemas e equipamentos;

- Trajectória esperada dos principais parâmetros registados no tempo;
- Principais acções esperadas pelos operadores durante as operações.

No quarto passo, através duma análise cuidada, irão ser definidos os HFEs e as UAs, embora já no primeiro passo possa ter ficado definido algum deles como sendo relevante para a análise. É ainda de considerar que com a progressão da análise prospectiva poderão ser identificados novos HFEs e UAs, voltando-se novamente a este passo sempre que haja necessidade. Se tal acontecer e, mesmo sendo especificado pela ATHEANA que primeiro são identificados os HFEs e só depois as UAs, bastará apenas rever só uma destas identificações.

Se por um lado um HFE é um termo específico das PSAs, requerendo conceitos das mesmas para a sua definição, já a UA não se encontra especificamente ligada às PSAs, embora faça a ponte entre o comportamento humano e estas.

A metodologia ATHEANA fornecesse assim um processo sistematizado e constituído por 7 tarefas que tem por objectivo a identificação dos HFEs:

1 - Definição do tipo de tarefa, de acordo com os requisitos de resposta do acidente para o evento iniciador ou para a sequência específica:
    a – necessária;
    b – indesejada.
2 - Identificação dos equipamentos/sistemas que realizam determinada função;
3 - Identificação da situação do evento pré-iniciador dos equipamentos/sistemas;
4 - Definição do critério de sucesso funcional para os equipamentos/sistemas;
5 - Identificação dos modos de falha funcionais dos equipamentos/sistemas;
6 - Definição de quais os erros (erros de comissionamento, erros de omissão ou ambos) que são mais relevantes para a tarefa seleccionada;
7 - Identificação, de entre as descrições aplicáveis, das UAs que possam ser consideradas "candidatas" para a descrição dos HFEs.

Para a realização dos passos acima identificados utilizam-se as tabelas que constam do Anexo E e que foram retiradas da obra de referência da metodologia (NUREG-1624, Rev. 1). Da mesma forma e para a identificação dos HFEs recorre-se à Tabela 6, onde o modo de falha funcional

é transformado numa categoria do modo de falha funcional. Este último, por sua vez, é utilizado na Tabela 7, onde se conjuga com a descrição da falha humana no sistema ou equipamento (recorrendo-se na maioria dos casos a aproximações), para se transformar num novo código correspondente à falha humana identificada. Este último código será depois utilizado nas restantes tabelas (Tabela 8, Tabela 9, Tabela 10, Tabela 11 e Tabela 12), permitindo diferentes combinações de tipos de erros (EOOs e EOCs), tipos de falhas dos sistemas/equipamentos (arrancar/parar, manual/automaticamente), falhas em acções de recuperação e modos de operação (activos/passivos), para identificar a UA que causou o HFE estudado.

Algumas destas tarefas podem já ter sido realizadas em passos anteriores e/ou até mesmo, em casos específicos, não haver necessidade de virem a ser realizadas. Por exemplo, se no passo 1 já tiver sido definido um modo de falha funcional, ou mesmo a UA, não há necessidade de se realizarem os restantes passos, conforme aqui descrito. Nesses casos, a obra de referência fornece uma tabela simplificada para consulta directa onde se consegue identificar a UA (através da sua descrição), recorrendo apenas ao modo de falha funcional, conforme se pode ver na Tabela 13.

Deste quarto passo resultará então uma lista dos vários HFEs e respectivas descrições que se considerem relevantes para a tarefa e/ou para as árvores de eventos das PSAs, assim como das UAs associadas a cada HFE identificado.

No quinto passo encontramos as vulnerabilidades potenciais no conhecimento básico do operador em relação aos eventos iniciadores ou cenários de interesse (que podem resultar dos HFEs ou UAs identificados no passo anterior), funcionando como passo preliminar para as pesquisas dos desvios do cenário-base que serão identificadas nos passos seguintes. Estas vulnerabilidades podem advir tanto das implicações geradas pelas expectativas dos operadores como de factores-surpresa associados a estas e inerentes ao evento iniciador e/ou ao cenário-base. Estes factores-surpresa, podem ser identificados através de quatro etapas:

1 - Investigação das potenciais vulnerabilidades nas expectativas dos operadores em relação aos eventos iniciadores/cenários-base;
2 - Estudo e compreensão da cronologia do cenário-base e das dificuldades inerentes;
3 - Identificação das tendências das acções dos operadores e de regras informais;
4 - Avaliação das regras formais e dos procedimentos de emergência que se espera serem utilizados em resposta ao cenário.

O sexto passo tem por objectivo a identificação, através de uma pesquisa bem definida e estruturada, dos desvios do cenário-base (desvios físicos reais no comportamento e nas condições das instalações) que possam ocorrer e que podem resultar em UAs, aumentando assim os níveis de risco associados à tarefa em causa. Estes desvios acontecem porque os eventos sérios nunca ocorrem exactamente nos cenários-base descritos nas PSAs, pelo que a sua identificação é extremamente importante.

A realização deste passo pressupõe a elaboração de quatro tipos de pesquisas para identificar as características que estão presentes nos cenários ditos "divergentes":

1 - Pesquisa dos desvios físicos em relação ao cenário-base, através da utilização de palavras-guia, tal como acontece na metodologia de avaliação de risco HAZOP (ver Anexo F). É efectuada a identificação e definição de como os cenários reais se podem desviar do cenário-base e, desse modo, causar complexidades que podem contribuir para os EFCs;
2 - Identificação e avaliação das decisões-chave relacionadas com procedimentos formais e respeitantes aos possíveis desvios determinados na primeira pesquisa;
3 - Pesquisa de dependências entre sistemas de suporte, de segurança e operacionais;
4 - Pesquisa de tendências dos operadores e tipos de erros que correspondam aos HFEs e aos UAs mais relevantes para estudo.

No sétimo passo continua a definir-se o EFC iniciado no passo 6. Para tal, deverão ser tidos em linha de conta os PSFs e condições físicas adicionais. Assim, se o contexto identificado no passo 6 for considerado suficientemente forte (definido pelos desvios físicos), então apenas os PSFs gerados por este contexto serão identificados neste passo. Por outro lado, se o contexto identificado no passo anterior requerer factores adicionais, tanto os PSFs como as condições das instalações serão identificados.

Existem dois tipos de PSFs que podem ser incluídos no cenário divergente inicialmente definido no passo anterior:

- PSFs gerados pelo contexto identificado no passo 6, que incluem os relacionados com as condições específicas das instalações e ainda os asssociados aos mecanismos de erro (descritos na literatura de referência - NUREG-1624, Rev1);

- PSFs adicionais que não são especificos do contexto, ou seja, que não estão relacionados com as condições específicas das instalações, como é o caso dos procedimentos, factores organizacionais, *stress*, condições ambientais ou outros.

Tal como a inclusão dos PSFs, poderão também ser incluídas mais condições físicas no EFC inicial, identificado no sexto passo reduzindo, eventualmente, a probabilidade ou frequência dos HFEs. Assim, deverão ser considerados os seguintes tipos de condições adicionais:

- indicações de falhas;
- falhas adicionais de equipamentos;
- condições das instalações que possam confundir os operadores;
- outros factores que por norma não são considerados nas PSAs.

A avaliação e inclusão destas condições físicas adicionais no cenário original identificado no sexto passo é realizada com recurso a tabelas fornecidas pela literatura de referência (US NRC, 2000).

Caso efectivamente se verifique a introdução destes novos elementos, a descrição do cenário divergente inicial deverá ser revista para reflectir estas novas considerações. Particularmente, os PSFs e/ou as novas condições das instalações deverão ser integrados na descrição do cenário, uma vez que podem activar mecanismos de erros diferentes ou adicionais.

O sétimo passo, em suma, permite que se tenha um EFC suficientemente forte para fazer os cálculos das probabilidades dos HFEs e das UAs pretendidos.

No oitavo passo serão completadas as definições dos HFEs e dos EFCs associados, tendo em consideração as oportunidades de recuperação dos erros iniciais. Este passo tem interactividade com os passos 6 e 7, uma vez que envolve a extensão do contexto definido nesses passos. Assim e, no decorrer da análise, se for garantido que um HFE pode ser recuperado, pára-se a análise e passa-se imediatamente para a solução da tarefa. Caso isto não ocorra, continua-se de acordo com a análise.

A análise deve ter em consideração que existe para correcção com sucesso de um determinado erro inicial. Para efectuar a avaliação que permita a análise de acções de recuperação potencial deverão ser tidos em consideração os seguintes elementos:

- Definição de uma possível acção de recuperação, caso a UA e/ou o HFE já tenham sido realizados;
- Tempo disponível para realizar as acções de recuperação, de modo a evitar consequências mais graves;
- A existência e o tempo em que se deram os sintomas adicionais que podem alertar os operadores para a necessidade de recuperação, assim como podem fornecer informações suficientes para a identificação das acções de recuperação aplicáveis;
- Avaliação da intensidade dos sinais da necessidade de recuperação, tendo em consideração o EFC inicial, ou seja, os PSFs e as condições das instalações que, consequentemente, permitem obter a probabilidade de sucesso da recuperação.

Considerando o atrás descrito, deve decidir-se quais as acções de recuperação necessárias assim como determinar o tempo necessário para as suas recuperações, antecipando desta forma a ocorrência de danos indesejáveis. Deverá, posteriormente, ser desenvolvida uma progressão do cenário divergente que começará na perda inicial ou na degradação de função ou de equipamentos de segurança. O registo desta progressão deverá destacar as mudanças previstas nas condições e principais parâmetros do sistema, assim como qualquer novo sinal que possa surgir, o que irá permitir definir mais tarde os elementos contextuais adicionais que estarão associados a uma situação de não recuperação.

O tempo, por seu lado, também é um factor fundamental uma vez que pouco ou nenhum tempo disponível para a correcção, desde o erro inicial, reduzirá enormemente as hipóteses de uma recuperação bem sucedida. Caso o tempo seja suficiente deverão ser tomadas em consideração as dependências que possam existir entre o EFC da UA e a falha em corrigir a acção inicial.

Quaisquer novos elementos do EFC que estejam associados às acções de recuperação deverão ser acrescentados no EFC da UA inicial, de modo a completar o EFC para o HFE, que será modelado na PSA.

Deverá ainda comparar-se o contexto do EFC desenvolvido neste passo com as características de acidentes graves (devendo, obviamente, comparar-se as situações parecidas, isto é, mesmo tipo de indústria, cenários semelhantes, etc), assim como com os factores complicadores que não sejam frequentemente modelados nas PSAs. A obra de referência *NUREG-1624* (US NRC,

2000) fornece tabelas que identificam alguns desses factores complicadores, permitindo uma comparação mais correcta.

Deste oitavo passo resulta um EFC, totalmente finalizado, para determinação das probabilidades dos HFEs e as UAs de interesse.

No nono passo realiza-se uma análise quantitativa dos EFCs e das UAs para a incorporação na PSA (10º passo). Para o efeito esta análise quantitativa pressupõe a realização de três processos independentes, embora relacionados entre si:

- Determinação da probabilidade do EFC num cenário específico;
- Determinação da probabilidade das UAs, condicionadas a este contexto, que podem causar os HFEs;
- Determinação da probabilidade de que estas UAs não serão recuperadas antes que uma falha catastrófica ocorra.

A quantificação do EFC é normalmente realizada tendo por base a árvore de eventos da PSA, para um determinado evento iniciador, calculando-se a probabilidade de ocorrência do EFC (onde poderia ocorrer a UA), da UA e da falha na sua recuperação.

O EFC, conforme foi atrás exaustivamente demonstrado, é constituído por dois elementos diferentes, embora fortemente dependentes entre si: PSFs e as condições das instalações. Estes dois elementos são quantificados em separado para, uma vez juntos, permitirem a determinação da probabilidade total do EFC. Deverão assim ser reunidas várias informações específicas das instalações e relativas ao EFC estudado, tais como:

- probabilidade dos PSFs específicos (definida nos passos 6 e 7);
- probabilidade de falhas de equipamentos, instrumentos e indicadores;
- probabilidade de falhas dependentes de múltiplas peças de equipamentos, instrumentos e indicadores;
- indisponibilidade de equipamentos, instrumentos e indicadores por paragens relativas a testes e manutenções;
- frequência do evento iniciador;
- frequência de certas condições das instalações dentro de um determinado tipo de evento iniciador;

- Outras.

Estas informações irão depender dos elementos dos EFCs identificados no processo de pesquisa, podendo obter-se de quatro modos distintos:

- Retiradas directamente das instalações;
- Utilizando cálculos de engenharia (podendo alguns estarem já disponíveis para outras aplicações como é o caso da própria PSA);
- Recorrendo ao julgamento qualitativo e quantitativo de especialistas;
- Realizar entrevistas junto dos operadores, cuja experiência e conhecimento podem permitir obter informações necessárias à quantificação (normalmente utilizado quando não existem dados disponíveis para gerar as frequências e probabilidades necessárias).

Relativamente aos PSFs e conforme anteriormente se constatou, existem os motivados pelo contexto do cenário divergente e os que são genéricos. Quanto aos primeiros e na grande maioria dos casos, a probabilidade de ocorrência é de 1,0. Contudo, existem cenários em que os PSFs são apenas aplicáveis a determinadas condições existentes. Para estas situações e caso a frequência ou a probabilidade destas condições poderem ser determinadas, então os PSFs poderão ser avaliados. No caso dos PSFs genéricos que são específicos das instalações deverá verificar-se primeiro se existe alguma condição das instalações que possa tornar esses PSFs mais prováveis de ocorrer. Caso existam, a sua inclusão no EFC deverá ser considerada, de acordo com os moldes e procedimentos descritos nos passos 6 e 7. Para os PSFs que não têm qualquer relação com as condições das instalações deverão ser consultados os operadores para que, com as observações obtidas a partir destes, se possam determinar as probabilidades. Deverá ainda procurar identificar-se os PSFs cujas influências aumentam a probabilidade de ocorrência de EFCs e de UAs. Em suma, a inclusão destes PSFs permitirá reduzir a probabilidade do EFC, mas certamente aumentará também a probabilidade da UA.

A quantificação das UAs para determinação da probabilidade deverá ter em consideração os seguintes tipos de condições:

- O EFC é tão forte que a ocorrência da UA é praticamente certa;

- Comparado com o contexto normal da PSA, o EFC é mais fraco, o que não permite o aumento da probabilidade da UA;
- A influência do EFC é variada, pelo que a probabilidade de ocorrência da UA pode recair em qualquer ponto entre os extremos do intervalo probabilístico.

Para estimar as probabilidades das UAs deverão ser primeiramente realizadas estimativas das UAs que não requeiram elevado nível de precisão. Assim e no caso em que o EFC é tão forte que a UA é quase certa, a probabilidade de ocorrência pode ser estimada em 0,5. Esta probabilidade pode ser aplicada nos casos onde o contexto que se apresenta ao operador leva-o a crer que a UA é a acção mais correcta a realizar, perante as circunstâncias. No caso em que o EFC é tão fraco que não permita o aumento da probabilidade de ocorrência da UA, o *NUREG-1880* (Forester et al., 2007) recomenda a utilização dos métodos tradicionais de HRA que não são dirigidos a erros causados por EFCs. Na prática, ao não forçarem significativamente o erro, estas condições podem ser identificadas e eliminadas aquando das avaliações realizadas nos passos 6 e 7 anteriormente descritos. No terceiro caso, em que a maioria dos contextos irá cair entre os extremos citados, existem duas possibilidades para as estimativas da probabilidade da UA:

- Os instrutores de operadores experientes observam, durante o treino e formação, a ocorrência de situações semelhantes às condições do sistema, verificando ainda que há uma fracção relativamente grande de operadores que executou excatamente as mesmas UAs, sendo estas modeladas;
- Situações que requerem estimativas da probabilidade da UA, usando métodos de modelação.

A situação desejável é aquela em que estes instrutores possam fornecer o seu julgamento como complemento relevante para a quantificação da UA.

A mesma fonte recomenda que para estimar as probabilidades de ocorrência das UAs deverão ser utilizadas duas abordagens distintas, de entre as várias existentes. Em ambas será efectuado um julgamento sobre o quão intenso pode ser o EFC, realizando-se numa escala de pontos extremos da faixa de valores de probabilidade. Assim, numa extremidade a probabilidade é igual a 1,0 enquanto que na outra corresponde ao valor estimado da probabilidade de erro humano, calculado pelas metodologias tradicionais de HRA que considera, pelo menos, algumas contribuições mínimas de

contextos negativos. Deste modo e para a quantificação da UA, é importante estimar onde está a influência exercida pelo contexto, tal como se observa na Fig. 16.

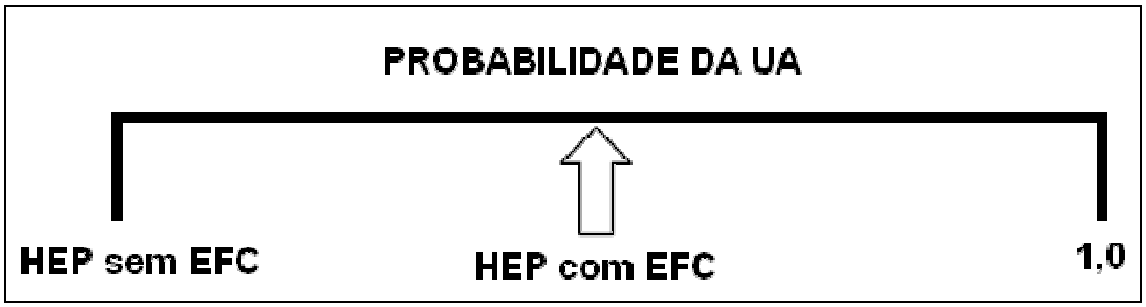

Fig. 16 - Estimativa da probabilidade da UA

Considerando o anteriormente mencionado, torna-se importante referir que não existe um método único e absoluto para realizar o dito julgamento, sendo o mais importante a explicação das bases da avaliação, os factores considerados importantes (e respectiva justificação), assim como o grau de precisão das metodologias.

Pelo que se infere ser a HEART (resumida em 4.4) a metodologia mais utilizada e aquela que fornece uma base mais sólida para avaliar o grau segundo o qual o contexto influencia a probabilidade de falha. Numa breve revisão, esta metodologia consiste em identificar numa tabela (ver Tabela 3) a descrição genérica da actividade que mais se aproxima do contexto da acção que se está a analisar, aplicando-se de seguida um factor multiplicador (ver Tabela 4) que corresponde ao PSF, de modo a ajustar a probabilidade.

A segunda metodologia mais utilizada é a SLIM, método que determina um índice de probabilidade de sucesso e cuja aplicação na ATHEANA implica a resposta às seguintes questões:

- Atendendo ao contexto, qual é a probabilidade de geração dos mecanismos de erro?
- Uma vez gerados os mecanismos de erro, qual é a probabilidade de ocorrer uma UA?
- Ocorrida a UA, qual é a probabilidade de que esta levará a um HFE?

Conforme foi referido no passo 6, os PSFs e as condições das instalações estão associados com os mecanismos de erro, aquando do desenvolvimento do cenário divergente. Deste modo, quanto mais negativos forem os PSFs e as condições das instalações existentes num determinado cenário, mais provável será a ocorrência de mecanismos de erros e, potencialmente, de UAs. Perante isto, torna-se importante definir quais os PSFs e as condições das instalações associados a um

determinado mecanismo de erro que são mais importantes, assim como o grau para o qual estes PSFs existem no cenário em análise. Posteriormente realiza-se a avaliação da probabilidade da UA, dada a ocorrência do mecanismo de erro, recorrendo novamente à escala de graduação do SLIM.

O processo de avaliação culmina com o cálculo da probabilidade de que a UA perdurará até ao HFE. Neste processo serão realizadas várias actividades de recuperação que podem evitar a continuidade da UA até um determinado ponto crítico, tais como: ocorrência de alarmes ou outras indicações que se seguem à UA e que podem levar ao levantamento de questões relacionadas com a acção realizada ou não realizada, oportunidade de novas equipas questionarem o que está a ocorrer, eventuais alterações posteriores que se possam realizar nas instalações, de modo a obter novos alarmes e indicações, entre outros.

Torna-se então necessária uma detalhada avaliação do tempo restante da sequência do acidente, assim como dos sinais, das informações e do modo como estas serão avaliadas em relação aos mecanismos de erros iniciais e à UA resultante, de maneira a analisar as oportunidades que cada uma das actividades de recuperação tem em levar a uma efectiva recuperação da UA e, consequentemente, ao fim da sequência do acidente.

Resumindo o nono passo, as probabilidades das UAs são estimadas de três maneiras distintas utilizando-se para o efeito estratégias diferentes para cada caso. Num primeiro caso, em que a probabilidade de ocorrência da UA é praticamente certa, a literatura de referência recomenda que se utilize a incerteza na faixa de 0,5 a 1,0. No segundo caso, em que os operadores têm uma grande experiência e treino em cenários semelhantes, nos quais uma relativamente grande fracção da equipa realiza uma UA relevante, são registadas informações com o número de equipas que foi avaliada, assim como o número de vezes que realizaram a UA. Estes dados serão posteriormente utilizados para desenvolver uma distribuição de incertezas. No caso de um grupo de operadores experientes fornecerem estimativas e não existirem dados registados, então existe um processo que permite gerar uma distribuição de incertezas baseada na estimativa colectiva.

No décimo e último passo, são finalmente incorporados os HFEs nas PSAs, utilizando as designadas árvores de eventos. Tal acontece, uma vez que os HFEs definidos pela ATHEANA são considerados de máxima prioridade por tenderem a levar directamente para o resultado mais indesejável (que, no caso da indústria nuclear, é o dano no núcleo dos reactores). Os HFEs devem

ser definidos de modo a capturar os EOCs (considerados de prioridade superior) e os EOOs que não foram tidos em consideração no presente processo de PSA o que pode, no global, causar efeitos indesejáveis.

Na árvore de eventos, o local específico onde está representado o HFE identificado pela metodologia ATHEANA dependerá do modo como este se relaciona cronologicamente com as funções e sistemas envolvidos na resposta ao evento iniciador. A sua inclusão fornecerá a análise mais eficiente de todas as sequências possíveis representadas na árvore de eventos, assim como a dependência lógica dos outros eventos para com o HFE na sequência. Caso o sucesso ou falha na sequência altere significativamente o tratamento do HFE incorporado (por exemplo, através do fornecimento de novas indicações para as acções), a árvore de eventos poderá necessitar de incluir vários HFEs semelhantes. Contudo, a definição e/ou quantificação destes pode ser diferente devido às possíveis diferenças no tempo, estado do sistema, entre outras razões.

Com a incorporação da metodologia ATHEANA na árvore de eventos, poderá esperar-se a eliminação de algumas falhas funcionais causadas por falhas humanas e modeladas como erros pós-iniciadores, nas árvores de falhas das PSAs. Tal pode ocorrer, uma vez que os HFEs identificados pela ATHEANA incluem, por definição, os EOOs, correntemente incluídos nas árvores de falhas, embora alguns HFEs pré e pós-iniciadores, relacionados com equipamentos bastante específicos, possam permanecer nas árvores de falhas.

Tal como acontece nas árvores de falhas, alguns dos eventos de recuperação podem ser eliminados quando os HFEs identificados pela ATHEANA forem largamente definidos, de modo a incluir falhas na recuperação do erro original. Contudo, todas as possíveis considerações de recuperação podem não ser evidentes até à obtenção da solução inicial da ATHEANA, podendo ainda haver a necessidade de aplicar alguns dos eventos de recuperação.

Deste 10º passo conclui-se que o processo de incorporação dos HFEs identificados pela ATHEANA pode reduzir o número total de diferentes HFEs nas PSAs, bem como o número de vezes que múltiplos HFEs aparecem numa mesma sequência, dado o grau de definição utilizado na identificação destes. Quando a eliminação total dos múltiplos HFEs da mesma sequência não acontece deverá ser utilizada a mesma propriedade de dependências entre HFEs, na sequência final, recorrendo ao auxílio das actuais técnicas e métodos de HRA e PSA.

6. CONCLUSÕES

Tendo como tema principal a Fiabilidade Humana, muitos outros assuntos pertinentes foram abordados nesta tese de mestrado que, no seu global, permitiram desenvolver um estudo mais complementar e directo sobre o escopo da temática central.

Assim, urge concluir que a fiabilidade humana, embora muitas vezes esquecida em detrimento da fiabilidade de máquinas e equipamentos é, acima de tudo, um factor fundamental na fiabilidade de qualquer sistema homem-máquina. Cada vez mais se observa uma crescente inclusão deste factor nas várias indústrias sendo, a par da fiabilidade de equipamentos, um dos factores preponderantes na determinação da fiabilidade geral de sistemas. Muitas das vezes e, embora sejam considerados directamente os factores humanos do ponto de vista de análises cognitivas, experiência laboral, etc., os sistemas surgem dimensionados tendo em consideração a interacção homem-máquina. Assim, aspectos ergonómicos são desenvolvidos em prol da segurança e eficiência dos sistemas homem-máquina o que, em geral, permite aumentar a fiabilidade humana e, consequentemente, a fiabilidade geral dos sistemas.

Na indústria da produção de energia nuclear, por ser uma indústria onde os erros podem ser extremamente graves no que respeita à segurança de milhares, senão mesmo de milhões de pessoas, o estudo dos factores humanos foi bastante desenvolvido, o que levou à criação de várias metodologias de análise da fiabilidade humana (HRA). Estas metodologias, embora diferentes a nível de processos e precisão de resultados, têm tido um contributo bastante positivo no que respeita à prevenção de acidentes laborais na indústria de produção de energia nuclear, assim como em várias outras indústrias. Contudo, importa referir que muitas das HRAs estão sujeitas a julgamentos de peritos (*experts*) que variam de pessoa para pessoa, permitindo considerações completamente diferentes, o que influencia a avaliação real da fiabilidade humana. Conclui-se assim que, não só a fiabilidade humana é difícil de determinar como está, inclusivamente, sujeita a erros, também eles humanos, dos referidos julgamentos.

Relativamente à metodologia estudada, ATHEANA, conclui-se que esta marcou um importante avanço no aprimoramento da análise e avaliação da fiabilidade humana, uma vez que tem em consideração os contextos nos quais os operadores estão inseridos, enquanto possuidores de características que podem proporcionar a ocorrência de falhas humanas. Conclui-se ainda que esta

metodologia não substitui os métodos tradicionais de HRA, que tratam dos erros de omissão, actuando como um complemento que se ocupa dos erros de comissionamento, tendo sido criada para preencher essa lacuna. No que respeita à sua abordagem quantitativa, esta difere significativamente das outras metodologias de HRA, uma vez que enquanto estas estimam a probabilidade de ocorrer um erro humano aleatório, em condições nominais de acidentes (ou sob outras condições especificadas nas árvores de eventos e árvores de falhas das PSAs), a ATHEANA avalia a probabilidade de uma classe específica de EFCs dentro de uma larga faixa de condições alternativas que podem existir na definição de um cenário e, desse modo, avaliar a probabilidade condicional de uma UA ocorrer, dada a existência desse contexto.

Ainda no que respeita à metodologia estudada, espera-se que o seu desenvolvimento não seja tão alargado no tempo, como ocorreu com as metodologias de primeira geração, dado que cada vez mais são desenvolvidos estudos, testes e experiências nesta área científica. Espera-se ainda que o desenvolvimento não seja impulsionado por falhas catastróficas, como aconteceu em *Three Mile Island* e *Chernobyl*, mas sim pelo bom senso e cultura de segurança que devem prevalecer, aliados aos avanços tecnológicos, em prol da segurança necessária em indústrias consideradas de risco.

Em geral, o estudo das ciências cognitivas ultrapassa o âmbito da engenharia mecânica, embora confira uma total integração de conhecimentos, que permite outras abordagens aos sistemas homem-máquina. Enquanto que o engenheiro mecânico, vocacionalmente, está mais direccionado para o bom funcionamento dos equipamentos (através do conhecimento profundo que detem destes), o conhecimento dos factores humanos, assim como dos mecanismos de erro, análises e técnicas para a prevenção de falhas humanas, dota o profissional de uma capacidade de análise ímpar, em todos os componentes/fases do sistema homem-máquina.

A nível particular, o conhecimento adquirido aquando da realização deste trabalho científico é para mim uma mais-valia a nível pessoal e, acima de tudo profissional, uma vez que, inevitavelmente, estarei mais apto para identificar os meus erros e os dos outros, assim como para avaliar as causas de determinadas falhas e calcular a fiabilidade humana relativa a certas acções/tarefas. Serei certamente um profissional mais esclarecido nesta área o que, indiscutivelmente, a par de um maior enriquecimento humano, poderá contribuir em muito para aumentar os meus índices de produtividade, independentemente da função profissional que desempenho ou que possa vir a desempenhar futuramente.

REFERÊNCIAS

Bibliografia

Barriere, M. T., Wreathall, J., Cooper, S. E., Bley, D. E., Luckas, W., Ramey-Smith, A. M. (1995). Multidisciplinary framework for human reliability analysis with an application to errors of Commission and dependencies. NUREG/CR-6265. Washington, DC, U.S. Nuclear Regulatory Commission.

Baysari, M. T., Caponecchia, C., McIntosh, A. S., Wilson, J. R. (2009). Classification of errors contributing to rail incidents and accidents: a comparison of two human error identification techniques. In: *Safety Science*, Vol. 47, issue 7, Aug. 2009, pp. 948-957.

Benedetti, J. L. (2006), Como intensificar a confiabilidade humana em sistemas aéreos e industriais. Trabalho de conclusão do Curso da Ciência da Computação da Faculdade de Jaguariúna, Brasil.

Blackman, H. S., Gertman, D. I., Boring, R. L. (2008). Human error quantification using performance shaping factors in the SPAR-H Method. In: *52nd Annual Meeting of the Human Factors and Ergonomics Society*, New York, September 22-26, 2008.

Blackman, H. S., Gertman, D. I., Boring, R. L. (2008). Human error quantification using performance shaping factors in the SPAR-H method. In: *Human Factors and Ergonomics Society Annual Meeting Proceedings*, Vol. 52, nº 21, 2008, pp. 1733-1737

Blashe, K. M., Shrivastava, A. B., (1994). Defining failure of manufacturing and equipment. In: *Proceedings of the Annual Reliability and Maintainability Symposium*, Anaheim, CA, January 24-27, 1994, pp. 69-75.

Bley, D. C., Cooper, S. R., Forester, J. A., Kolaczkowski, A. M., Ramey-Smith, A., Thompson, C. M., Whitehead, D. W., Wreathall, J. (1999). Philosophy of ATHEANA. Albuquerque, NM, Sandia National Laboratories

Blischke, W. R., Murthy, D. M. P. (2000). Reliability: Modeling, Prediction, and Optimization, Wiley series in Probability and Statistics, New York, John Wiley & Sons.

Boring, R. L. (2006). Modeling human reliability analysis using MIDAS. In: *International Workshop on Future Control Station Designs and Human Performance Issues in Nuclear Power Plants*, Halden, Norway, May 8-10, 2006.

Boring, R. L., Gertman, D. I., Joe, J. C., Marble, J. L. (2005). Human reliability analysis in the U.S. nuclear power industry: a comparison of atomistic and holistic methods. In: *Proceedings of the 49th Annual Meeting of the Human Factors and Ergonomics Society*, Portland, Oregon, April, 2-7, 2005, pp.1815-1819..

Cĕpin, M. (2008a). Comparison of methods for dependency determination between human failure events within human reliability analysis. In: *Science and Technology of Nuclear Installations*, vol. 2008

Cĕpin, M. (2008b). DEPEND-HRA—A method for consideration of dependency in human reliability analysis. In: *Reliability Engineering and System Safety*, vol. 93, issue 10, Oct. 2008, pp. 1452–1460.

Cĕpin, M. (2008c). Importance of human contribution within the human reliability analysis (IJS-HRA). In: *Journal of Loss Prevention in the Process Industries*, vol. 21, nº 3, pp. 268–276.

Collier, S. (2003). A simulator study of CREAM to predict cognitive errors. In: *Proceedings of the International Workshop on Building the New HRA: Errors of Commission from Research to Application, Rockville, 7-9 May 2001*. Washington, DC.

Cooper, S. E., Ramey-Smith, A. M., Wreathall, J., Parry, G. W., Bley, D. C., Luckas, W. J., Taylor, J. H., Barriere, M. T. (1996). A Technique for Human Error Analysis (ATHEANA): technical basis and methodological description. NUREG/CR-6350. Washington, DC, U.S. Nuclear Regulatory Commission.

Cox, S. J., Tait, N. R. S. (1998). Reliability, safety & risk management: an integrated approach, 2nd ed., Oxford, Butterworth-Heinemann.

Dhillon, B. S. (2007). Human reliability and error in transportation systems. London, Springer.

Drouin, M., Parry, G., Lehner, J., Martiniz-Guridi, G., LaChance, J., Wheeler, T. (2009). Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making: Main Report, NUREG-1855, Vol. 1. Washington, DC, U.S. Nuclear Regulatory Commission.

Embrey, D. (2000a). Data collection systems. Human Reliability Associates.

Embrey, D. (2000b). Performance influencing factors.Human Reliability Associates.

Embrey, D. (2000c). Preventing human error: developing a consensus led safety culture based on best practice. Human Reliability Associates.

Embrey, D. (2000d). Task analysis techniques. Human Reliability Associates.

Embrey, D. (2000e). Understanding human behaviour and error. Human Reliability Associates.

Everdij, M. H. C., Blom, H. A. P.,(Eds.) (2008). Safety Methods Database Version 0.8, 31 January 2008, Amsterdam, NLR.

Fields, R. E. (2001). Analysis of erroneous actions in the design of critical systems. DPhil thesis, Department of Computer Science, University of York.

Forester, J. A., Kiper, K., Ramey-Smith, A. (1998). Application of a new Technique for Human Event Analysis (ATHEANA) at a pressurized-water reactor. Albuquerque, NM, Sandia National Laboratories.

Forester, J. A., Kolaczkowski, A. M., Cooper, S. R., Bley, D. C., Lois, E. (2007). ATHEANA User's Guide: Final Report. NUREG-1880, Washington, DC, U.S. Nuclear Regulatory Commission.

Forester, J. A., Kolaczkowski, A., Lois, E., Kelly, D. (2006). Evaluation of analysis methods against good practices: Final Report. NUREG-1842. Washington, DC, U.S. Nuclear Regulatory Commission.

Fullwood, R. R. (2000). Probabilistic safety assessment in the chemical and nuclear industries. Woburn, MA, Butterworth.Heinemann.

Gertman, D. I., Blackman, H. S., Marble, J. L., Byers, J. C., Smith, C. L. (2004). The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883. Washington, DC, U.S. Nuclear Regulatory Commission.

Hallbert, B., Kolaczkowski, A. (2007). The employment of empirical data and Bayesian methods in Human Reliability Analysis: A Feasibility Study, NUREG-CR-6949. Washington, DC, U.S. Nuclear Regulatory Commission.

Hallbert, B. P., Gertman, D. I., Marble, J., Lois, E., Siu, N. (2004). Using information from operating experience to inform human reliability analysis. In: *International Conference on Probabilistic Safety Assessment and Management*, Berlin, Germany, Jun. 14-18, 2004.

Higgins, J. C., O'Hara, J. M. (2000). Proposed approach for reviewing changes to risk-important human actions, NUREG-CR-6689. Washington, DC, U.S. Nuclear Regulatory Commission.

Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method. Amsterdam, Elsevier.

Hollnagel, E. (2005). Human reliability assessment in context. In: *Nuclear Engineering and Technology*, Vol. 37, nº 2, Apr. 2005, p.p. 159-166

Hollnagel, E., Woods, D. D. (2005). Joint cognitive systems: foundations of cognitive systems engineering, New York, CRC Press.

Houghton, F. K., Morzinski, J. A. (1998). Integration of Human Reliability Analysis into the High Consequence Process. In: *International Conference on Probabilistic Safety Assessment and Management*, New York, September 13-18, 1998.

International Atomic Energy Agency (IAEA) (2008). Collection and classification of human reliability data for use in probabilistic safety assessments, Vienna, Austria

Karwowski, W. (Ed.) (2001). International Encyclopedia of Ergonomics and Human Factors, Vol. 1. London, Taylor & Francis.

Kennedy, R., Kirwan, B., and Summersgill, R., Rea, K. (2000). Making HRA a more consistent science. In: *Foresight & Precaution: Proceedings of ESREL 2000, SARS and SRA-Europe Annual Conference, Edinburgh, 14-17 May 2000*. Eds. M. P. Cottam, D. W. Harvey, R. P. Pape, and R. J. Tait. London, Taylor & Francis

Kirwan B. (1988). A comparative evaluation of five human reliability assessment techniques. In: *Human Factors and Decision Making*. Sayers, B.A. (Ed.), London: Elsevier, pp. 87-109

Kirwan, B (1994). A guide to practical human reliability assessment. London, Taylor & Francis.

Kirwan, B. (1999). Some developments in Human Reliability Assessment, In: *The Occupational Ergonomics Handbook*. W. Karwowski, W., Marras, W. (orgs), New York, CRC Press, pp. 643-666.

Kirwan, B., Kennedy, R., Taylor-Adams, S., Lambert, B. (1997). The validation of three human reliability quantification techniques, THERP, HEART and JHEDI: Part II – results of validation exercise. *Applied ergonomics*, 28 (1), 17-25.

Kletz, T. A. (2001). Hazop and Hazan: identifying and assessing process industry hazards, 4th ed. Rugby, UK, Institution of Chemical Engineers.

Kohlhepp, K. D. (2005). Evaluation of the use of engineering judgements applied to analytical human reliablity analysis methods (HRA). Master's thesis, Texas A&M University.

Kolaczkowski, A., Forester, J., Lois, E., Cooper, S. (2005). Good practices for implementing Human Reliability Analysis (HRA): Final Report, NUREG-1792. Washington, DC, U.S. Nuclear Regulatory Commission.

Lees, F. P. (2005). Loss prevention in the process industries: hazard identification, assessment and control, vol. 1-3, 3rd ed., Amsterdam, Elsevier.

Leva, Maria Chiara (2005). Human errors analysis and safety management systems in hazardous activities. Interim Report IR-05-003. Laxenburg, Austria, IIASA.

Liu, H., Hwang, S. L., Liu, T. H. (2009). Economic assessment of human errors in manufacturing environment. In: *Safety Science*, vol. 47, nº 2, pp. 170–182

López Droguett, E., Moura, M. C., Jacinto C. M., Silva Jr., M. F. (2008). A semi-Markov model with Bayesian belief network based human error probability for availability assessment of downhole optical monitoring systems. In: *Simulation Modelling Practice and Theory*, vol. 16, nº 10, Nov. 2008, p. 1713-1727.

Marseguerra, M., Zio, E., Librizzi, M. (2007). Human Reliability Analysis by Fuzzy CREAM. In: *Risk Analysis*, vol. 27, nº 1, pp. 137-154.

Matoba, M. (1999). Human reliability in grounding and collision of ships. In: *Transactions of the 15th International Conference on Structural Mechanics in Reactor Technology (SMiRT-15).* Seoul, Korea, August 15-20, 1999, pp. 475-482.

Meister, D., (1993). Human reliability database and future systems, In: *Reliability and Maintainability Symposium Proceedings,* Atlanta, 26-28 Jan. 1993, pp. 276-280.

Miguel, A. S. S. R. (2006). Manual de higiene e segurança do trabalho, 9ª ed., Porto Editora.

Montague, M. L., Lee, M. S., W., Hussain, S. S. (2004). Human error identification: an analysis of Myringotomy and ventilation tube insertion. In: *Archives of Otolaryngology Head Neck Surgery*, 130 (10), pp. 1153-1157.

Montmollin, M. (1995). A ergonomia. Lisboa, Piaget.

Nunes, I. L., Jacinto, C. (2003). Fiabilidade humana: uma breve revisão do estado da arte. In: *Organizações e Trabalho*, nº 29-30, pp. 117-126

O'Hara, J. M., Higgins, J. C., Brown, W. S., Fink, R., Persensky, J., Lewis, P., Kramer, J., Szabo, A. (2008). Human factors considerations with respect to emerging technology in nuclear power plants, NUREG-CR-6947. Washington, DC, U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W. S., Lewis, P. M., Persensky, J. J. (2002a). Human-System Interface Design Review Guidelines, NUREG-0700, Rev. 2. Washington, DC, U.S. Nuclear Regulatory Commission.

O'Hara, J., Higgins, J., Persensky, J., Lewis, P. (2002b). Human factors engineering program review model, NUREG-0711, Rev. 1. Washington, DC, U.S. Nuclear Regulatory Commission.

Pallerosi, C. A. (2008). Confiabilidade Humana: nova metodologia de análise qualitativa e quantitative. In: *6º Simpósio Internacional de Confiabilidade*, Florianópolis, Brasil, 7-9 Maio.

Pyy, P. (2000). Human reliability analysis methods for probabilistic safety assessment. Espoo, Technical Research Centre of Finland.

Rasmussen, J. (1987). The definition of human error and taxonomy for technical system design, In: *New Technology and Human Error*, Rasmussen, J., Dunkan, K. e Leplat, J. (orgs), Chichester, John Wiley & Sons, pp. 23-30.

Read, P. P. A. (1987). The Chernobyl errors. In: *The Psychologist: Bulletin of the British Psychological Society*, v. 4.

Reason, J. T. (1990). Human error. Cambridge University Press.

Reer, B. (2008a). Review of advances in human reliability analysis of errors of commission, Part 1: EOC identification. In: *Reliability Engineering and System Safety*, vol. 93, nº 8, pp. 1091–1104

Reer, B. (2208b). Review of advances in human reliability analysis of errors of commission, Part 2: EOC quantification. In: *Reliability Engineering and System Safety*, vol. 93, nº 8, pp. 1105–1122

Sampaio, J. J. (2002). Cognitive Automation, Operational Decision and Human Error. In: *Sociedade e Trabalho*, nºs 12/13, pp. 119-128.

Shappell, S. A., Wiegmann, D. A. (2004). HFACS analysis of military and civilian aviation accidents: a North American comparison. Queensland, International Society of Air Safety Investigators, pp. 2-8

SOUSA, G. V. (2005). Metodologia da investigação, redacção e apresentação de trabalhos científicos. Porto, Civilização.

Swain, A. D., Guttmann, H. E. (1980). Handbook of human reliability analysis with emphasis on nuclear power plant applications. Draft Report. NUREG/CR-1278, Washington, DC, U.S. Nuclear Regulatory Commission.

Swain, A. D., Guttmann, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. Washington, DC, U.S. Nuclear Regulatory Commission.

Swain, A. D. (1987). Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772. Washington, DC, U.S. Nuclear Regulatory Commission.

Swain, A. D. (1990). Human reliability analysis: Need, status, trends and limitations, In: *Reliability Engineering and Systems Safety*, 29, pp. 301-313.

Topmiller, D. A., Eckel, J. S., Kozinsk, E. J. (1982). Human reliability data bank for nuclear power plant operation, Vol. 1: A review of existing human reliability data banks, NUREG/CR-2744. Washington, DC, U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission (2000). Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC.

Williams, J. C. (1985). HEART – a proposed method for achieving high reliability in process operation by means of human factors engineering technology. In: *Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society*, Southport, U.K., 16th Sep. 1985.

Williams, J. C. (1986). HEART - a proposed method for assessing and reducing human error. In: *Proceedings of the 9th Advances in Reliability Technology Symposium*, Bradford, University of Bradford, 1986, pp. B3/R/1 – B3/R/13.

Williams, J. C. (1988). A data-based method for assessing and reducing human error to improve operational performance. In: *Proceedings of IEEE Fourth Conference on Human Factors in Power Plants*, Monterey, California, June 5-9, 1988, pp. 436-450.

Williams, J. C. (1992). Toward an improved evaluation analysis tool for users of HEART. In: *Proceedings of the International Conference on Hazard Identification and Risk Analysis, Human Factors Factors and Human Reliability in Process Safety*, January 15-17, 1992.

Zio, E. (2009). Reliability engineering: old problems and new challenges. In: *Reliability Engineering and System Safety*, vol. 94, nº 2, Feb. 2009, pp. 125– 141.

Webografia

- Associação Portuguesa de Ergonomia: http://www.apergo.pt
(consultado em 09-08-2009)

- Confiabilidade humana - PCS5006: http://pcs5006.blogspot.com
(consultado múltiplas vezes entre 02/2009 e 07/2009)

- Confiabilidade Humana: http://www.confiabilidadehumana.com.br
(consultado em 09-05-2009)

- Department of Computer and Information Science - Linköping University: http://www.ida.liu.se
(consultado em consultado em 14-06-2009)

- Engineering Workstations: http://www.ews.uiuc.edu
(consultado em 18-07-2009)

- HEART Online Calculator: http://tricenote.com/safety/heart-calculator
(consultado em 18-07-2009)

- International Applied Reliability Symposium: http://www.arsymposium.org
(consultado múltiplas vezes entre 06/2009 e 09/2009)

- International Labour Organization: http://www.ilo.org
(consultado em 09-08-2009)

- ReliaSoft Brasil: http://www.reliasoft.com.br
(consultado múltiplas vezes entre 05/2009 e 09/2009)

- System Reliability Center: http://src.alionscience.com
(consultado em 14-06-2009)

- Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE): https://saphire.inel.gov
(consultado em 16-05-2009)

- The Dow Chemical Company: http://www.dow.com
(consultado em 09-05-2009)

- The International Ergonomics Association: http://www.iea.cc
(consultado em 09-08-2009)

- U.S. Nuclear Regulatory Commission: http://www.nrc.gov
(consultado múltiplas vezes entre 04/2009 e 08/2009)

- University of Illinois at Urbana-Champaign - http://www.ews.uiuc.edu
(consultado em 20-06-2008)

- Weibull - Reliability Engineering Resources: http://www.weibull.com
(consultado múltiplas vezes entre 05/2009 e 08/2009)

- University of Glasgow – Department of Statistics: http://www.gla.ac.uk/departments/statistics
(consultado em 12-04-2009)

Anexo A. Bases de Dados de Fiabilidade Humana

AIR Data Storage

Foi desenvolvida pelo *American Institute for Research* (AIR) para estimar o valor de determinadas características ergonómicas com vista a conferir uma melhor manuseabilidade de equipamentos electrónicos.

Consultar: Munger, S. J., Smith, R. W., Payne, D. (1962). An Index of Electronic Equipment Operability: Data Store, Report. AIR- C43-1/62RP(1). Pittsburgh, American Institute for Research.

Aerojet General Method

Teve como base a AIR Data Storage, tendo sido expandida de modo a incluir tarefas de manutenção e inspecção associadas ao sistema de propulsão dos míssseis balísticos intercontinentais *Titan II* (propriedade da extinta *Glenn L. Martin Company* – EUA).

Consultar: Irwin, I. A., Levitz, J. J., Freed, A. M. (1964). Human Reliability in the Performance of Maintenance, LRP 317/TDR-63-218. Sacramento, CA, Aerojet-General Corporation.

Bunker-Ramo Tables

A *Air Data Store* foi novamente expandida com o objectivo de incluir informação adicional de 37 estudos experimentais sobre a performance dos operadores da *Bunker-Ramo Corporation*.

Consultar: Hornyak, S. J. (1967). Effectiveness of Display Subsystem Measurement and Prediction Techniques, RADC Report TR-67-292. New York, Rome Air Development Centre, Griffiss Air Force Base.

The Operational Recording and Data System (OPREDS)

Contém dados adquiridos através da monitorização automática de operações básicas como ligar/desligar interruptores e pressionar botões, levada a cabo pela marinha de guerra norte-americana (*US Navy*).

Consultar: Urmston, R. (1971).Operational Recording and Evaluation Data System (OPREDS), Descriptive Brochures, Code 3400. San Diego, CA, Navy Electronics Laboratory Center.

The Aviation Safety Reporting System (ASRS)

Esta base de dados contém dados relativos a acidentes na aviação civil e fornecidos voluntariamente pela *Federal Aviation Administration*.

Consultar: Federal Aviation Administration (1979). Aviation Safety Reporting Programs, FAA Advisory Circular 00-46B, Washington, DC, FAA.

The Savannah River Laboratory (SRL)

Este laboratório desenvolveu uma base de dados com taxas de erros dos operadores, bem como taxas de falhas dos equipamentos existentes em centrais de reprocessamento nuclear.

Consultar: Durant, W. S., Lux, C. R., Galloway, W. D. (1988). Data bank for probabilistic risk-assessment of nuclear-fuel reprocessing plants. In: *IEEE Transactions on Reliability*, 37(2), 138-42.

The Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)

Esta biblioteca virtual de dados contém taxas de erros e de falhas de equipamentos de tarefas operacionais e de manutenção de centrais nucleares.

Consultar: Gertman, D. I., Gilmore, W. E., Galtean, W. J., Groh, M. J., Gentillon, C. D., Gilbert, B. G. (1988) Nuclear Computerized Library for Assessing Reactor Reliability. NUREG/CR-4639, US Nuclear Regulatory Commission, Washingon, DC.

Anexo B.RELATO DOS PRINCIPAIS ACIDENTES NUCLEARES

Anexo C1. Three Mile Island – Estados Unidos da América, 1979

No dia 28 de Março de 1979, pelas quatro horas da manhã, ocorreu mais uma das frequentes avarias na central nuclear de *Three Mile Island 2,* na Pensilvânia, EUA. Porém, desta vez, o que normalmente não passaria de um incidente habitual e recorrente transformou-se num grave acidente, tendo o núcleo do reactor ficado a descoberto durante mais de duas horas e meia, facto este que originou prejuízos materiais graves, obrigando ainda à evacuação de 144.000 pessoas de toda aquela região.

O que terá então ocorrido? Examinemos em primeiro lugar um resumo do desenrolar dos acontecimentos que estiveram na origem do acidente, que começa com o desligamento da bomba que faz a alimentação de água ao gerador de vapor. Automaticamente, o turbo-alternador pára e as bombas auxiliares são accionadas. O tempo para que a alimentação auxiliar esteja em funcionamento traduz-se por uma breve interrupção do arrefecimento, com consequente subida da temperatura e da pressão do fluído primário. Ao fim de três segundos, a válvula de descarga abre-se para baixar a pressão. Com a descarga ainda insuficiente e, após decorridos 8 segundos, ocorre uma paragem devido ao alto nível de pressão, provocando a queda das barras de segurança do núcleo. Passados 13 segundos, a pressão baixou e o sistema de controlo accionou o fecho da válvula de descarga. Estamos na presença de uma sequência comum de operações restando apenas a retirada da potência residual e a preparação para um novo *"start up"*.

Mas naquele dia a válvula de descarga não se fechou tendo-se observado no painel da sala de controlo apenas a ordem de fecho e não o fecho propriamente dito pelo que a indicação existente passa, então, a ser de que a válvula se encontrava fechada. Na realidade, ela deixa passar 60 t/h de fluído primário que se acumulam num reservatório da área. A pressão do primário cai, e após 2 minutos o sistema de injecção de alta pressão

é accionado e introduz água no circuito primário. Neste momento, o essencial da actividade dos operadores está voltado para o secundário. Com efeito, o corte das bombas provocou o accionamento das bombas auxiliares. Porém, no circuito secundário, houve válvulas de segurança que tinham ficado fechadas no seguimento de um ensaio periódico que tinha sido anteriormente efectuado. Nestas condições, o gerador de vapor extingue-se em três minutos e, sem que pudesse ocorrer a troca de calor, o fluído primário é levado até à ebulição.

Efectivamente os operadores acabam por se aperceber que as válvulas de segurança se encontravam encerradas quando já se tinham passados 8 minutos, dando então a ordem de abertura imediata, ficando a situação estável do lado secundário só passados 25 minutos. Logo que o sistema de injecção de segurança é accionado os operadores obedecem a uma instrução complementar (não deixar perder o nível de vapor no pressurizador). Ignorando que a válvula de descarga se encontrava aberta, cortam o sistema de injecção de emergência após 4 minutos e 38 segundos, para não encher por completo o circuito primário com água no estado líquido. A partir deste momento o fluído primário perdido através da abertura deixa de ser compensado. O núcleo vai ficando descoberto pouco a pouco e a temperatura sobe. Só às 2 horas e 22 minutos é que se observou a abertura e nessa altura foi fechada uma válvula de segurança no circuito de descarga. Um diagnóstico preciso só foi elaborado ao fim de dez horas. Mas, nessa altura, grande quantidade de fluído primário já se tinha perdido e foram necessárias dezasseis horas para voltar a atingir uma situação estável.

O relatório do inquérito concluiu que os operadores cometeram um grave erro ao cortarem o sistema de injecção de emergência decorridos 4 minutos e 38 segundos. Com efeito, trata-se de um caso típico de erro retrospectivo, ou seja, que pode ser reconstituído como tal, após verificados os factos.

Durante as duas primeiras horas do acidente os operadores não sabiam, com efeito, que havia uma fuga de fluído no circuito primário, pois:

- existia a indicação de que a válvula de descarga se encontrava fechada;
- não existia indicador do nível geral do primário;
- o nível do reservatório que recebe o fluído descarregado era indicado do outro lado do painel de comando e, não suspeitando de fuga, os operadores não tinham motivo para consultá-lo;
- a temperatura da linha de descarga era mais elevada do que o habitual mas os operadores sabiam que esta indicação não era confiável, porque desde há muito tempo que existia uma ligeira fuga;
- o nível indicado no pressurizador passa a ser aceitável ao fim de 10 minutos, levando os operadores a convencerem-se de que recuperariam o nível mas, nesta altura, a indicação já não tinha qualquer significado, dado que o pressurizador contém uma mistura bifásica vapor-água;
- os alarmes estavam inoperantes visto que a impressão já não se fazia em tempo real mesmo antes de ocorrer esta avaria;
- a indicação da pressão do núcleo estava em baixa, enquanto a do pressurizador estava em alta. Os operadores, que estavam habituados a ver as duas pressões evoluírem paralelamente concluíram, sem comprovar, que o manómetro do núcleo se encontrava defeituoso;
- a sala de controlo enchia-se progressivamente de engenheiros. Nenhum deles notou que havia uma fuga no primário;
- recorde-se que eram quatro horas da manhã, ou seja, horário em que o organismo humano geralmente se encontra em estado de desactivação.

Portanto, as diferentes indicações produzidas pelo sistema de controlo não colocavam em causa o diagnóstico inicial, pelo que são interpretadas à luz deste mesmo diagnóstico como originando actuações que, aparentemente, poderiam ter sido eficazes mas que agravaram, de facto, a situação e originaram ou foram incapazes de evitar o acidente.

adaptado de: Montmollin, M. - A ergonomia. Lisboa, Piaget, 1995

Anexo C2. Chernobyl – Ex-União Soviética, 1986

Era 1:24h do dia 26 de Abril de 1986, um sábado de manhã, quando ocorreu o pior acidente de energia nuclear da história da geração industrial. Duas explosões seguidas, lançaram para o ar as 1000 toneladas de cimento da tampa de selagem do reactor nuclear número 4 de *Chernobyl***.** Fragmentos fundidos do núcleo espalharam-se na região vizinha e produtos da fissão foram libertados para a atmosfera. O acidente, provavelmente, custou centenas de vidas e contaminou vastas áreas de terra na Ucrânia e não só.

Diversas razões contribuíram para este desastre. Convém aqui salientar que o projecto do reactor não era novo – tinha cerca de 30 anos de idade na data do acidente - e havia sido concebido ainda antes da época dos sofisticados sistemas de segurança controlados por computador. Por esta razão os procedimentos para lidar com situações de emergência relacionadas com o reactor dependiam fortemente da capacidade dos operadores. Este tipo de reactor também tinha uma tendência para sair de controlo quando operado a baixa capacidade. Por tal razão, os procedimentos operacionais para o reactor proibiam estritamente que fosse operado abaixo de 20% da sua capacidade máxima. Foi, sobretudo, uma combinação de circunstâncias e de erros humanos que originaram tão grave acidente.

Ironicamente e, por estranho que pareça, os acontecimentos que conduziram ao desastre tinham por finalidade tornar o reactor mais seguro. Os testes, planeados por uma equipa especializada de engenheiros, foram realizados para avaliar se o sistema de emergência para refrigeração do núcleo podia ser accionado no caso de ocorrer uma interrupção de energia externa. Este dispositivo de segurança, embora já tivesse sido testado antes, não tinha ainda funcionado satisfatoriamente pelo que novos testes desse dispositivo modificado foram realizados com o reactor operando com uma capacidade reduzida durante o período de teste. Os testes foram programados para a tarde de sexta-feira 25 de Abril de 1986, tendo-se iniciado a redução da capacidade de produção às 13:00h desse dia. Entretanto, logo após as 14:00h, quando o reactor estava a operar a

cerca de metade da sua capacidade total, o controlador de Kiev solicitou que o reactor continuasse a fornecer electricidade para a rede local.

Na realidade, continuaram ligados à rede até às 23H10. O reactor deveria ser parado para a manutenção anual na terça-feira seguinte e a solicitação do controlador de Kiev na realidade reduziu o tempo e o espaço de manobra disponível para os testes.

Posteriormente foi elaborado um relatório cronológico das últimas horas que antecederam o desastre, junto com uma análise de James Reason, que foi publicada no *Bulletin of the British Psychological Society* no ano seguinte, no qual se destacam em itálico as acções significativas dos operadores e que são de dois tipos: *erros* (indicados por um "E") e *violações de procedimentos* (marcadas por um "V").

25 abril de 1986

13:00h - A redução de capacidade começou com a intenção de conseguir 25% de capacidade para reunir as condições de teste.

14:00h - O sistema de emergência para arrefecimento do núcleo (ECCS -*Emergency Core Cooling System)* foi desconectado do circuito principal, acção que constituía parte do plano de teste.

14:05h - O controlador de Kiev solicitou que a unidade continuasse a alimentar a rede. O *ECCS não foi reconectado* (V). Contudo, não se considera que esta violação específica tenha contribuído materialmente para o desastre mas é indicativa de uma atitude de descuido por parte dos operadores em relação à observância dos principais procedimentos de segurança.

23:10h - A unidade foi desligada da rede e a redução de capacidade foi continuada para conseguir o nível de capacidade de 25%, planeado para o programa de teste.

26 de abril de 1986

00:28h - *Um operador ultrapassou para baixo o ponto de ajuste para a redução pretendida (E).* A potência caiu então para um perigoso 1%. O operador havia desligado o controlador automático e tinha tentado conseguir o nível desejado através de controlo manual.

01:00h - Após um longo e intenso esforço, a potência do reactor finalmente foi estabilizada em 7% - muito abaixo do nível pretendido mas ainda na zona de perigo de baixa capacidade. *Neste momento a experiência deveria ter sido abandonada mas isso não aconteceu (E).* Este foi o mais sério erro relacionado com a aplicação das regras de segurança uma vez que todas as actividades subsequentes conduziriam à zona de máxima instabilidade do reactor, factos que, aparentemente, não foram percebidos pelos operadores.

01:03h - *Todas as oito bombas foram accionadas (V).* Os regulamentos de segurança limitavam a seis o número máximo de bombas simultaneamente em uso, demonstrando um profundo desconhecimento da física do reactor. Como consequência ocorreu um aumento do fluxo de água e a redução da fracção de vapor que absorveram mais neutrões, exigindo que mais elementos de controlo fossem retirados para sustentar este baixo nível de potência.

01:19h - O *fluxo de água de alimentação foi aumentado três vezes* (V). Parece que os operadores estavam a tentar lidar com uma pressão de vapor e nível de água decrescente. O resultado das suas acções, entretanto, foi reduzir ainda mais a quantidade de vapor a passar através do núcleo, exigindo que muito mais elementos de controlo precisassem de ser retirados. *Também suprimiram a paragem automática do colector de vapor (V).* O efeito consequente foi desprover o reactor de um dos seus sistemas automáticos de segurança.

01:22h - O supervisor de turno solicitou um relatório impresso para estabelecer quantos elementos de controlo estavam realmente no núcleo. O relatório indicou que eram somente de seis a oito os elementos remanescentes. Era estritamente proibido operar o reactor com menos do que 12 elementos de controlo. *Apesar disso, o supervisor de turno decidiu continuar com os testes (V).* Esta foi uma decisão fatal: por isso o reactor ficou sem controlo.

01:23h - *As válvulas da linha de vapor para o turbo-gerador número 8 estavam fechadas (V).* O objectivo era estabelecer as condições necessárias para testes repetidos, mas o resultado foi desconectar os desengates automáticos de segurança. Esta talvez tenha sido a mais séria de todas as violações.

01:24h - Foi feita uma tentativa para desligar repentinamente o reactor, accionando os elementos de paragem de emergência, mas estes emperraram nos tubos já deformados. Duas explosões ocorreram, uma logo após a outra. O tecto do reactor foi lançado para o ar, provocando 30 incêndios na vizinhança.

01:30h - Os bombeiros de serviço foram chamados. Outras unidades foram chamadas de *Pripyat* e *Chernobyl.*

05:00h - Os incêndios externos foram extintos, mas o incêndio do grafite do núcleo continuou por diversos dias. A investigação posterior do desastre detectou diversos pontos significativos que contribuíram para a sua ocorrência.

Destacam-se entre eles:

- O programa de testes foi mal planeado e os itens referentes às medidas de segurança eram inadequados. A segurança do reactor estava, na realidade, substancialmente reduzida pelo facto do sistema de emergência de arrefecimento do reactor (ECCS) ter sido desactivado durante o período de testes;
- O planeamento dos testes foi colocado em prática antes de ser aprovado pelo grupo de projecto, responsável pelo reactor;
- Os operadores e os técnicos que estavam a conduzir a experiência tinham competências diferentes e não sobrepostas;
- Os operadores, embora altamente habilitados, provavelmente estimavam que a realização do teste antes da paragem melhoraria a sua reputação profissional. Estavam orgulhosos da sua competência para lidar com o reactor mesmo em condições invulgares e estavam conscientes da rápida redução significativa de tempo no qual deveriam completar o teste. Provavelmente tinham perdido qualquer sensibilidade para os perigos envolvidos na produção do reactor;

- Os técnicos que tinham planeado o teste eram engenheiros eléctrotécnicos de Moscovo e o seu objectivo era resolver um problema técnico complexo. Apesar de terem planeado os procedimentos de teste, provavelmente não sabiam muito sobre a produção da central nuclear propriamente dita.

Novamente, nas palavras de James Reason: *"Juntos, fizeram uma mistura perigosa: um grupo de engenheiros de uma modalidade, mas não engenheiros nucleares, dirigindo uma equipa de operadores dedicados, porém demasiado confiantes. Cada grupo provavelmente assumiu que o outro sabia o que estava a fazer. E as duas partes tinham pouco ou nenhum conhecimento dos perigos que estavam a ocasionar ou do sistema de que estavam a abusar."*

adaptado de: Read, P. P. A. - The Chernobyl errors. ***The Psychologist: Bulletin of the British Psychological Society*****, v. 4, 1987**

Anexo C. HEART: Tabelas Auxiliares de Cálculo

Tabela 3 - Probabilidades de erro humano

Tarefa:	Descrição	5%	50%	95%
Não familiar	Tarefa não familiar executada à mesma velocidade do que se fosse uma tarefa habitual.	0.35	0.55	0.97
Mudança sem procedimentos	Mudar ou restaurar o sistema para um novo estado ou estado original numa única tentativa sem supervisão e/ou sem procedimentos definidos.	0.14	0.26	0.42
Complexa	Tarefa complexa que requira um alto nível de compreensão e destreza.	0.12	0.16	0.28
Simples	Tarefa simples executada muito rapidamente e/ou sem a devida atenção.	0.06	0.09	0.13
Rotineira, pouco exigente	Tarefa rotineira, praticada muitas vezes e de execução rápida que envolva um nível relativamente baixo de competências.	0.007	0.02	0.045
Restaurar com procedimentos	Mudar ou restaurar o sistema para um novo estado ou estado original seguindo os procedimentos, com alguma supervisão.	0.0008	0.003	0.007
Familiar, praticada	Tarefa completamente familiar, bem desenhada, altamente praticada e rotineira, que ocorra várias vezes numa hora, executada segundo as regras mais exigentes e por pessoas altamente motivadas, bem formadas e altamente experientes, totalmente conscientes das implicações da falha, com tempo para corrigir possíveis erros, mas sem o benefício de ajudas de trabalho significativas.	0.00008	0.0004	0.009
Responder correctamente	Responder correctamente a comandos do sistema mesmo quando existe um sistema supervisor aumentado ou automático que providencie uma detalhada interpretação do estado do sistema.	0.000006	0.00002	0.0009
Várias	Tarefas várias para as quais não foi encontrada nenhuma descrição.	0.008	0.03	0.11

adaptado de: http://tricenote.com/safety/heart-calculator

Tabela 4 - Condições geradoras de erros (EPCs)

Condição Geradora de Erro (EPC)		Descrição	Multiplicador
1	Não familiariedade	Não familiaridade com uma situação que é potencialmente importante mas que raramente acontece ou é uma situação nova.	17
2	Falta de tempo	Falta de tempo para a detecção e correcção do erro.	11
3	Baixo S/N	Baixo som para o sinal.	10
4	Características dominantes	Informação ou características que são de excessivo fácil acesso .	9
5	Incompatibilidade	Sem meios de informação espacial e funcional para o operador, de forma a que o mesmo consiga assimilar a mesma rapidamente.	8
6	Divergência de Modelos	Divergência entre o mundo real do operador e o que foi imaginado por quem desenhou a máquina.	8
7	Irreversibilidade	Sem meios óbvios de reverter uma acção não intencionada.	8
8	Sobrecarga do canal	Uma sobrecarga da capacidade do canal, especialmente causada pela apresentação simultânea de informação não redundante.	6
9	Desaprendizagem de uma técnica	Necessidade de "desaprender" uma técnica e aplicar outra que tenha uma filosofia completamente diferente.	6
10	Transferância de conhecimento	Necessidade de tranferir conhecimento específico de tarefa para tarefa, sem qualquer perda.	5.5
11	Ambiguidade do desempenho	Ambiguidade nos standards de desempenho necessários.	5
12	Má percepção do risco	Divergência entre o risco real e o risco percepcionado.	4
13	Escasso feedback	Pobre, ambíguo ou fraco sistema de feedback.	4
14	Sinal fraco	Sem confirmação clara, directa e atempada de uma acção intencionada da porção do sistema na qual o controlo deve ser exercido.	4
15	Inexperiência	Inexperiência do operador (exemplo: um recém qualificado e não um especialista).	3
16	Informação pobre	Uma baixa qualidade da informação transmitida nos procedimentos e pelo indivíduo.	3
17	Baixa verificação	Pouca ou nenhuma verificação ou teste dos outputs.	3
18	Conflito de objectivos	Um conflito entre objectivos imediatos e objectivos a longo-prazo.	2.5
19	Nenhuma diversidade	Nenhuma diversidade nos inputs de informação para testes de veracidade.	2.5
20	Divergência Educacional	Um desencontro entre o nível educacional de um indivíduo e os requisitos de uma determinada tarefa.	2
21	Incentivos perigosos	Um incentivo para utilizar outros procedimentos mais perigosos.	2
22	Falta de exercício	Poucas oportunidades de exercitar a mente e o corpo fora do âmbito restrito da função.	1.8
23	Instrumentação não fiável	Instrumentação não fiável (facilmente percepcionada).	1.6

Condição Geradora de Erro (EPC)		Descrição	Multiplicador
24	Decisões absolutas	Necessidade de decisões que estão para além das capacdades do operador.	1.6
25	Função e responsabilidade pouco clara	Alocação pouco clara da função e responsabilidades.	1.6
26	Registo da evolução de uma actividade	Sem forma clara de manter registo do progresso/evolução durante uma actividade.	1.4
27	Capacidade física	O perigo de que o limite máximo das capacidades físicas seja ultrapassado.	1.4
28	Baixo significado de uma tarefa	Baixo ou nenhum significado intrínseco a uma tarefa.	1.4
29	Stress Emocional	Nível elevado de stress emocional.	1.3
30	Limitações na Saúde	Evidência de doença ou fraqueza nos operadores, especialmente febre.	1.2
31	Baixa moral	Baixa moral nos colaboradores.	1.2
32	Inconsistência	Inconsistência entre o significado dos outputs da máquina e os procedimentos efectuados.	1.2
33	Meio ambiente perigoso	Um meio ambiente pobre ou hóstil (mais de 75% de risco na saúde ou vida).	1.15
34	Baixa exigência mental	Prolongada inactividade ou ciclos altamente repetitivos de tarefas pouco especializadas.	1.1
35	Interrupção do sono	Interrupção dos ciclos normais de trabalho-sono.	1.1
36	Velocidade da tarefa	Velocidade da execução da tarefa causada pela intervenção de outros.	1.06
37	Excedentes da equipa	Membros da equipa a mais que os necessários para executar o trabalho de forma regular e satisfatória.	1.03
38	Idade	Idade das pessoas que executam tarefas relacionadas com a percepção.	1.02

adaptado de: http://tricenote.com/safety/heart-calculator

Anexo D. Eventos iniciadores aplicados à indústria nuclear

Tabela 5 – Classes de eventos iniciadores aplicados à produção de energia nuclear

Classes de eventos iniciadores	Exemplos de iniciadores
Acidentes relacionados com roturas em tubagens	Grande, médio ou pequeno.
Transientes internos, com e sem água de alimentação	Perda de água de alimentação principal, perda de vácuo, desarme do reactor, desarme da turbina, perda de potência eléctrica externa, fecho da válvula de isolamento de vapor principal, perda de água de circulação, etc.
Falha de sistemas de suporte	Perda do caudal de água de serviço, da água de refrigeração dos componentes e do ar dos instrumentos, assim como falhas na ventilação e perdas eléctricas em corrente contínua e alternada
Eventos externos	Sismos, fogos, cheias, vento forte, etc.
Eventos especiais	Rotura de tubagens de interfaces entre sistemas, rotura dos tubos geradores de vapor, falha no vaso do reactor, etc.
Modos alternativos	Potências reduzidas e fecho de sistemas.

adaptado de: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Anexo E. ATHEANA: Determinação dos HEFs e UAs

Tabela 6 - Modos de falha funcionais baseados em requisitos das PRAs

Table 9.6 Functional Failure Modes Based upon PRA Requirements[a]

Function Required in PRA? (1)	Systems that Perform Function (2)	Pre-Initiator Status (3)	Functional Success Criteria (4)	Functional Failure Modes (5)	Functional Failure Mode Category[b] (6)	Example Systems
(a) Needed		Standby	Equipment automatically actuates (short mission time)	Equipment fails to initiate or actuate automatically	1	RPS, accumulators
			Equipment automatically actuates and continues to operate for duration of mission time (longer mission times)	Equipment fails to initiate or actuate automatically	2	HPI, LPI, AFW, CS, CI
				Equipment fails to continue to operate for duration of mission time	3	
			Equipment manually actuated and continues to operate for duration of mission time	Equipment fails to be manually initiated or actuated when required	4	HPR, LPR, RHR, SDC
				Equipment fails to continue to operate for duration of mission time	3	
		Standby or Operating	Equipment manually operated as necessary to control plant parameters for duration of mission time	Equipment manually not actuated when required	4	PORVs, ADS
				Equipment fails to continue to operate for duration of mission time	3	MFW, Condesate, AFW, HPI, LPI, RCPs, CVCS, SLC
				Equipment fails to be controlled or operated as required	5	
		Passive	Equipment maintains required status	Equipment status inappropriately changed	6	
(b) Undesired		Operating	Equipment stopped and remains stopped for duration of mission time	Equipment fails to stop automatically	7	RCPs
		Standby	Equipment maintains pre-initiator (or immediate post-initiator) status	Equipment fails to remain stopped for required duration Equipment fails to be stopped manually Equipment fails to maintain desired status Equipment status changes spuriously and inappropriately	8 9 10 11	SLC, SI, CI, CS

[a] Acronym's: HPI-high pressure injection; LPI-low pressure injection; AFW-auxillary feedwater; CS-core spray; HPR-high-pressure recirculation; LPR-low-pressure recirculation; RHR-residual heat removal; SDC-shutdown cooling; PORVs-power-operated relief valves; ADS-automatic depressurization system; MFW-main feedwater; RCPs-reactor coolant pumps; CVCS-chemical and volume tank coolant; SI-safety injection.

[b] Note that the numbers assigned in column 6 to the functional failure mode categories provide a link to the associated rows in Tables 9.7 and 9.9a-3.

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 7 - Exemplos de falhas humanas mais comuns e modos de falha humana das PRAs

Table 9.7 Examples of Likely Human Failures and Human Failure Modes by PRA Functional Failure Mode

PRA Functional Failure Modes (5)	Functional Failure Mode Category (6)	EOC or EOO? (7)	Example Human Failures (8)	Transfer to Unsafe Action Table for Step #7
Equipment fails to initiate/actuate automatically	1	EOC	Equipment inappropriately removed from automatic control Equipment inappropriately removed from armed or standby status	Table 9.9a
	2			
		EOO	Automatic actuation fails, and no backup, manual startup	Table 9.9d
Equipment fails to continue to operate for duration of mission time	3	EOC	Equipment inappropriately terminated Equipment inappropriately isolated or aligned Equipment output and/or resources inappropriately diverted Equipment output and/or resources inappropriately depleted	Table 9.9b
Equipment fails to be manually initiated or actuated when required	4	EOC/EOO	Equipment fails to be actuated when required Equipment inappropriately actuated	Table 9.9c
Equipment fails to be controlled or operated as required	5	EOC/EOO	Equipment fails to be operated or controlled Equipment inappropriately operated or controlled	
Equipment fails to maintain desired status	6	EOC/EOO	Equipment status inappropriately changed Fails to maintain integrity Inappropriately breached integrity	Table 9.9c
	10	EOC	Equipment inappropriately operated	Table 9.9b
Equipment fails to stop automatically	7	EOC	Equipment inappropriately removed from automatic control	Table 9.9a
		EOO	Automatic stop fails, and no backup, manual stop	Table 9.9d
Equipment fails to be stopped manually	9	EOO	Equipment fails to be stopped when required	Table 9.9c
Equipment fails to remain stopped for required duration	8	EOC	Equipment inappropriately restarted (and continues to operate)	Table 9.9b
		EOO	Equipment spuriously restarts, and no backup, manual stop	Table 9.9d
Equipment status changes spuriously and inappropriately	11	EOO	Spurious actuation, with no backup stop of equipment Spurious reconfiguration, with no backup realignment	

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 8 - EOCs possíveis para sistemas ou equipamentos que arrancam ou param automaticamente

Table 9.9a Possible EOCs for Systems or Equipment that Automatically Start or Stop

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	1 and 2	Inappropriately removed from automatic control	Operators take equipment out of armed or standby status (e.g., pumps put in pull-to-lock) Operators change equipment configuration/lineup from armed, standby, or normal status
		Inappropriately removed from armed or standby status	Operators bypass or suppress automatic signals Operators disable automatic signals/sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment
Equipment fails to stop automatically	7	Inappropriately removed from automatic control	Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 9 - EOCS possíveis para continuação da operação ou paragem de sistemas e equipamentos

Table 9.9b Possible EOCs for Continuation of Operation or No Operation of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to continue to operate for duration of mission time	3	Inappropriately terminated	Operators stop equipment (e.g., pumps stopped) Operators both stop and disable equipment for future service (e.g., pumps put in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop equipment and disable automatic signals/sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
		Inappropriately isolated or aligned	Operators realign equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals
		Output and/or resources inappropriately diverted	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.)
		Output and/or resources inappropriately depleted	Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident (Also considerations with ...resources diverted above)
Equipment status inappropriately changed	10	Inappropriately operated	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control
Equipment fails to remain stopped for required duration	8	Inappropriately restarted (and continues to operate)	

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 10 - EOCs e EOOs possíveis para actuação manual e controlo de sistemas e equipamentos

Table 9.9c Possible EOCs or EOOs for Manual Actuation and Control of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to be manually intiated or actuated when required	4	Fails to be actuated when required (EOO)	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late
		Inappropriately initiated or actuated (EOC)	Operators actuate equipment prematurely (i.e., too soon) Operators release or unsuppress equipment automatic initiation signals prematurely
Equipment fails to be stopped manually	9	Fails to be stopped when required (EOO)	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late
Equipment fails to be controlled or operated as required	5	Fails to be operated or controlled (EOO) Inappropriately operated or controlled (EOC)	Operator control of equipment operation results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 11 - EOOs possíveis para recuperação de sistemas e equipamentos em falha

Table 9.9d Possible EOOs for Backup (i.e., Recovery) of Failed Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	2	Fails to perform backup, manual startup (after automatic actuation fails)	Operator fails to manually start/stop Operator fails to manually isolation/alignment Operator fails to manually open/close Operator fails to manually lockout/trip Operator fails to manually insert/withdraw Operator fails to manually transfer
Equipment fails to stop automatically	7	Fails to perform backup, manual stop (after automatic stop fails)	
Equipment fails to remain stopped for required duration	8	Fails to perform backup, manual stop (after spurious re-start)	
Equipment status changes spuriously and inappropriately	11	Fails to perform backup, manual stop (after spurious actuation) Fails to perform backup, manual re-alignment (after spurious re-configuration)	

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 12 - EOCs e EOOs possíveis para falhas em sistemas e componentes passivos

Table 9.9e Possible EOCs or EOOs for Failures of Passive Systems and Components

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment status inappropriately changed	6	Fails to maintain integrity (EOO)	Operator actions (e.g., operator fails to operate/control, operator inappropriately operates/controls) from other categories that have these consequential effects
		Inappropriately breached integrity (EOC)	

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Tabela 13 - Exemplos de UAs para modos de falha funcionais de equipamentos gerais

Table 2.3 Example Unsafe Actions for Generalized Equipment Functional Failure Modes

Equipment Functional Failure Mode	Example Unsafe Action(s)
Failure of automatic actuation	Operators take equipment out of armed or standby status Operators change equipment configuration from armed, standby, or normal state Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators disable or fail equipment Operators reset signal setpoints
Inappropriate actuation	Operators actuate equipment prematurely (i.e., too soon) Operators prematurely release or unsuppress equipment automatic initiation signals Operators manually actuate equipment (when not needed) Operators manually actuate equipment automatic control
Failure to control	Operator control of equipment results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach
Failure of manual initiation or actuation	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late Operators fail to perform backup, manual startup after automatic actuation fails (recovery)
Inappropriate termination	Operators stop (e.g., pumps stopped Operators both stop and disable equipment for future service (e.g., pumps in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop eqipment and disable automatic signals or sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
Inappropriate isolation	Operators re-align equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals
Inappropriate diversion or depletion of resources	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.) Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident
Failure to terminate	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late Operators fail to perform backup, manual stop after automatic stop fails (recovery) Operator fail to perform backup, manual stop after spurious start or re-start (recovery)
Inappropriate status change	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control Operator actions (e.g., operator fails to operate or control, operator inappropriately operates or controls) from other categories result in failure to maintain integrity , inappropriately breached integrity, etc.

fonte: U.S. Nuclear Regulatory Commission – Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624, Rev.1. Washington DC, U.S. NRC, 2000

Anexo F. HAZOP - *Hazard And Operability Technique*

HAZOP é um método de avaliação de risco que foi desenvolvido em 1964 pela companhia ICI, com o intuito de analisar processos químicos. Actualmente tem um uso bastante mais vasto, sendo aplicado a outros tipos de sistemas, embora seja ainda largamente utilizado na indústria química. O método HAZOP deve ser utilizado, preferencialmente, na fase de projecto de novos sistemas quando já se dispõe dos fluxogramas de engenharia e de processo da instalação ou durante ampliações ou modificações de sistemas já em operação. No entanto pode também ser utilizado para revisão geral de sistemas já em funcionamento. É um método de identificação de perigos baseado em palavras-guia e levado a cabo por uma equipa multidisciplinar durante uma série de reuniões. Visa identificar os problemas de operabilidade de uma instalação, baseando-se na ideia de que os problemas operacionais ou de segurança estão sempre relacionados com desvios nos parâmetros ou variáveis do processo. Tem em consideração a operação normal de um dado equipamento ou processo e analisa os possíveis cenários de desvio dessa operação. Esses desvios podem ser de pouca importância ou vir a ter consequências muito graves. A execução do HAZOP exige uma equipa multidisciplinar, de 4 a 6 pessoas, constituída especialmente pelos seguintes elementos:

Líder – pessoa com experiência de aplicação do método, responsável por orientar as reuniões, seleccionar os membros da equipa, planear e preparar o estudo, verificar imprecisões e omissões;
Projectista – tem que estar apto a responder a perguntas, no entanto, pode não ter consciência de alguns perigos por estar demasiado próximo;
Especialista – pessoa com bons conhecimentos do sistema em causa e que não está directamente envolvido com a instalação;
"Perguntador" – pessoa sem qualquer experiência e conhecimento do sistema em causa que tem a função de fazer perguntas, mesmo que sejam absurdas;
Secretário – pessoa responsável por preparar a folha de trabalho, registar todas as ideias verbalizadas e preparar relatórios.

O líder deve ser independente do sistema, ou seja., não deve ter qualquer tipo de responsabilidade pelo processo ou pela *performance* das operações. A constituição da equipa é flexível podendo, por vezes, uma mesma pessoa representar o líder e o especialista, tal como acontece com o "perguntador" e o secretário. A metodologia do HAZOP é composta pelos seguintes passos:

1. Descrição completa do sistema em estudo aos participantes;
2. Selecção da parte do sistema a analisar;
3. Análise da parte seleccionada utilizando palavras-guia;
4. Continuação da selecção de partes do sistema para analisar (passos 2 e 3) até se efectuar a análise completa do sistema;
5. Registar consequências e causas, assim como propor medidas.

Para o primeiro passo o projectista deve apresentar diagramas, complementados por uma memória descritiva do funcionamento, operações executadas e substâncias envolvidas. Toda a equipa deverá estudar o sistema e questionar o projectista de modo a assegurar que nenhuma informação foi omitida.

As palavras-guia são aplicadas a variáveis características de cada actividade, determinando-se as consequências. As variáveis normalmente utilizadas nas indústrias em geral, são: o caudal, pressão, vácuo, temperatura, nível, concentração, pH, viscosidade, voltagem, etc. Por sua vez as actividades usualmente analisadas são transferência, aquecimento, arrefecimento, condensação, mistura, combustão, diluição, dissolução e reacção, para não refeir outras mais.

Na tabela seguinte encontram-se as palavras-guia, usualmente utilizadas e exemplos da sua utilização:

Tabela 14 - Exemplos da utilização de palavras-guia na indústria química

Palavras-Guia	Exemplos
NÃO ou NENHUM	Ausência de caudal de água no condensador; falta de um reagente; falha da corrente eléctrica; ausência de mistura
OPOSTO	Juntar um ácido em vez de uma base; aquecimento em vez de arrefecimento; escoamento em sentido inverso
TAMBÉM	Água num tanque de combustível; ar numa tubagem com líquido; ligação indevida de um aquecedor; electricidade estática
MAIS	Demasiado quente; demasiado frio; excesso de um reagente; nível de líquido alto
MENOS	Arrefecimento insuficiente; combustão incompleta; mistura deficiente; nível de líquido baixo; caudal reduzido; ventilação deficiente
OUTRO	Ar em vez de azoto; ligar o aquecedor em vez do agitador

fonte: Kletz, T. A. - Hazop and Hazan: Identifying and Assessing Process Industry Hazards - 4.ª ed., Rugby, UK - Institution of Chemical Engineers, 2001