UNIVERSIDADE ESTADUAL DE CAMPINAS
UNICAMP

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA, E COMPUTAÇÃO CIENTÍFICA- IMECC

TESE DE MESTRADO EM QUALIDADE

A Técnica *HAZOP*, como ferramenta de aquisição de dados para avaliação da *CONFIABILIDADE HUMANA* na indústria química.

Autor: José Luiz Lopes Alves

Orientador: Prof. Dr. Manuel Folledo

Campinas, julho de 1997

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. José Luiz Lopes Alves e aprovada pela Comissão Julgadora.

Campinas, 22 de julho de 1997

Prof. Dr. Manuel Folledo

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Qualidade.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Alves, José Luiz Lopes

AL87t A técnica HAZOP, como ferramenta de aquisição de dados para avaliação da confiabilidade humana na indústria química / José Luiz Lopes Alves -- Campinas, [S.P. :s.n.], 1997.

Orientador : Manuel Folledo

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Engenharia humana. 2. Confiabilidade (Engenharia). 3. Avaliação de riscos. I. Folledo, Manuel. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Dissertação de Mestrado defendida e aprovada em 22 de julho de 1997

pela Banca Examinadora composta pelos Profs. Drs.

Prof (a). Dr (a). MANUEL FOLLEDO

Prof (a). Dr (a). ADEMIR JOSÉ PETENATE

Prof (a). Dr (a). CHARLY KUNZI

Aos operadores das unidades de processo, que dia e noite se defrontam com as mais variadas situações, muitas delas nunca vividas anteriormente, e que sustentam a confiabilidade, que preserva toda a sociedade.

Agradecimentos

➲ Ao engenheiro Luiz Roberto Pinto Gil, que dividiu comigo a tarefa de coordenar os estudos de segurança de processo na Usina Química de Paulínia, da Rhodia, e com quem durante anos troquei opiniões, sobre a complexa atividade de gerenciamento de riscos.

➲ À sra. Maria Célia Dubois, responsável pelo Centro de Documentação no Centro de Pesquisas da Rhodia, meu muito obrigado. A partir de contatos por telefone e correio eletrônico, pude receber com elevada qualidade muitos dos artigos que precisei.

➲ Um agradecimento especial à todas as equipes de operação, mecânicos, instrumentistas e eletricistas, engenheiros de processo e pesquisadores que, durante vários anos, se engajaram numa tarefa sem precedentes, plenamente cientes e dotados de elevada responsabilidade, para melhorar o nível de segurança das unidades de operação da Rhodia de Paulínia.

➲ O esforço que foi realizado, fruto exclusivamente de uma decisão da Rhodia, só teve sucesso devido a determinação da diretoria da empresa em executar o programa definido. Ao atual diretor de Ciência e Tecnologia, engenheiro R. Franchi, que gerenciou o processo, o agradecimento e reconhecimento pelos resultados que conseguimos alcançar.

➲ À UNICAMP, que através do Mestrado em Qualidade do IMECC, tem contribuído para a busca da excelência por um elevado número de empresas, e um crescimento pessoal de muitos profissionais. À todos os professores do mestrado, à professora Ana Guerra pelo primeiro incentivo a este trabalho, e ao professor Manuel Folledo, que me recebeu e orientou no mestrado.

Epígrafe

" ... Permanecemos assim durante longos momentos... o mestre se levantou e fez sinal para que eu o acompanhasse... me pediu para fixar uma haste de incenso, longa e delgada como uma agulha de tricotar, na areia diante do alvo...

... Sua primeira flecha partiu da intensa claridade em direção à noite profunda. Pelo ruído do impacto, percebi que atingira o alvo, o que também ocorreu com o segundo tiro. Quando acendi a lâmpada que iluminava o alvo constatei, estupefato, que não só a primeira flecha acertara o centro do alvo, como a segunda também o havia atingido, tão rente à primeira, que lhe cortara um pedaço, no sentido do comprimento...

Não é difícil imaginar o impacto que as flechas do mestre causaram em mim. Como se eu tivesse passado por uma transformação profunda. Já não me preocupava com minhas flechas e o seu destino.

Além disso, o mestre reforçava essa minha atitude não olhando jamais para o alvo, mas observando apenas o arqueiro, como se isso lhe permitisse comprovar de maneira mais precisa o resultado do tiro.

Em nome da mais profunda experiência pessoal, da qual eu sempre desconfiara, não hesito em afirmar que a comunicação direta de que tanto se fala não é uma fantasia, mas um fenômeno de palpável realidade."

A Arte Cavalheiresca do Arqueiro Zen *[1]*

Página

LISTA DAS SIGLAS

ASEP	*Accident Sequence Evaluation Program*
CADET	*Critical Action and Decision Evaluation Technique*
CLP	*Controlador Lógico Programável*
COBT	*Conversion d'Oxygène a Baisse Température*
COHT	*Conversion d'Oxygène a Haute Température*
DA	*Decision Action*
DAA	*Diacetona Álcool*
EPA	*Environmental Protection Agency*
EPC	*Error Production Condition*
EPI	*Equipamento de Proteção Individual*
FIC	*Flow Indicator Controler*
FMC	*Falhas de Modo Comum*
FMEA	*Failure Mode and Effect Analysis*
FR	*Flow Recorder*
GCC	*Gestão Centrada em Confiabilidade*
HAZAN	*Hazard and Analysis*
HAZOP	*Hazard and Operability*
HCV	*Handled Control Valve*
HEART	*Human Error Assessment and Reduction Technique*
HIC	*Handled Indicator Controler*
HGL	*Hexilenoglicol*
HMD	*Hexametilenodiamina*
HRA	*Human Reliability Analysis*
HTA	*Hierarchical Task Analysis*
IMAS	*Influence Modeling and Assessment Systems*
ISRS	*International Safety Rate System*
LAH	*Level Alarm High*
LI	*Level Indicator*
LIC	*Level Indicator Controler*
LSH	*Level Switch High*
MAST	*Memory and Search Test*

MCC	*Manutenção Centrada em Confiabilidade*
OAET	*Operator Action Event Trees*
OSHA	*Occupational Safety and Health Administration*
OSD	*Operational Sequence Diagram*
PAL	*Pressure Alarm Low*
PDI	*Pressure Diferencial Indicator*
PHA	*Process Hazard Analysis*
PHEA	*Predictive Human Error Analysis*
PHECA	*Potencial Human Error Cause Analysis*
PI	*Pressure Indicator*
PIAH	*Pressure Indicator Alarm High*
PIC	*Pressure Indicator Controler*
PMTP	*Pressão Máxima de Trabalho Permitida*
PR	*Pressure Recorder*
PROV	*Pilot Operated Relief Valve*
PSA	*Probabilistic Safety Assessment*
PSAL	*Pressure Switch Alarm Low*
RCM	*Reliability Centred Maintenance*
SDCD	*Sistema Digital de Controle Distribuído*
SFGS	*Signal-Flow Graph Analysis*
SHERPA	*Systematic Human Error Reduction and Prediction Approach*
SRK	*Skill, Rule, Knowledge - mode*
THERP	*Technique for Human Error Rate Prediction*
TAH	*Temperature Alarm High*
TAL	*Temperature Alarm Low*
TI	*Temperature Indicator*
TIAH	*Temperature Indicator Alarm High*
TISH	*Temperature Indicator Switch High*
TR	*Temperature Recorder*
TRC	*Temperature Recorder Controler*
UQP	*Usina Química de Paulínia*

RESUMO

No caminho da construção das organizações de alta performance encontram-se vários processos, com modelos particulares de gerenciamento. A excelência, caracterizada por um nível reconhecidamente diferenciado de qualidade da organização, é atingida quando uma visão sistêmica predomina na gestão, e todos os processos operam em um ambiente integrado.

Este nível de qualidade depende da confiabilidade das diversas partes que compõem todo o sistema, ou em outras palavras, pela probabilidade de sucesso no cumprimento das múltiplas missões definidas na organização. A excelência será atingida quando a qualidade total existir, com uma gestão centrada na confiabilidade. A confiabilidade, numa visão sistêmica, compreende todos os agentes dos processos, incluindo equipamentos, instrumentos, e as pessoas que desenvolvem, operam, modificam e melhoram as organizações.

O histórico da confiabilidade industrial, particularmente nas industrias químicas, demonstra que a maior parte das falhas que existem nos sistemas são de natureza humana, e a perda da confiabilidade, nestes tipos de empresas, origina elevadas perdas humanas e de investimentos. Desta forma, centrar na confiabilidade a gestão de uma atividade industrial química, requer esforços para a melhoria da confiabilidade humana.

Existem muitas técnicas para a avaliação da probabilidade do erro humano, a maioria complexas, exigindo alta especialização para a sua aplicação. Todas requerem, num primeiro momento, a caracterização " do que pode ser feito errado " em uma determinada tarefa.

Este trabalho apresenta considerações teóricas relativas à natureza das falhas humanas, e uma abordagem geral sobre estas metodologias. O foco principal do trabalho é o uso de uma destas técnicas - a metodologia HAZOP - desenvolvida inicialmente para a indústria química, para a identificação de perigos, como instrumento importante para aquisição de dados de falhas humanas.

O conteúdo mostra casos reais do desempenho da técnica, que foi aplicada em várias unidades de processo de um parque industrial químico, usando os procedimentos propostos pelos seus

idealizadores. Em cerca de 50 estudos realizados, as falhas potenciais de natureza humana variaram entre 17 % e 63 %, com uma média de 36 %.

A partir das falhas identificadas, foi possível determinar ações para reduzir os riscos avaliados, com impactos na segurança do processo, na produtividade das unidades e, desta forma, na qualidade das operações. O trabalho apresenta ainda exemplos de adaptação da técnica para o tratamento específico de erros humanos, tratando aspectos cognitivos envolvidos na realização das tarefas.

A realização de estudos de operabilidade e avaliação de riscos na indústria química, com a técnica HAZOP, tem crescido com o passar do tempo, e vem sendo exigido por órgãos oficiais de controle ambiental em todo o mundo.

A aplicação da metodologia HAZOP, com foco específico para avaliação de falhas humanas, pode ser de fundamental importância para o real aumento da confiabilidade industrial e, assim, para a busca da excelência.

1. Introdução

" Se fazemos escolhas certas, é possível melhorar a performance e, ao mesmo tempo, conter ou mesmo reduzir custos... Se fazemos escolhas erradas, novos problemas são criados, enquanto que os existentes tornam-se piores " - John Moubray [2]

Estudos sobre o comportamento humano nas mais variadas atividades, mantêm continuadamente o interesse de muitas pessoas. A busca da excelência, em qualquer ambiente de trabalho, sempre encontra a necessidade da melhora contínua da performance dos chamados "recursos humanos".

Ir em busca da Qualidade Total - no sentido mais amplo possível desta expressão - requer inicialmente aceitar o fato de que as pessoas falham devido sua própria natureza humana e, em segundo lugar, compreender os mecanismos, complexos em sua maioria, que agem na mente humana no dia a dia, durante situações normais de trabalho, e em momentos de elevada tensão.

Muitos estudos que são desenvolvidos sobre este assunto, encontram-se inseridos em trabalhos sobre confiabilidade industrial. O objetivo em geral, é a prevenção de acidentes em atividades como a exploração espacial; a aviação de modo geral; a indústria nuclear; a indústria química.

O objetivo principal destes esforços é criar um modelo de gestão que seja *centrado na confiabilidade*. E sem dúvida, os conceitos e as teorias que são desenvolvidos em todas estas atividades podem, em grande parte, ser usados em muitos outros ramos, mesmo fora da indústria.

Centrar uma determinada atividade ou processo na confiabilidade, significa *"ter o conhecimento do sistema"*. A abrangência deste conhecimento não é fácil de explicar, mas é relativamente simples de entender com um grande exemplo: quando o presidente John F. Kennedy em 1961 desafiou o povo americano para que até o final da década de 60, os Estados Unidos enviassem uma nave tripulada à lua, e a trouxessem de volta, não havia o "conhecimento" para esta tarefa. Ele teve de ser construído.

As milhares de equipes que participaram deste projeto construíram uma confiabilidade que não existia e, assim, ganharam o conhecimento do processo de ir e vir nas viagens espaciais.

Nestes grandes e audaciosos projetos e, principalmente a partir deles, algumas atividades estruturaram uma forma de adquirir este conhecimento. Entre elas está a manutenção dos sistemas industriais. Em 1974 o departamento de Defesa dos Estados Unidos encomendou à United Airlines um relatório sobre o processo usado para a manutenção na aviação civil. O relatório foi denominado *Reliability Centred Maintenance* (RCM). Em 1978 e 1984 a RCM chegou à marinha e à indústria nuclear americana, respectivamente.

Uma forma organizada de avaliar cada tarefa fora desenvolvida, para garantir não a sobrevivência dos elementos dos sistemas, mas das suas *funções no seu contexto operacional* e, assim, alcançar: alto nível de disponibilidade e confiabilidade nas plantas industriais; elevada segurança; melhor qualidade; redução de impactos ambientais; aumento da vida dos equipamentos; e grande redução dos custos [2].

O processo está sendo introduzido no Brasil como Manutenção Centrada em Confiabilidade (MCC). O método proposto no processo MCC é de particular ajuda na atividade de manutenção e, seu impacto sem dúvida, mudará o resultado econômico das empresas que o aplicarem.

Contudo, este exemplo precisa ir além das *fronteiras,* muitas vezes definidas nas organizações das empresas, onde *cada time* tem seu modo de gestão da *sua* performance. Isto é importante pois entre as principais mudanças ocorridas nas atividades industriais, está a gestão de *processos de trabalho integrados*, e não mais de processos e atividades isoladas que, numa visão antiga, eram muitas vezes considerados *independentes*.

A Figura 1 a seguir mostra alguns destes processos que, com certeza, impactam na *Confiabilidade da Empresa*: os Processos das Funções Produtivas (incluindo projeto, operação, manutenção, inspeção, testes, logística, etc...); os processos definidos no Sistema da Qualidade, conforme as normas da família NBR ISO 9000; os processos definidos nos Sistemas de Segurança, como por exemplo o ISRS - International Safety Rate System (Sistema Internacional de Avaliação da Segurança); e os processos definidos para o Gerenciamento Ambiental , como descritos na norma NBR ISO 14000.

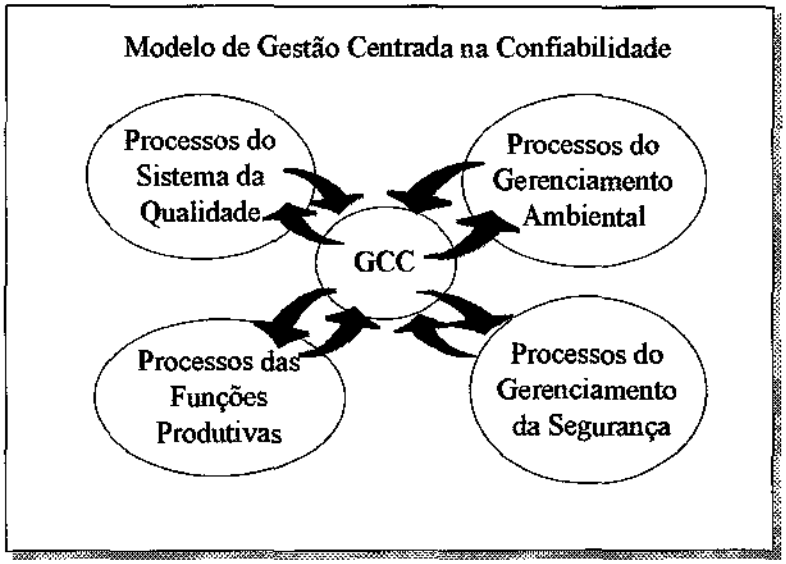


Figura 1 - Modelo de Gestão Centrada na Confiabilidade

A não inclusão de processos administrativos, de marketing ou financeiros neste modelo, é devida apenas à necessidade de salientar o foco principal deste trabalho - o ambiente industrial. Ainda, mesmo que existam opiniões de que centrar tudo na confiabilidade, é a mesma coisa que atingir a Qualidade Total, preferimos usar o enfoque em um modelo denominado Gestão Centrada na Confiabilidade como "invólucro", pelo simples fato dos conceitos de confiabilidade terem sido anunciados antes do Movimento da Qualidade. Ambos "invólucros" são bons e de certa forma complementares. Uma boa definição de confiabilidade é: a probabilidade de haver qualidade!

O primeiro fato que torna esta abordagem importante é a interligação que sem dúvida existe entre estes processos. O segundo, é que são as pessoas os principais agentes em todos eles. Mesmo com o desenvolvimento tecnológico existente, ainda são indivíduos que, de uma forma ou de outra: observam; fazem o diagnóstico; e tomam as decisões. Então, se uma gestão centrada na confiabilidade pode tornar-se o salto quântico para as empresas, é imperativo considerar, para que este modelo funcione, a confiabilidade humana. Todos estes processos se inter-relacionam através de pessoas, nos mais variados graus de " inteligência intelectual e emocional ".

Análises com ferramentas que *enxergam* sistemas, como árvore de falhas, comprovam que a maioria das causas são de natureza humana. Assim, uma visão sistêmica dos "por quês" as falhas ocorrem - principalmente as decorrentes de erros humanos - tornou-se imprescindível para

o aumento da confiabilidade. Causas especiais ou inerentes ao processo, se investigadas até suas raízes, com certeza sempre levarão à falhas humanas. A maioria delas, são falhas de gerenciamento, ou falhas da administração.

A "teoria dos dominós" desenvolvida por Heinrich (1936) mostra claramente como os eventos evoluem, numa seqüência invertida, desde a observação do(s) efeito(s) da falha, até os processos administrativos - suas verdadeiras causas raízes. A investigação de acidentes, realizada de forma científica e por profissionais habilitados, é um dos pontos fundamentais para a redução da freqüência dos acidentes [3] [4]. A identificação de possíveis falhas antes que elas aconteçam, deve ser, entretanto, o ponto de partida.

O objetivo deste trabalho foi comprovar o uso da técnica denominada HAZOP, usada na identificação de perigos, como instrumento de aquisição de dados de falhas humanas, como forma de prevenção de incidentes e acidentes industriais para o aumento da confiabilidade.

No que se refere a segurança das instalações químicas, o trabalho inclui questões importantes que devem ser levadas em consideração quando se fala em confiabilidade de sistemas, e se deseja avaliar o desempenho das pessoas, como forma de prevenção de possíveis falhas.

No contexto da qualidade, o trabalho mostra a técnica HAZOP como uma ferramenta para melhorar a produtividade e a competitividade, a partir do aumento da disponibilidade dos sistemas que fazem parte dos processos produtivos.

2. Considerações gerais e teorias aplicadas na confiabilidade humana

" O homem é uma criatura feita no final da semana ...
quando Deus estava cansado" - Mark Twain [5]

2.1 A influência das falhas de natureza humana

Falhas de materiais, equipamentos ou sistemas, sempre poderão ser atribuídas aos seus componentes. Contudo, também poderão ser originárias de falhas nas etapas de pesquisa, de projeto ou de construção, erros nos processos de compras, falhas de operação, falhas nos procedimentos de inspeção, de manutenção, e em testes. Os erros humanos gerados nestes processos são, provavelmente, os eventos iniciadores de maior contribuição para a perda de vidas, lesões em pessoas e danos em propriedades, na indústria química.

Erros em projetos que não consideram esforços de ventos sobre estruturas, ou aço especificado de forma errada, ou um inspetor que não detecta corrosão, são também exemplos de falhas humanas. As pessoas cometem erros por muitas razões, mas especialistas estimam que apenas 15 % dos erros nos ambientes de trabalho são devidos às influencias pessoais, tais como estado emocional, saúde, ou falta de cuidado. Todos os demais erros resultam de causas externas como: procedimentos deficientes; supervisão inadequada; pessoal de apoio insuficiente; treinamento inadequado; interface homem-máquina inadequada; e ambiente físico inadequado.

H. L Willians, conforme mencionado por Dhillon [6], foi uma das primeiras pessoas que identificou (em 1958) a necessidade de incluir a confiabilidade humana na avaliação da confiabilidade de sistemas. Dhillon menciona várias referências de erros humanos identificados por pesquisadores de diversas entidades, bem como indica um grande número de bancos de dados de falhas humanas.

Em março de 1974, uma explosão na fábrica da Nypro em Flixborough na Inglaterra, causou a morte de 28 pessoas, feriu 89, e danificou 1821 casas. O evento inicial foi a ruptura de uma tubulação improvisada, de 20 polegadas de diâmetro, que não foi projetada adequadamente [7].

Em 1976, numa planta química em Seveso na Itália, erros operacionais levaram à emissão de uma nuvem tóxica sobre a cidade, contendo dioxina, causando sua completa evacuação [8].

Em março de 1979, falhas de diagnóstico provocaram incêndios e emissão radioativa na usina nuclear de Tree Mile Island nos Estados Unidos, com elevado potencial de risco [9].

Em 3 de dezembro de 1984, um vazamento de metil-iso-cianato, causado por: falhas gerenciais; carência de ordens hierárquicas; erros de concepção; e vícios de fabricação, levou à fatalidade 2500 pessoas em Bhopal na Índia [10]. Estudos conduzidos por D. A. Lihou e S. P. Whalley, demostraram a forte ligação das causas com fatores modeladores de performance, da organização e das pessoas que operavam a unidade de processo [11].

Antes deste acidente, a maior catástrofe na indústria química ocorreu em Oppau na Alemanha em 1 de setembro de 1921, onde erros de avaliação de riscos causaram a morte de 561 pessoas, após uma explosão de uma mistura de sulfato e nitrato de amônia [12].

Em 26 de abril de 1986, na planta nuclear ucraniana de Chernobyl, a explosão do reator número 4 causou a morte de 30 pessoas, e danos ao meio ambiente até hoje não conhecidos. Os erros foram em sua maior parte causados por violações nos sistemas de segurança [13].

Particularmente nas indústrias químicas, uma série de dados históricos confirmam o grande impacto dos erros humanos [Ref. 14, pág. 5]. Garrison (1989) através da publicação *One Hundred Large Losses,* documenta a contribuição de erros operacionais nas maiores perdas financeiras ocorridas nas indústrias de processamento químico até 1984. Ele indica que erros causados no ambiente das indústrias (*on-site*), responsáveis diretamente pelas perdas, somavam 563 milhões de dólares, e eram a segunda causa principal das perdas.

Se fossem computados os erros fora do ambiente das fábricas (*of-site*), como por exemplo a falha de projeto que causou o acidente de Flixborough, os erros humanos seriam a causa predominante destas perdas.

Em análise mais recente, Garrison indicou que, no período de 1985-1990, o fator humano foi o fator significante para mais de dois bilhões de dólares de perdas na indústria química. Estudos de Uehara e Hasegawa sobre 120 incêndios em indústrias químicas japonesas, ocorridos entre 1968 e 1980, mostraram que 45 % dos casos foram devidos a erros humanos. Se nestes acidentes fossem incluídos os erros de projeto e escolha de materiais, a contribuição dos erros humanos passaria para 58 %.

Butikofer (1986) mostrou que nos acidentes ocorridos em unidades petroquímicas e em refinarias, 41 % foram causados por falhas de projeto e de equipamentos; 41 % por falhas de

manutenção; 11 % por procedimentos inadequados; 5 % por inspeção inadequada e 2 % por outras causas. Outros estudos complementam estes dados, conforme mostrado na Figura 2.

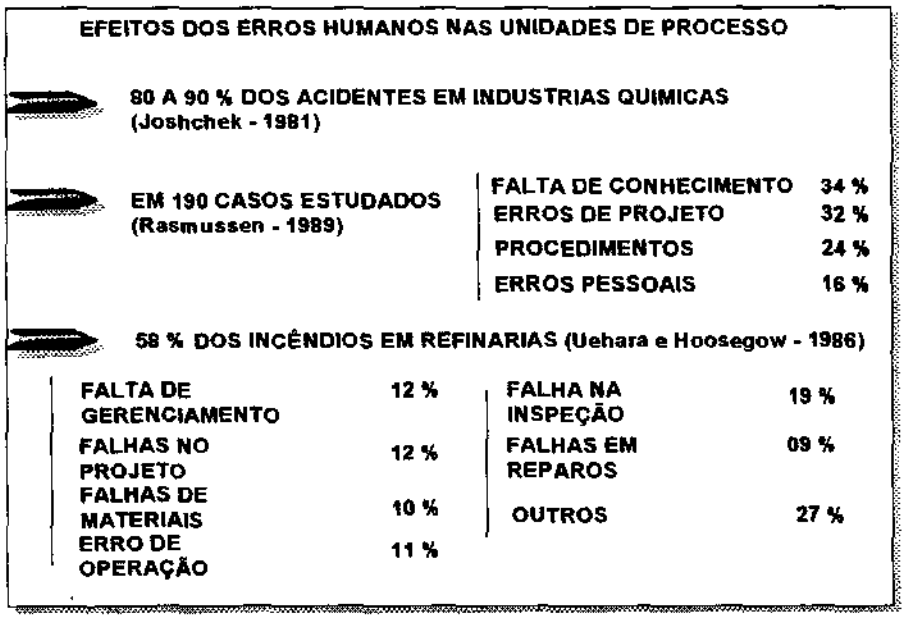


Figura 2 - Efeitos dos Erros Humanos nas Unidades de Processo (Ref. 14, pág. 6)

As Tabelas I e II a seguir mostram alguns dados de grandes eventos ocorridos em plantas de processo, que envolveram de alguma forma falhas de natureza humana [15] [12, pág. 14].

Tabela I. As grandes evacuações de população ocorridas em grandes acidentes industriais entre 1969 à 1987.

DATA	LUGAR	Nº	PRODUTO	CIRCUNSTANCIAS
1979	MISSISSAUGA (CANADA)	240 000	CLORO 70 T	TREM - EMISSÃO
1984	BHOPAL (INDIA)	200 000	METIL ISOCIANATO	REAÇÃO - EMISSÃO
1986	CHERNOBYL (URSS)	112 000	RADIOATIVIDADE	REAÇÃO - EMISSÃO
1979	THREE MILE ISLAND (USA)	50 000	HIDROGÊNIO	CENTRAL NUCLEAR
1984	MÉXICO	39 000	GLP	FOGO E EXPLOSÃO
1984	IXHUATEPEC (MÉXICO)	31 000	GLP	EXPLOSÃO
1981	SAO FRANCISCO (USA)	30 000	GASOLINA	TUBOVIA
1987	SALT LAKE CITY (USA)	30 000	TRICLOROETILENO	FABRICA
1969	GLENDORA (USA)	30 000	CLORETO DE VINILA	TREM - EMISSÃO
1983	CORINTO (NICARAGUA)	23 000	HIDROCARBONETOS	REAÇÃO - EXPLOSÃO
1980	SOMERVILLE (USA)	23 000	P C L 3	TREM - EMISSÃO
1982	TAFT (USA)	17 000	ACROLEINA	FÁBRICA - EMISSÃO
1975	HEIMSTETTEN (ALEMANHA)	10 000	NOx	FÁBRICA - EMISSÃO
1976	BATON ROUGE (USA)	10 000	CLORO 90 T	FÁBRICA - EXPLOSÃO
1978	MANFREDONIA (ITÁLIA)	10 000	AMÔNIA	FÁBRICA - EMISSÃO
1979	CRYSTAL CITY (USA)	6 000	AGROQUÍMICOS	ARMAZÉM - FOGO
1969	ESCOMBRERAS (USA)	5000	GASOLINA	REFINARIA-EXPLOSÃO
1976	SEVESO (ITÁLIA)	737	EMISSÃO DE DIOXINA	REAÇÃO - EMISSÃO

Tabela II. Registros de fatalidades ocorridas em acidentes industriais, envolvendo produtos perigosos, entre 1978 e 1989.

DATA	LUGAR	Nº	PRODUTO	CIRCUNSTANCIAS
1984	BHOPAL (ÍNDIA)	> 2000	METIL ISOCIANATO	REAÇÃO - EMISSÃO
1984	CUBATÃO (BRASIL)	508	GASOLINA	EXPLOSÃO TUBOVIA
1984	IXHUATEPEC (MÉXICO)	> 500	GLP	TANQUES - EXPLOSÃO
1979	NOVOSIBIRSK (URSS)	300	PRODUTOS QUÍMICOS	FABRICA - EMISSÃO
1978	LOS ALFAQUES (ESPANHA)	216	PROPILENO	VAGÃO - EXPLOSÃO
1989	PIPER ALPHA (MAR DO NORTE)	160	GÁS E PETRÓLEO	EXPLOSÃO
1982	TACOA (VENEZUELA)	145	HIDROCARBONETOS	REAÇÃO - EXPLOSÃO
1980	KIELLAND (NORUEGA)	123	PETRÓLEO	PLATAFORMA
1978	XILATOPEC (MÉXICO)	100	BUTANO	VAGÃO - EXPLOSÃO
1980	OCEAN RANGER (CANADA)	84	PETRÓLEO	PLATAFORMA
1979	ISTAMBUL (TURQUIA)	72	PETRÓLEO	VAGÃO - EXPLOSÃO
1984	GHARI BHODA (PAQUISTÃO)	60	GÁS NATURAL	TUBOVIA - EXPLOSÃO
1985	TANIL NADU (ÍNDIA)	60	GASOLINA	VAGÃO - EXPLOSÃO
1978	HUIMAN GUILLE (MÉXICO)	58	GÁS NATURAL	TUBOVIA - EXPLOSÃO
1986	CHERNOBYL (URSS)	33	RADIOATIVIDADE	REAÇÃO - EMISSÃO

2.2 A confiabilidade humana na visão sistêmica

As unidades de processo (plantas químicas) tipicamente começam a ser construídas a partir da definição dos requisitos necessários para a produção: seleção do processo; escolha do local; *layout*; projeto dos equipamentos; etc. Todas as primeiras decisões podem ser vistas, em conjunto, como o primeiro nível de proteção contra eventos indesejáveis. Embora estas decisões possam parecer corretas, ainda assim outros níveis de proteção são previstos.

Desta forma, sistemas de controle do processo são projetados criteriosamente, e uma seqüência de barreiras são colocadas "em série", com o objetivo de diminuir a probabilidade e a gravidade dos cenários críticos.

A Figura 3 mostra como estão arranjadas estas "camadas de proteção", que são (ou não) construídas a partir de critérios definidos pelas próprias empresas e/ou pela legislação local. É possível perceber que, em todas as camadas, tão ou mais importante que o *hardware* instalado, com características de confiabilidade intrínseca, existe de alguma forma a presença humana.

A figura do homem neste sistema, da mesma forma, possui uma determinada confiabilidade. Um evento iniciador percorrerá o caminho desde a camada interior até a última camada de proteção, até encontrar (ou não) uma barreira confiável.

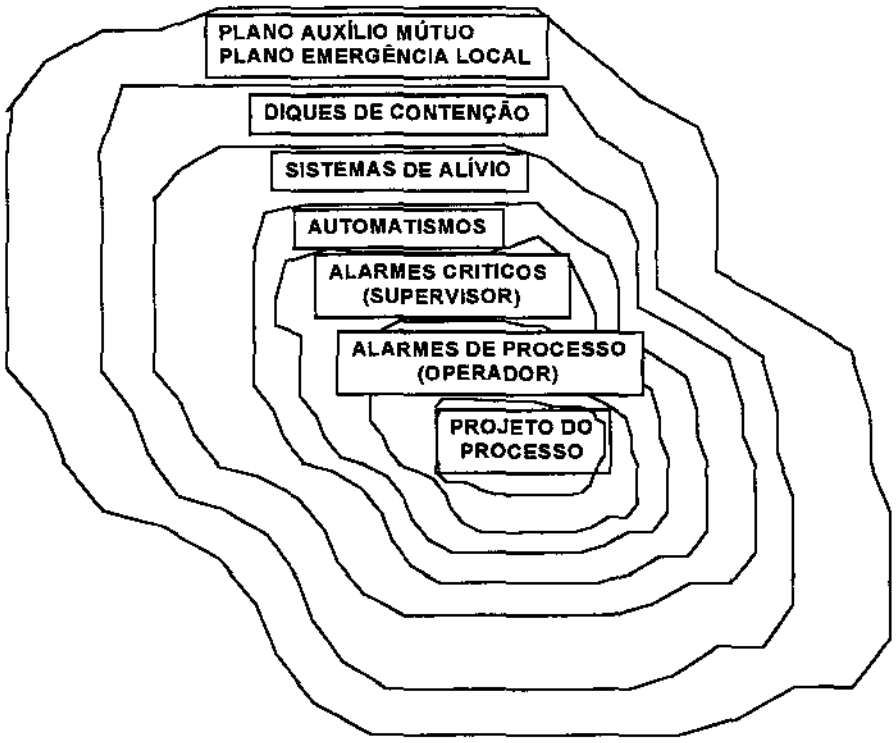


Figura 3. Típicas camadas de proteção encontradas nas modernas plantas químicas

Conforme a ABNT - Associação Brasileira de Normas Técnicas [16] - confiabilidade é uma característica de um item expressa pela probabilidade de que executará uma função exigida, sob condições estabelecidas e por um intervalo de tempo determinado.

Evans (1976) salienta que, de forma popular, confiabilidade é definida como sendo a probabilidade de um desempenho de uma missão com sucesso. Meister (1966) define a confiabilidade humana como a probabilidade de que um trabalho ou tarefa seja completada com sucesso, por pessoas, em qualquer estágio do sistema operacional, dentro do tempo mínimo requerido (se o limite de tempo mínimo existir). Swain [17] aproveitando as definições de Evans e Meister, sugere que a confiabilidade humana é a probabilidade de uma pessoa: (1) desenvolver corretamente uma atividade requerida pelo sistema, no período de tempo requerido (se este tempo existir) e (2) desenvolver uma atividade não requerida, que possa degradar o sistema.

A partir deste conceito, pode-se dizer que a Não Confiabilidade Humana é a "probabilidade que uma pessoa falhe, no cumprimento de uma função requerida pelo sistema, quando chamada a faze-la, num determinado período de tempo".

Gertman e Blackman [Ref.18, pág 1] definem o erro como sendo: " ações ou ausência de ações, não desejadas, que surgem com problemas de sequenciamento, tempo, conhecimento, interfaces e/ou procedimentos, que resultam em desvios em relação a padrões esperados, ou modelos que colocam pessoas, equipamentos ou sistemas, em situação de risco.

Meister (1977) classificou os erros humanos em quatro grandes categorias, complementadas por A.D. Swain com um quinto modo de falha [Ref. 14, pág 40]:

- realização de uma ação de forma incorreta,
- não realização da ação (omissão),
- falha na seqüência de realização,
- realização de uma ação não requerida (comissionamento),
- não realização da ação no tempo necessário.

As causas das falhas que ocorrem em um sistema podem ser atribuídas a variadas fontes. Aggarwal [19] relaciona algumas importantes, que podem ou não ser reconhecidas, em função da complexidade do sistema e do seu meio ambiente: projeto, produção e uso inadequado; complexidade do sistema; manutenção inadequada; e não confiabilidade humana.

Com relação aos erros humanos, o autor cita como modos de falhas: ausência do conhecimento do equipamento; ausência do conhecimento do processo; falta de cuidado; esquecimento; falha na habilidade de julgamento; ausência de instruções e procedimentos operacionais corretos, e falta de aptidão física.

A não confiabilidade, ou a sua perda no período da "missão", sugere uma visão geral dos processos envolvidos no meio ambiente. Embrey [14] propõe que a perda da confiabilidade, ou seja, a probabilidade do erro ocorrer, está intimamente relacionada com o sistema envolvido. O modelo apresentado mostra que, enquanto o sistema solicita às pessoas (realiza demandas), existe por outro lado uma determinada capabilidade humana.

As respostas estarão sempre sendo influenciadas pelo meio ambiente e pela cultura da organização. O modelo está representado na Figura 4.

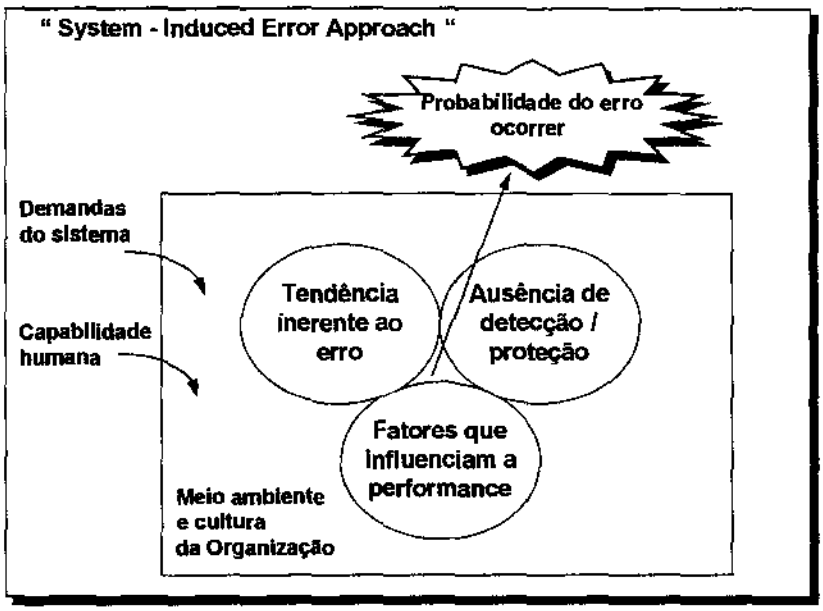


Figura 4 - Modelo para a indução ao erro [Ref. 14 Cap.1]

Esta representação do sistema tem sido denominada de *system-induced error approach* (abordagem do erro devido interferências no sistema). Ela mostra a influência dos fatores de performance (falhas em projetos, treinamento e procedimentos) como sendo causadores diretos das falhas, e o papel da administração e gerenciamento, que criam estas causas, ou circunstâncias para os erros.

Outro aspecto mostrado nesta forma de apresentação, é a interação dos fatores de performance com a tendência inerente ao erro que as pessoas possuem. A tendência intrínseca ao erro inclui a capabilidade limitada para processar informações, o apoio em normas que podem não ser apropriadas para lidar com situações normais, e a variabilidade que existe na realização de tarefas não rotineiras.

Contudo, as conseqüências de um erro apenas se manifestam se, apesar do erro ter sido cometido, o "sistema" não possuir capacidade de recuperação (*suport for recovery*). Esta capacidade pode estar alocada no próprio operador, quando ele consegue perceber e agir a tempo.

Pode ainda ser prevista no projeto do sistema, através de meios físicos de proteção. Neste particular, é sempre interessante que o sistema projetado seja intrinsecamente seguro, de tal forma que o estado após a falha, ainda seja tolerado (*fail safe*).

Muitos fatores, por sua vez, podem influenciar o desempenho de pessoas que naturalmente são sujeitas à falhas. A ocorrência do erro (ou melhor, da conseqüência do erro), dependerá se o sistema está provido de meios de detecção e proteção, também confiáveis.

O sistema estará equilibrado (balanceado) quando as demandas forem compatíveis com a capabilidade humana. Quando os recursos forem superiores, haverá um estado de "excelência" permitindo uma melhoria contínua. Quando o inverso ocorrer, surge o erro.

Formas de reduzir o número de erros normalmente são eficazes se houver um "aviso do sistema" - um *feed back* preventivo para que políticas e requisitos de capacitação possam ser revistos. Uma mudança cultural muitas vezes é imprescindível.

A visão do sistema, como descrito, está representada na Figura 5.

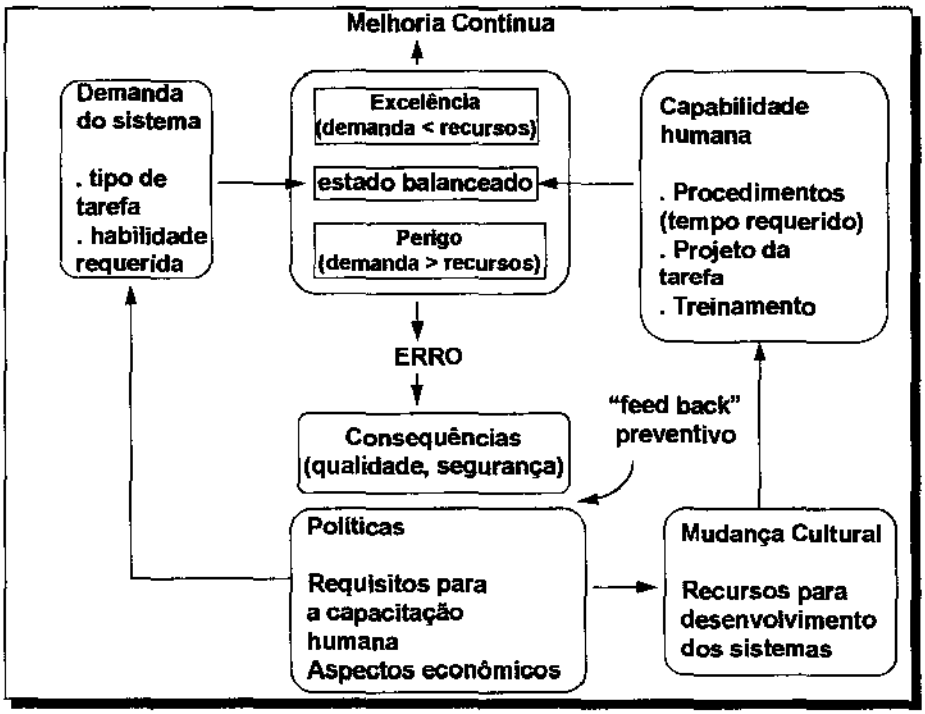


Figura 5 - Relação entre a demanda e a capabilidade humana [Ref. 14, Cap. 1]

2.3 Visão cognitiva das falhas humanas

Perspectivas diferenciadas são encontradas na questão dos processos que levam às falhas das pessoas. E em função desta diferença, no decorrer do tempo as formas de prevenção tem apresentado enfoques variados:

a) Engenharia de segurança tradicional - O controle das falhas age na motivação e na mudança de atitudes.

b) Erros são causados pela diferença entre demanda e recursos - O controle das falhas é realizado através de bons projetos (ergonomia, por exemplo), auditorias e *feed back* das experiências operacionais.

c) Perspectiva cognitiva - O controle das falhas acrescenta à perspectiva anterior os estudos das habilidades mentais (capacidade de diagnóstico).

d) Perspectiva sistêmica - O controle das falhas é feito através do aprimoramento das políticas de gerenciamento e culturas [20].

Na perspectiva cognitiva, existem basicamente dois tipos de falhas: Os **Deslizes** (*slips*), e os **Enganos** (*mistakes*). Na Figura 6, uma visão cognitiva *ampliada* é apresentada, baseada na classificação de erros humanos, adaptada por Reason em 1990 [Ref. 14, Cap. 2]. Pois além dos deslizes e enganos, podem existir também as **Violações**, como ocorreu no acidente da usina nuclear de Chernobyl [13].

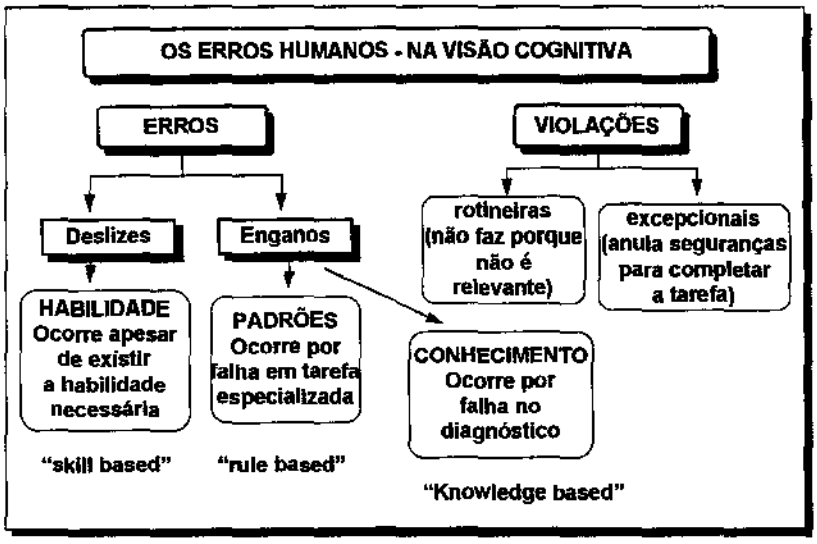


Figura 6 - Visão cognitiva dos erros humanos

A distinção entre deslizes e enganos foi feita pela primeira vez por Norman (1981). Segundo este autor, deslizes são erros nos quais a intenção é correta, mas a falha ocorre durante o desenvolvimento da tarefa. Um operador deve encher um determinado reator, mas enche outro, similar, localizado próximo.

Uma tarefa deve ser feita e o operador a faz de forma incorreta, por falhas de identificação, *layout* confuso, etc ... A tarefa é ligar a chave "A" e o operador liga a chave "B" devido, por exemplo, a uma identificação errada.

Enganos, ao contrário, ocorrem a partir de uma intenção incorreta, evoluindo para uma seqüência incorreta de ações, embora consistentes com a primeira ação realizada errada. Um operador que, por exemplo, pensa erroneamente que uma determinada reação é endotérmica e fornece calor ao equipamento, causando sobre-aquecimento. Intenções incorretas provém de falta de conhecimento ou falha de diagnóstico.

Neste último caso, o exemplo clássico foram os erros cometidos no acidente da usina nuclear de Tree Mile Island nos Estados Unidos.

A Figura 6 incorpora também o modelo formulado por J. Rasmussen, denominado SRK (*Skill, Rule, Knowledge - Based Classification*), que aborda a forma como são processadas as informações envolvidas nas tarefas industriais: tarefas baseadas na habilidade (*SB - Skill Based*); tarefas baseadas em regras (*RB - Rule Based*) e tarefas baseadas no conhecimento (*KB - knowledge based*). O modelo SRK refere-se ao grau de controle consciente, exercido pelo indivíduo na sua atividade [Ref. 18, pág 97].

Tarefas repetitivas, ou com ênfase no esforço físico, são baseadas na habilidade e são realizadas de forma natural, automaticamente, não havendo monitoramento consciente da tarefa. Já as tarefas baseadas no conhecimento, são desenvolvidas completamente no modo consciente.

Entre estes dois modos de resposta (automático e consciente), encontram-se as tarefas baseadas em regras, que são aprendidas pelas pessoas através de treinamentos ou experiências trocadas com operadores mais antigos. Esta distinção do modo de resposta pode ser melhor compreendida na Figura 7.

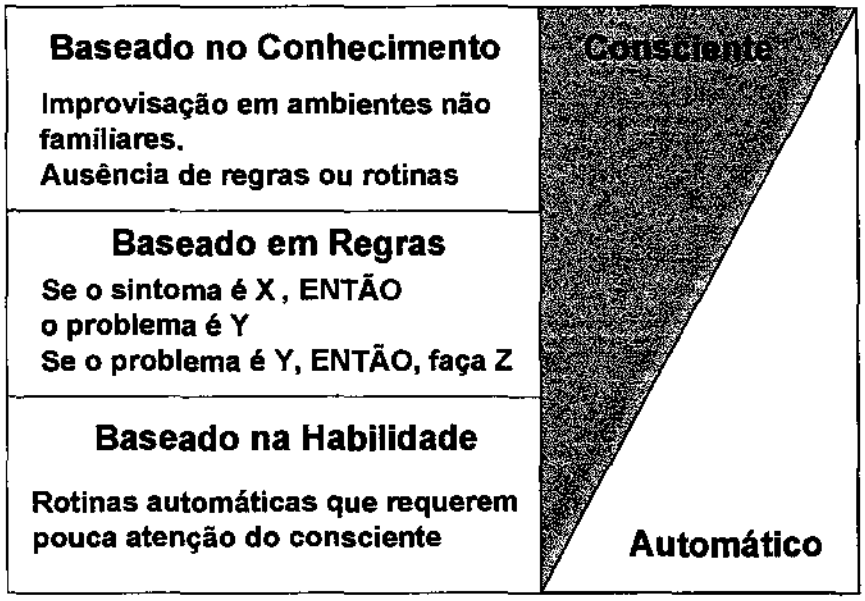


Figura 7 - O contínuo existente entre o comportamento consciente e automático (Reason, 1990).

Os deslizes são causados por falhas na competência, já que ocorrem em tarefas caracterizadas especificamente pela necessidade de habilidade. A pessoa no "modo habilidade" é capaz de agir em seqüências de comportamentos pré-programados, com pouco uso do controle através da consciência. Neste caso, apenas ocasionalmente é necessário verificar o progresso em alguns pontos particulares. O preço a pagar por esta economia de esforço é que hábitos fortes podem assumir o controle quando a atenção para verificações é desviada, e quando atividades não familiares estão inseridas em um contexto familiar.

Com relação aos enganos, dois mecanismos diferentes aparecem: erros baseados em regras e erros baseados no conhecimento. No modo baseado em regras, um erro pode ocorrer quando uma regra incorreta é usada para diagnóstico. Uma pessoa que está acostumada em um processo industrial descontínuo, pode usar formas de interpretação incorretas, em face de problemas durante a operação, em um outro processo que seja contínuo.

Ainda, pode existir a tendência do uso constante de regras que tenham sido bem usadas no passado. Regras muito fixadas, podem vir a ser constantemente usadas em primeiro lugar, mesmo que não apropriadas. Quando uma pessoa, por exemplo, coloca água no radiador do automóvel, pode vir a desprezar uma sinalização de alta temperatura instantes após, imaginando que a falha é na sinalização da temperatura que está incorreta. Estes tipos de enganos são

chamados de erros "fortes mas errados" (*"strong but wrong" error*), porque provêm de ações que deveriam estar certas, já que, aparentemente, tudo esta sob controle.

No modo baseado no conhecimento, outros fatores são importantes. Muitos destes fatores surgem da demanda considerável de capacidade de processamento de informações, que é necessária quando uma situação nova deve ser avaliada. A partir de demandas desta natureza, não é de se surpreender que o desempenho seja ruim em situações de elevada tensão ou não familiares, e na ausência de rotinas ou regras pré-estabelecidas.

Kontogiannis e Embrey (1990) e Reason (1990) descrevem um grande número de modos de falhas deste tipo, como por exemplo: se uma informação não está suficientemente clara, ou explicitamente disponível, não precisa ser levada em consideração (*out of sight, out of mind, syndrome*). O efeito chamado "eu sei que estou certo" (*I know I'm right*) ocorre, por sua vez, devido a superestima do conhecimento das pessoas ou mesmo de equipes.

O reparo de erros quando baseados no "modo habilidade", é relativamente rápido e eficiente, porque o indivíduo permanece ciente dos efeitos esperados das suas ações, conseguindo rápido *feedback* de eventuais desvios, podendo antecipar a correção. Isto é importante salientar, porque enfatiza a importância do *feedback*, como elemento crítico para o reparo de erros. No caso de enganos isto já não é verdadeiro, pois as pessoas tendem a ignorar informações que não suportam suas idéias, ou seu modelo mental (*mindset syndrome*). Já as violações ocorrem porque algo não é relevante, ou para completar alguma tarefa (foco exclusivo no resultado).

O conhecimento do modo predominante da tarefa é importante para a escolha dos meios de prevenção de falhas, usando-se o modelo SRK mencionado anteriormente. Embrey [21], propõe uma forma de definir o tipo de tarefa, usando um diagrama de decisão como mostrado a seguir.

O modelo foi inserido no método chamado de SHERPA (Systematic Human Error Reduction and Prediction Approach), utilizado para a redução de erros humanos, e desenvolvido pelo autor. Conforme mostrado na Figura 8, Embrey subdivide o modo baseado em regras em dois tipos: RBD (*Rule-Based Diagnostic*), que envolve tarefas do tipo " se o sintoma é X então o problema é Y "; RBA (*Rule-Based Action*), que envolve tarefas após o diagnóstico, como por exemplo, " se o problema é Y então faça Z ".

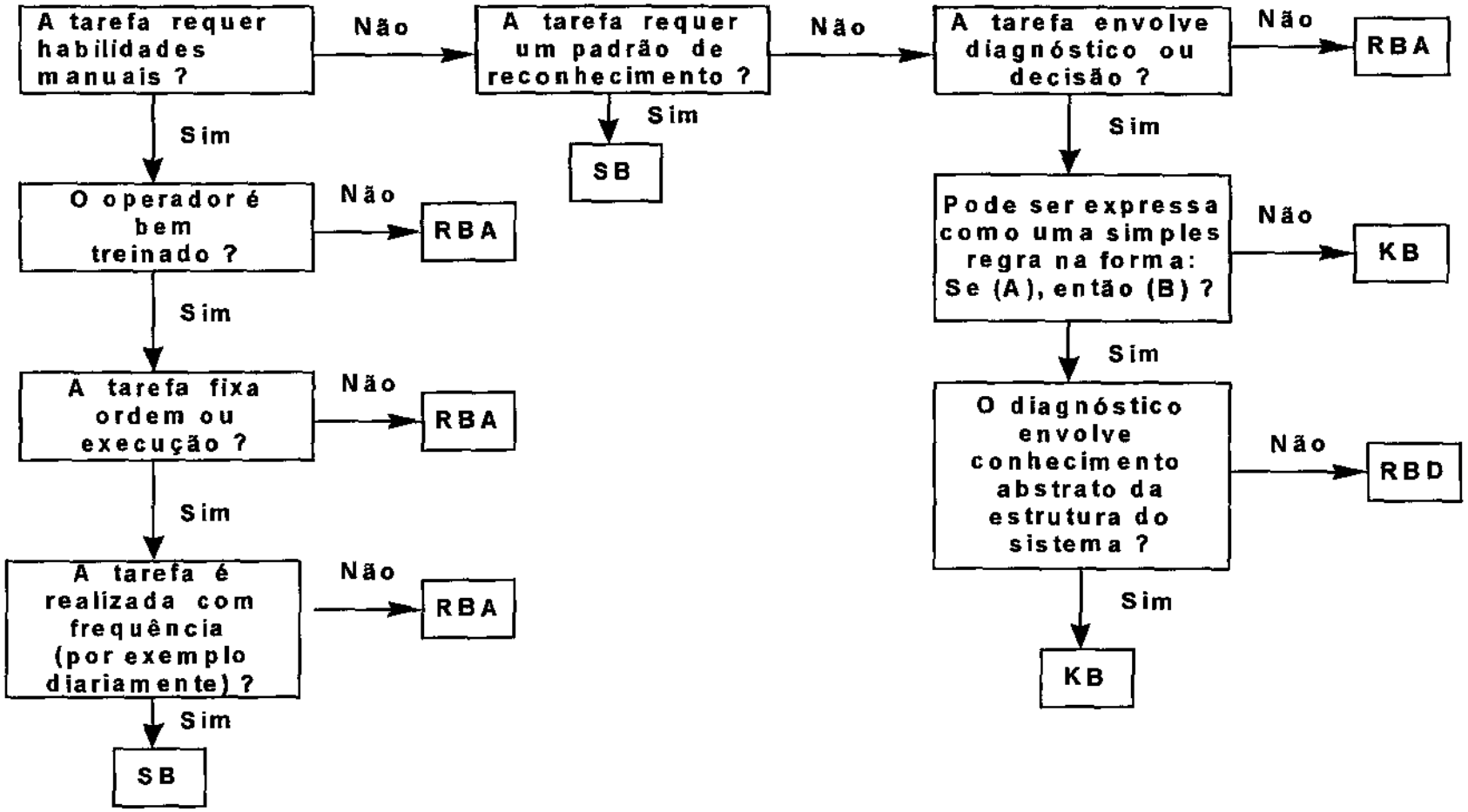


Figura 8. Diagrama de decisão para definição do tipo de tarefa [Ref. 21, pág. 190]

A partir deste diagrama, e após a definição do tipo característico da tarefa, pode-se usar as recomendações sugeridas para o modelo SRK, mostradas na Tabela III.

Tabela III. Estratégias para a redução dos erros, em função do tipo de processamento da informação, baseado no modelo SRK [Ref. 14, pág 83].

Erros típicos associados com os diferentes níveis de processamento da informação	Exemplos de Estratégias de Redução de Erros		
	Treinamento	Procedimentos e apoio ao trabalho	Projeto do equipamento
Erros baseados na habilidade - variabilidade natural - seqüência de ação errada	Treinamento para habilidades físicas e de manuseio	Listas de verificação para início e término de atividades	Layout e identificação de controles e linhas de processo Distinção de áreas com aparência similar mas com diferentes funções
Erros baseados em padrões - diagnóstico incorreto devido regras rígidas mas erradas - escolha incorreta de uma ação devido padrão errado ou não apropriado	Identificar as regras corretas para diagnóstico e ações requeridas para realizar o trabalho. Assegurar que o operador pratica extensivamente o uso de regras. Explicar as exceções e possíveis erros devidos à confusão de sintomas e regras rígidas	Para regras complexas e de uso não freqüente, providenciar apoio ao trabalho (matrizes de falhas e sintomas) para facilitar o diagnóstico correto e a seleção das ações apropriadas	Assegurar no projeto a existência de informações (*displays*) para que o operador não use padrões errados baseados em sintomas similares com diferentes causas. Prever *feedback*.
Erros baseados no conhecimento - processamento da informação - visão tipo "túnel"	Onde possível, prever simuladores para eventos complexos, para encorajar o desenvolvimento de estratégias para ambientes tolerantes. Prever treinamento na dinâmica do processo.	Prever dados da instalação (fluxogramas e configuração) com formato de fácil acesso. Prever diagramas para solução de problemas para garantir que todas as informações são levadas em conta.	Como acima.

2.4 A performance humana

2.4.1 Tarefas de rotina e durante eventos anormais

Muitas das falhas humanas que ocorrem poderiam ter seus efeitos reduzidos se, inicialmente, as pessoas responsáveis pelo projeto dos sistemas, levassem em conta que existe uma variabilidade natural no ser humano e que o meio ambiente influi na probabilidade de falha.

A performance das pessoas varia de hora para hora e de um dia para o outro. Depende também do nível de estresse a que está submetida. A Figura 9 mostra três tipos de erros, que podem ocorrer em situações de rotina.

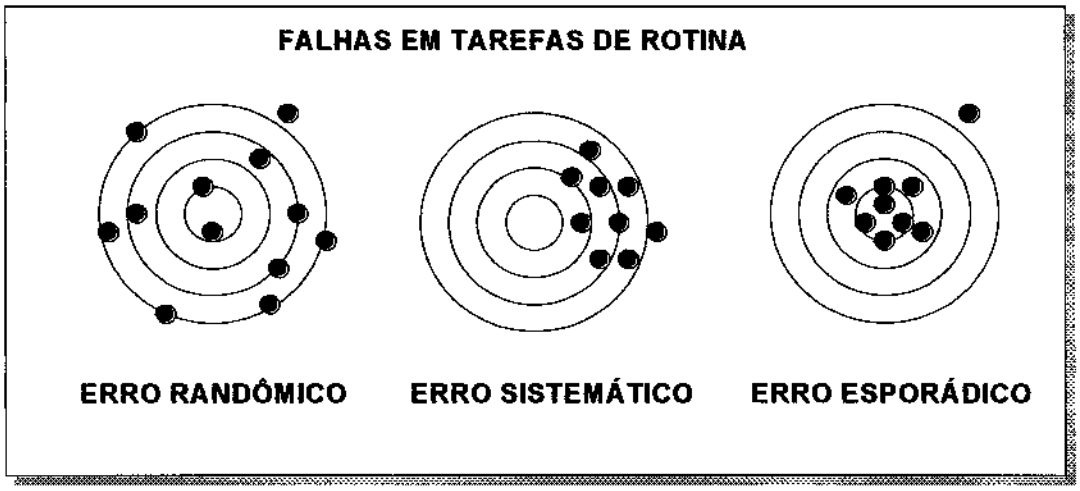


Figura 9 - Falhas em tarefas de rotina [Ref. 22, pág 352]

Os **erros randômicos** são dispersos em torno de um valor correto, mas com variança grande em relação a ele. Exemplos destes tipos de erros são as leituras de instrumentos, como a caracterização bem definida de uma interface homem/máquina.

Os **erros sistemáticos** ocorrem, por exemplo, por calibração de instrumentos com um padrão errado.

Os **erros esporádicos** são causados, por exemplo, por mudanças bruscas. Quando algo inesperado deve ser feito, ou uma mudança no sequenciamento de uma tarefa. Situações extremas, de baixo ou elevado estresse podem causar desatenção ou confusão, respectivamente, e ocasionar falhas deste tipo.

Durante situações de emergência (eventos anormais), a probabilidade de ocorrer um erro na tomada de decisão, aumenta. Nestes momentos - nos chamados eventos raros - muitas vezes as pessoas não acreditam que estejam vivendo a situação. Em salas de controle, por exemplo, após um alarme relacionado com um evento crítico, a equipe precisa perceber, discriminar, interpretar e diagnosticar, antes de decidir o que fazer. Se o tempo disponível para estas etapas for reduzido e a equipe sabe que se suas ações não tiverem sucesso haverá uma

grande perda, a probabilidade do erro é elevada. A probabilidade do erro diminui a medida que o tempo disponível para a tomada de decisão aumenta. Em períodos de elevado estresse, muitas vezes o modelo mental desenvolvido para lidar com a situação, é considerado correto, predominando a visão tipo "túnel". Estes comportamentos estão indicados na Figura 10.

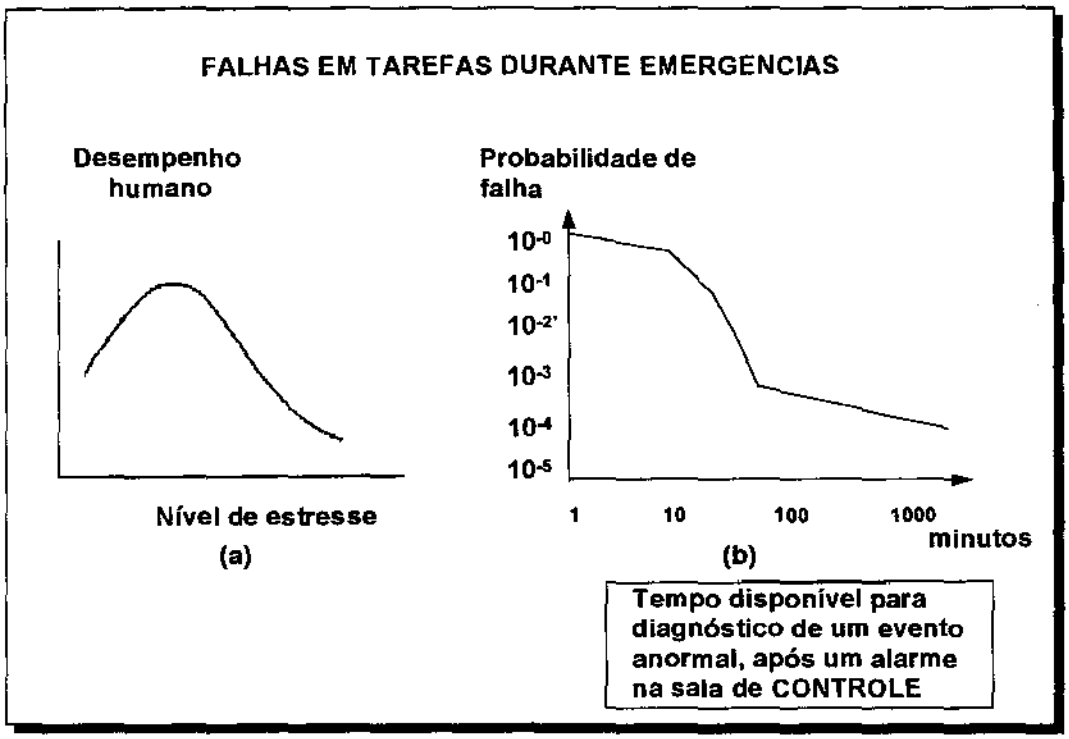


Figura 10 - (a) Falhas durante emergências [Ref. 22, pág 332]
(b) Falhas no diagnostico de eventos anormais [Ref. 23, pág. 242]

Existem duas outras situações onde a capabilidade humana é variável, conforme mostrado na Figura 11. A eficácia na detecção, por exemplo, é praticamente nula quando a rotina de procurar algo é diária. É devido a este fato que sempre os "chefes" que circulam nas áreas de fabricação uma vez por semana, enxergam aquilo que as pessoas, que normalmente estão no local, não percebem. Inspeções que são feitas diariamente não são eficazes, salvo quando, de forma intencional e previamente definida, possuem foco diferente (segurança, limpeza, organização, qualidade, etc...).

O fenômeno da perda da vigilância ocorre quando um operador precisa ficar vigiando por longo tempo um determinado instrumento ou ponto de observação estático. A probabilidade de que ele observe algo diferente, além de uma hora, é muito pequena.

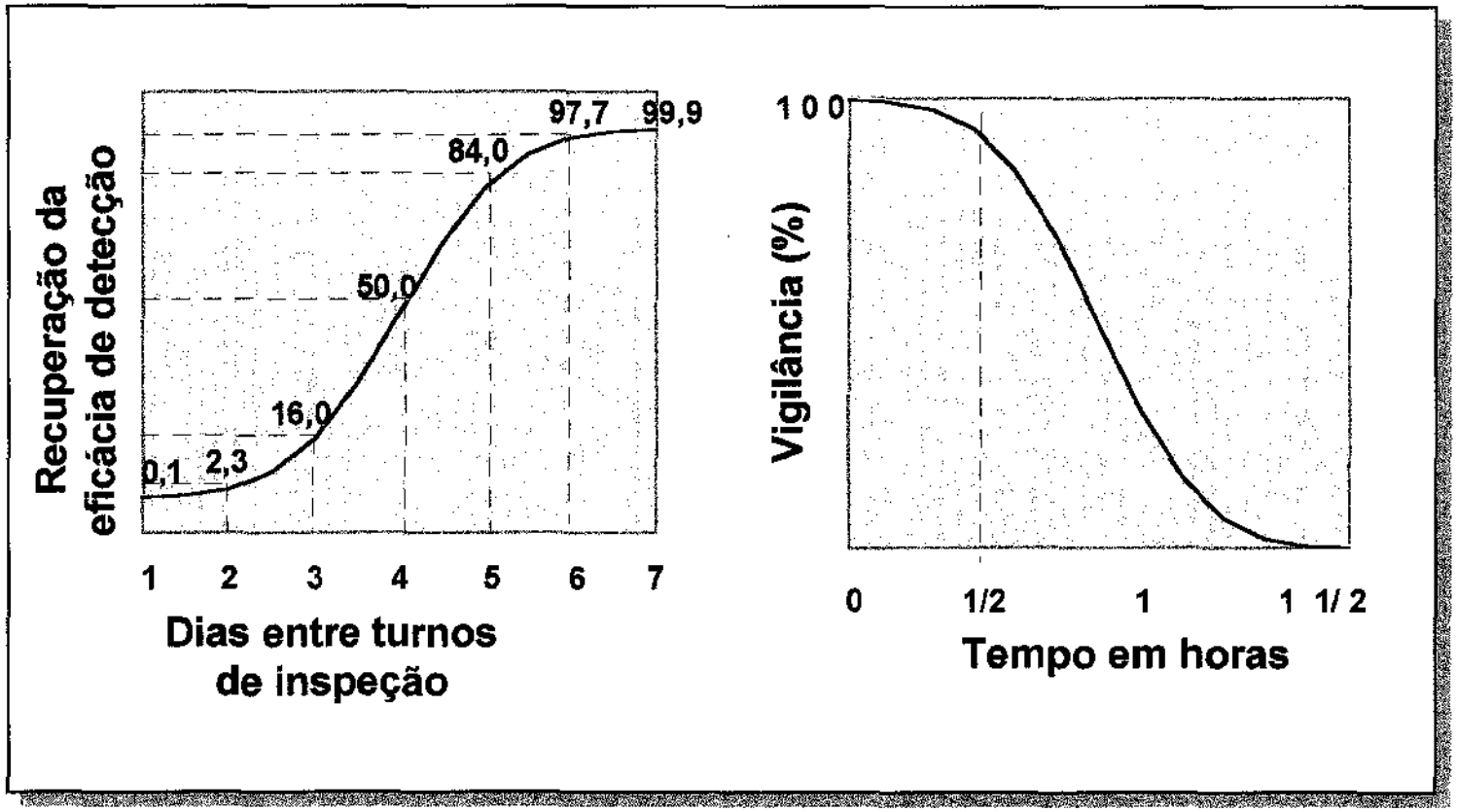


Figura 11 - Falha na detecção e na vigilância [Ref. 22, pág. 333]

Existem variados fenômenos cognitivos sob tensão, individuais ou característico de algumas equipes, que merecem atenção para a prevenção das falhas. Estes fenômenos normalmente podem aparecer em salas de controle de unidades de processo. A Tabela IV a seguir resume alguns deles.

Tabela IV. Características do comportamento das pessoas em função de alguns fenômenos cognitivos, em ambientes de elevado estresse [Ref. 14, Cap. 3].

Fenômeno cognitivo	**Característica**
Atitude defensiva	"Passa o bastão" confiando a decisão à outra pessoa.
Conformidade reforçada do grupo	O grupo protege seu próprio consenso, pressionando os que discordam e ignorando informações externas que poderiam eliminar a complacência do grupo.
Aumento da tomada de risco	Assumir maiores riscos quando se esta em grupo.
Paralisia mental temporária	Súbita mudança de uma sub-estimulação para uma super-estimulação, nos momentos de crise.
Concentração reduzida	A concentração - habilidade de fornecer atenção, sob demanda - cai com o estresse.
Visão cognitiva "túnel"	"Ancoragem em hipóteses" - procura informações que confirmem sua hipótese formulada inicialmente, sobre o estado do processo, e ignora informações que a refutem.
Rigidez da solução de problemas	Tendência a usar soluções "fora da prateleira", que não são necessariamente as mais eficientes.
Polarização do raciocínio	Explicação através de uma única causa global, e não por uma combinação de causas.
Insistência e superficialidade temática	A superficialidade temática se refere ao caso em que os pensamentos de uma pessoa voam através das questões, tratando cada uma de forma superficial. A insistência ocorre quando tópicos são tratados até o excesso, privilegiando pequenos detalhes, em detrimento de questões mais importantes.

2.4.2 Falhas de modo comum

As Falhas de Modo Comum (FMC) requerem um cuidado especial, pois podem ser introduzidas em várias etapas da instalação de um processo, desde a concepção até a operação [24].

Podem ocorrer em outras varias situações: O choque entre os dois jumbos da KLM e PANAM em Tenerif, ocorreu por falhas múltiplas, sendo uma delas a utilização de um mesmo canal de comunicação para as duas aeronaves que estavam (indevidamente) uma em cada extremo da pista.

Quando a torre disse "OK" para o jato que ia decolar, o piloto do outro avião também ouviu, e começou a andar na mesma pista em direção à cabeceira para a decolagem. A neblina tornou o choque inevitável. Mais de 400 pessoas morreram. A Figura 12 mostrada a seguir, apresenta algumas das falhas comuns que podem ocorrer e que merecem atenção para assegurar a confiabilidade requerida.

Em 1992 a comissão reguladora da atividade nuclear americana iniciou uma pesquisa sobre falhas de modo comum, de natureza humana, para auxiliar na estimativa das probabilidades dos erros humanos.

O produto da pesquisa é uma lista de causas raízes, tanto para etapas pré-operacionais como para o período de operação propriamente dito [Ref. 18, pág 368].

Causas de Modos Comuns de Falhas em Sistemas Redundantes

ENGENHARIA				OPERADOR			
PROJETO		CONSTRUÇÃO		PROCEDIMENTO		MEIO AMBIENTE	
Deficiências Funcionais	**Falhas na Ação**	**Fabricação**	**Instalação**	**Manutenção e Testes**	**Operação**	**Normal e Extremas**	**Energia**
Perigos não detectados	Canais com dependência	Controle de qualidade inadequado	Controle de qualidade inadequado	Reparo imperfeito	Erros do operador	Temperatura	Fogo
Controle inadequado	Mesmo componente para operação e proteção	Código inadequado	Comissionamento inadequado	Calibração imperfeita	Procedimento inadequado	Pressão	Enchente
Instrumentação inadequada	Erro de projeto	Inspeção inadequada	Código inadequado	Processo imperfeito	Erro de comunicação	Umidade	Terremoto
	Erro na definição de limites	Teste inadequado		Supervisão imperfeita		Vibração	Explosão
						Estresse	Energia elétrica
						Corrosão	Tempo
						Radiação	

Figura 12. Classificação dos sistemas para falhas dependentes [Ref. 23, pág. 223]

2.4.3 Fatores que influenciam o desempenho humano

Em acordo com o modelo da Figura 4 mostrada anteriormente, os erros normalmente são induzidos por inúmeros fatores. Uma lista proposta para estas variadas razões que levam as pessoas a errarem esta descrita na Tabela V, seguida de alguns comentários adicionais relacionados com os fatores mencionados na tabela.

O enfoque foi dado para indústrias químicas mas, como é possível observar, a maioria é aplicável a qualquer ambiente de trabalho.

Tabela V. Lista dos fatores que influenciam o desempenho humano, conhecidos como Performance Influencing Factors [Ref. 14, Cap.3].

Ambiente de Operação	Ambiente de processo químico	Freqüência do envolvimento do pessoal; complexidade dos eventos do processo; perigo percebido; dependência do tempo (estresse); velocidade do processo de detecção
	Ambiente físico de trabalho	Ruído; iluminação; condições térmicas; condições atmosféricas; lugares remotos ...
	Padrão de trabalho	Horas de trabalho e pausa de repouso; rotação de turnos de trabalho noturno (ciclos circadianos).
Características das Tarefas	Projeto dos equipamentos	Localização e acesso; identificação; equipamentos de proteção individual
	Projeto do painel de controle	Relevância da informação; identificação dos controles e *displays*; compatibilidade com as expectativas dos usuários; agrupamento das informações; visualização de informações e alarmes críticos.
	Ajudas no trabalho e procedimentos	Clareza na instrução; nível da descrição; especificações nas condições de entrada e saída; qualidade das verificações e alertas; grau de uso do diagnóstico de falhas; compatibilidade com a experiência operacional; freqüência de atualização.
	Treinamento	Treinamento para uso de novos equipamentos; prática com situações não familiares; conflitos com requisitos de produção e segurança; treinamento para trabalho com sistemas automáticos
Características das Pessoas	Experiência	Grau de habilidade; experiência com eventos "raros".
	Fatores da personalidade	Motivação; gostar de ambiente com riscos; manter o nível de risco percebido (homeóstase); controle "interno" ou "externo"; controle emocional; tipo "A" versus tipo "B"
	Condição física e idade	
Fatores Sociais e Organização	Times de produção e comunicações	Distribuição da carga de trabalho; clareza das responsabilidades; comunicações; autoridade e liderança; planejamento em equipe e orientação.
	Políticas gerenciais	Comprometimento da gerência; perigo da cultura "livro de normas"; excesso de confiança em métodos de segurança; aprendizagem da organização.

- *Eventos complexos* que nunca foram vividos, e cujo treinamento prévio inexiste, podem ter conseqüências desastrosas. O caso típico foi o acidente de Seveso na Itália em 1976, quando um descontrole de um processo químico ocasionou a emissão de uma grande nuvem tóxica na atmosfera. Ninguém no local sabia que tal evento era factível.

- Quando não há um estudo prévio de análise de riscos, normalmente predomina o *risco percebido*. Se este é baixo, ou é alto mas as pessoas "gostam" de viver com ele, as ações realizadas podem comprometer o sistema envolvido. Normalmente é fácil identificar estes ambientes: neles é rotina não aparecer nos relatórios diários alguma referência a anormalidades ou incidentes.

- Conforme a teoria da *homeóstase* (risco percebido) as pessoas quando percebem que o risco diminuiu, tratam de aumentá-lo de alguma forma, para sentirem-se melhor - com o nível de risco que gostam. Caso típico ocorre com pessoas que correm mais quando passam a usar o cinto de segurança ao dirigir.

- Falhas que ocorrem em um turno de trabalho e tem *desenvolvimento lento* podem, por sua vez, não ser detectadas nos turnos seguintes, até que os eventos ocorram.

- O *ambiente físico* segue sendo importante mesmo em sistemas de controle avançados. Em uma sala de controle a equipe de operação decidiu diminuir a iluminação para reduzir o reflexo sobre as telas de vídeo do Sistema Digital de Controle Distribuído (SDCD). Haviam, entretanto, vários instrumentos na mesma sala, com controle analógico. O resultado foi que, com o passar do tempo, os operadores tinham de usar lanternas para visualizar estes instrumentos, comprometendo a eficácia das observações.

- Muitos estudos existem sobre os *ciclos circadianos*. A importância é grande em ambientes de trabalhos com turnos de revezamento, onde mudanças repentinas nos horários "acostumados" podem refletir significativamente no desempenho das pessoas durante emergências.

A Figura 13 a seguir mostra a relação estreita que existe entre a temperatura do corpo e o estado de alerta.

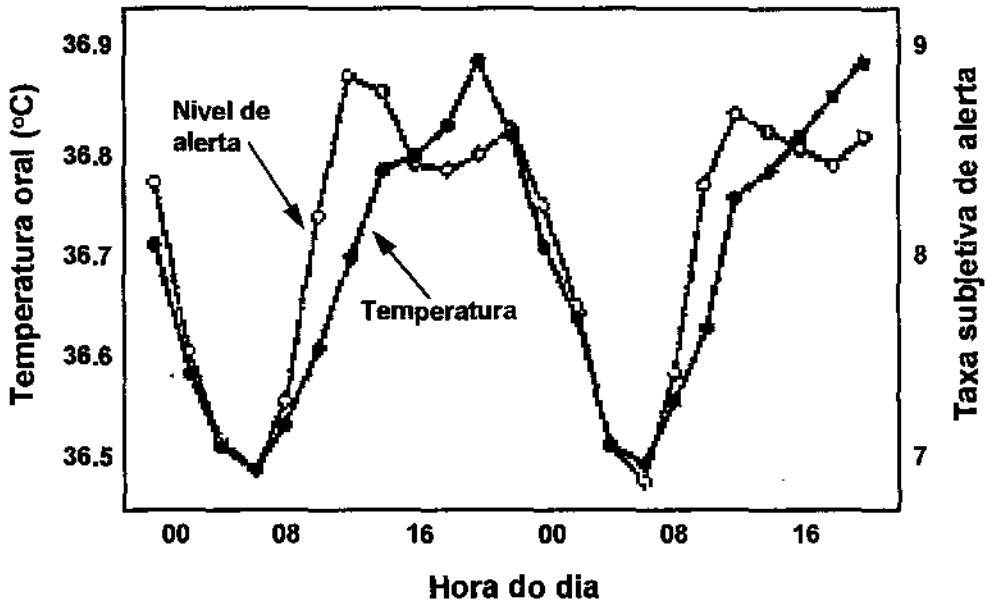


Figura 13. Variação circadiana na temperatura oral e o estado de alerta para 6 operadores de unidade de processo, identificado por Monk e Embrey em 1981 [Ref. 14, pág 117].

Para tarefas cognitivas complexas, onde a memória é muito importante, a variação na performance fica defasada da temperatura, ou seja, melhores performances ocorrem quando a temperatura esta mais baixa (à noite). A Figura 14 mostra a relação dos dois testes de performance realizados com operadores a cada duas horas (MAST - *Memory And Search Test*). Quanto maior o número, maior a carga de memória requerida.

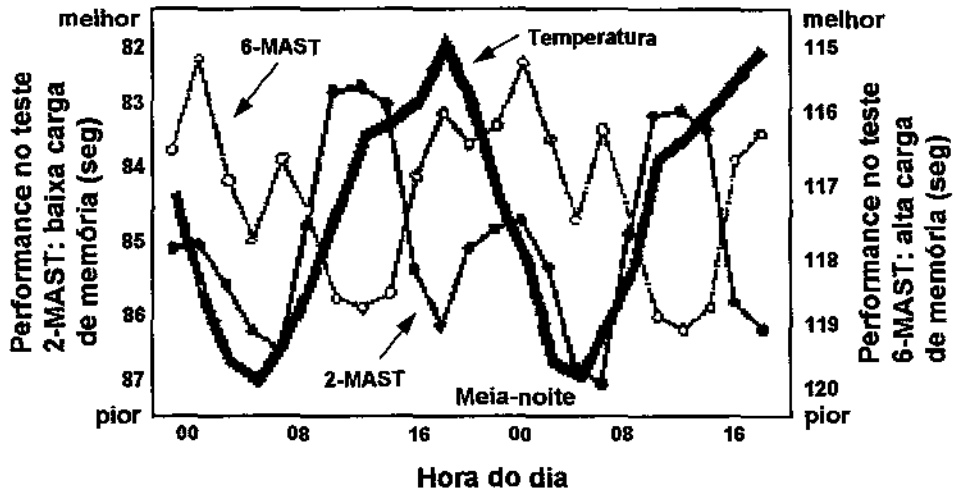


Figura 14. Variação circadiana na performance em tarefas de alta e baixa carga de memória, adaptado por Monk e Embrey em 1981 [Ref 14, pág.118].

Os dados dos testes da Figura 14 são confirmados quando o número de erros são plotados em relação à temperatura do corpo. A Figura 15 mostra que a temperatura segue temporalmente o mesmo perfil do teste 6-MAST, o que indica que tarefas cognitivas de alta carga de memória apresentam menor número de erros a noite, quando a temperatura esta mais baixa.

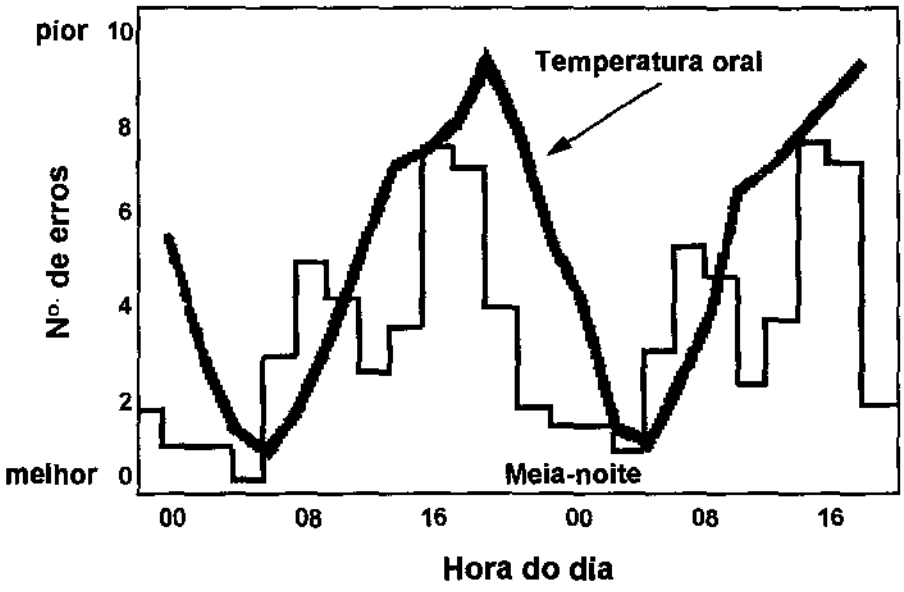


Figura 15. Variações circadianas em erros feitos por operadores de processo, comparados com as mudanças da temperatura do corpo, adaptado por Monk e Embrey em 1981 [Ref. 14, pág. 118].

Estes estudos são importantes pois podem influenciar na programação de tarefas para os operadores de processo. Tarefas baseadas na habilidade (*skill-based*), são de baixa carga de memória, enquanto que as tarefas baseadas no conhecimento são de alta carga de memória (*Knowledge based*).

Muitas pesquisas sobre ciclos circadianos tem sido realizadas, não só para analisar suas influências no desempenho humano, mas também para reunir informações que possam ajudar no planejamento das equipes que trabalham em turnos de revezamento. De acordo com Lehmann (1955), a eficiência biológica cresce a partir das 6 horas da manhã, hora após hora, alcançando um primeiro pico entre 9 horas e 11 horas. Um rápido decréscimo se segue ao redor do meio dia. Após, vagarosamente, a eficiência aumenta, alcançando um segundo pico entre as 15 horas e 16 horas, com um segundo decréscimo ocorrendo entre 2 horas e 4 horas da manhã. Diego Nogueira comparou estes ritmos, e vinculou-os aos acidentes ocorridos e observados em sua pesquisa [25].

A partir destas observações sua sugestão era de que havia nitidamente um "ritmo dos acidentes". Gertman [Ref. 18, pág 5], considera já de conhecimento generalizado o fato de que a taxa de acidentes é maior entre 3 e 6 horas da manhã.

P. Andlauer et al. [26] analisaram o desempenho de equipes em turnos, e chegaram a conclusão de que nenhum operador deveria trabalhar mais do que 4 ou 4,5 horas no turno da noite. Equipes reservas e um maior reforço no turno da noite deveriam existir. Cuidados especiais com o arranjo e troca dos turnos, por outro lado, são fatores importantes no gerenciamento dos riscos. Os riscos de acidentes estão relacionados com estes aspectos e, sobretudo, com a performance da troca das equipe. Deve se levar em conta no planejamento das mudanças dos horários de trabalho das pessoas que é mais difícil um operador adaptar-se a uma troca do dia pela noite, do que o inverso, conforme pesquisa realizada sobre 3200 acidentes no período de 1980 e 1987 em plataformas de petróleo [27]. O problema dos trabalhos em turnos de revezamento não é apenas uma questão do relógio biológico, ou de problemas relacionados ao tempo de sono, ou uma questão social. Ao invés disto, conforme Monk (1989), é uma interação entre estes três aspectos.

- As tarefas por sua vez são muito dificultadas quando o *acesso é inadequado*. Quando o operador da Plataforma Piper Alpha foi fazer "sua última manobra", não percebeu a ausência de um componente importante para a segurança, pois o local onde ele se encontrava era no piso inferior da plataforma. Não houve qualidade nas verificações do serviço de manutenção, que deveria ter instalado o componente.

- Um operador descarregou uma carreta de cloro sobre um tanque de ácido clorídrico, por *falha na indicação* correta dos reservatórios. Trinta pessoas foram removidas para o hospital. Em muitas situações semelhantes, os erros ocorrem porque não há *compatibilidade com a experiência operacional*: quem escreve os manuais nunca operou uma unidade de processo.

- As questões envolvendo as novas tecnologias de controle com *displays* (SDCD e CLP) têm despertado atenção especial. O meio ambiente associado com estes sistemas mais avançados é muito diferente daquele existente nas salas de controle mais antigas.

Com o uso de interfaces baseadas em computadores (ou processadores eletrônicos), as questões cognitivas do processamento das informações pelas pessoas estão superando as considerações físicas e ergonômicas, que prevaleciam no projeto das interfaces.

Uma outra questão importante envolvendo SDCD é o paradigma de que, nos sistemas antigos (analógicos), as pessoas "andavam" na frente do painel, enquanto que com SDCD, o "painel" anda na frente das pessoas. Na realidade, o SDCD retirou dos operadores a visão periférica. Cuidados especiais neste sentido devem ser levados em conta em bons projetos [28].

- A *clareza das instruções*, por sua vez, influencia na confiabilidade da informação. As equipes de operação normalmente tem operadores nas salas de controle e no "campo". A comunicação entre as pessoas se processa via, por exemplo, rádio ou interfone, em um ambiente onde há normalmente ruído. Erros de compreensão podem existir e, para uma melhor eficácia nas mensagens, são sugeridas ações como: repetição da instrução por quem escuta; escolha de um vocabulário "simples"; e ainda, algumas palavras podem ser reservadas para determinadas operações [29].

- O *treinamento para uso de novos equipamentos* tem como função assegurar que habilidades específicas, tarefas e procedimentos, são efetivamente e eficientemente aprendidas.

Quando do projeto de novos equipamentos, ou na avaliação da performance humana em sistemas existentes, é importante que as lacunas de conhecimento sejam identificadas de forma estruturada, visando definir claramente: por que uma tarefa é (ou deverá ser) realizada; que nível deve (ou deverá) ser atingido para garantir a confiabilidade; e em que contexto ela é (ou será) realizada [30].

- A eficácia da tarefa também é fortemente influenciada por *conflitos internos*, como por exemplo, entre princípios de segurança e necessidade de produção - caso típico ocorrido em Chernobyl. O teste tinha de ser feito pois: - " *só é possível agora* " , disse na ocasião a administração da usina nuclear.

- A *escolha de líderes* é uma tarefa importante, quando é possível no ambiente de trabalho a vivência de momentos de elevada tensão. Pessoas que nunca viveram momentos de estresse elevado não podem, por exemplo, ser líderes em salas de controle de instalações importantes, como centrais elétricas, centrais nucleares, indústrias químicas, etc...

- *Autoridade* e liderança são fatores relevantes, uma vez que podem conduzir os grupos a atitudes erradas. No acidente ocorrido em 1974 na Nypro, em Flixborough na Inglaterra, a liderança da fábrica tomou a decisão de avaliar sozinha uma determinada situação onde uma modificação importante havia ocorrido na instalação. A avaliação foi errada. Vinte e oito pessoas morreram e houve a destruição completa da fábrica.

- *Comprometimentos esquecidos pela gerência* - como no caso de Bhopal - podem causar tragédias do mesmo modo. Falhas neste nível não são comuns, mas repetem-se de tempos em tempos. Parte da explicação reside no fato da grande dificuldade das pessoas aprenderem com as experiências dos outros. Em 1966 houve um grande acidente em Feyzan na França, em um parque de estocagem de gás liquefeito. Em 1972, um acidente com causas iguais destruiu as estocagens da Refinaria Duque de Caxias no Rio de Janeiro.

Os fatores que influenciam na performance seguem sendo estudados por especialistas no assunto. Um dos objetivos destes estudos é auxiliar na escolha correta dos fatores que podem influenciar na ocorrência de um determinado cenário de risco. Gareth W. Parry [31] sugere algumas formas para a escolha destes modeladores de desempenho, enfatizando que o seu conhecimento ajudará na definição de melhores modelos para a avaliação da probabilidade de certos erros ocorrerem. Muitas vezes, mais de um fator atua em um mesmo cenário, e são dependentes entre si. Ainda, podem vir a aparecer com maior chance quando houver uma freqüência maior do evento onde eles podem ocorrer. A análise deve abordar não só os mecanismos internos dos erros, como por exemplo a priorização incorreta por parte do operador, mas também os fatores modeladores externos, como alta carga de trabalho, estresse, etc. Gertman e Blackman [Ref. 18, pág 6] sugerem uma lista de fatores modeladores de performance (*Performance Shaping Factors* - PSF) e questões relacionadas com eles (*check list*), que ajuda ao analista identificar a existência de condições propícias para as falhas.

2.5 Modelo para a Redução dos Erros Humanos.

As questões mencionadas anteriormente podem ser abordadas, cada uma com suas particularidades, para a identificação dos erros humanos. Contudo, a possibilidade de redução das falhas depende de uma estratégia gerencial. Ou seja, é a administração que, com políticas bem claras e definidas, pode influenciar substancialmente para a diminuição dos erros humanos.

Embrey apresenta uma forma de visualizar esta questão, a partir de dois enfoques distintos, que devem ser promovidos pela gerência das empresas: a prevenção dos erros, numa atitude proativa; e a utilização de todo o aprendizado possível, após a ocorrência das falhas, numa atitude reativa. As duas formas de atuação são mostradas na Figura 16.

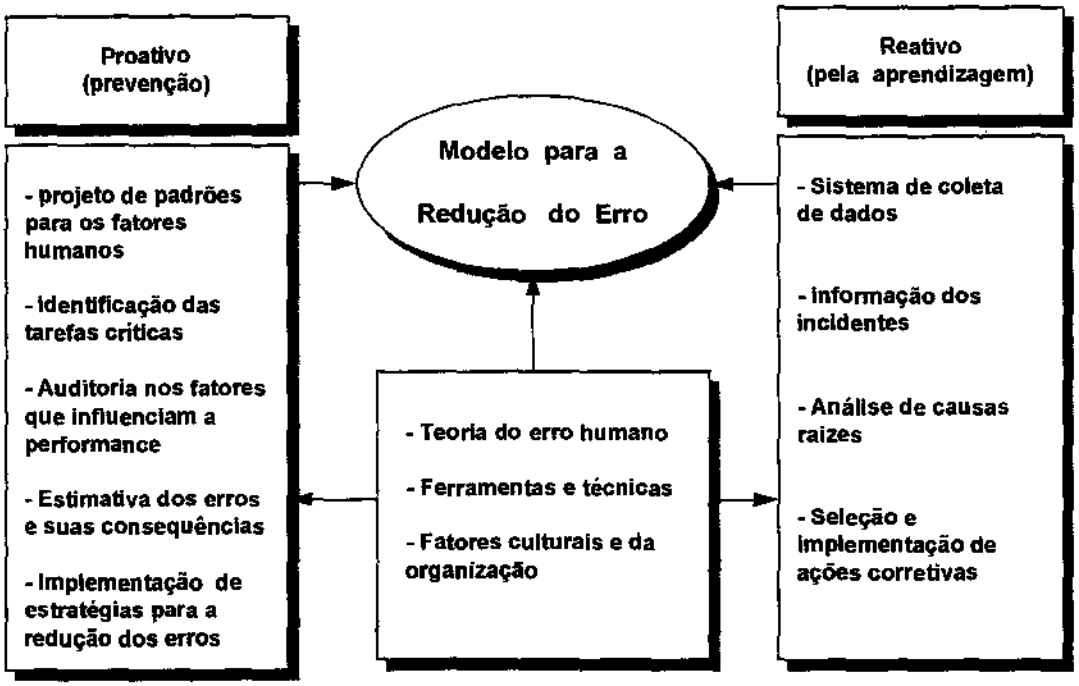


Figura 16. Modelo para a redução do erro [Ref. 14, pág. 357].

Assim, passa a ser não só importante como imperativo que a alta direção da empresa apoie as estratégias a serem adotadas, de forma proativa ou reativa. Todo e qualquer programa de desenvolvimento a ser iniciado deve possuir o compromisso e a adesão da administração, para que os recursos possam ser alocados quando e onde necessários. Cabe à administração a manutenção de um ambiente que permita que as atividades de um programa de redução de erros humanos sejam implementadas. Neste particular, é interessante ressaltar a importância da redução do "medo" na organização, para eliminar barreiras de comunicação e conseguir naturalmente a adesão de todas as pessoas da empresa. A eliminação do medo faz com que o operador sinta-se seguro e sem receio em falar e perguntar. Edward Deming sabiamente incluiu este aspecto nos seus conhecidos 14 princípios gerenciais [Ref. 32, pág 44].

3. Métodos para a identificação e redução dos erros humanos

Existem muitos métodos para a identificação de falhas de natureza humana, desde métodos analíticos, de pouca ou média complexidade, até metodologias muito sofisticadas, que normalmente são usadas por especialistas em erros humanos e com a ajuda de programas de computadores.

3.1 Métodos Analíticos para a Redução dos Erros Humanos [Ref 14, Cap. 4]

Os métodos analíticos para a avaliação e redução dos erros humanos podem ser agrupados em quatro grupos distintos:

3.1.1 Métodos com foco no processo de aquisição de dados

O primeiro grupo, trata da aquisição da informação necessária para a análise, ou seja, engloba metodologias para a obtenção de dados dos sistemas que se deseja analisar, como por exemplo:

Entrevistas com Especialistas (Interviews with "Experts")

O método compreende reuniões estruturadas com pessoas especializadas em determinadas tarefas. Seu sucesso está muito condicionado à habilidade do entrevistador, para que as informações importantes sejam transmitidas pelas pessoas que entendem do trabalho (operadores, supervisores, engenheiros, etc...).

Observação (Observation)

O método baseia-se em observações de tarefas realizadas com auxílio de audio e vídeo. Esta forma de aquisição de dados é importante, na medida em que consegue captar o meio ambiente e transientes que podem ocorrer no desenvolvimento da tarefa (ruídos, iluminação, interrupção, etc...)

Técnica de Incidentes Críticos (Critical Incident Technique)

O método é útil para a análise de dados de incidentes que se desenvolveram e quase se tornaram acidentes sérios. Nestes casos, as próprias pessoas que estiveram envolvidas com os cenários dos incidentes, são convidadas a falar a respeito dos seus próprios erros. Novamente neste método, o analista necessita ter aptidão necessária para garantir confidencialidade sobre a entrevista. A preocupação deve ser centrada nas questões gerais e não no evento em si.

Documentação (Documentation)

Manuais de operação, planos de emergência e relatos de acidentes ou "quase-acidentes" são documentos importantes para a análise das tarefas.

Outros métodos analíticos ainda incluem: **Análise de Atividade (Activity Analysis)**; e uso de **Simuladores (Simulators and Mock-ups)**.

3.1.2 Métodos com foco na "ação"

O segundo grupo trata com detalhe a análise de tarefas, com técnicas estruturadas, cujo foco é orientado exclusivamente para a "ação", não tratando das questões ligadas à capacidade de diagnóstico e modelos mentais das pessoas (enfoque cognitivo). Este grupo de métodos trata de questões importantes, como a análise de quais funções devem ser de responsabilidade das pessoas e quais devem ser realizadas por controles automáticos, como computadores e intertravamentos elétricos.

Análise Hierárquica de Tarefas (Hierarchical Task Analysis - HTA)

A técnica, de forma sistemática, descreve como um trabalho deve ser organizado de tal forma a poder ser realizado e cumprir seu objetivo. A representação das tarefas pode ser feita de forma gráfica ou através de uma tabela, conforme mostrado na Figura 17 e na Tabela VI [Ref 14, pág 164].

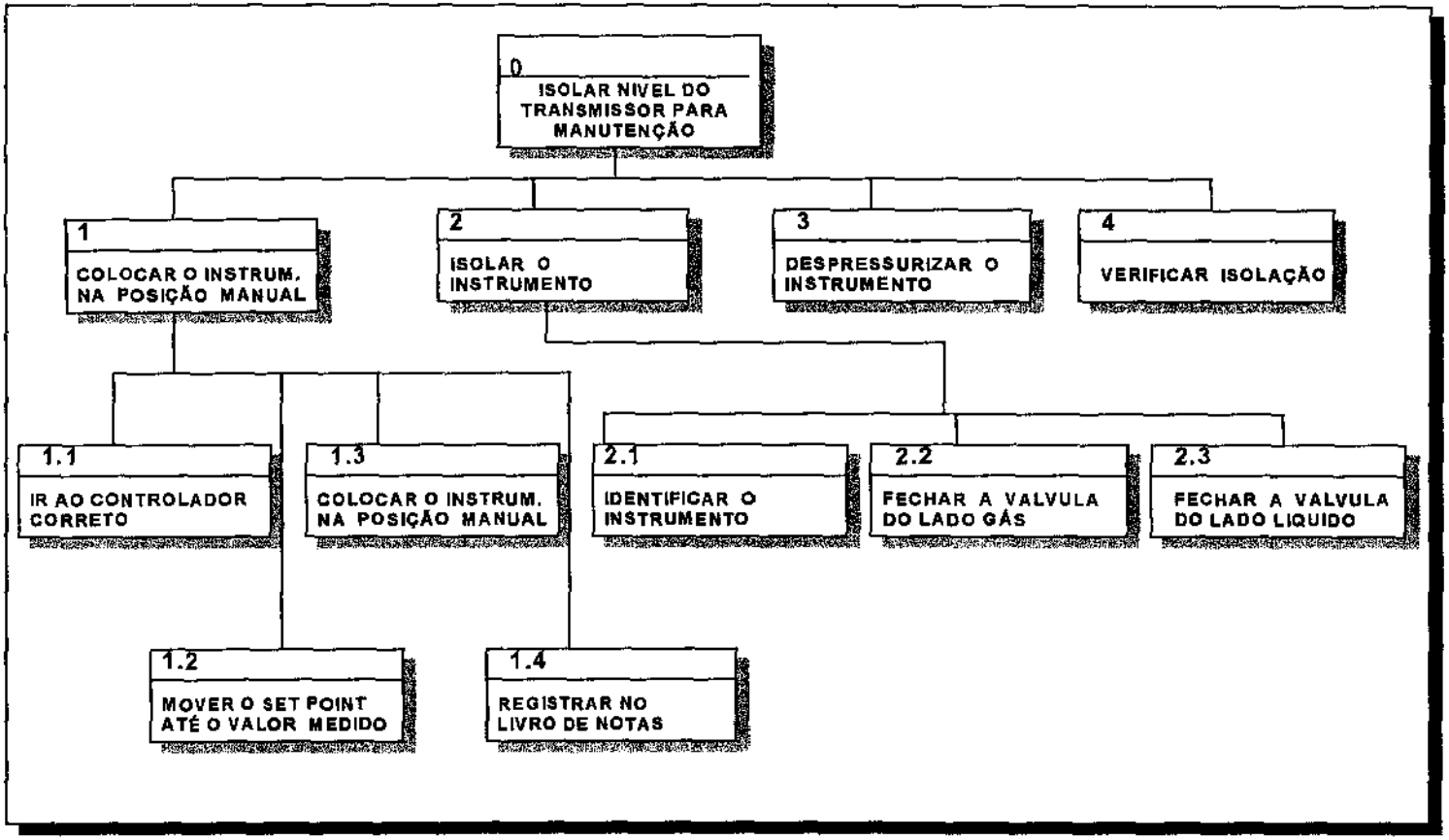


Figura 17. Análise hierárquica de tarefas - representação gráfica
(Diagrama para isolação de um transmissor)

Tabela VI. Representação através de tabela, de uma Análise Hierárquica de Tarefas (Otimização da Pressão em uma Coluna de Destilação)

Passo da tarefa	Dados de Entrada	Saídas (ações)	"Feedback)	Comunicação	Tempo	Condição	Outras tarefas	Notas
4 Otimizar o valor da pressão na coluna entre 1 - 1.5 atm	Registro de pressão indica P > 1.5 atm (sem alarme)	Se P > 1.8 atm, aumentar a vazão de resfriamento no condensador (4.2) e reduzir o aquecimento no refervedor (4.3) Se pressão < 1.8 atm, fazer apenas (4.2)	Registro de pressão Registro de temperatura Nível de condensado no balão de refluxo	Comunicação de rádio entre os operadores da sala de controle e os operadores de campo	Otimização deve iniciar no máximo 2 min após o início do desvio	Flutuação da temperatura degradará a qualidade do produto	Operador da sala de controle com outras tarefas na sala	Operador da sala pode falhar em perceber o aumento da pressão operadores de campo podem falhar no ajuste do resfriamento Perigo: explosão devido acúmulo de vapor na coluna

Outras técnicas também importantes, com enfoque na "ação", são: Árvore de Eventos sobre as Ações do Operador (Operator Action Event Trees - **OAET**); Diagramas de Ação e Decisão (Decision / Action Flow Diagrams - **DA CHARTS**); Diagramas de Seqüência Operacional (Operational Sequence Diagrams - **OSDS**); Análise Gráfica de Fluxo (Signal-Flow Graph Analysis - **SFGS**).

As técnicas de análise de tarefas, com enfoque cognitivo, ao invés da "ação", procuram por outro lado trabalhar as questões que abordam os processos mentais, diagnósticos e solução de problemas. Estas técnicas apresentam maior dificuldade de uso, devido a complexidade das considerações envolvidas. Estas técnicas podem ser usadas igualmente na prevenção de erros, como na investigação de acidentes ocorridos. As duas principais técnicas analíticas que usam a abordagem cognitiva são a Técnica de Avaliação de Decisão e Ações Críticas (Critical Action and Decision Evaluation Technique - **CADET**) e o Sistema de Avaliação e Influência de Modelos (Influence Modeling and Assessment Systems - **IMAS**). Alguns critérios, como os listados abaixo, podem ser usados para a definição da aplicabilidade da técnica a usar. Pela Tabela VII é possível verificar que os métodos HTA, IMAS e CADET preenchem a maioria dos critérios definidos. Estas técnicas cobrem os aspectos voltados à ação e aqueles com enfoque cognitivo.

Tabela VII. Comparação das técnicas quanto ao tipo de enfoque característico utilizado [Ref. 14, pág 188].

Métodos de Avaliação	HTA	OAET	DA	OSD	SFGS	CADET	IMAS
1- O enfoque do método é na observação do comportamento do operador?	Sim	Sim	Sim	Sim	Sim	Não	Não
2- O enfoque do método é no modelo mental que regula o comportamento?	Não	Não	Não	Não	Não	Sim	Sim
3- O método pode identificar pontos onde decisões críticas devem ser tomadas?	Sim	Sim	Sim	Não	Não	Sim	Sim
4- O método pode identificar informações importantes sobre o painel de controle?	Sim	Não	Sim	Parcial	Sim	Sim	Sim
5- O método descreve características temporais da tarefa?	Parcial	Não	Parcial	Sim	Não	Não	Não
6- O método pode correlacionar os passos das tarefas com possíveis efeitos secundários?	Sim	Não	Sim	Não	Não	Sim	Sim
7- O método descreve interações entre as pessoas e o sistema de controle?	Sim	Parcial	Não	Sim	Sim	Parcial	Parcial
8- O método descreve os requisitos de comunicação entre os membros da equipe?	Sim	Não	Não	Sim	Não	Não	Não
9- O método classifica as tarefas em diferentes categorias?	Não	Não	Não	Parcial	Não	Sim	Não
10- O método descreve de forma qualitativa o sistema técnico?	Não	Não	Não	Não	Sim	Não	Não

3.1.3 Métodos com foco na análise dos erros

O terceiro grupo, trata das técnicas de análise de erros. Em primeiro lugar, podem ser citadas as próprias técnicas voltadas para a análise de tarefas. Estas metodologias podem ser escolhidas conforme outros critérios diferentes dos anteriores, para definir a técnica que melhor se adapta ao objetivo do estudo.

A Tabela VIII mostra uma classificação baseada nas áreas de aplicação, a partir de diferentes fatores humanos envolvidos.

Tabela VIII. Comparação das técnicas quanto à aplicação [Ref. 14, pág 189].

Métodos de Avaliação	HTA	OAET	DA	OSD	SFGS	CADET	IMAS
1- Projeto de procedimentos operacionais	Sim	Não	Sim	Não	Não	Parcial	Parcial
2- Análise de necessidade de treinamento	Sim	Não	Sim	Não	Não	Sim	Sim
3- Organização de equipes	Sim	Não	Não	Sim	Não	Parcial	Não
4- Interface homem / máquina	Sim	Parcial	Parcial	Sim	Sim	Sim	Parcial
5- Projeto do painel de controle	Sim	Não	Sim	Parcial	Sim	Sim	Sim
6- Análise de Carga de trabalho	Parcial	Não	Não	Sim	Não	Sim	Não
7- Fonte para análise de erros humanos mais elaborada	Sim	Sim	Sim	Não	Não	Sim	Sim

Análise Preditiva de Erros Humanos (Predictive Human Error Analysis - PHEA)

Este método inclui a caracterização de vários modos de falhas que, juntamente com a verificação de fatores que influenciam a performance, auxiliam muito nos estudos quantificados de análise de riscos. Podem ser citados como exemplos de modos de falhas:

Ação do operador é demorada ou adiantada
Ação do operador é demasiada ou insuficiente
Ação de omissão
A verificação não é realizada
A verificação é realizada em local errado
A informação requerida é incompleta
A informação não é transmitida
Ocorre erro na seleção de uma chave de comando
Pre-requisitos para a ação são ignorados
etc...

Murgatroyd e Tait (1987), durante a validação desta técnica, mostraram que ela é capaz de identificar uma alta proporção (98 %) de erros com potencial para sérias conseqüências. Do

total de 60 erros identificados neste estudo de validação, 70 % foram iguais para os dois analistas. Dos erros restantes, 11 foram devido a diferença de conhecimento dos analistas sobre o equipamento. Cinco foram devido a diferenças de interpretação sobre os procedimentos [Ref. 14, págs. 193-194].

3.1.4 Métodos com foco no julgamento de especialistas

O último grupo de técnicas analíticas de avaliação, compreende basicamente o uso de listas de verificação (**Check List**) principalmente usadas para questões de ergonomia. Nestas listas, o *layout* dos painéis, posição de instrumentos de campo, chaves de atuação de emergência, identificação dos componentes, são questionados, bem como a qualidade de procedimentos, sobre variados aspectos.

3.2 Métodos Qualitativos e Quantitativos para Identificação dos Erros Humanos

O primeiro propósito de uma análise de confiabilidade humana em um estudo de análise de riscos, é a determinação da probabilidade das falhas das pessoas. O resultado de uma análise de confiabilidade humana é normalmente expresso pela probabilidade ou taxa de falhas, da seguinte forma [Ref. 23, pág. 239]:

$$\text{Probabilidade do erro humano} = \frac{\text{Número de erros}}{\text{Número de oportunidades de erro}}$$

$$\text{Taxa de falha humana} = \frac{\text{Número de erros}}{\text{Duração total da tarefa}}$$

As principais técnicas para a obtenção da probabilidade dos erros são as seguintes:

3.2.1 Técnica de Predição das Taxas de Falhas Humanas (*Technique for Human Error Rate Prediction -THERP*)

A técnica foi desenvolvida inicialmente para a indústria nuclear, por Swain e Guttmann em 1983. Sua característica é a combinação da análise de tarefas e árvore de eventos, com análise de sucesso e falha de cada tarefa. O método necessita a identificação detalhada de cada tarefa, bem como a sua decomposição em sub-tarefas, quando possível. Doze passos são propostos para a execução do método. Uma listagem geral dos componentes do sistema é feita no inicio do estudo. Passos intermediários são conduzidos, usando-se árvore de eventos e análise de tarefas. Fatores de performance são introduzidos na avaliação, bem como uma análise de sensibilidade. Por último, probabilidades dos erros são identificadas, com base na publicação de Swain e Guttmann (1983) [Ref.14, pág. 226-228] [Ref. 23, pág 239]. [Ref. 18, pág. 60].

3.2.2 Avaliação da Seqüência de Acidentes (*Accident Sequence Evaluation Program - ASEP*)

Desenvolvida por Swain em 1987 [Ref. 23, pág. 239], a técnica baseia-se em algumas condições bem específicas, entre as quais, que a probabilidade de erro em cada atividade crítica é igual a 0,03.

3.2.3 Simulação do Desempenho das Equipes de Manutenção (*Maintenance Personnel Performance Simulation*)

Desenvolvido por Siegel em 1984 [Ref. 23, pág 244], o método baseia-se como na técnica THERP, na análise de tarefas. O produto da análise é a probabilidade de sucesso, o tempo para a execução da tarefa e nível de estresse.

A partir dos valores encontrados para as probabilidades dos erros humanos, técnicas como Árvore de Eventos e Árvore de Falhas são usadas para a quantificação do cenário completo de risco, com outros modos de falha além daqueles de natureza humana.

3.2.4 Técnica para Redução e Avaliação dos Erros Humanos (Human Error Assessment and Reduction Technique - HEART, Williams, 1986) [Ref. 33, pág. 236]

A premissa fundamental desta técnica baseia-se na análise dos fatores ergonômicos de fundamental impacto na confiabilidade. Sua principal ajuda é a facilidade de diálogo que permite entre engenheiros e ergonomistas. A técnica usa a análise de tarefas, como ponto de partida, e avalia as condições que levam aos erros. Para cada tipo de tarefas (familiares ou não rotineiras)

uma probabilidade de erro é estipulada. Sobre esta probabilidade, são aplicados fatores de redução da confiabilidade, de acordo com a situação, como por exemplo: falta de experiência do operador; baixa confiabilidade dos instrumentos; falta de percepção dos riscos; conflitos de objetivos; etc.

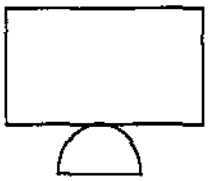
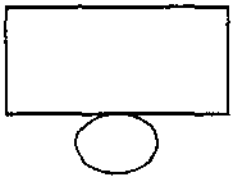
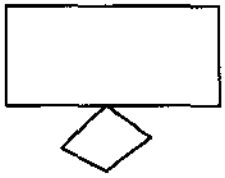
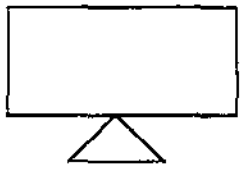
3.2.5 Árvore de Falhas

Análise através de Árvore de Falhas é uma representação gráfica das relações que existem entre os componentes de um sistema [34]. A análise mostra como uma seqüência de falhas pode conduzir a um evento final indesejável, chamado de Evento Topo, fornecendo as combinações das falhas que levam a este evento e a sua probabilidade de ocorrência. O objetivo da análise é a determinação de como o sistema, incluindo as pessoas envolvidas no *processo*, pode falhar.

O Evento Topo deve sempre conter claramente o "atributo" de confiabilidade que se deseja analisar: confiabilidade propriamente dita; indisponibilidade; freqüência de ocorrência; mantenabilidade.

Na aplicação da técnica, são usados os símbolos seguintes, conforme mostrado na Tabela IX.

Tabela IX. Símbolos gerais usados na representação de sistemas, através da técnica árvore de falhas.

SÍMBOLO	DESENHO	UTILIZAÇÃO
EVENTO TOPO		Usado para representar o evento indesejável, objeto da análise. Deve conter claramente a definição do atributo escolhido.
PORTÃO TIPO " E"		Usado na representação lógica, quando TODAS as "entradas" inferiores do portão, precisam ocorrer para que o evento ocorra.
PORTÃO TIPO "OU"		Usado na representação lógica, quando apenas UMA das "entradas" inferiores do portão, precisa ocorrer para que o evento ocorra.
EVENTO BÁSICO		Evento que caracteriza uma falha no sistema (ex.: falha de bomba; falta de energia; falha humana; falha de segurança, ...)
EVENTO NÃO DESENVOLVIDO		Evento que poderia ser ainda decomposto em outros modos de falhas, mas que não se deseja especificar (falha da empresa distribuidora de energia)
TRANSFERÊNCIA		Símbolo que é usado para identificar a continuação da árvore em outro local.

O processo de construção da árvore inicia pelo Evento Topo. A partir daí, são definidos os eventos intermediários e eventos básicos que, de uma forma lógica, estão relacionados entre si, para gerar o Evento Topo. Para isto, são usados os portões lógicos do tipo "E" ou "OU" e, através de simbologia adequada, todos os eventos possíveis, como no exemplo seguinte, mostrado na Figura 18.

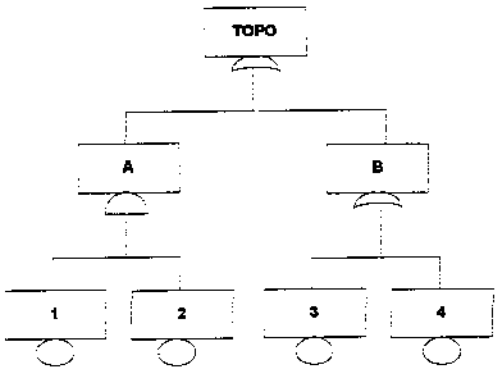


Figura 18. Representação de uma árvore de falhas, a partir de um evento topo, com portões lógicos do tipo "E" e "OU".

O passo seguinte é a determinação dos "cortes" e dos "cortes mínimos" da árvore. Um corte em uma árvore de falhas é um conjunto de eventos básicos, cuja ocorrência implica na ocorrência do Evento Topo. Um corte mínimo é um corte que não pode ser reduzido sem perder a sua condição de corte. Um corte mínimo por definição é um evento, ou combinação de eventos que, se ocorrer, gera a ocorrência do Evento Topo. No caso de combinações de eventos, Todos necessitam ocorrer para que o Topo ocorra. Assim, cada combinação representada por um corte mínimo, pode ser expressa por uma lógica do tipo "E". Cada corte mínimo é, por sua vez, caracterizado por sua ordem: número de eventos que contem a combinação. Um corte de primeira ordem contem apenas um evento; um corte de segunda ordem contém dois eventos; e assim por diante. O resultado final pode ser resumido, simplificando-se a árvore em um único portão "OU", ao qual estão ligados todos os "cortes mínimos". A soma das probabilidades dos cortes, refletirá a probabilidade do Evento Topo ocorrer. A representação da árvore através dos seus cortes mínimos, é mostrada na Figura 19.

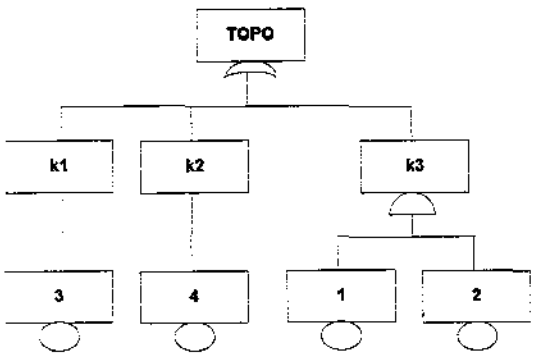


Figura 19. Representação da árvore através dos seus cortes mínimos, a partir da árvore de falhas mostrada na Figura 18.

A quantificação da Árvore de Falhas é realizada usando-se as seguintes regras: quando o portão é do tipo "E" com dois eventos básicos, como na árvore mostrada na Figura 20, a probabilidade do evento topo é dada pela expressão: P (TOPO) = P(1) x P(2), onde P(1) e P(2) são, respectivamente, as probabilidade de ocorrência dos eventos 1 e 2.

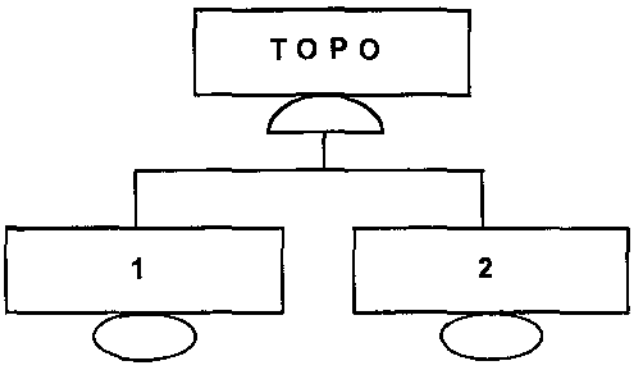


Figura 20. Árvore de falhas com um portão "E"

Quando o portão é do tipo "OU", com dois eventos básicos, como na árvore da Figura 21, a probabilidade do evento topo é dada pela expressão: P (TOPO) = P(1) + P(2) - P(1) x P(2) onde P(1) e P(2) são, respectivamente, as probabilidade de ocorrência dos eventos 1 e 2. Esta forma de cálculo só é válida se os eventos básicos forem independentes, ou seja, que o fato de um evento ocorrer, não altera a probabilidade do outro ocorrer.

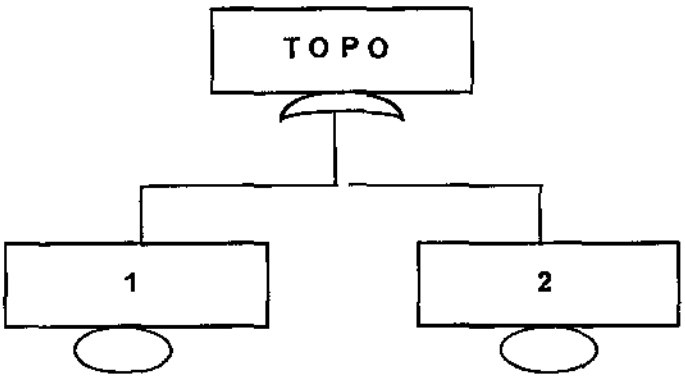


Figura 21. Árvore de falhas com um portão "OU"

Quando o portão é do tipo "OU", com três eventos básicos, como na árvore da Figura 22, a probabilidade do evento topo é dada pela expressão: P (TOPO) = P(1) + P(2) + P(3) - P(1) x P(2) - P(1) x P(3) - P(2) x P(3) + P(1) x P(2) x P(3), onde P(1), P(2) e P(3) são, respectivamente, as probabilidade de ocorrência dos eventos 1, 2 e 3. Da mesma forma como no exemplo anterior, esta forma de cálculo só é válida se os eventos básicos forem independentes, ou seja, que o fato de um evento ocorrer, não altera a probabilidade do outro ocorrer. A regra segue sendo válida para 4 ou mais eventos básicos.

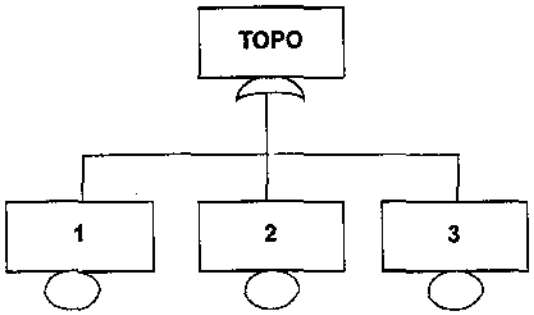


Figura 22. Árvore de falhas com um portão "OU" com 3 eventos básicos.

A probabilidade de cada evento básico é determinada em função das características da missão do componente em questão, como intervalos entre testes, tempos de reparo após a detecção das falhas, graus de dependência, etc.

Na maioria dos casos, análises qualitativas são preferidas em lugar dos estudos quantificados. Isto é normalmente consenso entre muitos especialistas que trabalham com confiabilidade, em virtude do tempo necessário para a elaboração das avaliações quantificadas, bem como pelas incertezas nos dados de probabilidade das falhas. Em alguns casos, quando decisões importantes devem ser tomadas, como o local de instalação de unidades de processamento, análises quantificadas são realizadas.

Muitas técnicas qualitativas e quantitativas são usadas para a avaliação de riscos. A maioria delas pode, de alguma forma, identificar os possíveis erros humanos existentes no processo. A referência [35] apresenta de forma didática cada uma, para ser aplicada na indústria química.

Uma das técnicas qualitativas mais simples e de uso genérico é o método chamado "*What If*". A metodologia baseia-se na aplicação da pergunta "o que ocorre se" (*What If*), sobre um determinado sistema ou equipamento. Na referência [36] são encontradas várias recomendações, vantagens e desvantagens no uso da técnica.

Para sua melhor eficiência, uma série de listas de verificação (*checklist*) contendo perguntas típicas que podem ser feitas, são apresentadas. Estas listas incluem tópicos como: processo, eletricidade, equipamentos, tubulações e proteções contra incêndios. Algumas destas perguntas, mostram a extensão da técnica, no que se refere às questões voltadas para os erros humanos, como as seguintes:

- Quando o manual de operação foi revisto e revisado pela ultima vez?
- Que requisitos especiais de limpeza existem antes do início de operação?
- Como estes requisitos foram verificados?
- Que perigos são introduzidos por procedimentos rotineiros de manutenção?

Para um determinado perigo (por exemplo, incêndio), perguntas do tipo *what if* (o que ocorre se) são feitas, como: o que ocorre se o operador realiza de forma errada a tarefa "A"? Conseqüências para esta falha são descritas, bem como os meios de proteção existentes para diminuir a probabilidade da falha ou mitigar as conseqüências. Se necessário, recomendações são sugeridas, definindo-se responsabilidades para a sua implementação. L. Zoller e J. P. Esping [37] recomendam esta técnica, apesar da sua aparente simplicidade, para a análise de riscos, inclusive aqueles provenientes de falhas humanas.

3.2.6 Análise de Modos de Falhas e Efeitos (Failure Mode and Effect Analysis - FMEA)

Esta análise tem como sua característica principal o nível de detalhe sobre os modos de falhas dos componentes envolvidos em um sistema. A técnica FMEA é conduzida de forma qualitativa e, se bem aplicada, pode auxiliar na identificação de erros humanos [38]. Goyal [39] recomenda que a técnica seja usada em substituição ao HAZOP, pelo menor consumo de tempo, e pela característica da metodologia, que analisa em maior detalhe: os equipamentos do processo; sistemas de segurança; equipamentos com usos variados; lógicas de paradas de emergência; etc.

3.2.7 HAZOP (**HAZ**ard and **OP**erability Studies)

Origem da técnica HAZOP

A técnica mais abrangente usada para a identificação de riscos na indústria química é o HAZOP. O método, derivado da técnica conhecida como *critical examination* (exame crítico), inicialmente foi apresentado por H. G. Lawley em 1974 [40], com o propósito de mostrar uma metodologia desenvolvida na Divisão Petroquímica da ICI (Imperial Chemical Industries), que tinha como premissa o fato de muitas coisas serem esquecidas nas fases de projeto, devido à complexidade dos sistemas, e não pela falta de conhecimento das pessoas integrantes das equipes projetistas.

O método foi apresentado para ser usado tanto nas fases preliminares do desenvolvimento de projeto, quando se usam fluxogramas do processo simplificados, como nas fases mais adiantadas, quando "fluxogramas de engenharia" (*Piping and Intrument Diagrams*) já foram concebidos.

No desenvolvimento da técnica HAZOP, são usadas "palavras guias" (*guide words*) para a colocação de perguntas, sobre alguns desvios típicos que podem ocorrer durante o funcionamento normal de uma unidade de produção. O método apresentado por Lawley incluiu diversas palavras guias, como: nenhum; maior; menor; mais de; menos de; parte de; mais do que; outros. Estas palavras guias foram combinadas com desvios do tipo: fluxo; pressão; temperatura; manutenção; inspeção; etc, para identificar possíveis conseqüências indesejáveis no processo.

A planilha sugerida, foi desenvolvida com o propósito voltado para a "operabilidade" (**OP**perability) da unidade de fabricação. O enfoque sobre os perigos (**HAZ**ard) foi apresentado por Lawley através do desenvolvimento quantificado da técnica Árvore de Falhas. Assim, na realidade o autor apresentou duas técnicas separadas para a análise da operabilidade e dos perigos.

Alguns exemplos extraídos da referência [40] são apresentados a seguir na Tabela X, usando o modelo da planilha apresentada por Lawley, em um estudo sobre uma unidade de dimerização de olefinas:

Tabela X. Modelo da planilha HAZOP apresentado por Lawley em 1974.

Palavra Guia	Desvio	Possíveis Causas	Conseqüências	Ação Requerida
NENHUM	Nenhum Fluxo	Erro no fechamento da válvula de isolação	Perda da alimentação para a reação e perda de produção. Polimerização formada no trocador de calor devido a ausência de fluxo.	Instalar um alarme de nível baixo no LIC (malha de controle de nível) do tanque de sedimentação.
MAIOR	Maior Fluxo	*By pass* da válvula LCV aberto indevidamente	Nível do tanque de sedimentação sobe acima do previsto	Instituir o procedimento de manter o *by pass* fechado, quando não estiver em uso.
	Maior Pressão	Erro no fechamento da válvula de bloqueio, quando a bomba está funcionando.	Linha de transferência sujeita a fluxo máximo da bomba.	Instalar uma linha de retorno na bomba (*Kickback*)

Muitos especialistas começaram a usar o método proposto, introduzindo algumas variações na metodologia. A principal foi a de acrescentar na planilha os dois enfoques: segurança e operabilidade. Trevor Kletz, também da ICI, reuniu os dois enfoques e desenvolveu o método HAZOP, como é conhecido atualmente. Novos desvios típicos foram sugeridos conforme mostrado na Tabela XI.

Tabela XI. Lista de desvios usados em um HAZOP convencional, sugerida por Kletz.

Palavra Guia	Desvios
Nenhum (None)	Ausência de fluxo quando deveria existir, ou seja, fluxo zero ou fluxo reverso (fluxo em sentido contrário ao desejado)
Mais de (More of)	Elevação de qualquer propriedade física relevante em relação ao nível que deveria existir, como fluxo maior, temperatura maior, pressão maior, viscosidade maior, etc.
Menos de (less of)	Diminuição de qualquer propriedade física relevante em relação ao nível que deveria existir, como fluxo menor, temperatura menor, pressão menor, viscosidade menor, etc.
Parte de (Part of)	Mudança da composição que deveria existir (troca da relação entre os componentes da mistura)
Mais do que (More than)	Mais componentes no sistema, em relação ao que deveria existir, como uma fase extra presente (vapor, sólido), impurezas (ar, água, ácidos, produtos de corrosão), etc.
Outros (Other than)	Qualquer outra ocorrência que saia da condição normal de operação, como os transientes de partida e parada das unidades, modos alternativos de operação, falta de fluidos de utilidades, manutenção, troca de catalisador, etc.

O processo para a realização da técnica HAZOP foi incluído e detalhado no livro escrito por Trevor Kletz, HAZOP and HAZAN, lançado pelo *Institution of Chemical Engineers*. Foi indicado como base para o trabalho o documento conhecido como Fluxograma de Engenharia, cujo conteúdo compreende: todos os equipamentos usados no processo de produção; as linhas (tubulações) que os interligam; os instrumentos de controle e os dispositivos de segurança.

Um esquema do processo desenvolvido na metodologia, sugerido por Kletz, está apresentado a seguir na Figura 23, onde o começo é a definição de uma linha (nó, ou circuito) no fluxograma de engenharia:

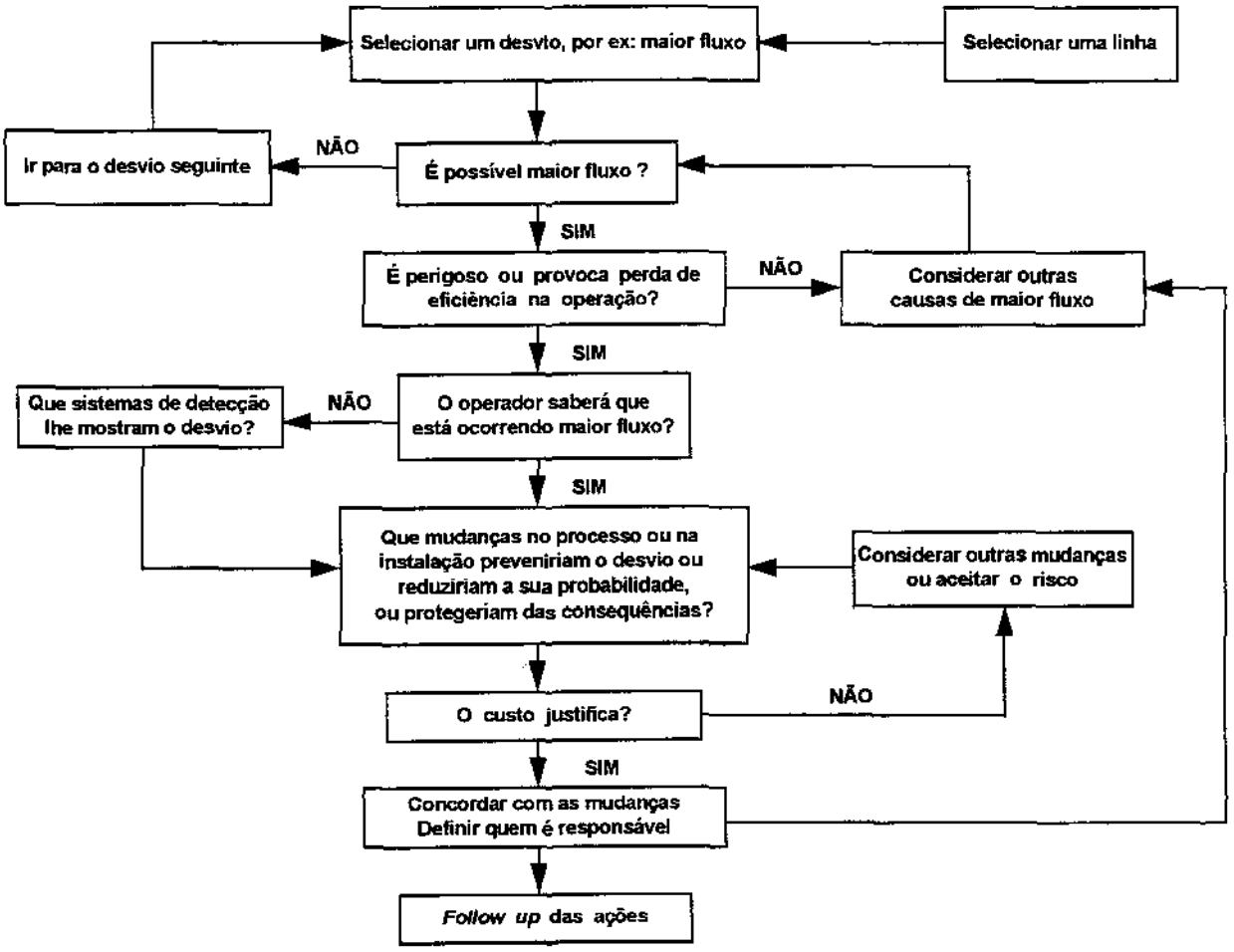


Figura 23. Processo de realização da técnica HAZOP, sugerido por Kletz [41]

O tempo necessário para analisar um nó depende do tamanho do circuito em questão. Goyal [42] sugere 45 minutos, indicando inclusive alguns dados para cálculo do número de reuniões em função deste valor.

Outras referências indicam 2 horas [43]. Ao que tudo indica, 45 minutos corresponde à um nó equivalente à uma linha de tubulação, enquanto que 2 horas corresponde à um equipamento principal e seus periféricos.

Observações gerais sobre o método HAZOP

Para a identificação de falhas de modo geral, Kletz [44] sugere que, independente da técnica usada (HAZOP ou métodos quantitativos), permanece sob responsabilidade gerencial a manutenção de um procedimento sistemático para a avaliação dos riscos inerentes às tecnologias e a sua plena compreensão. Há ainda o reforço de que é necessário, de qualquer forma, sempre responder quatro perguntas nestas análises [45]: a) Que perigos podem ocorrer? A falha na identificação dos perigos significativos pode levar a esforços dirigidos para eventos de menor importância, enquanto que os principais permanecem não sendo estudados? b) Com que freqüência os eventos podem ocorrer? c) Quais as conseqüências para os empregados e pessoas da comunidade? Quantas fatalidades podem ocorrer? d) Qual a relação da probabilidade avaliada e o nível requerido?

A técnica HAZOP é desenvolvida por uma equipe, composta de pessoas de várias especialidades, com grande experiência. Normalmente participam das reuniões representantes das áreas de processo, manutenção elétrica e automação, manutenção mecânica, segurança de processo, pesquisa e operação. O método é conduzido durante dias, semanas ou meses, dependendo da complexidade e do número de circuitos ou equipamentos a analisar. A organização da equipe normalmente requer a definição de um líder, de um calendário para as reuniões, e de uma preparação prévia da documentação necessária. O sucesso da aplicação da metodologia depende de muitos fatores, sendo um dos principais a qualidade dos documentos verificados, no que se refere ao seu grau de atualização.

Além do uso na indústria química, a técnica pode ser usada em outras atividades industriais. O método já foi utilizado para projetos de laboratórios, em operação de usinas nucleares, e para determinação de perigos em máquinas (dispositivos mecânicos). Um método alternativo, denominado de GENHAZ foi desenvolvido para identificar perigos ao meio ambiente oriundos das fabricações de organismos geneticamente modificados [41].

Considerações recentes tem sido feitas para a aplicação da metodologia HAZOP para processos descontínuos, e não apenas contínuos, como inicialmente previsto. Isto torna a técnica aplicável a uma grande variedade de processos, onde operações em bateladas (descontínuas) são realizadas [46].

Trevor Kletz [41] sugere, usando um exemplo de carregamento de um produto em um reator, algumas palavras guias para o uso da técnica nestas condições:

O produto A não é carregado
Ocorre carga de A em maior quantidade
Ocorre carga de A em menor quantidade
Ocorre carga de produto diferente de A
O produto A é carregado tarde
O produto A é carregado cedo
A carga é feita rapidamente
A carga é feita lentamente

Kelly [47] salienta a necessidade de completar o relatório HAZOP, para a sua emissão final, com análise de alguns ítens que normalmente não são cobertos pela metodologia, como por exemplo: a classificação elétrica da área; revisão dos sistemas de alívio; distâncias de implantação dos equipamentos; etc. O autor comenta a abrangência maior da técnica para a identificação de problemas de operabilidade, do que propriamente segurança. Sugere a emissão de relatórios separados para as duas questões.

Larkin [48], salienta que para a realização do HAZOP, além dos fluxogramas de engenharia, é necessário reunir: as especificação dos materiais de construção; as características químicas e físicas que conferem risco aos produtos; as utilidades envolvidas (vapor, água, etc...); os dados sobre os sistemas elétricos; os procedimentos operacionais; e dados dos sistemas informatizados.

Bullock et al. [49], propõem o uso da técnica além da fronteira dos equipamentos de processo, sugerindo planilhas de trabalho, desvios e palavras guias para os sistemas elétricos e para o estudo das interfaces entre os equipamentos e as pessoas. Palavras guias como *maior* e *menor*, são aplicadas para corrente e tensão elétrica. A palavra *nenhum*, é aplicada, por exemplo, para o aterramento elétrico.

Turner [50], através de um seminário reunindo diversos usuários da técnica HAZOP, conclui que entre as questões mais relevantes no que se refere a aplicação da metodologia, estão: a necessidade de auditar o estudo; a necessidade de criar um procedimento padrão; como realizar HAZOP sobre fatores humanos; validação dos treinamentos das equipes e dos estudos; como realizar HAZOP nas etapas de projeto; como avaliar os riscos ambientais; como incluir as lições

aprendidas, nos estudos HAZOP. Um protocolo para auditoria em nível gerencial e operacional é sugerido pelo autor.

HAZOP na investigação de erros humanos

Vários autores tem citado a técnica HAZOP como uma ferramenta com muita eficácia sobre vários aspectos, para conhecimento do processo, ganhos de operabilidade e, ainda, para auxiliar na identificação de cenários nos quais erros operacionais podem gerar conseqüências graves [51, 52].

Wells [53], inclui a abordagem de erros humanos quando sugere com o uso da palavra *outros*, que sejam contemplados erros operacionais ocasionados durante: testes; inspeção; amostragem; manutenção e procedimentos de emergência.

William Bridges, John Kirkman e Lorenzo [38], sugerem que a análise de erros humanos, normalmente realizada separadamente das análises de risco, devido sua complexidade, seja integrada na metodologia HAZOP, em função da ocorrência recente de muitos acidentes e a imposição da legislação americana.

Duas organizações nos Estados Unidos impõem no momento a inclusão nas análises de risco das falhas de natureza humana: OSHA - U. S. Occupational Safety and Health Administration, e EPA - U. S. Environmental Protection Agency:

- OSHA Final Rule 29 CFR 1910.119 (Feb. 24, 1992) - "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents".

.- EPA Proposed Rule, 40 CFR 68 (Oct. 20, 1993) - "Risk Management Program for Chemical Accident Release Prevention"

Estes autores propõem a utilização da técnica em duas etapas distintas: durante o processo convencional, ou seja, usando as palavras guias normalmente aplicadas quando se analisa o lado "*hardware*" do sistema e, posteriormente, a aplicação da técnica sobre os procedimentos operacionais, usando outras palavras guias, que auxiliam na identificação de falhas humanas, o lado "*software*" do sistema.

Quatro passos são propostos [38]:

a) Incorporação dos fatores humanos na técnica HAZOP, através da pergunta "por que"?

b) Análise sobre os procedimentos operacionais, com novas "palavras guias".

c) Análise dos fatores de gerenciamento, através de um questionário (lista de verificação)

d) Análise detalhada da confiabilidade humana, por especialistas no assunto.

Trevor Kletz tem analisado com grande extensão o papel humano nos acidentes industriais. Vários incidentes e acidentes são relatados por ele [54] como tendo sido causados por falhas humanas. Em *Engineer's View of Human Error* [5], o autor publica vários modos de erros humanos e sua probabilidade de ocorrência.

Uma questão importante é colocada pelo autor [55] quando menciona a confiabilidade do sistema homem / máquina. Neste contexto, Kletz salienta que, numa situação onde o operador é chamado a atuar após o toque de um alarme, é possível conhecer a confiabilidade do sistema que alerta o operador, bem como do componente onde ele deve atuar. Mas é difícil prever a confiabilidade da pessoa envolvida.

Ainda, qualquer melhoria no sistema de alarme e no componente onde a ação deve ser feita, é relativamente fácil de fazer. Contudo, da mesma forma, é difícil melhorar o desempenho do homem. Sempre se espera que o operador consiga ter sucesso na ação.

Quanto a questão da performance da técnica HAZOP para a identificação de erros humanos e de gerenciamento, Kletz confirma sua possibilidade com vários exemplos em todas as suas obras.

HAZOP de sistemas informatizados

Os sistemas informatizados usados no controle dos processos industriais têm merecido constante interesse, com relação a confiabilidade que podem agregar às unidades de processo, bem como com respeito à preocupação dos seus modos de falhas, inclusive aqueles de natureza humana.

Eddershaw [56] da Imperial Chemical Industries (ICI), relata um incidente ocorrido em uma unidade de fabricação de Nylon, quando um computador provocou a parada da planta em situação crítica. Inúmeras válvulas posicionaram-se em situação incorreta, inversamente ao previsto, colocando em risco a unidade e os operadores. A técnica HAZOP foi utilizada para avaliar os riscos e propor recomendações para a segurança da unidade.

Kletz [57] adverte que os computadores (ou também chamados "sistemas lógicos programáveis") não estão trazendo novas formas de erros, mas novas oportunidades de "velhos erros". Falhas nas instruções introduzidas nos programas destes sistemas e a visão desta forma de controle como uma "caixa preta" podem, segundo o autor, ser analisadas e reduzidas com o auxílio da técnica HAZOP.

Como a dependência no uso de sistemas informatizados tem aumentado, sugestões tem sido feitas para garantir a performance [58], a partir do aprendizado em simuladores e no correto projeto de apoio *on line* aos operadores, com *menus* criteriosamente desenhados. A interface homem-sistema requer atualmente novas considerações, tendo em vista que as metodologias usadas para as análises de risco, em sua maior parte, assumem uma independência entre as falhas.

Falhas de modo comum passam a ser um assunto de elevada importância em sistemas informatizados. Elizabeth Drake [59] sugere a técnica What If nas etapas iniciais dos projetos, e a técnica HAZOP como uma ferramenta de análise qualitativa para a avaliação destes tipos de sistemas, quando o projeto já está em fase adiantada de realização.

Collins [60], apresenta uma sugestão para a utilização do HAZOP sobre sistemas informatizados, usando palavras guias complementares, como: falhas nos sensores; falhas na interface de entrada; falhas de programação; falhas na interface de saída; falhas na saída do controle.

Fecontt [61], sugere que sejam incluídos nos estudos HAZOP diagramas que representem o modelo sobre o qual está baseado o processo químico, para que possam ser avaliados os requisitos de operabilidade, ou intenções, dimensionados através de *softwares* aplicados à engenharia química.

Sistemas informatizados para a realização de HAZOP

Para facilitar a aplicação desta técnica, *softwares* tem sido desenvolvidos para o registro das análises realizadas durante as reuniões [43] [62]. Os *softwares* permitem ao usuário editar o banco de dados de falhas existente no programa, criando uma biblioteca própria para ser usada

por determinada indústria. Os bancos de dados já incluem alguns modos de falhas humanas, que ajudam os usuários a identificar desvios que iniciam com erros dos operadores.

Raymond et al. [63], desenvolveram um modelo para permitir o planejamento dos estudos HAZOP, baseado em uma série de estudos realizados. O modelo permite estimar o tempo necessário para a análise, a partir de dados como a experiência do líder do grupo e o número e complexidade dos fluxogramas de engenharia envolvidos.

Independente do uso ou não de sistemas informatizados, os autores que se manifestam a respeito do assunto, são unânimes em afirmar que a experiência da equipe e principalmente do líder definirá a qualidade do estudo

Todas as técnicas mostradas anteriormente de alguma forma servem para a identificação de erros humanos. Algumas delas são reconhecidamente melhores que as outras, mas todas tem aspectos particulares que fazem com que sejam escolhidas. Whalley e Kirwan [64], analisaram cinco técnicas (algumas já apresentadas) para avaliar sua capacidade de identificação de falhas de natureza humana: *PHECA - Potencial Human Error Cause Analysis* (Análise de causas potenciais dos erros humanos); *Work Analysis Method* (Método de análise do trabalho); *SHERPA; THERP; Own Judgment*. Entre as conclusões do trabalho, os autores mencionam a necessidade de futuros desenvolvimentos, tendo em vista que o texto limitava-se a uma pequena exploração sobre o assunto.

Este estudo foi usado como um dos pontos de partida, para uma análise mais detalhada realizada por Kirwan [65], em 1992, sobre 12 técnicas consideradas úteis para a identificação de erros humanos, incluindo a metodologia HAZOP. Foram avaliadas técnicas baseadas em "simples" classificação de erros, até aquelas que utilizam sofisticados programas de computador.

As técnicas foram descritas e detalhadas nas suas características principais: quanto à abordagem do modelo SRK e, principalmente, do modo de falha Rv (violação de regras), que tem sido considerado importante ultimamente, na avaliação da probabilidade de falha; quanto ao nível estruturado da metodologia; quanto à validação através de um modelo teórico; quanto à assessibilidade de "erros externos" e "erros internos" (psicológicos) e/ou fatores modeladores de performance; quanto à capacidade de contribuição para a redução dos erros identificados; quanto aos recursos necessários para o desenvolvimento da técnica; quanto à documentação produzida

para auditoria; quanto à aceitabilidade comprovada da metodologia. O estudo apresenta o "estado da arte" das metodologias para identificação de erros humanos.

Como seguimento ao estudo, Kirwan [66] apresenta a comparação destas 12 técnicas em relação às características mencionadas acima. A técnica HAZOP é identificada no trabalho como uma metodologia capaz de:

- Identificar erros baseados em falta de habilidade, mal uso de regras e violações;
- Identificar "erros externos" (operador abre uma válvula errada);
- Identificar claramente mecanismos para a redução dos erros;
- Identificar erros sem uso de ferramentas complexas (*softwares*);
- Permitir auditoria, em função da elevada documentação produzida.

O autor considera o HAZOP uma técnica com poder "moderado" para a identificação de erros humanos, apesar de ser extensivamente usada como fonte de dados para a avaliação da probabilidade de ocorrência de eventos críticos.

Em 1994 Kirwan [Ref. 33, pág. 97] propõe com ênfase muito clara a adaptação do HAZOP tradicional para ser usado na identificação de falhas humanas. O autor relata um exercício usando a técnica "estendida", através de 16 novas palavras guias, cujo foco são erros operacionais. A expressão *Human HAZOP* é usada para caracterizar a forma diferenciada da metodologia. Kirwan [67] apresenta em 1995, o uso da técnica HAZOP para a análise de erros de comissionamento (executar uma tarefa de forma inadequada ou uma tarefa que não deve ser feita), em um programa de avaliação de falhas humanas em centrais nucleares, usando como palavras guias: erro de interpretação; visão tipo túnel; ou persistência.

De forma geral, as técnicas para a redução das falhas buscam ao mesmo tempo a otimização da performance, através de projetos de sistemas que levem em conta as limitações humanas, de estudos detalhados da interface homem / ambiente, e das análises das tarefas. O início do processo, contudo, baseia-se na eficiência de identificação dos perigos existentes nos sistemas. Esta performance depende não só das pessoas envolvidas, mas do "poder de identificação" de cada técnica. A Figura 24 mostra uma aproximação desta capacidade.

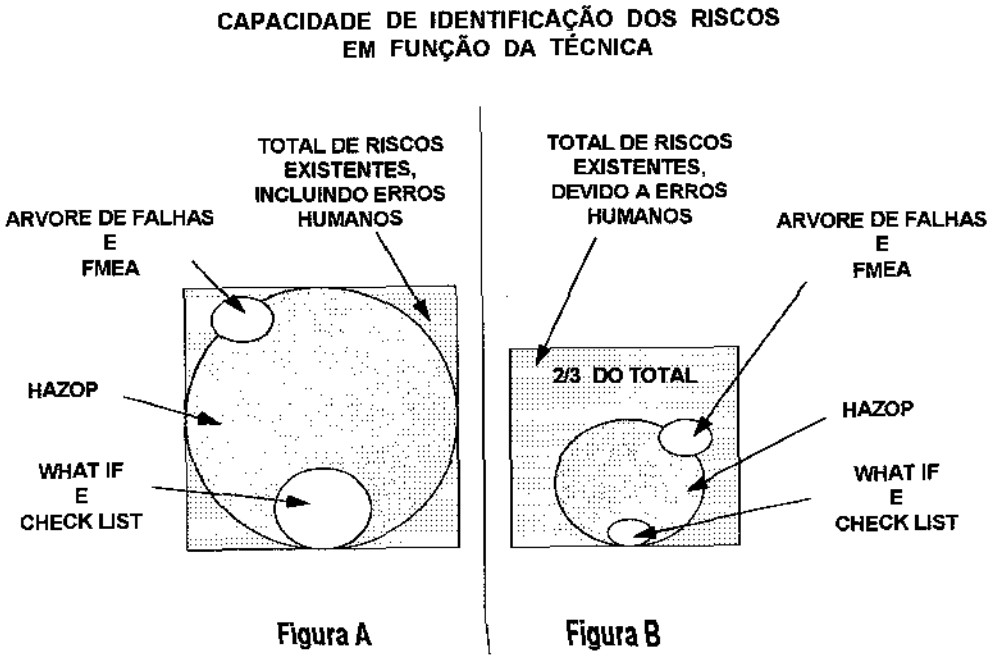


Figura 24. Representação da comparação da capacidade das técnicas HAZOP, What If, FMEA e árvore de falhas: (a) de identificar perigos (b) de identificar erros humanos.

A Figura 24 (a) sugere de forma relativa, que a metodologia HAZOP é a ferramenta ideal para a identificação de grande parte das falhas que podem ocorrer nas unidades de processo químico, enquanto que os métodos What If e as listas de verificação (check list) tem potencial limitado, por não serem estruturadas na mesma proporção da técnica HAZOP.

Em princípio, pode-se afirmar que os riscos identificados com a técnica What If, também o são com o HAZOP. Já a técnica árvore de falhas, é uma ferramenta muito poderosa para identificar com maior detalhe desvios possíveis em sistemas. Muitas vezes ela é usada paralelamente à técnica HAZOP, quando se deseja avaliar a probabilidade de um evento já identificado, que é indesejável, ocorrer na vida útil da instalação. Modos de falhas e alguns riscos que a técnica HAZOP não consegue facilmente identificar, "aparecem" quando a árvore de falhas é desenvolvida. Falhas de modo comum, por exemplo, não são facilmente caracterizadas pelo HAZOP, mas são explicitadas nas árvores de falhas. Tudo isto é verdade, naturalmente, dependendo da experiência dos usuários destas técnicas.

A Figura 24 (b) mostra, por outro lado, o desempenho parcial que o HAZOP possui na identificação de erros humanos. Muitos eventos que iniciam com falhas humanas são identificados no HAZOP, mas uma grande parte deixa de sê-lo em função, em parte, da forma como são conduzidas as reuniões de estudo. O foco principal normalmente é a análise de falhas de equipamentos e seus periféricos (tubulações, instrumentos, controles, etc).

Estas comparações são importantes no momento em que, em vários países, um programa de revisão de segurança de processo está sendo exigido das indústrias químicas. Estes programas tiveram início a partir do acidente de Seveso na Itália. A Diretiva Seveso, emitida em 1982 [68, 69], seis anos após o acidente, obriga os países membros a desenvolver estudos de segurança de processo em todas as unidades de fabricação, em fase de projeto ou em operação.

A legislação americana, da mesma forma, através dos dois organismos oficiais mencionados anteriormente (OSHA e EPA), regulamenta a emissão compulsória das Revisões de Segurança de Processo. No Brasil, a ABIQUIM - Associação Brasileira da Indústria Química, desenvolve um programa semelhante, para que as empresas associadas procurem identificar os riscos nos seus processos e também desenvolvam planos para mitigar suas conseqüências.

Não há menção na Diretiva Seveso das técnicas a usar, e nas legislações americanas, as várias técnicas são listadas como sugestões para a aplicação. Contudo, sempre que há menção das metodologias para uso nos programas de identificação de perigos nos processos (Process Hazard Analysis - PHA), a técnica HAZOP aparece em primeiro plano [51].

PARTE EXPERIMENTAL

4. Metodologia

Para alcançar os objetivos desta dissertação o método usado foi o de identificar, através da técnica HAZOP, as falhas humanas com potencial de "eventos iniciadores" para eventos críticos. Os estudos HAZOP foram realizados em unidades de processamento químico. Duas situações foram focadas:

a) a aquisição de dados com processo HAZOP convencional, com as palavras guias usuais, conforme proposto pelos autores da técnica

b) a aquisição de dados expandindo a técnica, usando um número maior e seletivo de desvios e palavras guias.

Para cada uma destas situações, foram usados métodos diferentes, que serão descritos a seguir.

4.1 Aquisição de dados em um programa de revisão de segurança de processo usando a técnica HAZOP convencional

4.1.1 Local dos estudos HAZOP

As análises foram realizadas na Usina Química de Paulínia (UQP), pertencente a empresa Rhodia S/A. Neste local são produzidos produtos intermediários para a indústria química, como: fenol e seus derivados; sal nylon; solventes acéticos e cetônicos; silicatos e pigmentos; ácido salicílico; látex; estireno butadieno; hidrogênio; dióxido de carbono; cicloexanol; hexametilenodiamina (HMD).

4.1.2 Processo de revisão

O processo para a revisão das unidades foi definido conforme mostrado na Figura 25 a seguir.

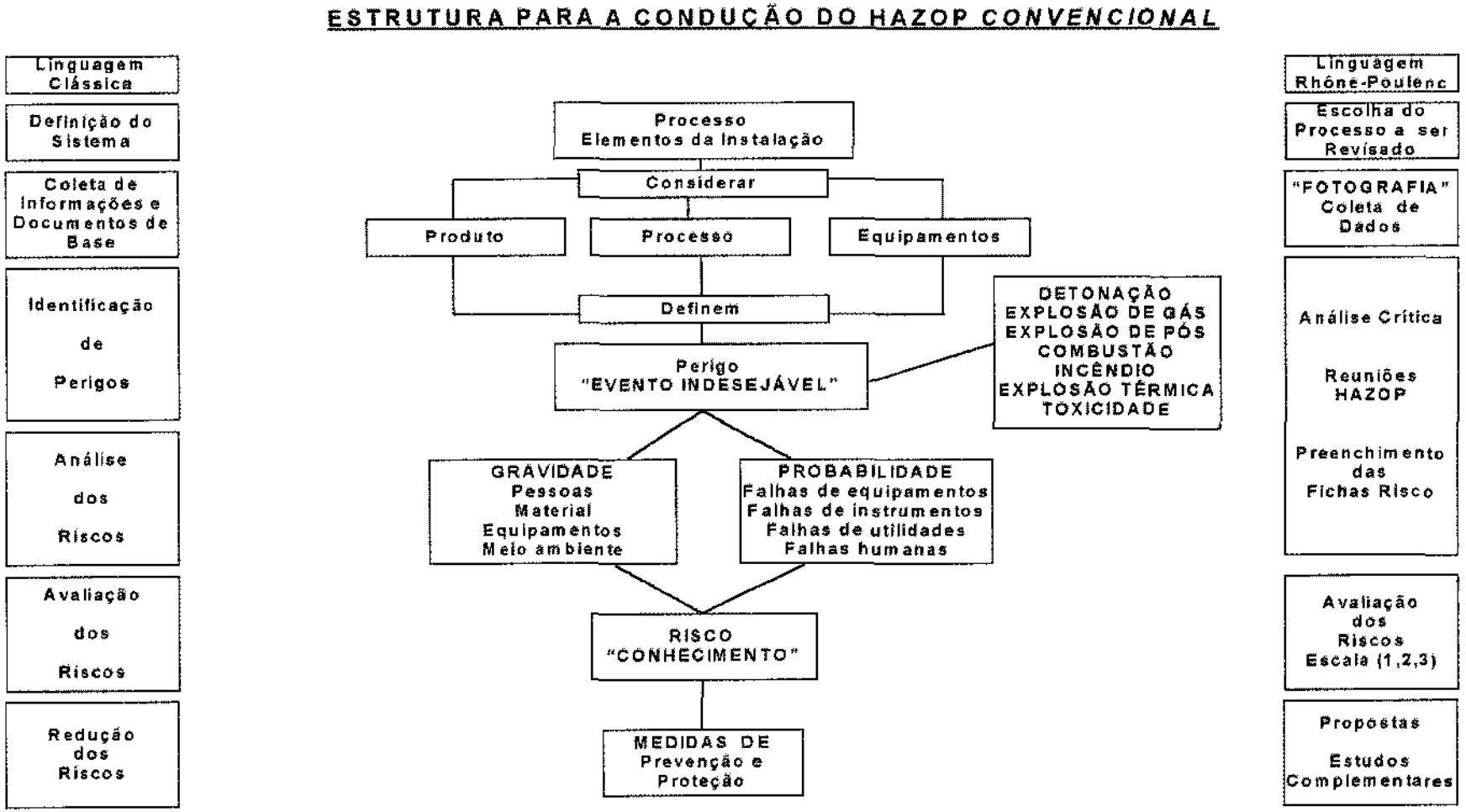


Figura 25. Processo para a revisão de segurança em uma unidade de produção ou estocagem.

A "Fotografia" de cada unidade foi elaborada, para permitir a organização das informações necessárias para consulta durante as reuniões. A Tabela XII mostra um resumo dos tópicos que constaram da fase de levantamento de dados.

Tabela XII. Lista dos documentos agrupados na fase "fotografia", para permitir o início do estudo de revisão de segurança de processo em uma unidade de fabricação ou estocagem.

	I	II	III	IV	V
	HISTÓRICO	**PRODUTO**	**PROCESSO**	**EQUIPAMENTO**	**MEIO AMBIENTE**
1	**Acidentes**	**Lista**	**Descrição Processo**	**Fluxogramas de Engenharia (P & I)**	**Site - Implantação**
2	**Incidentes**	**Fichas-Produto**	**Fluxogramas Simplificados**	**Especificação dos Equipamentos**	**Densidade de População**
3	**Modificações**	**Fichas-Processo**	**Partidas**	**Procedimentos de Manutenção**	**Climatologia Local**
4	**Confiabilidade**	**Tabela Incompatibilidade Produto x Produto**	**Marcha Normal**	**Procedimentos de Inspeção**	**Agressões Externas**
5	**Capacidade**	**Tabela Incompatibilidade Produto x Material**	**Parada**	**Dossiê de Válvulas**	**Emissão de Poluentes**
6	**Conhecimento**	**Balanço Material**	**Tomada de Amostras**	**Matriz Alarmes e Segurança**	**Permissão de Funcionamento**
7	**Legislação**	**Balanço energético**	**Organização do Trabalho**	**Testes dos Dispositivos de Segurança**	**Plano de Emergência**

A partir da fotografia pronta, foi realizada a identificação de perigos em cada unidade de fabricação, através de reuniões com pessoas de diversas áreas (processo, fabricação, manutenção mecânica, instrumentação e segurança de processo).

Após, ou mesmo durante as sessões, reuniões de análise dos riscos foram conduzidas para a definição dos atributos de probabilidade e gravidade de cada evento. Sempre que necessário, modelos de simulação de impactos foram usados para avaliar a radiação decorrente de incêndios; ondas de pressão causadas por explosões; e a dispersão de nuvens tóxicas, para definir com maior clareza o atributo da gravidade do cenário em questão. Da mesma forma, árvores de falhas foram usadas, quando julgado importante, para a definição da probabilidade do evento ocorrer.

Matrizes para critérios de gravidade, probabilidade e risco foram definidas, conforme mostrado nas Tabelas XIII, XIV, XV, respectivamente, mostradas a seguir.

Tabela XIII. Critérios para a definição da gravidade dos eventos identificados como possíveis

Nível	Pessoas	Meio Ambiente	Atividade
0	Pessoas podem ser atingidas fora da Propriedade da Rhodia	Poluição irreversível no exterior do site	Parada da atividade de fabricação (perda do mercado)
1	Danos Irreversíveis dentro dos limites da propriedade	Poluição reversível no exterior do site	Parada de algumas semanas ou meses
2	Danos reversíveis	Poluição limitada ao site	Parada de alguns dias
3	Primeiros Socorros	Poluição limitada à unidade de processo	Parada de algumas horas

Tabela XIV. Critérios para a definição da probabilidade dos eventos identificados como possíveis

Nível	Freqüência (ocorrências / ano)
1	10 a 10^{-1}
2	10^{-1} a 10^{-3}
3	10^{-3} a 10^{-5}
4	10^{-5} a 10^{-7}

Tabela XV. Critérios para a definição do risco caracterizado pelos eventos identificados como possíveis

Gravidade ⇒ Probabilidade ⇓	0	1	2	3
1	1	1	1	2
2	1	1	2	3
3	1	2	3	3
4	2	3	3	3

Os riscos foram definidos em três categorias, como segue:

Risco 1 ⇒ Representa uma situação inaceitável

Risco 2 ⇒ Representa uma situação a ser melhorada

Risco 3 ⇒ Representa uma situação aceitável

Para diminuir a variabilidade nos grupos de análise, foi criado um *menu* de palavras guias e desvios, para auxiliar às equipes na identificação dos perigos.

A Tabela XVI a seguir lista estas palavras que, na realidade, foram detalhadas a partir dos princípios gerais da metodologia.

Tabela XVI. Lista detalhada dos desvios, usado como apoio para a realização do HAZOP convencional.

Palavras guias	Desvios (ou parâmetros)
Maior	Vazão
	Pressão
Menor	Temperatura
	Fluxo reverso
Nenhuma	Nível
	Agitação
Mais	Viscosidade
	Mudança de composição
Menos	Componentes a mais
	Manutenção
Ocorrência de	Teste
	Partida
Falha na	Parada
	Água de resfriamento
Falha no	Água fria
	Água bruta
Falta de	Salmoura
	Ar de serviço
	Ar de Instrumentação
	Vapor
	Condensado
	Energia Elétrica
	Amostragem
	Outras condições
	Projeto
	Modo Operatório

As palavras da coluna da esquerda, quando combinadas com as da coluna da direita, forneceram de modo geral os desvios possíveis. Assim, por exemplo, ao analisar um circuito (nó), puderam ser questionados:

Falta de vazão
Ocorrência de fluxo reverso
Pressão maior
Falha no Projeto
Falta de teste
Falha no modo operatório
etc...

Para cada desvio fixado, uma lista de causas possíveis foi listada, como por exemplo: falha numa determinada válvula; furo em um equipamento; erro de calibração de um instrumento; instrução errada; descarga atmosférica; etc. Quando todas as causas possíveis eram tabuladas, a equipe voltava-se para a definição das conseqüências de cada uma. As conseqüências (o evento indesejável) podiam ser:

Explosão de gás confinada
Explosão de gás não confinada
Explosão térmica
Explosão física
Explosão de poeira
Embalo térmico
Incêndio
Detonação
Emissão tóxica para o meio ambiente
Indisponibilidade da unidade

O foco principal dos estudos foi procurar desvios que caracterizavam um "risco maior" (risco nível 1), através da ocorrência de um dos eventos listados acima. Contudo, falhas que ocasionassem "apenas" perda de produção, também foram listadas. A planilha de trabalho usada durante as reuniões é semelhante a mostrada na Tabela XVII.

Tabela XVII. Planilha de trabalho usada nas reuniões HAZOP, contendo as colunas necessárias para o registro dos desvios, das conseqüências, das seguranças, das recomendações e dos riscos avaliados.

DATA:_____ **PLANILHA HAZOP** **FOLHA:**_____

SISTEMA:_____
INTENÇÃO:_____
DESENHO N°:_____

PALAVRA CHAVE / DESVIO	CAUSAS	CONSEQÜÊNCIAS	DETECÇÕES	PROTEÇÕES	RECOMENDAÇÕES	P	G	R	N° FICHA RISCO

Após cada conseqüência ser caracterizada, foram descritos os meios de detecção e proteção já existentes na instalação, para diminuir a probabilidade da falha ocorrer (causa) ou reduzir a conseqüência. Foram identificados alarmes; automatismos; dispositivos de alívio de pressão; diques de contenção; ação do operador; etc. A partir do cenário identificado, o risco foi definido e as ações necessárias foram listadas.

4.1.3 Levantamento dos dados

Para cada estudo concluído, foram identificados os modos de falhas explicitados nas planilhas HAZOP: falhas de natureza humana; falhas em instrumentos; falhas em equipamentos de processo; falta de utilidades; ocorrência de eventos externos; e falhas em tubulações.

4.2 Aplicação do HAZOP modificado

A metodologia adotada foi a de ampliar a técnica HAZOP, com base em sugestões existentes na literatura, criando algumas "expressões específicas", quando necessário, para atingir o objetivo: identificar não só "o que" as pessoas podem fazer errado, mas "por que" podem fazê-lo. A Tabela XVIII mostra os desvios considerados e as causas possíveis, que foram inicialmente usadas para analisar as falhas decorrentes de erros humanos e a performance das pessoas em cada tarefa.

Tabela XVIII. Lista de desvios usada para identificação de erros humanos no HAZOP ampliado.

Desvios	Causas
Ação muito lenta	Tarefa não familiar ou complexa Tarefa manual, que deveria ser automática
Ação muito rápida	Risco não conhecido ou o tempo é insuficiente Desvio ocorre subitamente
Ação no tempo errado	Ruído elevado ou iluminação inadequada Calor excessivo ou condição atmosférica ruim
Ação na direção errada	Excesso de horas no posto de trabalho Mudança no horário do turno
Ação a mais	Acesso inadequado EPI inadequado (proteção individual)
Ação a menos	Painel com informação excessiva Display com má identificação
Alinhamento errado	Estereótipo do operador Agrupamento das informações é errado
Ação certa, sobre objeto errado	Mesmo símbolo para operação normal e com desvio (formato) Falta de clareza na instrução
Ação errada, sobre objeto certo	Nível de instrução insuficiente Falha na especificação das condições de entrada
Ação errada, sobre objeto errado	Falha na especificação das condições de saída Alertas e avisos inadequados
Ação incompleta	Suporte para diagnóstico de falhas inadequado Projetista não conhece a unidade suficientemente
Verificação omitida	Procedimentos não atualizados Conflito entre produção e segurança
Verificação incompleta	Equipamento novo, com modos de falhas desconhecidos Falta de treinamento em situação de emergência
Verificação certa, sobre objeto errado	Falta de treinamento com controles e sistemas de segurança Treinamento não é adequado ou falta de motivação
Verificação errada, sobre objeto certo	Habilidade requerida é acima da existente Falta de experiência do operador com eventos de alto estresse
Verificação errada, sobre objeto errado	Risco percebido pelo operador é pequeno Operador muda hábitos para manter o "seu" nível de risco
Verificação atrasada	Operador necessita de ajuda "externa" Condição física não é apropriada ou idade avançada
Informação não obtida	Equipe não é treinada para uma boa comunicação Carga de trabalho mal distribuída
Informação obtida errada	Informação dada diferente da informação recebida Falha na sinalização ou sinal errado
Informação recebida incompleta	Informação não pode ser confirmada com outra indicação Situação "no campo" esta errada, devido tarefa realizada por
Informação não transmitida	outra pessoa, e desconhecida Confusão na hierarquia (formal é diferente da normal). Quem
Informação transmitida errada	sabe não detém o poder de decidir Falta de planejamento
Informação transmitida incompleta	O comprometimento não é adequado Cultura excessiva em "livros de normas"
Omissão na seleção	Estudos de segurança realizados não contemplaram mudanças na organização ou falhas humanas de forma detalhada
Seleção realizada errada	Falha na aprendizagem de acidentes já vividos Modelo mental baseado fortemente em eventos já vividos
Pré-requisitos ignorados	Espera demasiada por uma informação confirmatória Paralisia mental temporária
Plano executado errado	Visão tipo "túnel" Polarização da idéia

Alguns casos foram estudados, correspondendo a cenários envolvendo riscos de segurança e de perda de qualidade e produtividade:

4.2.1 Caso I

O experimento foi efetuado de duas formas: a) em reuniões normais de HAZOP b) em reunião específica para tratar de determinada tarefa, cuja importância era relevante, para a segurança da unidade. Neste caso, foi usado o fluxograma de engenharia em conjunto com o manual de operação. Este último documento, de forma geral, contém os procedimentos que devem ser seguidos pela equipe de produção, compreendendo as diversas tarefas que devem ser executadas em diferentes situações.

4.2.2 Caso II

Um cenário de risco foi identificado em um HAZOP convencional, e uma árvore de falhas foi desenvolvida para estudar a confiabilidade do sistema de segurança projetado para reduzir a probabilidade do evento indesejável. O software FTW (Fault Tree Workstation) foi usado para o desenho e cálculo dos cortes mínimos. A técnica HAZOP foi expandida para auxiliar neste estudo de confiabilidade, visando identificar falhas humanas no sistema. O software HAZOP-PC foi usado para registrar todos os cenários imaginados.

5. Resultados

5.1 Capacidade da técnica HAZOP convencional para a identificação de erros humanos

A Tabela XIX a seguir, mostra de forma resumida a lista dos trabalhos efetuados e alguns indicadores que dependem, entre outros, do processo de fabricação avaliado, da tecnologia de controle usada, e do perfil da equipe.

Foram analisados cerca de 1000 equipamentos principais (reatores, colunas de destilação, fornos, trocadores de calor, reservatórios de estocagem, etc.) e seus equipamentos acessórios (bombas e pequenos potes), através de aproximadamente 50 estudos HAZOP.

O número de nós, representa o número de circuitos avaliados. Um nó é por definição um sub-sistema, que contém um equipamento principal e sobre o qual são aplicadas as palavras guias e os desvios previstos na metodologia.

O número de reuniões refere-se a cada sessão de 3 ou 4 horas realizadas com cada equipe. O número de homens-hora (H/h) mede o número total de horas de cada grupo durante as sessões. Cinco pessoas durante 3 horas de reunião, representam 15 H/h, por exemplo.

A distribuição das falhas diz respeito aos modos de falhas que as equipes conseguem "enxergar" durante o processo das reuniões. No caso específico das falhas de natureza humana, os desvios foram quase que na totalidade centrados em falhas de operação e manutenção.

Tabela XIX. Resumo das informações retiradas dos estudos realizados em cerca de 50 estudos HAZOP, envolvendo unidades de fabricação, estocagens, processos contínuos e descontínuos.

				Distribuição das Falhas Nº					
Instalação	**Nº de reuniões**	**Nº de nós**	**H/h**	**Humanas**	**Instrumentos**	**Linhas**	**Utilidades**	**Equipamentos**	**Externos**
Ácido Acético	35	10	447	8	15	4	2	13	0
Ácido Adípico	105	57	2232	183	152	29	22	112	5
Ácido Nítrico	34	16	594	19	19	6	4	11	0
Aldeído Acético	75	36	1049	20	44	10	5	21	2
Ar Líquido	17	11	334	53	10	5	6	24	4
Bic. de Amônia	6	5	108	12	1	1	0	5	0
Bisfenol	63	58	1050	49	97	13	50	47	18
Cicloexanol	29	18	378	6	18	7	4	0	0
Estocagens	95	92	1506	123	55	35	4	69	40
Fenol	120	120	1860	82	74	12	26	40	0
Hexilenoglicol	33	18	577	19	11	2	8	9	1
Diamina (HMD)	70	44	1668	69	15	25	7	12	9
Látex	21	11	317	19	6	4	3	13	1
Reforming	129	126	2160	108	59	21	21	30	3
Sal Nylon	11	8	204	8	5	0	0	2	0
Salicílico	42	66	696	54	34	39	15	41	13
Sílicas	36	22	439	23	21	1	1	5	1
Solventes	89	73	1154	45	60	17	16	47	5
Utilidades	157	118	2210	631	485	120	85	233	56
TOTAL	1167	909	18983	1531	1181	351	279	734	158

O percentual de falhas identificadas na Figura 25(a), refere-se à relação entre o número de cenários cujos eventos iniciadores foram um dos seguintes tipos:

erros humanos;

falha de instrumentos;

falhas em linhas;

falhas no fornecimento de utilidades;

falhas intrínsecas de equipamentos;

eventos externos;

e o total de cenários identificados com potencial de risco para a segurança.

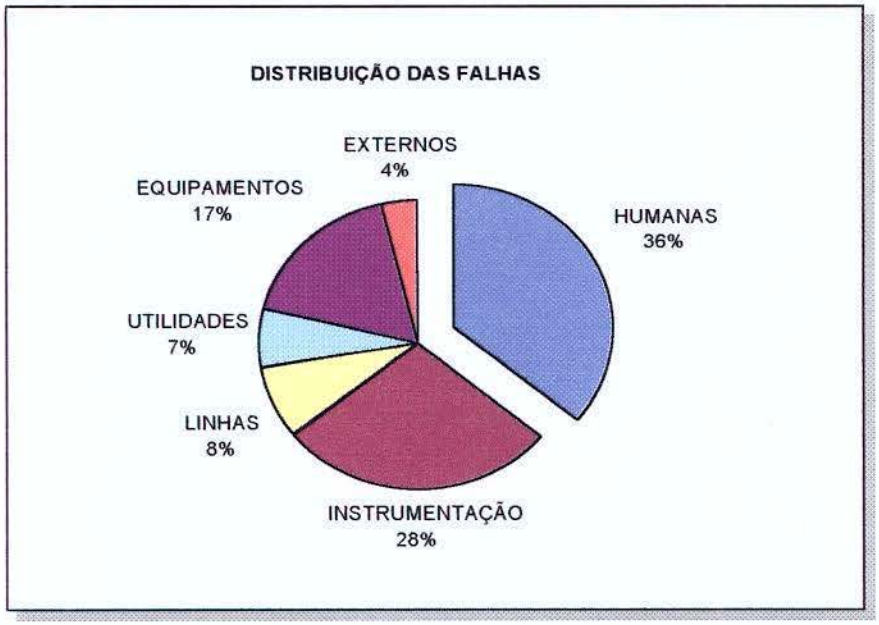


Figura 25(a). Distribuição das falhas por tipo

Foram considerados como falhas de equipamentos, por exemplo: a ruptura de aparelhos por corrosão; entupimentos; quebra de agitadores; quebra de internos de colunas de destilação; quebra de rotores ou acoplamentos de bombas com os motores; etc.

Foram consideradas falhas de instrumentos: válvulas de controle abrindo ou fechando indevidamente; falhas em indicadores e controladores de nível, pressão, vazão, temperatura; falhas em sistemas de segurança, como chaves de fluxo, chaves de nível; etc.

Entre as falhas de utilidades foram consideradas: falta de vapor; falta de energia elétrica localizada; falta de ar de instrumentação; falta de água de resfriamento; etc.

Foram consideradas falhas em linhas, por exemplo, o rompimento ou entupimento de tubulações ou acessórios, como filtros, purgadores, visores de fluxo, etc.

Como eventos externos, foram considerados: impurezas em matérias primas; fogo em unidades ou equipamentos vizinhos; radiação solar; falta geral de energia elétrica pela concessionária; falta de energia gerada internamente (cogeração). Tipos variados de falhas humanas foram identificadas em todos os estudos, em situações diversas, envolvendo momentos de operação normal e durante os transientes usuais, como partida, parada, testes, mudança de capacidade de produção, etc. Falhas de gerenciamento também foram identificadas.

Exemplos destas falhas são apresentados de forma resumida na lista a seguir:

Falha operacional durante a purga da fornalha das caldeiras. Purga não realizada.
Partida da caldeira é realizada com o "by pass" da válvula de óleo aberto.
Controlador de alimentação de óleo é deixado na posição manual.
Estoque de cumeno de segurança é deixado abaixo do nível mínimo recomendável.
Teste dos ventiladores das caldeiras com rotação acima do permitido.
Bloqueio indevido de válvulas de segurança, após manutenção.
Alinhamento indevido de um circuito de processo.
Falta de gás inerte por bloqueio indevido pelo operador.
Operador transfere óleo quente sobre óleo frio na estocagem.
Atraso na operação de limpeza do oleoduto da refinaria.
Erro na avaliação do volume dos reservatórios.
Erro na regulagem da descarga de bombas.
Na operação de partida o operador não liga o sistema de agitação.
Abertura indevida de drenos.
Não colocação do elemento filtrante nos filtros após manutenção.
Confinamento de produto entre válvulas.
Falha na interpretação da identificação na nota fiscal de entrada do produto.
Partida indevida de uma segunda bomba.
Aquecimento do sistema de óleo bloqueado.
Alinhamento de diesel para caldeira permanece após alimentação de óleo pesado.
Falta de aterramento durante a descarga de carretas.
Transmissor de pressão fechado após manutenção.
Estoque de segurança de gás inerte cai abaixo do normal.
Recebimento de resíduo fora de especificação.

Na Figura 25(b), pode ser observado o percentual de falhas humanas identificado em cada estudo HAZOP em particular. O número variou de 17 % à 63 %, com um valor médio de 36 %.

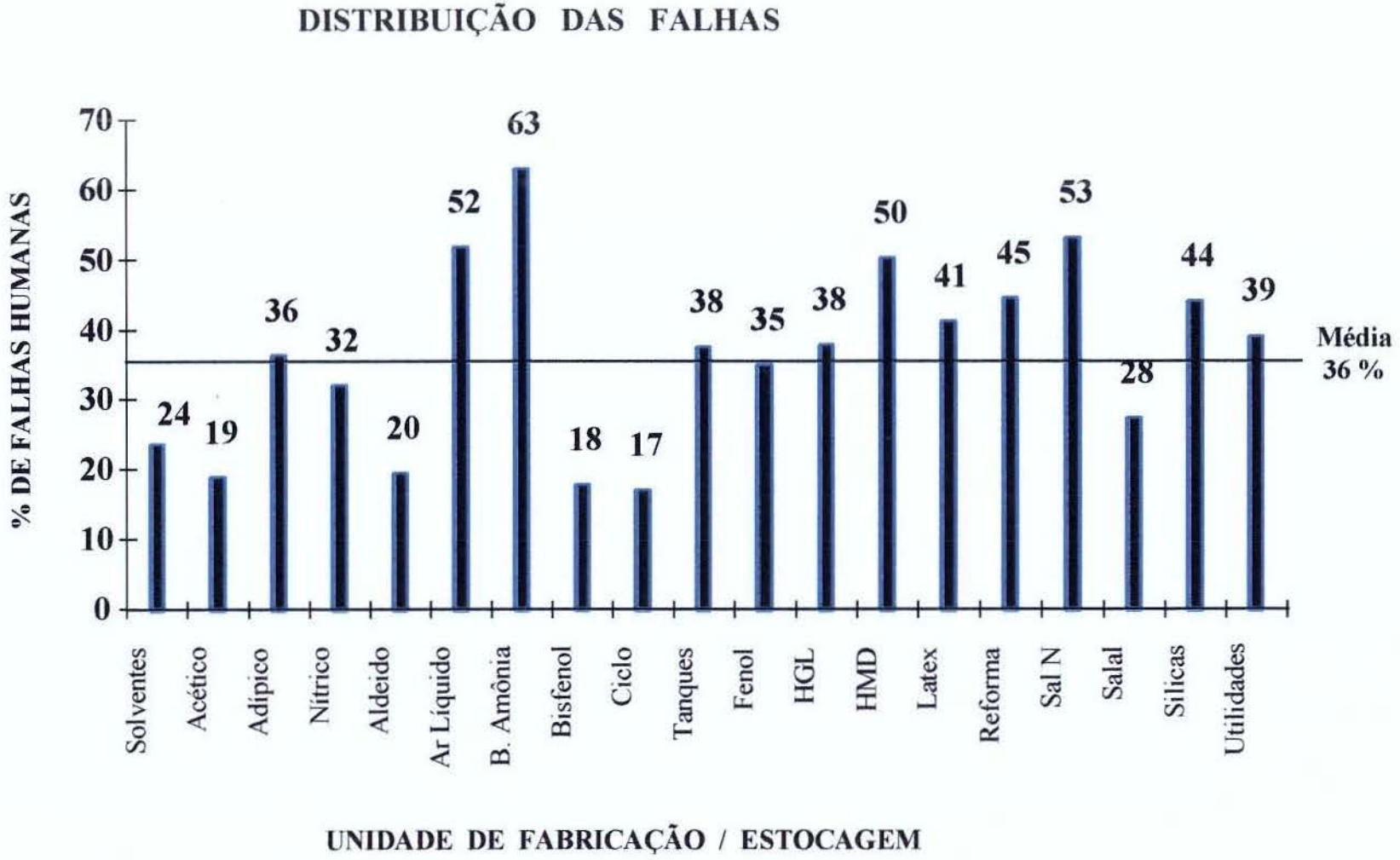


Figura 25 (b). Percentagem de falhas humanas identificadas em cada estudo HAZOP

O estudo HAZOP das utilidades identificou cerca de 38 % das 4234 falhas identificadas em todos os estudos realizados. Neste estudo em particular, uma análise sobre o perfil das falhas com potencial de gerar um cenário crítico (risco 1, conforme o conceito de aceitabilidade definido anteriormente), aparece na Figura 25 (c).

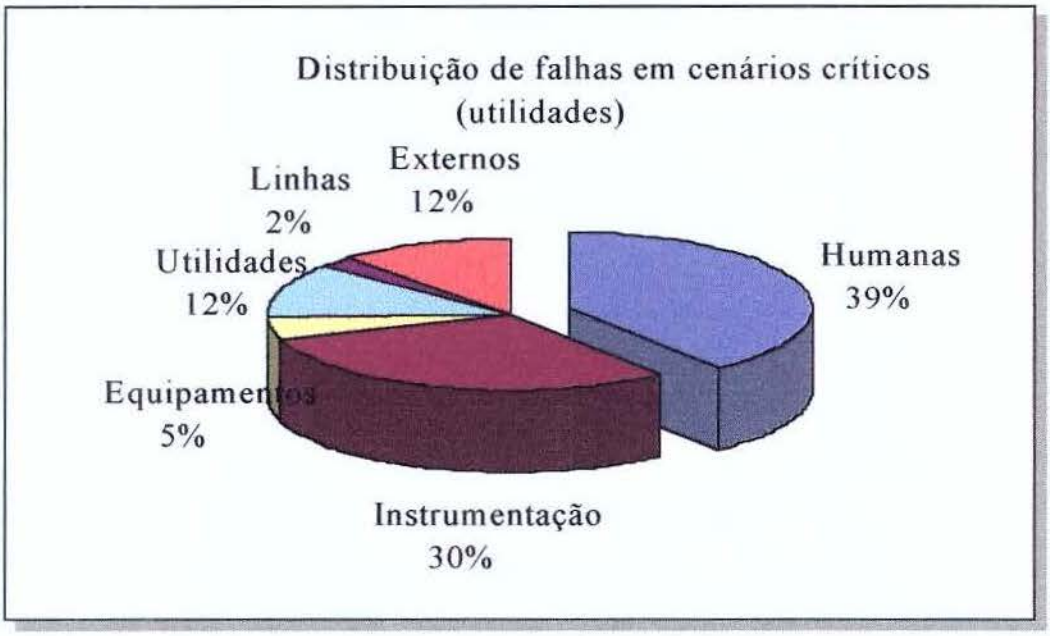


Figura 25 (c). Distribuição das falhas em cenários críticos, identificadas no HAZOP das utilidades

Como os circuitos analisados nos estudos listados acima foram maiores do que o normal numa relação de cerca de 3:1 aproximadamente (considerando o normal duas horas), o tempo despendido foi superior. Assim, um valor de seis horas para os nós, pode ser considerado normal, assumindo que o grupo tenha analisado cerca de três equipamentos principais, ou um principal e dois secundários, com todas as linhas de entrada e saída, durante a reunião.

A Figura 26 mostra a variação do tempo gasto e a comparação com o total de falhas identificadas.

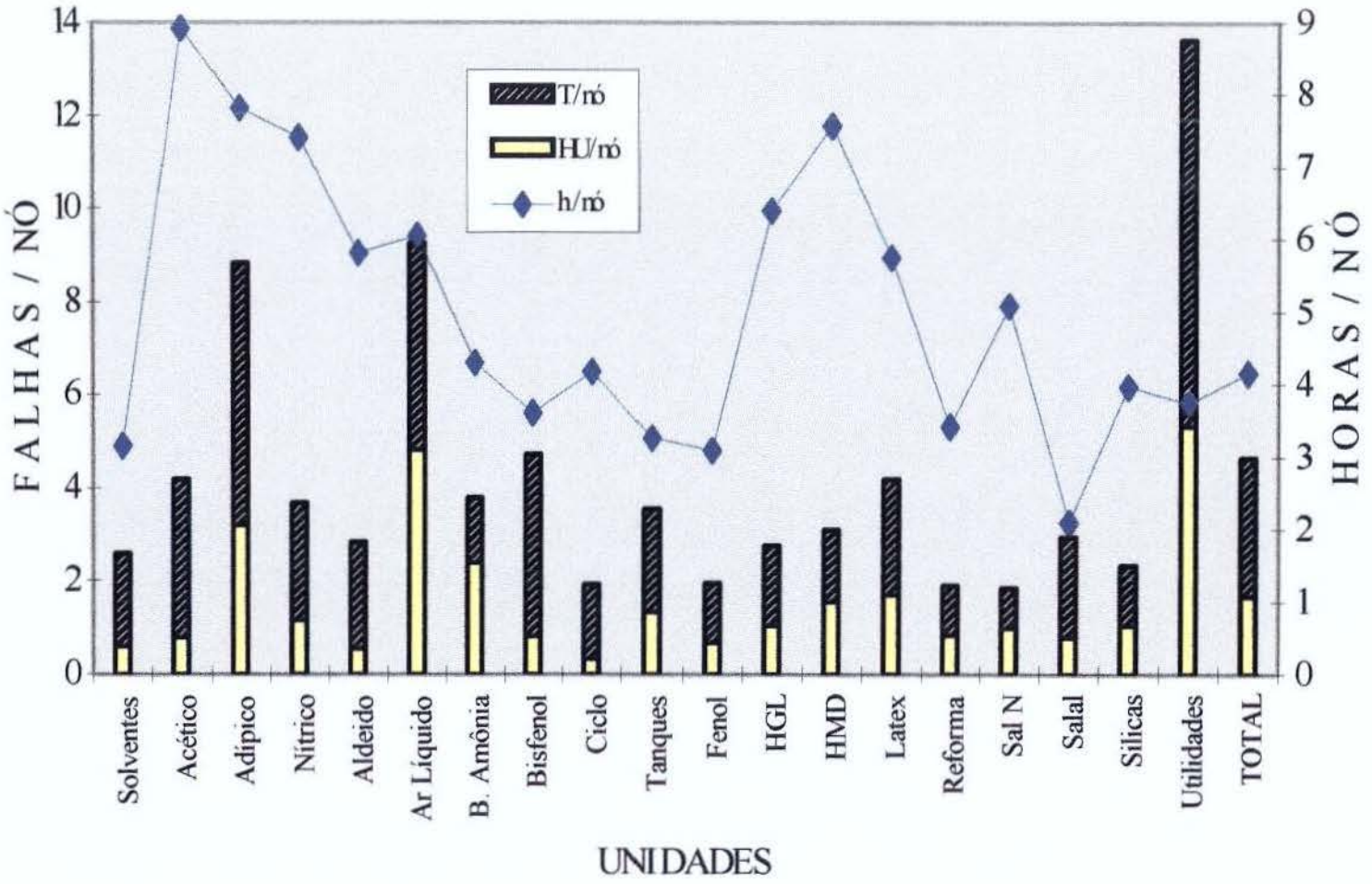


Figura 26. Comparação entre o tempo gasto e o número de falhas identificadas(Total e Humanas)

Alguns exemplos de cenários de falhas humanas, como identificados e descritos nas reuniões HAZOP, são apresentados nas planilhas a seguir através de exemplos reais, incluindo as recomendações propostas e outras informações que normalmente são listadas durante as reuniões.

Exemplo 1

Data: 13/02/96 PLANILHA HAZOP

Sistema: Tanque de estocagem e carreta de DAA
Intenção: Carga da carreta
Desenho: 1ZES 19892

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Falha no modo operatório	Operador não realiza o aterramento da carreta	Possível geração de faísca eletrostática, com provável ignição e explosão da carreta	Não há	Não há	Alterar sistema de aterramento, incluindo automatismo que impossibilite a descarga sem que a carreta esteja aterrada. Indicar com sinal luminoso o estado "aterrado".

Exemplo 2

Data: 15/03/94 PLANILHA HAZOP

Sistema: B-6 Tanque de estocagem final de MIBK
Intenção: 90 % máximo nível
Desenho: 1-ZE-S-19888

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Nível maior	Falha de informação com relação ao estoque. O tanque é carregado sem que haja volume disponível	O nível e a pressão sobem. Possível ruptura do tanque	Indicador de nível na sala de controle.	Teto com junta frágil. Válvula de alívio de pressão.	Alarme e segurança de nível alto. Chave de nível alto redundante

Exemplo 3

Data: 21/02/94 PLANILHA HAZOP

Sistema: Circuito de esgotamento lento - Fenol
Intenção: Esgotamento sob comando manual
Desenho: 3047730106

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Vazão maior	Operador abre o fundo dos oxidadores sem haver necessidade	Sobe o nível no tanque pulmão. Rompimento do disco de ruptura. Formação de nuvem inflamável. Risco de explosão	Identificação do bloqueio de fundo. Alarme de nível, temperatura e pressão alta no tanque pulmão.	Dique de contenção	Procedimento para resfriamento total da alimentação do tanque pulmão (permanente).

Exemplo 4

Data: 16/03/94 PLANILHA HAZOP

Sistema: Coluna de destilação E-4203
Intenção: Alinhamento do coletor de esgotamento
Desenho: 3430-APQ-242-002 folha 2/2

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Falha na parada	Operador falha na retirada do disco-cego do coletor de esgotamento das colunas	Possível lesão no operador devido projeção de produto. Local de difícil acesso.	Não há	Proteção individual normal (EPI)	Colocar dupla válvula em lugar de disco ou sistema CAN-SET. Usar roupa de proteção total.

Exemplo 5

Data: 14/03/96 PLANILHA HAZOP

Sistema: Zona 400 - R 2415
Intenção: Pulmão a 40 %
Desenho: 3192 55 0016

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Maior nível	Operador deixa bomba 0167 ligada durante transferência da estocagem	Transbordamento da guarda hidráulica 2407, no piso de 12 m. Vazamento de éter. Possível incêndio	LAH 4416 (60 %)	Não há	LSH desligando a bomba. Relocalizar a guarda hidráulica

A expressão HAZOP, como visto anteriormente, possui o significado de equilíbrio entre a segurança e a operabilidade (*HAZard and Operability*). Contudo, já na sua criação, Lawley [40] focava a questão da manutenção da função produtiva, analisando cenários que colocassem em risco a indisponibilidade da unidade de fabricação. Os números de falhas apresentados nos estudos desenvolvidos nas diversas unidades de processo listadas acima, referem-se quase que exclusivamente a eventos com conseqüências para a segurança, por um simples motivo: o foco do trabalho era indentificar os riscos maiores nas instalações. Entretanto, variadas vezes cenários com impactos diferentes de segurança foram avaliados, em função do interesse da equipe responsável pelo estudo. Desta forma, tornou-se evidente a aplicação da metodologia para outros eventos indesejáveis, como perda de produtividade ou perda da qualidade. Alguns cenários são apresentados a seguir:

Exemplo 6

Data: 14/03/96 PLANILHA HAZOP

Sistema: Preparação de solução amoniacal
Intenção: Tarefa : dosar glicerina

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Falha no procedimento	Operador não dosa a glicerina no vaso 1901	Afeta a qualidade do produto, causando empedramento. O produto sai fora de especificação	Controle de qualidade (teor de matéria não volátil). Produto não é enviado ao cliente	Não há	Melhorar o sistema atual de dosagem de glicerina. Revisar o procedimento se necessário

Exemplo 7

Data: 30/10/96 PLANILHA HAZOP

Sistema: Reação Sílicas
Intenção: Dosagem de Gel > tempo definido

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Tempo maior	Densidade das matérias primas fora de especificação (ácido / silicato)	Muda o tempo exato para o corte dos reagentes. Ácido é adicionado a mais devido instrução CLP. Perda de qualidade	Auto-Controle analítico. Totalizador de ácido	Redundância no controle de tempo de dosagem Ação do operador, para parar a adição de ácido	Informar o risco de perda de qualidade aos operadores

5.2 Resultados com o HAZOP ampliado

5.2.1 CASO 1

Para caracterizar as "expressões novas" registradas, que não são comuns nas reuniões tradicionais quando se aplica a metodologia, os textos estão escritos em "Itálico"

Data: 07/12/96 PLANILHA HAZOP

Sistema: Lavagem ácida de orgânicos
Intenção: 2500 kg/h
Desenho: IB-S-12992

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Vazão zero	Fechamento indevido do bloqueio na saída de orgânico. *Risco não conhecido ou falta de experiência do operador com eventos de alto estresse (parada de energia elétrica).*	Aumenta a pressão no vaso 492 acima da permitida (PMTP) Arraste de orgânico. Perda de eficiência na coluna E 303.	PI no campo. Amostragem da interface no 492 LI no vaso 501	Ação do operador para corrigir o desvio	Estudar um sistema de alívio. *Informar o risco à equipe. Definir a ação necessária em situação de emergência.*

Data: 07/12/96 PLANILHA HAZOP

Sistema: Lavagem ácida de orgânicos
Intenção: 2500 kg/h
Desenho: IB-S-12992

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Vazão zero	Fechamento indevido do bloqueio do medidor de vazão de água. *Identificação inadequada ou tarefa não familiar.* *Operação manual, quando deveria ser automática.*	Aumenta a pressão no vaso 492 acima da permitida (PMTP) Arraste de água ácida e corrosão no vaso 501	PI no campo. Amostragem da interface no 492	Ação do operador para corrigir o desvio	Estudar um sistema de alívio. *Melhorar a identificação do bloqueio no campo Reciclar o treinamento.* *Automatizar a tarefa.*

Data: 07/12/96 PLANILHA HAZOP

Sistema: Lavagem ácida de orgânicos
Intenção: Interface sem inversão
Desenho: IB-S-12992

Desvio	Causa	Conseqüência	Detecções	Proteções	Recomendações
Mudança de composição	Alinhamento errado dos leves para vaso 421. *Estereótipo do operador: operador antigo acostumado a esta operação*	Inversão e camadas com arraste de água para o vaso 501 e orgânico para o vaso 303. Envio de fenol para piscina cumênica.	Amostragem da interface no 492	Ação do operador para corrigir o desvio	Colocar disco cego na linha de leves. *Incluir o disco cego no procedimento de liberação do equipamento, para que não seja removido após manutenção.*

Para estudar o uso da "ampliação do HAZOP", um teste foi desenvolvido na unidade de produção de Fenol, no sistema de esgotamento do oxidador de cumeno R-104, mostrado na Figura 27. A escolha deste sistema se justifica pelo fato da operação de descarga do oxidador ser crítica, realizada em situações muito especiais, nas quais a melhor escolha para contornar problemas de degradação do produto dentro do equipamento, é o esgotamento para um local seguro. A degradação ocorre com uma exotermia muito rápida, acompanhada por aumento de pressão, que coloca em risco a unidade. O processo de descarga, uma vez tomada a decisão pela equipe, é realizado em conjunto pelos operadores de campo e os operadores da sala. Dois passos são importantes para o sucesso da tarefa:

- O resfriamento da corrente através do trocador de calor C 106, onde deve circular água fria. Já resfriado, o produto é enviado para o tanque F-107, que esta localizado em um dique de contenção, para prevenir eventuais transbordamentos. O tanque F-107 possui um disco de ruptura (DR) que, na ocorrência de um aumento de pressão, abre liberando o produto para o dique. Este evento não é desejável, pois forma uma nuvem de vapores inflamáveis no local, apesar de manter seguro o reservatório.

- Realizar o esgotamento em não mais de duas horas. Este tempo é importante, pois além deste período pode haver degradação no produto que ainda resta no oxidador.

As tarefas necessárias para o esgotamento do oxidador e definidas no manual de operação são as seguintes:

Tarefa 1 Abrir a circulação de água no trocador C 106
Tarefa 2 Alinhar o circuito de esgotamento para o F 107
Tarefa 3 Iniciar o esgotamento lentamente pela válvula HCV 125
Tarefa 4 Acompanhar a pressão no F 107 pelo PIAH
Tarefa 5 Manter a temperatura no F 107 em 70 °C
Tarefa 6 Esgotar em 2 horas

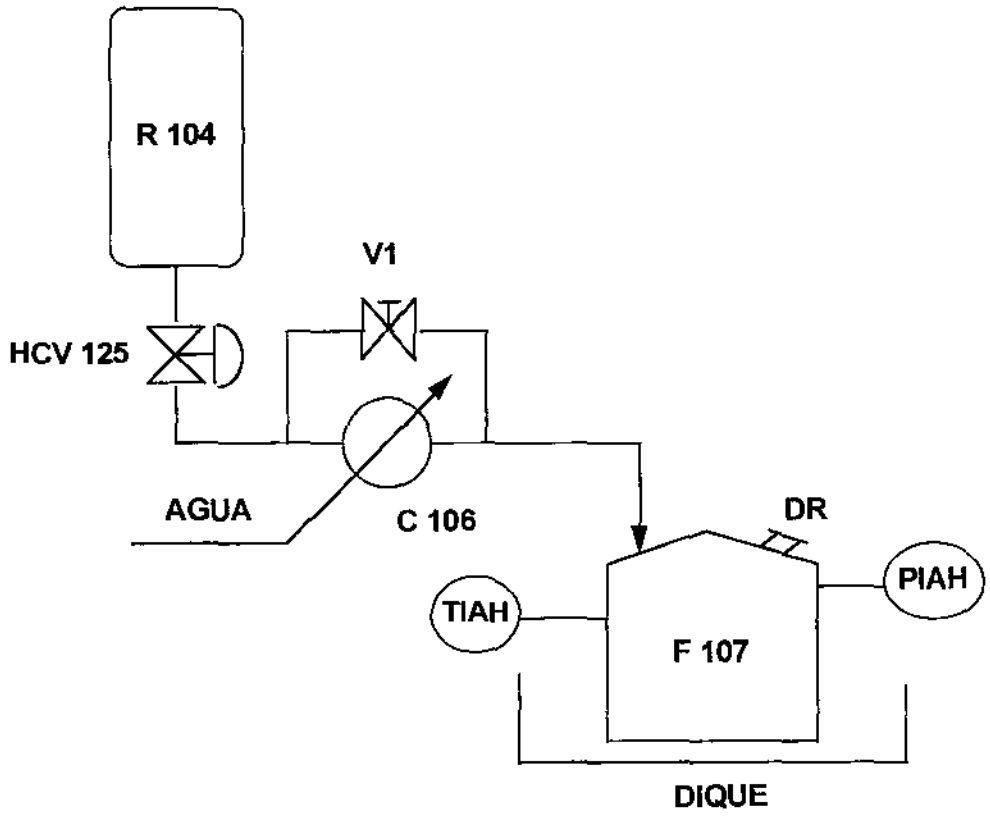


Figura 27. Fluxograma simplificado do sistema de esgotamento

Neste ensaio o método HAZOP foi alterado, para tratar não apenas de um transiente importante (parada de emergência), mas para avaliar as possíveis falhas humanas durante o procedimento de esvaziamento. Este teste mostra a extensão que foi possível alcançar em relação ao exemplo 6, mostrado anteriormente. Em substituição aos "nós" (ou circuitos) usados no HAZOP normal, foram usadas as tarefas, com sua definição resumida. A coluna proteção foi excluída para facilitar a apresentação, levando em conta que a única barreira existente é o dique de contenção. As planilhas geradas na reunião do grupo estão apresentados a seguir.

Data: 13/12/96 PLANILHA HAZOP

TAREFA 1 Abrir a circulação de água no trocador C 106
Intenção Resfriamento da corrente durante o esgotamento

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Ação não executada	*Falta de experiência DO OPERADOR DE CAMPO com eventos de alto estresse*	Temperatura alta no F 107. Risco de degradação no tanque de esgotamento	TIAH Treinamento com gestão individual para cada operador (plano de treinamento	*Radio para comunicação entre o operador da sala e o de campo*
	Há o treinamento, mas o evento nunca foi vivido	Idem	TIAH	*Rever intervalo para a reciclagem do treinamento*
	Instrução não recebida pelo operador de campo. Suporte de diagnóstico de falhas inadequado. Operador de sala não instrui para a tarefa	Idem	TIAH	*Troca de experiência com outras plantas. Treinamento da equipe para diagnóstico de falhas (simulador).*
	Instrução não recebida pelo operador devido falta de experiência DO OPERADOR DE SALA, com eventos de alto estresse	Idem		*Simulador Garantir que na sala de controle sempre existam alguns operadores com vivência em eventos críticos*
	Falha na aprendizagem de acidente já vivido	Idem		*Divulgar eventos já vividos*
	Nível da instrução insuficiente. Operador de campo não entende que deve ser aberta toda a válvula	Idem		*Treinamento para comunicação*

TAREFA 2 Alinhar o circuito de esgotamento para o F 107
Intenção Esgotamento para o tanque F 107

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Ação não executada. Operador não fecha o by pass do C106	*Esquecimento*	Esgotamento não passa pelo trocador. Sobe a temperatura no F 107	TIAH	*Reforçar treinamento com o "guia circuito" existente. Garantir comunicação do operador de sala com o de campo (rádio)*
	Tarefa executada com baixa freqüência	Idem	Idem	*Definir intervalo para a reciclagem do treinamento*

TAREFA 3 Iniciar o esgotamento lentamente pela válvula HCV 125
Intenção Descarregar sem elevar a pressão no F 107

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Ação muito lenta	*Tarefa executada com baixa freqüência*	Eleva pressão no F 107. Abertura do disco de ruptura em 3 minutos	PIAH	*Rádio para comunicação. Completar a instalação das válvulas automáticas para comando da vazão pela sala de controle*
	Falta de experiência do operador com eventos de alto estresse	Idem anterior		*Em cada turno devem existir operadores que tenham experiência com eventos críticos*

TAREFA 4 Acompanhar a pressão no F 107 pelo PIAH
Intenção Monitorar a pressão

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Check omitido	*Painel com informação excessiva. O operador que confirma o alarme não é do posto.*	Sobe a pressão e rompe o disco de ruptura		*Estudo de hierarquia de alarmes*
Informação errada (falha no PIAH)	Falha do instrumento	Idem		Instrumento deve ser testado a cada 6 meses

TAREFA 5 Manter a temperatura no F 107 em 70 °C
Intenção Prevenir risco de embalo no F 107

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Informação não é obtida pelo operador de campo	*Não há instrução do operador de sala para o operador de campo, que não esta havendo resfriamento*	Subida da temperatura no F 107 e possível degradação do produto	TIAH	*Indicar no manual de operação a necessidade de manter a vigilância sobre o sistema (indicação da temperatura durante todo o esgotamento).*

TAREFA 6 Esgotar em 2 horas
Intenção Tempo seguro para a descarga é de 2 horas

Desvio	Causa	Conseqüência	Prevenção	Recomendações
Ação muito lenta	*Risco não conhecido pelos operadores*	Degradação do produto pode ocorrer no oxidador		*Divulgar o risco para os operadores*
	Erro de projeto (cálculo)	Idem		*Revisar o cálculo do sistema*

5.2.2 Caso II

O caso descrito a seguir compreende uma análise da confiabilidade humana em uma unidade de reforma de nafta (denominada de Reforming II), destinada a produção de hidrogênio e dióxido de carbono. O hidrogênio é usado na cadeia de fabricação de Nylon (hidrogenação do fenol em cicloexanol; na de adiponitrila em hexametilenodiamina) e na cadeia acética (hidrogenação da acetona em metilisobutilcetona - MIBK). O CO_2 é usado na fabricação de bicarbonato de amônio e vendido à empresa Liquid Carbonic para uso como agente gaseificante.

O caso foi escolhido por mostrar a utilidade da técnica HAZOP, como fonte de dados para auxílio na quantificação de um cenário de risco identificado. As Figuras 28, 29, 30, mostram de forma simplificada os principais equipamentos da unidade.

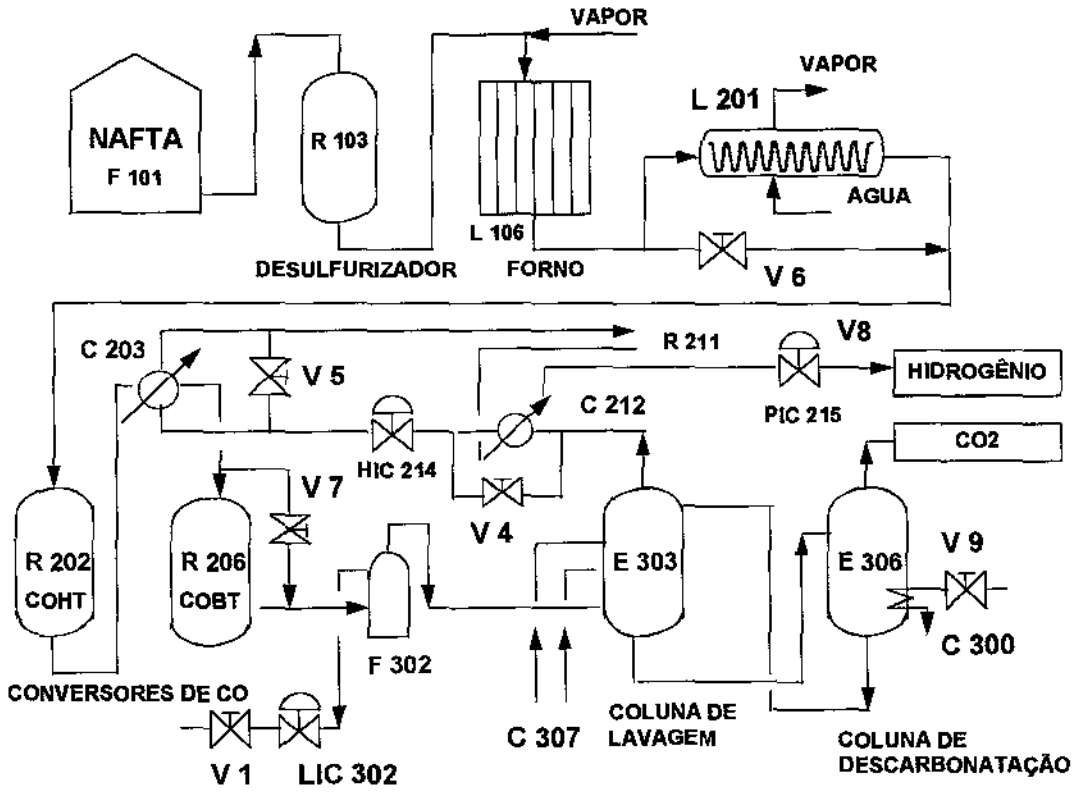
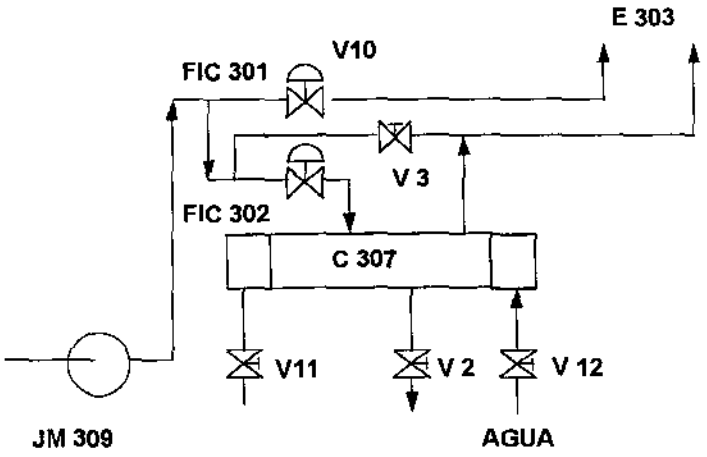


Figura 28. Fluxograma geral da unidade de Reforming

Em um processo contínuo Nafta (mistura de hidrocarbonetos parafínicos) estocada no reservatório F 101, é enviada para o dessulfurizador R 103 para a retirada de enxofre que vem como impureza com o produto recebido das refinarias de petróleo. O enxofre é considerado um veneno para os catalisadores, principalmente na etapa de metanização. Após a hidrodessulfurização, a nafta é enviada à 520 °C para o forno de reforma L 106 junto com vapor a alta pressão onde, à 990 °C, decompõe-se em 72,5 % hidrogênio (H_2), 7 % de monóxido de carbono (CO), 19 % de dióxido de carbono (CO_2) e 1,5 % de metano (CH_4). Os produtos, à pressão de 40 Kgf/cm^2 e à temperatura de 800 °C, trocam calor com água na caldeira L 201, para geração de vapor e economia de energia. Os gases então são enviados à 410 °C para os equipamentos R 202 e R 206, para a conversão de CO em CO_2., à alta temperatura (COHT) e à baixa temperatura (COBT), respectivamente. O teor de CO na saída do conversor de alta temperatura cai para 1,7 % e na saída do conversor de baixa temperatura cai para 0,3 %.

Com um teor baixo de CO, os gases passam em seguida pelas colunas de lavagem e descarbonatação, E 303 e E 306, respectivamente. Para a realização da descarbonatação na coluna E 306, vapor é introduzido na sua base, através do trocador de calor C 300. Neste ponto do sistema, o dióxido de carbono é separado do hidrogênio e enviado aos consumidores. Já na saída da coluna E 303 o teor de CO_2 é de 0,1 %. Uma purga é realizada no sistema para a retirada de água condensada, que é recuperada. A purga é enviada para o pote F-302, cujo nível é mantido sob controle pelo controlador LIC 302. A Figura 29 mostra o trocador de calor C 307, que é usado para resfriar a solução de Vetrocoke, usada nas colunas E 306 e E 303.



RESFRIADOR DA SOLUÇÃO DE VETROCOKE

Figura 29. Trocador de calor C 307 usado para resfriamento de Vetrocoke

Os gases, contendo hidrogênio como componente principal, são enviados à 300 °C para o equipamento denominado de Metanizador R 211, mostrado na Figura 30, para transformação do CO e CO_2 remanescente e metano.

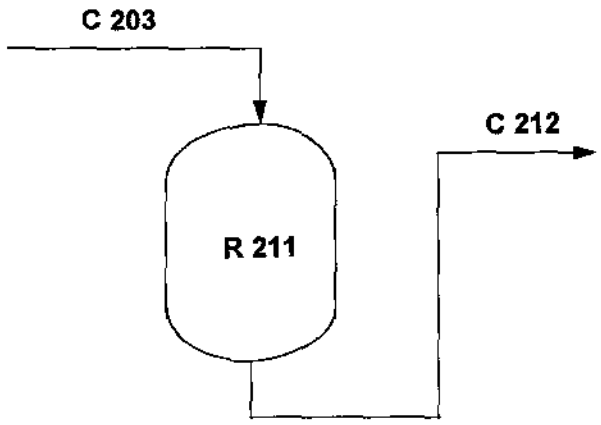


Figura 30. Metanizador da unidade de Reforming

Do metanizador, hidrogênio (97,9 %), metano (2,1 %) e traços de CO e CO_2 são enviados ao coletor de distribuição para outros consumidores. A pressão no coletor é regulada pela válvula V8 (PIC 215). Para aproveitamento de calor, o hidrogênio que sai do metanizador à 320 °C passa pelo trocador de calor C 212 existente entre os conversores de CO.

Perigo identificado no HAZOP

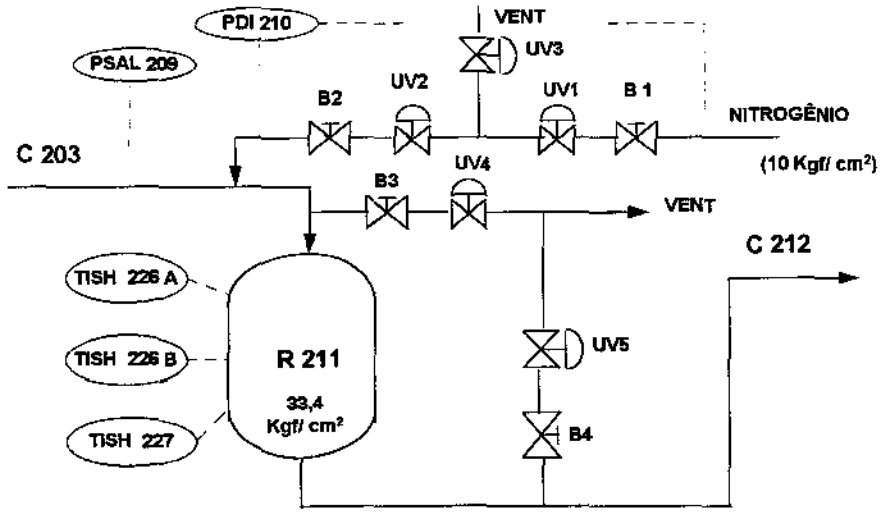
Durante o estudo HAZOP da unidade, foi identificado o perigo de envio de CO e CO_2 em quantidade elevada para o metanizador. Cada 1 % molar de CO eleva a temperatura do metanizador em 72 °C, e cada 1 % molar de CO2 eleva a temperatura do metanizador em 61 °C.

Este evento, vivido algumas vezes, torna a reação realizada no metanizador sem controle e com crescimento da temperatura de forma rápida, podendo atingir o limite de projeto do aparelho. Se este limite fosse ultrapassado, poderia haver a ruptura do equipamento, com emissão de hidrogênio para a atmosfera e conseqüente explosão.

Há ainda o agravante devido a presença de hidrogênio a alta temperatura sob o aço carbono, material de construção do equipamento.

Solução proposta

Como vários distúrbios no processo nas fases anteriores ao metanizador podiam ocasionar o desvio de temperatura alta, a solução encontrada inicialmente foi concentrar as melhorias necessárias no metanizador, com a instalação de um sistema de segurança voltado para diminuir as conseqüências do cenário de alta temperatura. A Figura 31 mostra o princípio de funcionamento deste sistema.



SISTEMA DE SEGURANÇA DO METANIZADOR

Figura 31. Sistema de segurança proposto para a redução do risco de ruptura do metanizador

Para detectar a temperatura alta, foram previstas 3 sondas de temperatura (TISH 226 A; TISH 226 B; TISH 227). Válvulas do tipo "on-off" (de fechamento rápido) foram previstas para isolar o sistema, quando da ocorrência de temperatura alta, e despressurizar o aparelho para a atmosfera em um local seguro.

Para diminuir o tempo da exposição a temperatura alta, um sistema de injeção de nitrogênio foi previsto, a fim de provocar o resfriamento dos gases durante a fase de despressurização. Como o coletor de nitrogênio opera com pressão inferior a do metanizador, o sistema de segurança foi projetado de tal forma que o nitrogênio apenas possa ser introduzido se três condições forem satisfeitas:

a) ocorrência de temperatura alta confirmada por pelo menos duas das três sondas (maior do que 400 °C);

b) diferença de pressão medida pelo transmissor de pressão diferencial PDI 210 abaixo do valor especificado (- 2 Kgf/cm²);

c) a indicação de pressão baixa através do transmissor PSAL 209 (menor que 6 Kgf/cm²).

Desta forma, foi previsto uma redundância de medição de pressão para não abrir indevidamente a entrada de nitrogênio. Este evento também é indesejável, pois caso ocorra, hidrogênio poderia retornar, e contaminar o coletor geral da fábrica usado como gás inerte.

A lógica de votação 2/3 (dois de três) escolhida para as sondas, foi proposta para não causar abertura indevida, caso alguma sonda atuasse de forma espúria (indicar temperatura alta sem que realmente o fato exista).

Esta decisão foi tomada para não comprometer a disponibilidade da unidade. Para garantir uma boa confiabilidade do sistema de segurança, válvulas de bloqueio (B1, B2, B3, B4) foram previstas para permitir testar o sistema periodicamente.

Árvore de falhas do sistema de segurança

A fim de avaliar a indisponibilidade do sistema de segurança, ou seja, a probabilidade do insucesso na detecção e ação para despressurização do metanizador durante um cenário de temperatura alta, uma árvore de falhas foi elaborada e quantificada.

O desenho dos eventos superiores da árvore, estão representados a seguir na Figura 32, com a probabilidade calculada para cada evento, os eventos intermediários e o evento topo: falha do sistema de bloqueio e despressurização.

As taxas de falhas foram extraídas das referências [36, 70-72].

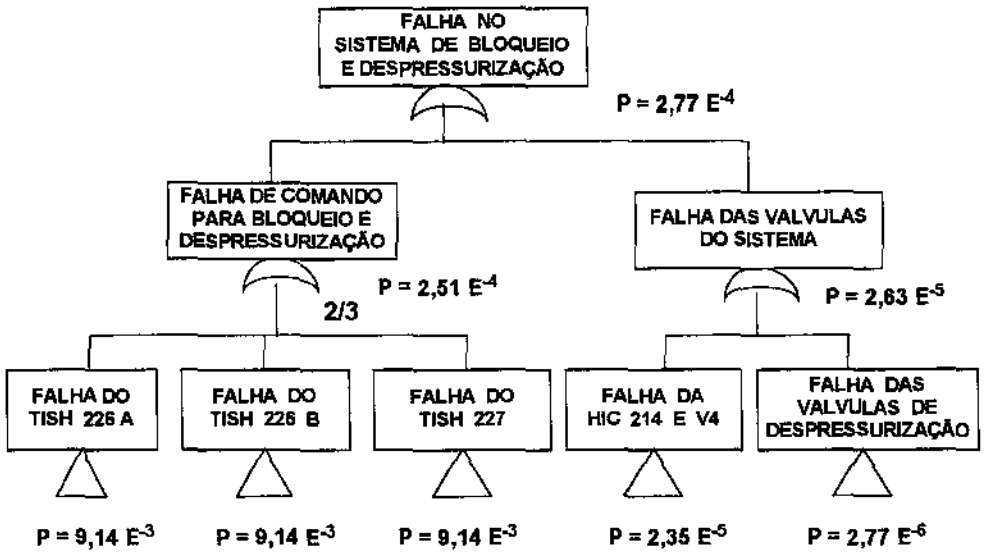


Figura 32. Representação resumida da árvore de falhas elaborada para o sistema de segurança proposto para o metanizador

O resultado mostra que a probabilidade do sistema de segurança estar indisponível, ou seja, estar em falha quando necessário atuar, é de 2,77 E^{-4}. Como o valor é relativamente pequeno, pode-se dizer que ele representa também a freqüência esperada para a falha do sistema de segurança. Assim, o inverso deste valor indica que, a proteção projetada, levaria o sistema a falhar a cada 3610 anos. Este valor poderia ser menor se, por exemplo, fosse adotada uma lógica 1/3 para o comando. Neste caso, qualquer sonda de temperatura, poderia a partir da detecção do desvio, acionar o sistema de segurança. Contudo, como explicado anteriormente, foi optado por uma lógica 2/3, necessitando assim a confirmação de pelo menos duas sondas. Este fato fez com que a probabilidade tenha sido aumentada de 3 vezes, em benefício de uma maior disponibilidade da instalação.

Contribuição da técnica HAZOP

Em um cenário de risco não é importante conhecer apenas a probabilidade de falha do sistema de segurança, mas também a freqüência esperada ou a probabilidade do evento indesejável. Em outras palavras, conhecer qual o número de vezes esperado em um intervalo de tempo, para o cenário ocorrer, ou a probabilidade neste mesmo período.

Desta forma, é importante conhecer a freqüência ou a probabilidade dos eventos iniciadores. Conhecendo-se este dado é possível, usando também a técnica da árvore de falhas,

calcular de forma completa a confiabilidade do sistema como um todo. A resposta a esta questão foi encontrada no HAZOP realizado na unidade de Reforming. No estudo efetuado, vários modos de falhas, principalmente de natureza humana, foram identificados como causadores do aumento da temperatura no metanizador, durante operação normal, na partida da unidade, ou na troca de marcha (mudança da capacidade de produção). Estas falhas estão listadas a seguir (ver como referência as Figuras 27, 28, 29).

a) Operador não alinha (não abre) na partida da lavagem, o registro manual do LIC 302 (V1).

b) Operador realiza, em partida ou em marcha normal, a abertura indevida do dreno do trocador C 307 (V2).

c) Operador realiza, durante a partida, a abertura indevida do *by pass* do trocador C 307 (V3).

d) O *by pass* do trocador C 212 é fechado indevidamente pelo operador, numa situação que deveria ficar aberto (V4).

e) O *by pass* do trocador C 203 é fechado indevidamente pelo operador, em partida, parada ou troca de marcha (V5).

f) O *by pass* da caldeira L 201 é fechado indevidamente pelo operador, em partida, parada ou troca de marcha (V6).

g) Na operação de partida, o by pass do R 206 (COBT) não é fechado pelo operador (V7).

h) Operador reduz indevidamente a pressão do sistema, atuando na válvula PIC 215 (V8).

i) Durante o aumento de marcha da unidade, operador não abre vapor para o C 300 (V9).

j) Durante o aumento de marcha da unidade, operador não aumenta a vazão da solução de Vetrocoke para a coluna E 303 (V10).

k) Durante a partida, o metanizador é colocado em marcha antes da estabilização da etapa de lavagem (E 303).

l) Durante a partida o operador não abre a água para o trocador C 307 (V11 e V12).

m) Durante a partida o operador deixa a temperatura dos conversores de CO abaixo do normal.

Para auxiliar na análise das falhas humanas listadas acima foram usadas as listas de apoio mostradas no Caso I. Os desvios, as falhas e os meios de detecção ou proteção (D/P) encontram-se mencionadas na Tabela XX mostrada a seguir. Outras falhas humanas possíveis, acrescidas devido ao novo sistema de segurança, foram analisadas no decorrer da construção da árvore de falhas mostrada anteriormente, e o valor encontrado para a probabilidade, já inclui estas contribuições. Foi omitida a coluna "conseqüência", para facilitar a apresentação, tendo em vista que o evento final é o mesmo: aumento de temperatura no metanizador. Contudo, esta coluna é sempre importante, pelo fato de nela ser registrado também o "caminho" do evento, com suas etapas intermediárias. Foi incluído neste caso, um código para cada erro, para ser usado posteriormente na revisão da árvore de falhas.

Não foi considerada a proteção já existente antes do estudo (uma sonda de temperatura com ação para o isolamento do sistema) pelo fato de não ser eficaz. Sabia-se que era atribuição do operador a tarefa de rapidamente despressurizar o sistema, e a prática havia mostrado que isto não ocorria com sucesso.

Tabela XX. Lista dos desvios e das causas identificadas no HAZOP ampliado para identificação de erros humanos

Desvio	Causas	D/P	Código
Operador não alinha (não abre), na partida da lavagem, o registro manual do LIC 302 (V1)	Tempo da tarefa é de 5 min. A tarefa não é familiar devido ao número de operadores novos e que ainda não "partiram" a unidade. A revisão dos manuais de operação é feita a cada 3 meses. O treinamento é realizado de forma teórica, baseado na experiência dos operadores mais antigos. Há falta de experiência com cenários já vividos a partir desta falha	LAH 311 (E 303) LAH 312 (F 302) PDI 303 (E 303) TAH do (R 211)	EH_NA__V1
Abertura indevida do dreno do trocador C 307 (V2) em partida ou marcha normal	O erro principal é de comissionamento. Pode ser efetuado por pessoas estranhas à unidade (pintores, por exemplo). Pode haver a falha também após a limpeza do trocador.	TR 311 LIC 301	EH_AI__V2
Abertura indevida do *by pass* do trocador C 307 (V3) na partida	Pode ocorrer após o processo de limpeza do trocador	TR 311	EH_AI__V3
O *by pass* do trocador C 212 é fechado indevidamente (V4)	O erro principal é de comissionamento. Pode ser efetuado por pessoas estranhas à unidade (pintores, por exemplo). Pode haver a falha também após a limpeza do trocador.	TR 229	EH_FI__V4

Desvio	Causas	D/P	Código
O *by pass* do trocador C 203 é fechado na partida, parada, ou troca de marcha, indevidamente (V5)	Processo de comunicação pode falhar. É cultura da equipe usar expressões do tipo " ajuste o by pass", sem explicitar "abrir mais" ou "fechar mais".	TIR 229 TIR 227 TI 228	EH_FI___V5
O *by pass* da caldeira L 201 é fechado na partida, parada, ou troca de marcha indevidamente (V6)	A válvula, ao contrário das demais, "abre no sentido horário" ao invés de "abrir no sentido anti-horário". Existem duas válvulas iguais, próximas, sem boa identificação.	Não há	EH_FI___V6
Na operação de partida, o by pass do R 206 não é fechado (V7)	O erro pode ocorrer devido a velocidade imposta nas tarefas da partida (pressão dos consumidores). O desvio é muito rápido (segundos) e não é possível ao operador agir. Não há indicação da posição da válvula na sala de controle.	Não há	EH_AI___V7
Operador reduz indevidamente a pressão do sistema, atuando na PIC 215 (V8)	Pode ocorrer quando o sistema fica indevidamente na posição manual. Durante a partida, hidrogênio é mal lavado na coluna E 303		EHPIC215V8
Durante o aumento de marcha da unidade, operador não abre vapor para o C 300 (V9)	Operador por não conhecer o risco, realiza a tarefa na seqüência errada: depois de aumentar a marcha da unidade. A tarefa tem uma freqüência elevada durante o ano.	PR na sala de controle	EH_VAPORV9
Durante o aumento de marcha da unidade, operador não aumenta a vazão da solução de Vetrocoke para a coluna E 303 (V10)	Operador por não conhecer o risco, realiza a tarefa na seqüência errada: depois de aumentar a marcha da unidade. A tarefa tem uma freqüência elevada durante o ano.	FR FIC	EHVAZAOV10
Durante a partida, o metanizador é colocado em marcha antes da estabilização da etapa de lavagem (E 303)	Pode haver pressa para atender os consumidores. Há falta de experiência com cenários já vividos a partir desta falha.	Não há	EH_LAVAGEM

Desvio	Causas	D/P	Código
Durante a partida o operador não abre a água para o trocador C 307 (V11 e V12)	O evento a partir desta falha ocorre em torno de ½ hora. Pode ocorrer devido ao número elevado de tarefas na partida e devido ao grau de treinamento da equipe.	Não há	EHNAV11V12
Durante a partida o operador deixa a temperatura dos conversores de CO abaixo do normal	Idem V11 e V12. Há falta de experiência com cenários já vividos a partir desta falha	Não há	EH_COBAIXO

Árvore de falhas incluindo os erros humanos

A árvore de falhas já elaborada, foi ampliada, incluindo as probabilidades dos erros humanos, listados anteriormente. A Tabela XXI a seguir mostra alguns dados adicionais que caracterizam melhor o cenário das falhas, os valores das probabilidades (P) encontrados na literatura [Ref. 33, pág 379], e os valores revisados, a partir de alguns fatores de influência (Pi).

Tabela XXI. Dados adicionais considerados na avaliação dos desvios ocasionados pelos erros humanos, para revisar as probabilidades de falhas usadas de forma genérica.

Erro humano	Dados adicionais	P	Pi
EH_NA____V1	Erro de omissão. Existe um alarme de nível alto no F 302, mas em 5 min a temperatura sobe e o operador deve corrigir no campo a falha. Existe uma segurança de nível alto no F 302, mas fica inativa (após a V1) e um LSH na E 303, que fica em *by pass* na partida.	0,0003	0,0018
EH_AI____V2	Erro de comissionamento. Por exemplo um pintor que executa trabalhos no local	0,001	0,001
EH_AI____V3	O evento pode ocorrer quando a unidade esta em marcha máxima. Neste caso, a falha é deixar na posição errada após uma limpeza.	0,01	0,0612
EH_FI____V4	Erro de comissionamento ao fechar indevidamente. Normalmente o by pass esta aberto e precisa ficar aberto quando os conversores de CO estão com baixa eficiência.	0,01	0,0612

Erro Humano	Dados adicionais	P	Pi
EH_FI____V6	Executa mal a tarefa devido erro de identificação	0,003	0,0184
EH_AI____V7	Erro de omissão, sem possibilidade de recuperação devido a velocidade do evento.	0,01	0,0612
EHPIC215V8	Executa mal a tarefa. Erro considerado remoto.	0,0001	0,0001
EH_VAPORV9	O operador altera a seqüência "de forma consciente" . Não há detecção direta deste desvio, considerando que o PR não é eficaz	0,003	0,0184
EHVAZAOV10	Erro de omissão	0,01	0,0612
EH_LAVAGEM	Erro ao realizar a tarefa, devido a pressa para cumpri-la	0,003	0,0184
EHNAV11V12	Erro de omissão. Há apenas um TR após o trocador de calor	0,01	0,0612
EH_COBAIXO	Erro ao realizar a tarefa, devido à pressa para cumpri-la	0,003	0,0184

Os fatores de influência (Pi) mencionados na Tabela XXI, referem-se às duas condições para a produção dos erros (*EPC - Error-production conditions*) que foram considerados no cálculo, sugeridos por Kirwan [Ref 33, pág 239], quando o autor apresenta a técnica HEART - *Human error assessment and reduction technique* :

a) pelo fato de haver relativa falta de experiência dos novos operadores, principalmente em momentos de partida, os valores foram multiplicados por 2,8,

b) pelo fato dos novos operadores e, em parte também os antigos, mostrarem ausência do conhecimento dos riscos avaliados, não percebendo as conseqüências dos erros, os valores foram multiplicados por 3,4.

Apenas os eventos relativos as válvulas V2 e V8 não sofreram o decréscimo de confiabilidade. Normalmente pessoas estranhas (pintores) não são influenciados pelos fatores mencionados e, além disto, o operador da sala de controle foi considerado no estudo como tendo

experiência, e conhecimento razoável dos riscos. Dois cálculos foram realizados com a árvore de falhas ampliada. A primeira estimativa foi feita usando-se os valores das probabilidades listados na coluna "P". Neste caso, a probabilidade do conjunto das falhas humanas (combinação dos erros) é de 6,64 E^{-2}.

Quando este valor é colocado na árvore, junto com a probabilidade do sistema de segurança estar indisponível, a probabilidade do evento indesejável ocorrer é de 1,76 E^{-5}. Ou, expressando a probabilidade como uma freqüência, pode-se esperar que o evento ocorra a cada 56800 anos.

Este valor é baixo e poderia ser aceito, considerando-se que para este tipo de cenário, uma chance em 56800 é satisfatória. Contudo, duas questões podem ser colocadas: a) uma ruptura deste aparelho poderia causar sérios danos à instalação e um longo tempo de parada, além de colocar pessoas em perigo devido à onda de choque de uma explosão e ainda aos efeitos térmicos de um incêndio; b) as falhas de natureza humana podem estar sub-avaliadas e não refletirem a realidade da equipe. Uma segunda estimativa foi feita, usando-se os valores das probabilidades listados na coluna "Pi". Para esta situação, a combinação das falhas humanas representa uma probabilidade de 4,01 E^{-1}, ou seja de 40 % em um ano, conforme mostrado na Figura 33.

O evento topo nestas circunstâncias passa a ter uma probabilidade de 1.10 E^{-4}, ou uma ocorrência esperada a cada 9000 anos, conforme mostrado na Figura 34. Este valor não pode ser aceito para um sistema global, que compreenda os eventos iniciadores e a falha do sistema de segurança. Desta forma, recomendações adicionais foram feitas, para diminuir a probabilidade das falhas humanas e do sistema de segurança permanecer indisponível.

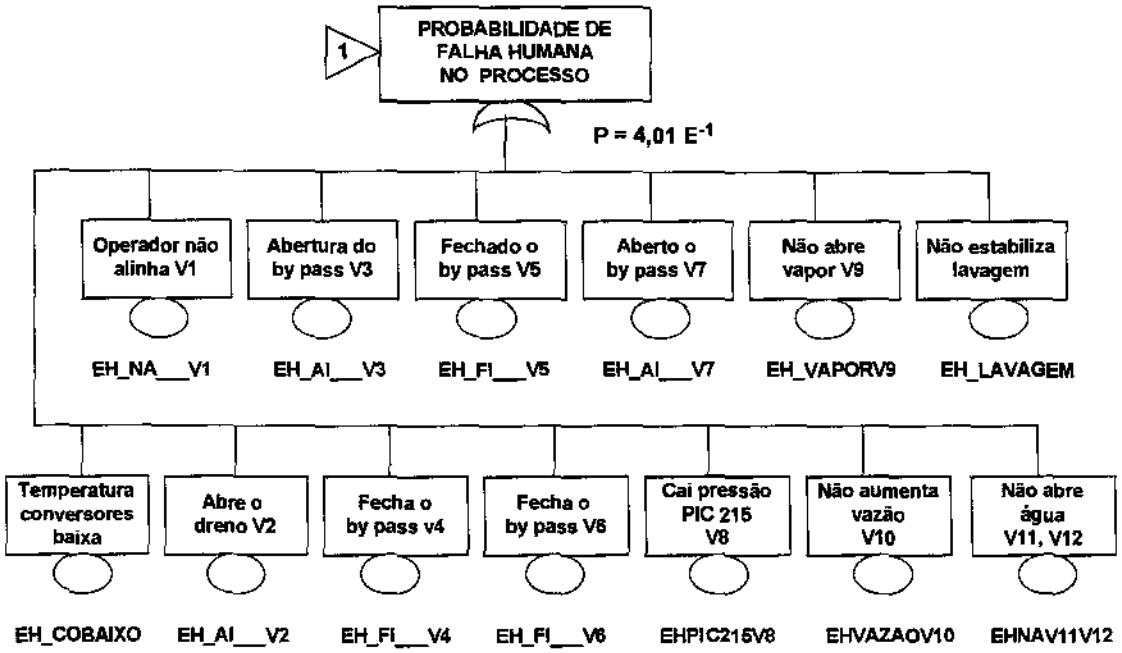


Figura 33. Representação da árvore de falhas dos erros humanos possíveis

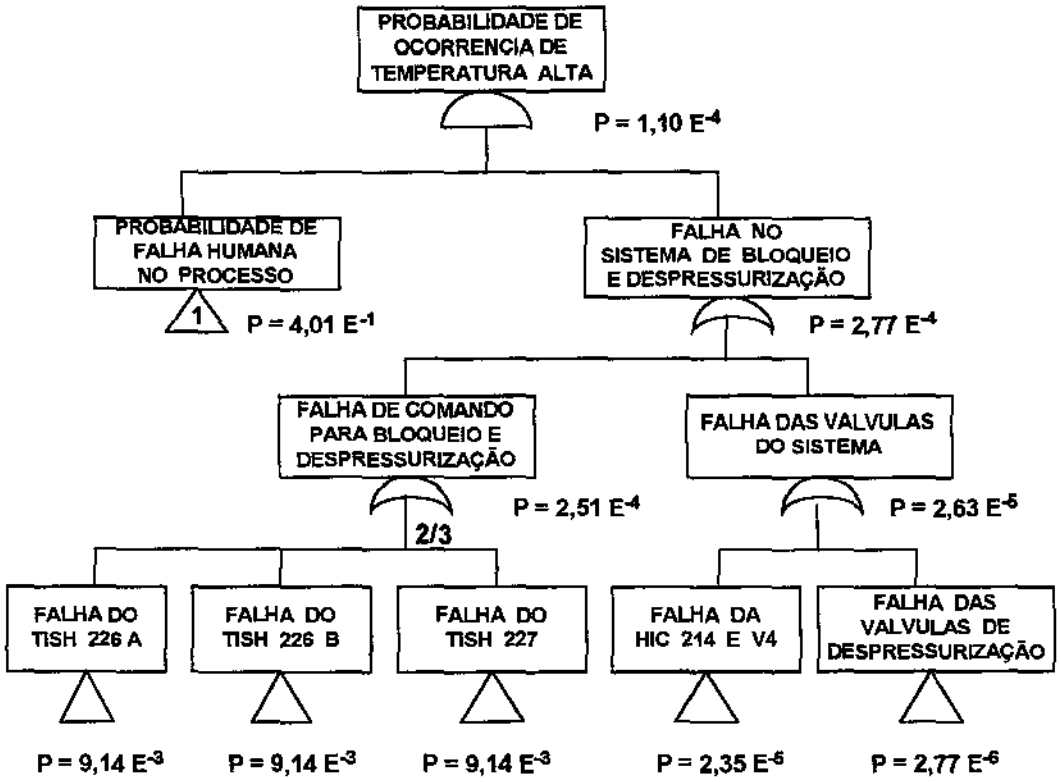


Figura 34. Representação resumida da árvore de falhas de todo o sistema, incluindo os erros humanos

As Recomendações propostas após a análise das falhas humanas estão listadas na Tabela XXII, mostrada a seguir.

Tabela XXII. Lista das recomendações sugeridas a partir da análise dos erros humanos possíveis, tanto como evento iniciador, como para criar indisponibilidade no sistema de segurança

Desvio	Recomendações
EH_NA____V1	Eliminar manobra neste bloqueio. Melhorar a vedação no LIC 302. Testar o LAH 312 periodicamente. Partir a lavagem com as seguranças do metanizador e da coluna E 303 alinhadas. Montar programa de treinamento para próxima parada.
EH_AI____V2	Colocar raquete ou "figura 8" no dreno. Colocar alerta no "check list" após limpeza.
EH_AI____V3	Colocar alarme de temperatura alta.
EH_FI____V4	Colocar alerta no volante da V4.
EH_FI____V5	Instalar um TRC no *by pass*. Treinamento em comunicação.
EH_FI____V6	Colocar TAL na saída do R 202. Identificar as válvulas e o sentido de abertura.
EH_AI____V7	Colocar um fim-de-curso para não abrir a HIC 214. Alertar o risco no manual de operação. Treinamento antes da próxima partida.
EHPIC215V8	Colocar um PAL independente. Prevenir quanto ao risco no manual de operação.
EH_VAPORV9	Instalar um FR. Alertar operadores quanto ao risco.
EHVAZAOV10	Alertar no sistema especialista existente.
EH_LAVAGEM	Alertar quanto ao risco antes da próxima partida. Definir tempo para cada tarefa. Fazer análise das tarefas.

Desvio	Recomendações
EHNAV11V12	Colocar um TAH na saída do C 307.
EH_COBAIXO	Colocar um TAL. Prevenir quanto ao risco antes da próxima partida.
Falhas devido ao novo sistema. Após testar, o sistema fica indisponível	Reciclar processo de liberação e recepção dos serviços.
Não testar o sistema novo	Definido teste a cada três meses. Colocar a tarefa no sistema de gestão da manutenção.
Erro ao testar o sistema novo	Não testar todo o sistema no mesmo dia, para diminuir a possibilidade das falhas de modo comum (FMC). Elaborar procedimento escrito para o teste.

Para tornar o sistema confiável, as ações após implementadas, serão incluídas no plano de auditoria do ISRS (International Safety Rate System).

6. Discussão dos resultados

6.1 Uso do HAZOP convencional

Com o HAZOP realizado utilizando-se as palavras guias e desvios tradicionais, foi possível identificar um número grande de falhas humanas em todas as unidades. Nos exemplos das planilhas geradas nas reuniões, apresentado no capítulo 5, pode-se observar que falhas humanas foram identificadas não só através do desvio *modo operatório* (exemplo 1), mas também com outros desvios, como: *nível maior; vazão maior; e falha na parada* (exemplos 2, 3 e 4 respectivamente). Isto ocorreu com a totalidade dos desvios incluídos no roteiro fornecido para as equipes.

No exemplo 7, usando-se o desvio *tempo maior*, foi descoberto um potencial de falha cujo evento indesejável não era a segurança, mas a perda de qualidade. Centenas de casos ocorreram semelhantes a este exemplo, mostrando que a metodologia realmente possui uma eficácia elevada para a identificação de outros tipos de cenários, envolvendo a operabilidade do processo. No caso particular do exemplo 7, o grupo decidiu registrar todo o cenário, o que não ocorreu na maioria das ocasiões, onde apenas foi caracterizado uma perda de produção, sem conseqüências para a segurança. Na maioria das instalações o número de erros humanos superou os demais modos de falhas (instrumentação, equipamentos, linhas, eventos externos, utilidades). Quatro unidades atingiram um percentual acima de 50 %, destacando-se entre as demais. As razões podem ser explicadas pelos seguintes aspectos:

As unidades Ar Líquido (52 %), Bicarbonato de Amônia (63 %), HMD (50 %) e Sal Nylon (53 %), são instalações que operam com processos descontínuos, com várias operações de preparação de reagentes e inúmeros transitórios (aquecimento, resfriamento, transferências, amostragens, purgas, lavagens, etc.). Além disto, todas estas plantas possuem um nível de automação reduzido em relação às demais, com muitas tarefas realizadas por operadores de "campo". As salas de controle possuem instrumentos de indicação, alarme e registros, mas poucos controladores. Nas maiores unidades existentes (Fenol e Ácido Adípico), bem como na que gerou o maior número de circuitos (Utilidades), foram identificados valores próximos da média (36 %). Estas três instalações possuem elevado grau de automatismo, justificando desta forma a identificação elevada de falhas de instrumentação. A Figura 35 mostrada a seguir apresenta os dados das unidades Adípico, Fenol, Ar Líquido e Bicarbonato de Amônia. Pode-se perceber a sensível diferença entre as duas primeiras e as duas últimas.

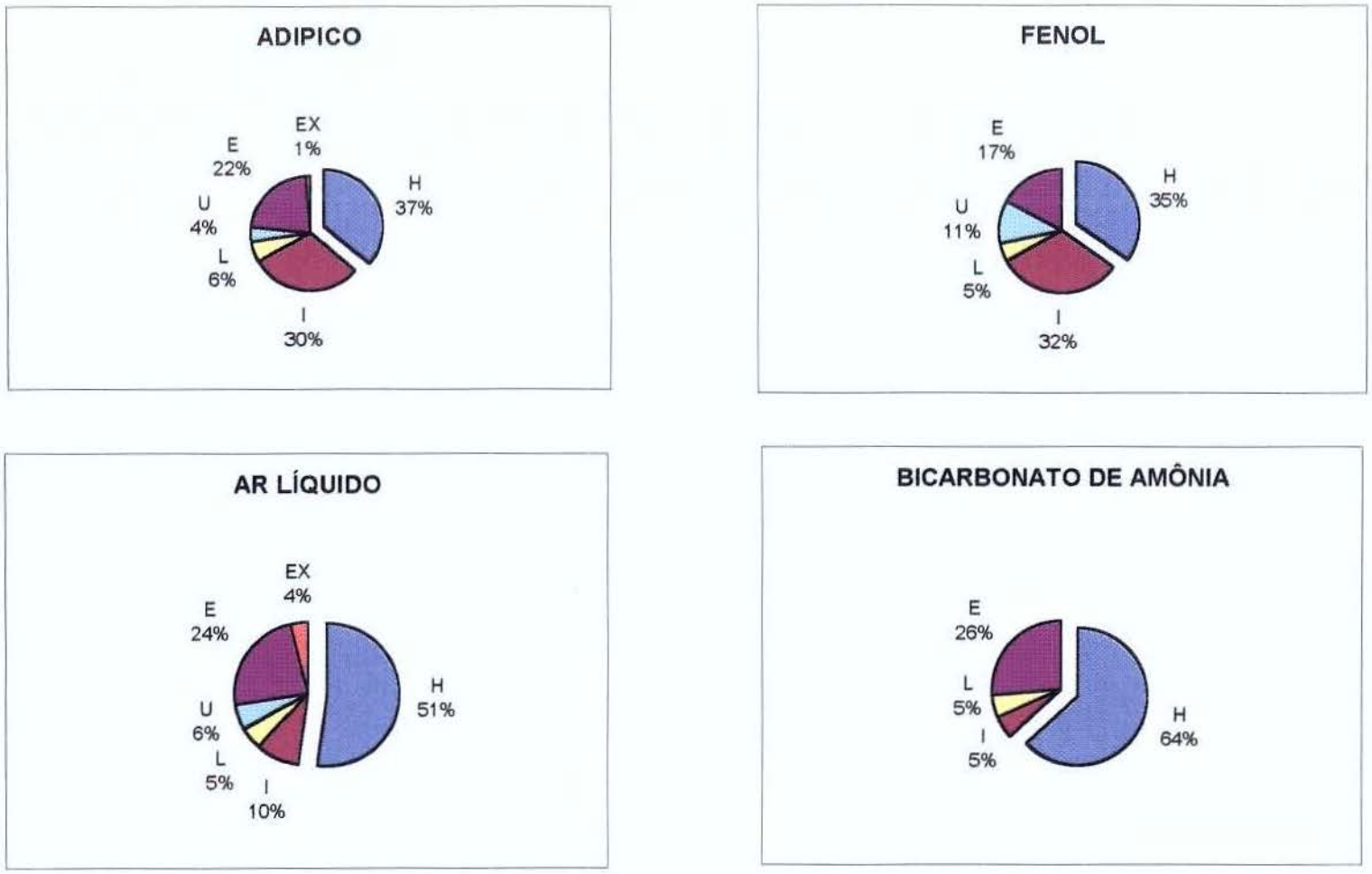


Figura 35. Distribuição das falhas nas unidades Ácido Adípico, Fenol, Ar Líquido e Bicarbonato de Amônia. (H = Humanas; I = Instrumentação; L = Linhas; U = Utilidades; E = Equipamentos; EX = Externos).

O objetivo principal dos estudos foi a determinação dos riscos maiores nas unidades. Na Figura 25(c) mostrada anteriormente para o caso específico das Utilidades, pode-se ver que cerca de 39 % das falhas que podem gerar riscos graves, são devidas a erros humanos. Ainda no caso desta instalação, o valor elevado de falhas encontradas em relação as demais, deve-se ao fato de que: a) foram considerados eventos indesejáveis qualquer perda de disponibilidade, para não afetar as unidades de produção; b) o grupo de análise trabalhou as causas aproximando-se de uma FMEA, incluindo modos de falhas que normalmente as equipes não estudam como, por exemplo, as falhas de elementos dentro de uma malha de controle. A decisão de considerar a operabilidade como aspecto importante neste estudo, foi tomada na etapa de planejamento do trabalho.

6.2 Uso do HAZOP ampliado

Nos exemplos mostrados no Caso I, a inclusão de fatores influenciadores de desempenho permitiram clarear melhor os possíveis cenários de falhas e, com isto, melhorar a qualidade das recomendações. Expressões como " falta de experiência com eventos de alto estresse" não foram encontradas nas análises desenvolvidas anteriormente à ampliação do HAZOP. Nunca o estereótipo do operador ou problemas de comunicação, por exemplo, haviam sido questionados ou, pelo menos, formalmente caracterizados como desvios possíveis.

A ampliação e flexibilização do HAZOP, como mostrado na Figura 27, permitiu a análise mais detalhada de uma série importante de tarefas realizadas nos principais equipamentos da unidade Fenol: os oxidadores. Pela primeira vez, foi incluída uma recomendação que trata a organização da equipe, de tal forma a orientar o plano de treinamento e a mínima experiência necessária para os operadores da sala de controle.

A partir da experiência com o HAZOP ampliado, uma lista nova foi adicionada ao roteiro básico, usado para a identificação das falhas durante as reuniões de trabalho.

6.3 Uso do HAZOP com a árvore de falhas

No exemplo do Caso II, um sensível aumento da qualidade da análise foi obtido. A árvore de falhas inicialmente construída havia sido feita com foco apenas na confiabilidade do sistema de segurança, sem levar em conta, em detalhe, os eventos iniciadores. A pesquisa das planilhas HAZOP preenchidas durante as reuniões, revelou um importante número de falhas de natureza humana, que não seriam levadas em consideração com a devida atenção.

O detalhamento das condições das falhas foi realizado por entrevistas com os operadores, o que permitiu conhecer melhor o ambiente envolvendo os diversos cenários. Este método, mencionado no item 3.1, qualificou melhor o estudo do risco, e integrou várias técnicas de análise. A partir deste estudo, foi montado um plano para levantamento de dados reais de falhas, com o propósito de verificar a real possibilidade de ocorrência de cada erro. O objetivo era de verificar também o possível engajamento das pessoas, no registro de falhas operacionais, normalmente difíceis de serem mencionadas. Em dezembro de 1996 a válvula V9, mostrada na Figura 28 como um dos possíveis pontos de erro, não foi aberta como deveria, e a temperatura do equipamento subiu, sendo controlada pela equipe da sala de controle, antes do sistema de segurança atuar. O valor da probabilidade usado no cálculo (0,0184) parece ser mais coerente que o previsto sem considerar algumas penalizações (0,003). O próprio sistema de medição instalado, serviu como forma de informar e alertar os operadores quanto aos desvios. O engajamento das equipes superou as expectativas.

6.4 Considerações gerais

A eficácia da técnica HAZOP, semelhante a das demais, está muito relacionada com o tempo requerido para as análises, com os recursos que são alocados, e com o perfil da liderança e da equipe. Os grupos que analisaram as unidades Bisfenol e Cicloexanol identificaram um número baixo de falhas humanas (18 % e 17 %, respectivamente) em virtude da decisão de estudar as falhas do modo operatório separadamente, não incluindo-as na primeira avaliação.

Várias experiências foram feitas no decorrer dos estudos, com relação a conveniência de analisar os riscos no momento da definição do cenário, na própria reunião HAZOP. A análise do risco no momento da reunião facilita na medida em que o assunto está sendo detalhado no instante da reunião e, normalmente, operadores participam nestas ocasiões com contribuições fundamentais para o esclarecimento do "ambiente" do evento imaginado. Ainda, a análise imediata do cenário, permite maior rapidez no início das ações necessárias.

Por outro lado, a análise do risco neste momento prejudica a velocidade do trabalho de identificação dos perigos. Ainda, muitas vezes as pessoas que podem ajudar na análise da probabilidade (confiabilidade dos dispositivos existentes) e na gravidade do evento (alcance do impacto), não estão presentes. Muitos especialistas são de opinião que os dois momentos devem ser separados.

As duas maneiras foram usadas, ocasionando uma grande variabilidade no número de horas gastas para cada circuito (nó). Isto pode ser observado nos valores da Tabela XIX. O tempo mínimo foi de 2,1 horas/nó (Salal), o valor médio foi de 4,2 horas/nó, e o valor máximo foi de 8,9 horas/nó. Estes valores foram estimados admitindo-se 5 pessoas em média participando de cada reunião. Esta questão foi deixada a cargo de cada equipe decidir como fazer. Em programas de longa duração, como o desenvolvido neste trabalho, é conveniente que as pessoas percebam as vantagens e desvantagens de cada maneira de trabalhar e, sem perder o espírito da técnica, decidam como fazer.

Considerando os estudos que despenderam acima de 6 horas por circuito ou que apresentaram um número menor de falhas identificadas, os grandes desvios mostrados na Figura 26 (representado pela distância entre as barras e a linha), podem ser explicados pelos seguintes fatos:

- durante o estudo da unidade de Ácido Acético foram analisadas modificações da tecnologia do processo, que seriam introduzidas em breve, com muitas questões sendo discutidas longamente durante as reuniões;
- no estudo da unidade de Ácido Adípico, as pessoas foram formadas durante a própria realização do trabalho, ocasionando uma redução sensível da velocidade;
- os estudos das unidade de Ácido Nítrico e HMD foram os primeiros a serem feitos, e as equipes, apesar da formação prévia recebida, determinaram uma velocidade menor. Ainda, os dois processos apresentam perigos relevantes (manuseio de hidrogênio e reações com catalisadores) que mereceram atenção especial;
- em vários estudos, a análise dos riscos foi realizada durante as reuniões, determinando um longo tempo para o processo de identificação;
- na revisão das unidades Salal, Ciclo, HGL, e Bisfenol, os índices foram mais baixos do que a média, pelo fato de que as equipes consideraram apenas a operação em marcha normal, sem levar em conta os períodos de partida e parada;
- na revisão das unidades Fenol e Reforma, o tamanho dos circuitos foram menores que a média, levando a um número reduzido de falhas por nó;
- na unidade Sal N, o número de componentes é muito pequeno, em relação às demais instalações.

Em nenhum momento, vale ressaltar, foi procurado um determinado tipo de desvio ou causa. O resultado das análises refletiram o que a metodologia é capaz de proporcionar.

Um fator que influenciou o desempenho dos trabalhos, foi o nível de qualidade dos documentos. Nas unidades já certificadas no sistema ISO 9000, a organização e precisão dos documentos era sensivelmente maior, facilitando muito os estudos. Em alguns casos, foi decidido começar o estudo HAZOP, somente após a documentação ter sido colocada em conformidade e controlada, conforme a norma ISO.

O principal fator de sucesso dos estudos, foi sem dúvida a postura e determinação da liderança principal da empresa. Os estudos HAZOP tornaram-se parte integrante do gerenciamento dos riscos industriais e, as ações sugeridas, agrupadas conforme as prioridades, passaram a ser estudadas e implantadas nas unidades de fabricação. O planejamento realizado anualmente, integrando todas as funções produtivas, passou a incorporar o processo HAZOP.

6.5 Erros humanos na aplicação da técnica

A metodologia HAZOP foi criada para identificar perigos, como ponto de partida para a análise dos riscos associados a estes perigos. Contudo, a realização da técnica é feita por pessoas, que também erram de diversas formas e por variadas causas. A seguir são apresentados alguns desvios e suas causas características:

- a falta de planejamento, fazendo com que as pessoas realizem as reuniões com muita freqüência e durante muito tempo (meses), torna o estudo muito cansativo, e muitas falhas podem passar desapercebidas. O número elevado de reuniões durante a semana, com pessoas com outros compromissos, também dificulta a atenção;

- recomendações seguidas à risca, logo após o estudo, podem não ser as melhores. Em muitas ocasiões as ações propostas pelos grupos precisaram ser revistas, para realmente tratar de forma adequada o cenário imaginado. Uma das causas deste tipo de falha, são alguns paradigmas que as equipes já trazem para as reuniões: " isto ocorre com certeza por que ... ";

- alguns cenários imaginados durante a análise do risco, podem não ser factíveis. A equipe pode sugerir que um vazamento de um determinado produto ocasiona um grande acidente, quando na verdade, através de uma verificação por especialistas em cálculos de dispersão de vapores na atmosfera, o evento não possa ocorrer, por não haver quantidade do produto suficiente ou por a concentração no ar ficar abaixo do limite inferior de explosividade;

- uma falha de natureza humana foi cometida ao não se levar em conta, no estudo de confiabilidade do metanizador da unidade de Reforma, os erros humanos.

Conclusão

Quando em face de questões complexas as pessoas tendem a pensar de forma linear, e são sensíveis aos principais efeitos de suas ações num modelo de objetivo imediato, não se atendo aos efeitos paralelos no restante do sistema. As conseqüências de ações sobre sistemas complexos, propagam-se como "ondas numa piscina". Mas as pessoas enxergam apenas uma parcela do que está sendo tratado no momento. Esta noção é explicada pela teoria da "racionalidade limitada" lançada por Simon em 1957 : quanto maior a seletividade nos objetivos, menor a chance de se ter uma visão global num determinado tempo.

Ainda, podem predominar comportamentos grupais com patologias do tipo "*group think*", em grupos pequenos, coesos e de elite. Nestes casos, persiste uma noção de invulnerabilidade. Todas as adversidades são consideradas como improváveis por todos. Se alguém tem dúvida, é " naturalmente censurado ", mesmo antes de ser ouvido. Nestes grupos, a pessoa para permanecer no time, precisa concordar sempre. É neste ambiente que fica difícil identificar formalmente falhas devido, por exemplo, à *"estudos de segurança realizados que não contemplaram mudanças na organização ou falhas humanas, de forma detalhada "*.

Todas as teorias e observações, mencionadas nesta dissertação, permanecem sendo estudadas por muitos pesquisadores em todo mundo. Este trabalho resume algumas questões importantes que devem ser levadas em conta no campo das falhas humanas.

Uma das sugestões possíveis, fruto desta dissertação, é de que *todos* os processos operacionais passem a aplicar técnicas estruturadas, para que venham a construir Projetos Centrados na Confiabilidade, Operações Centradas na Confiabilidade, Gerenciamento Centrado na Confiabilidade, e assim por diante, para criar efetivamente um modelo de gestão centrada na confiabilidade, conforme inicialmente mostrado através da Figura 1.

Para que isto seja possível, o uso das ferramentas estruturadas como o HAZOP poderia ser implantado com o conceito de instrumento "vivo", de tal forma a permitir que sempre estivessem atualizadas as planilhas de trabalho, contendo todos os modos de falhas conhecidos.

Esta forma de operar esta ferramenta é uma sugestão para ser pesquisada e experimentada, para tornar uma técnica de uso amplamente conhecido, num sistema especialista, que apoie às equipes operacionais durante situações críticas, e às equipes de engenharia enquanto desenvolvem estudos de melhorias. Nesta mesma linha de pesquisa, a medição do aumento da aprendizagem em grupo, pelo uso continuado da técnica HAZOP pode ajudar no planejamento e construção de uma confiabilidade humana mais elevada.

Para que isto possa ser alcançado, na sua plenitude, haverá a necessidade da correta compreensão e prática daquilo que Deming chamou de "Saber Profundo" [32]: uma visão geral do que é um sistema; elementos de teoria da variabilidade; elementos de teoria do conhecimento e elementos de psicologia.

Mas, a maior falha humana, advém da dificuldade intrínseca que todos temos em aprender. Possivelmente este seja o ponto de partida para melhorar a confiabilidade de todos os sistemas - *a necessidade de aprender a aprender*.

Apêndice

Exemplos de acidentes ou incidentes causados por falhas humanas

"Eu mesmo cumpro ordens, como meus soldados. Eu digo à um: vai!
e ele vai; para outro digo: vem aqui! e ele vem; e para o meu servo,
Faze isto! e ele o faz - Um Centurion, em São Mateus,
cap. 8, versículo 9 - Nova Bíblia Inglesa [5].

Existem numerosas publicações que apresentam de forma mais ou menos detalhada, a história de grandes e importantes acidentes [5][54][9]. Bradley [73], apresenta várias catástrofes, utilizando uma forma modificada da técnica árvore das falhas, para mostrar como os fatos se sucederam, com falhas que se manifestaram em ambientes que não possuíram capacidade de recuperação. A maioria das falhas são de natureza humana.

Com a técnica usada, torna-se claro a identificação dos "cortes mínimos" da árvore, que ocasionaram os eventos. A metodologia usada por Bradley fixa alguns códigos para determinadas características encontradas nos diversos cenários, como descrito a seguir.

Códigos dos erros

Código	Tipo de erro
B	Buying (erro na aquisição, incluindo a falha na aceitação)
C	Comissioning (erro de comissionamento)
D	Design (erro no projeto)
F	Failure of equipment (falha no equipamento, sem causa humana diretamente associada)
M	Management (gerenciamento)
O	Operating (operação)
P	Production (produção)
R	Repair (reparo)

Código dos sufixos

Sufixo	Título	Explicação
1	Erro evitável	Erro de uma pessoa que deveria ter o conhecimento, mas que na realidade, não o teve quando necessário
2	Erro inevitável	Um erro cometido por uma pessoa devido ser a situação fora do seu conhecimento ou experiência

Falhas em equipamentos

Código do sufixo	Descrição
a	Equipamento falha na operação quando requerido
b	Equipamento opera quando não deveria

Alguns destes relatos são mostrados a seguir.

a) Usina nuclear Tree Mile Island [9]

Na Figura 36 está representado de forma simplificada o reator, do tipo água pressurizada, existente na usina nuclear Tree Mile Island. Neste tipo de reator o calor é gerado no núcleo por fissão nuclear e é removido por água que circula em um circuito primário. Este circuito é mantido sob pressão e a água não entra em ebulição durante a operação. O reator é, assim, chamado de reator de água pressurizada, para distinguí-lo de outros modelos nos quais a água entra em ebulição.

A água primária fornece calor para um circuito de água secundária que, ao contrário da água primaria, entra em ebulição, gerando vapor que movimenta turbinas. O vapor é condensado e é reciclado no sistema.

Todos os equipamentos que mantém contato com a radioatividade, incluindo o sistema de água primária, são mantidos confinados em um prédio, para evitar que radiação seja emitida para o meio ambiente em caso de vazamentos. O sistema de água secundário passa através de leitos de resinas de troca iônica, para a remoção de impurezas.

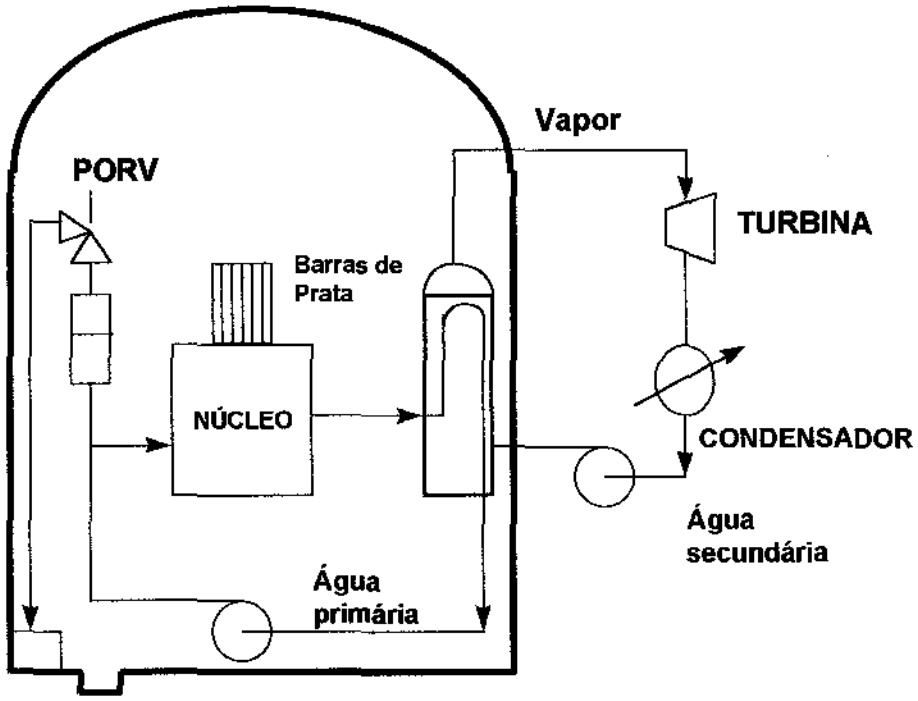


Figura 36. Reator de água pressurizado de Tree Mile Island - 1979

No dia 28 de março de 1979, um dos leitos de resinas de troca iônica entupiu. A equipe de operação, na intenção de resolver o problema, utilizou ar comprimido do circuito que alimenta os instrumentos da usina - chamado ar de instrumentação - para circular no leito entupido. O evento iniciador do incidente ocorreu pelo fato da pressão no sistema de água ser superior à do sistema de ar e, ainda, de não haver nenhuma válvula de retenção que impedisse o fluxo reverso na tubulação, ou seja: água entrar no circuito de ar de instrumentação. Este fluxo no sentido inverso, quando ocorreu, causou a contaminação do sistema de ar com água, e iniciou uma série de problemas com os instrumentos de controle. A turbina parou de funcionar e, assim, cessou a retirada de calor do núcleo do reator. A produção de calor parou de forma automática em poucos minutos, com a descida das barras de prata que, ao entrarem no núcleo, absorvem neutrons e param o processo de fissão. O calor produzido pelo reator, entretanto, baixou até o nível de 6 % da carga normal e deveria ainda ser removido. Neste instante, o sistema de segurança do reator, abriu a válvula PORV (válvula de alívio piloto operada) devido o aumento de pressão pelo aumento da temperatura.

O segundo momento importante no incidente ocorreu quando esta válvula travou aberta. Bombas de água começaram a funcionar, também automaticamente, para repor o nível no sistema, já que parte da água estava saindo pela válvula PORV.

O sistema de desligamento *como um todo* funcionava perfeitamente seguro, até que a equipe de operação, vendo no painel de alarmes UMA informação de que a válvula PORV estava fechada, desligou o sistema de reposição de água, com receio de inundar o reator, fato também considerado preocupante. Várias outras informações podiam identificar que a válvula estava na realidade aberta e não fechada, como o nível de água e a temperatura e pressão do sistema, mas estes fatos não foram considerados. Na verdade, por uma falha de projeto, a sinalização na sala de controle indicava como a válvula deveria estar, e não como ela realmente estava. Não havia nenhum sensor para indicar a posição real da válvula. Naqueles momentos de elevado estresse, erros de diagnóstico ocorreram, e todas as indicações que contrariavam o modelo mental desenvolvido para o fenômeno que se passava, foram descartadas. O nível do sistema primário baixou e a água se decompôs, formando hidrogênio no interior do reator. Vários pequenos incêndios iniciaram e por muito pouco uma grande explosão não ocorreu. O *interessante* neste acidente é que, se o operador não fizesse absolutamente nada, o evento não teria ocorrido.

Na classificação de Bradley a combinação dos eventos foi a seguinte: $F_a^3F_b^2M_1M_2O_1O_2^3$. Ou seja, cinco falhas de equipamentos, duas de gerenciamento, e quatro de operação. Uma falha de gerenciamento e uma de operação eram evitáveis.

b) A tragédia de Chernobyl [13]

À 01:24 de sábado, dia 26 de abril de 1986, duas explosões arrancaram a cúpula de concreto de 1000 toneladas, que selava o reator n° 4 de Chernobyl, liberando fragmentos fundidos do núcleo do reator nas vizinhanças e produtos da fissão nuclear na atmosfera. Este foi o pior acidente na era da geração de energia nuclear comercial. Trinta e uma pessoas morreram e outras 206 foram atingidas, 7 destas com prejuízos irreversíveis. Houve contaminação de cerca de 1000 km² de terra ao redor da planta ucraniana e foi significativamente aumentado o risco de câncer na região da Escandinávia e oeste europeu.

A radiação emitida foi de 200 vezes a da bomba atômica lançada em Hirochima no Japão. A maioria dos desastres nesta escala são causados por uma combinação de falhas humanas e mecânicas. Mas o acidente de Chernobyl foi especial: um acidente causado inteiramente por falhas humanas. Uma questão imediata foi colocada: como e por que, um grupo de operadores

bem-intencionados, altamente motivados e (de alguma forma pelo menos) competentes, cometem uma mistura de erros e violações de segurança, necessários para explodir um reator aparentemente construído com qualidade e seguro?

Na classificação de Bradley a combinação dos eventos foi a seguinte: $D_1^4M_1O_1^7$. Ou seja, quatro falhas de projeto evitáveis, uma de gerenciamento evitável, e sete de operação também evitáveis.

c) O DC-10 de Chicago

Um avião DC-10 caiu após a decolagem em Chicago (USA) em maio de 1979. Houve ruptura do sistema de fixação de uma das turbinas. Após a investigação foi provado que a falha foi gerada em função do procedimento adotado nas intervenções da manutenção, que introduziam tensões na estrutura quando da retirada do motor. O processo da manutenção havia sido alterado em relação ao originalmente projetado, para economizar 200 homens-hora por avião [73].

Na classificação de Bradley a combinação dos eventos foi a seguinte: $D_1FaM_1O_2^2R_1$. Ou seja, uma falha de projeto evitável, uma falha de equipamento quando requerido, uma falha de gerenciamento evitável, duas falhas de operação inevitáveis, e uma falha de reparo evitável.

d) A Plataforma Piper Alpha

Na catástrofe ocorrida na plataforma Piper Alpha, em junho de 1988, que culminou com sua completa destruição e 160 vítimas, houve uma enormidade de falhas no sistema como um todo. O evento iniciador foi a parada de uma bomba.

A primeira explosão ocorreu por falhas de comunicação e no processo de liberação de trabalhos, que permitiram que a bomba reserva partisse sem uma válvula de alívio no seu recalque e com a sua conexão bloqueada com uma flange apertada simplesmente com a mão.

A parada da bomba ocorreu basicamente por entupimento, causado por um desvio previsto em estudos de segurança mas não observado pela equipe de operação. Mas a catástrofe, só foi alcançada porque as bombas de incêndio estavam indisponíveis, os sprinklers estavam subdimensionados, o plano de evacuação não estava adequado, as outras plataformas continuaram a alimentar o incêndio com combustível até uma hora após seu início, e vários

outros motivos. Nitidamente falhas de projeto, operação, manutenção e, sobretudo gerenciamento, foram os causadores da tragédia.

Na classificação de Bradley a combinação dos eventos foi a seguinte: $FaM_1^3O_1^4R_1$. Ou seja, uma falha de equipamento quando requerido, três falhas de gerenciamento evitáveis, quatro falhas de operação evitáveis e uma falha de reparo evitável.

Muitas das falhas avaliadas por Bradley nestes relatos, poderiam ser identificadas pela metodologia HAZOP. Mas não foram principalmente por falhas de gerenciamento. Este modo particular de falha é de vital importância para a confiabilidade. Outros acidentes ou incidentes são descritos a seguir, envolvendo este tipo de falha ou falha na visão sistêmica dos processos:

- a balsa " Herald of Free Enterprise ", afundou por estarem abertas duas portas, violando os regulamentos de navegação. Mais de cem pessoas morreram. Haviam três áreas grandes para vigilância e apenas dois funcionários para cobri-las. O capitão da embarcação não atentou para o fato das portas estarem abertas. A balsa operava com o sistema de "lógica negativa" : se ninguém avisar que algo vai mal, é por que tudo vai bem !

- no dia 3 de setembro de 1989, o Boeing 737-200 da Varig que fazia o vôo 254 com destino à Belém, depois de perder o rumo na Amazônia, caiu sem combustível na selva perto de São José do Xingu [74]. O piloto ao invés de digitar 27 graus para a rota ao norte de Marabá, digitou 270 graus à oeste, dirigindo o avião na direção da Cordilheira dos Andes. A tripulação ao tentar aterrissar no local onde "achava que estava", não recebeu a confirmação em código da torre, mas não percebeu que algo estava errado. A torre também não percebeu que autorizava um pouso de um avião que estava a 1000 quilômetros de Belém, e nem percebia que o avião não recebia seus sinais. O radar meteorológico não foi acionado, o que poderia ter ajudado. A posição da lua em relação ao avião denunciaria o erro, mas não foi percebida. Na queda onze pessoas morreram e quarenta e três sobreviveram;

- uma falha humana, conforme noticiado na imprensa no Brasil, foi o motivo do *blackout* ocorrido em vários estados brasileiros, ao mesmo tempo, numa manobra realizada em uma central elétrica em 1996. "As pessoas são intrinsecamente boas " conforme afirmava o Sr.

Deming [75] e, sem dúvida, é a crença de muitas pessoas. Mas isto não quer dizer que elas não erram. Este tipo de evento normalmente ocasiona um efeito " dominó " imprevisível, e na maioria das vezes não é identificado com provável pelos administradores;

- uma pane no reversor da turbina do avião Fokker 100 da TAM era considerada impossível (1 chance em 1 trilhão). Após a homologação um relé destinado a evitar que o reversor abrisse com o avião estacionado foi acrescentado, sem nova verificação da confiabilidade do sistema. O motivo era evitar acidentes no solo com algum mecânico durante a manutenção. Um outro relé em outra parte da aeronave falhou horas antes. A falha deste relé e a existência do novo, inverteu a lógica de segurança e o reversor abriu na decolagem, quando não deveria, dia 31 de outubro de 96, causando a queda do avião [76];

- no dia 10 de julho de 1976, ocorreu um acidente no norte da Itália, na planta química da Icmesa, durante a fabricação de 2,4,5 - triclorofenol. Uma emissão de gases contendo 2,3,7,8 - tetraclorodibenzo-*p*-dioxina, foi liberada para a atmosfera. Vários procedimentos deveriam ter sido executados antes da saída da equipe às 6 horas da manhã do dia 10. O acidente ocorreu 7,5 horas após a parada da unidade, devido a várias omissões cometidas: apenas 15 % do solvente usado na reação foi destilado antes da parada; água não foi adicionada no reator como previsto; e a agitação mantida durante 15 minutos não foi realizada. Não havendo nenhuma supervisão, uma reação exotérmica descontrolada ocorreu dentro do reator elevando sua pressão acima do previsto. O disco de ruptura instalado protegeu o reator, liberando para a atmosfera a nuvem contendo dioxina [8];

- um operador de uma planta de Reforma de Nafta abriu uma válvula no fundo de um aparelho, ao invés de abrir, como previa o procedimento, a válvula no topo do equipamento. Uma emissão de hidrogênio a alta pressão ocorreu, inflamou por eletricidade estática, e explodiu. Não houve danos, em função da pequena quantidade inicial emitida e do pronto socorro da equipe de operação. Na investigação do incidente foi percebido que as duas válvulas eram exatamente iguais e estavam colocadas uma ao lado da outra. Ainda, foi identificado que o operador não realizava a tarefa solicitada pelo supervisor, há pelo menos dez anos;

- um reservatório de estocagem de um produto químico necessitava de um medidor de nível. Um projetista foi incumbido de especificar o instrumento e planejar sua instalação. De posse

dos dados de que dispunha, acreditando que todos os desenhos do aparelho estavam corretos, o projetista determinou o local de instalação do medidor em um dos bocais no topo do tanque. O instrumento foi instalado, mas no momento da colocação em operação, a pressão no tanque caiu e as paredes se contraíram. Não havia sido percebido que o bocal escolhido era o respiro do aparelho para a atmosfera;

- outro tanque de estocagem passou por uma análise de segurança pela metodologia HAZOP, e foi identificado que uma eventual contaminação do produto contido no tanque, com outros com diferentes características, representava um risco elevado de corrosão no tanque. Um alerta foi feito para a equipe de operação. Devido ao número elevado de atividades, a tarefa de resolver o problema não pode ser priorizada. Antes da solução já conhecida, ter sido implantada, o tanque sofreu corrosão e furou, vazando produto para o meio ambiente. Danos maiores não ocorreram devido ao dique de contenção existente;

- uma lista de verificação foi feita para avaliar o risco de desmontagem de uma unidade química de porte médio, ocupando uma quadra inteira de uma fábrica. Além da lista, uma visita cuidadosa foi realizada no local, para se perceber de perto o ambiente de trabalho e as dificuldades. A desmontagem foi realizada sem acidentes ou incidentes. Uma segunda desmontagem semelhante foi necessária, e o mesmo processo de avaliação foi desenvolvido. Da mesma forma, nenhum incidente ocorreu. Para a desmontagem de uma terceira unidade, cerca de dez vezes menor do que as anteriores, uma nova análise foi solicitada. A equipe, contudo, achou que não precisaria visitar o local, baseando-se em alguns documentos e impressões de pessoas que "conheciam " os riscos. Durante a desmontagem um operário da empreiteira bateu como uma haste de ferro no volante de uma válvula "que não se sabia que existia". Havia hidrogênio na tubulação. Houve vazamento e uma explosão;

- várias plantas químicas bombeavam resíduos para queima em uma central térmica para geração de vapor, economizando energia. Apenas uma podia enviar o resíduo a cada momento. Um acidente ocorreu quando uma planta ao invés de enviar para a caldeira central, enviou para uma das outras plantas, pelo fato de todas as tubulações estarem interligadas. O acidente foi avaliado e medidas de prevenção foram adotadas, como a colocação de uma válvula de retenção para impedir o fluxo no sentido contrário. Três anos após o mesmo incidente voltou a repetir-se, na seqüência seguinte: o operador da planta A não conseguia enviar o resíduo para a caldeira,

telefonou para a central térmica e perguntou se havia alguma outra unidade enviando resíduo; a central comunicou que não, pois a planta B havia bombeado há 3 horas, e já deveria ter concluído o bombeamento, que normalmente durava apenas 45 minutos; o operador da planta A pensou então que o sistema estivesse entupido, e usou o procedimento para desentupir, tentando injetar vapor no sistema; a planta B na realidade continuava a enviar, demorando mais que o normal por problemas operacionais, mas com uma pressão superior a do vapor da rede de limpeza; o operador que tentava " desentupir " o sistema, havia escolhido um posto sem a válvula de retenção prevista (por motivo do custo elevado, em apenas um posto a válvula havia sido instalada); houve novamente fluxo reverso e envio de uma planta para outra;

- era necessário realizar um teste em uma unidade de produção. Por medida de prevenção, foi proposta a instalação de duas válvulas em paralelo, uma para a operação normal, e uma para fazer o teste. O objetivo era permitir voltar para a operação normal sem parar a unidade, se o teste falhasse. O desenho para a construção, como ocorre normalmente nos canteiros de obras, ficou ilegível devido a chuva que ocorria no dia da montagem. O líder da empreiteira solicitou um desenho novo para o encarregado da contratante. O encarregado, com a melhor das intenções, ressaltou uma das válvulas (considerada imprescindível) com uma caneta tipo "lumicolor". O líder da empreiteira pediu uma cópia do desenho para não levar o original para o campo. Na cópia realizada, devido a tinta usada na caneta, a válvula não aparecia com clareza. A válvula não foi instalada, o teste não foi bem sucedido, e a unidade foi obrigada a parar;

- em uma planta petroquímica de grande porte, durante a partida da unidade um grande vazamento ocorreu, inflamando uma mistura de nafta e ar, causando um grande jato de fogo. Três pessoas que estavam no local morreram. Várias causas foram identificadas na investigação, entre elas a cultura de tolerar pequenos vazamentos como situações normais durante uma partida. A cultura principal, que causou as fatalidades, foi a de permitir que pessoas que não precisavam estar no local, estivessem trabalhando. Os três operários que morreram eram pintores de uma empreiteira, que não precisariam estar próximos, em um momento que sabidamente é o mais crítico para uma unidade de processo;

- Em 1975 um estudante estava concluindo o curso de graduação em engenharia, ao mesmo tempo em que trabalhava no projeto, construção e montagem de uma planta química para a fabricação de um defensivo agrícola. Sua performance e dedicação foram tão boas, que a partida da unidade foi deixada para o seu comando.

Dois engenheiros consultores, estrangeiros, foram solicitados para auxiliar na colocação da unidade em operação. Como de costume, o horário dos preparativos ocorreu durante o horário normal do expediente, mas os momentos decisivos só à noite.

Às 2 horas da manhã a carga das matérias primas estava dentro do reator, e tudo iniciara conforme o previsto. Contudo, uma instrução no procedimento não podia ser realizada, pois o processo não estava correspondendo ao que estava escrito no manual de operação. Havia um operador, o "engenheiro responsável" no local, e uma decisão precisava ser tomada.

Os consultores haviam se retirado para o hotel, pois o processo era muito simples! A decisão foi tomada pelo engenheiro, e uma nova instrução foi dada e seguida à risca pelo operador. Como resultado, a reação foi interrompida, e a fábrica parou durante uma semana para poder recuperar o produto fora de especificação.

Summary

There are many processes, with particular models of management, within the path of building the called high performance organizations. The excellence, which is characterized by a recognized high level of quality, is achieved when a systemic vision predominates in the management and, beyond that, when all the processes take place in an integrated environment.

This level of quality depends on the reliability of the several parts of the whole system, or in another words, on the probability of success in achieving the goals of the multiple functions defined by the organization. The excellence will be accomplished when the total quality is reached, with the management centred on reliability.

One culture based on reliability must include all the agents of the processes as the equipments, instruments and the persons who are responsible for the operations, modifications and improvements within the organization.

The history of industrial reliability, particularly in the chemical industries, shows that the most part of failures within the systems are of human nature, and that the lost of reliability, in the chemical plants, originates both human and capital losses. In this way, to center the management of chemical plants on reliability requires significative efforts to improve the human reliability.

There are many thecniques to evaluate the probability of human errors, most of them are complexes, requiring high specialization to their application. These thecniques need, at first, the identification of "what can be done in a wrong way", when someone perform a task.

This work presents theoretical aspects concerning the nature of human failures, and general considerations over the methodologies used for its evaluation. The main focus of this work is the use of one thecnique - the methodology HAZOP - which was initially developed to be used in the chemical industries to identify hazards, and as an important instrument to human failure data acquisition.

The content includes real cases showing the HAZOP performance, applied on several process units in a chemical site, running the method with the procedures suggested by the authors. About fifty studies were performed, and the potential human failures identified varied from 17 % to 63 %, with an average value of 36 %.

Several recommendations were defined from the failures identified, in order to reduce the risk assessed, with impact on the process safety, the productivity, and so, on the operation's quality. The work also presents examples of the modified HAZOP, to specific treatment of human errors, dealing with cognitive aspects of task performing.

The need of operability and risk studies by chemical industries, using HAZOP, has been growing up in the last years, and has been proposed and required by the environmental control agencies all over the world.

The use of this methodology, with a specific focus on human errors evaluation, may be of great importance to the actual improvement of industrial reliability, and to the search of excellence.

Referências bibliográficas

[1] HERRIGEL, EUGEN - A Arte Cavalheiresca do Arqueiro Zen. Editora Pensamento, pág. 72, 1975.

[2] MOUBRAY, JOHN - Reliability Centred Maintenance (RCM). Butterworth-Heinemann Ltd, 1991. 5.

[3] SUOKAS, J. - The Identification of Human Contribution in Chemical Accidents. 6th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Oslo, 32-1;32-14, June, 1989.

[4] GEYER, TIM A. W., BELLAMY, LINDA J.; ASTLEY, JANE A.; HURST, NICK W. - Prevent Pipe Failures Due to Human Errors. Chemical Engineering Progress, 66-69, November, 1990.

[5] KLETZ, TREVOR A. - Engineer's View of Human Error. The Institution of Chemical Engineers, 1985.

[6] DHILLON, B. S. - Human Error Data Banks. Microelectronics and Reliability. Vol. 30, No 5, 963-971, 1990.

[7] WARNER, FREDERICK - The Flixborough Disaster, Chemical Engineering Progress, Vol 71, No. 9, 77-84, 1975

[8] SAMBETH, J. - What Really Happened at Seveso. Chemical Engineering, 44-47, May, 1983.

[9] KLETZ, TREVOR A. - Three Mile Island: Lessons for the HPI. Hydrocarbon Processing, 187-192, June 1982.

[10] GRENOUILLET, P.; LAVENANT, D.; PICOT, A.; BERTIN, O. - BHOPAL: L'ARBRE DES CAUSES. Préventique, 10: 17-22, 1986.

[11] LIHOU, D. A.; WHALLEY, S.P.- Bhopal, Some Human Factor Consideration, Proceedings of World Conference on Chemical Accidents, Rome, 88-92, 1987

[12] LOSS PREVENTION BULLETIN - 081. The Institution of Chemical Engineers, pág 2, junho, 1988.

[13] ALVES, JOSÉ LUIZ LOPES - Falha Humana. Proteção, *50*: 50-55, fevereiro, 1996.

[14] EMBREY, DAVID; KONTOGIANNIS, TON; GREEN, MARK - Guidelines for Preventing Human Error in Process Safety. American Institute of Chemical Engineers, 1994.

[15] Rhône - Poulenc Industrialization. Dados publicados no dossiê elaborado para o curso de Formation Sécurité Procédes, outubro,1989.

[16] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - Norma NBR 5462, Setembro/1981, - CONFIABILIDADE, Terminologia, pág. 2.

[17] SWAIN, A. D.; GUTTMANN, H. E. - Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report. U. S. Nuclear Regulatory Commission, NUREG/CR-1278, pág. 2-3, 1983.

[18] GERTMAN, DAVID I.; BLACKMAN, HAROLD S. - Human Reliability & Safety Analysis Data Handbook. John Wiley & Sons, Inc, 1994.

[19] AGGARWAL, K. K. - Reliability Engineering. Kluwer Academic Publishers, pág. 7-8, 1993

[20] ALVES, JOSÉ LUIZ LOPES - Segurança de Processos. Proteção, *22*: 30-33, 1993.

[21] EMBREY, D. E. - SHERPA: A Systematic Human Error Reduction and Prediction Approach. International Typical Meeting on Advances in Human Factors in Nuclear Power Systems, 184-193, abril 1986.

[22] LEWIS, E. E. - Introduction to Reliability Engineering. John Wiley & Sons, 1987

[23] CCPS, CENTER FOR CHEMICAL PROCESS SAFETY - Guidelines for Chemical Process Quantitative Risk Analysis. American Institute of Chemical Engineers, 1989.

[24] BOUME, A. J.; EDWARDS, G.T.; HUNNS, D.M.; POULTER, D.R.; WATSON, I.A.- Defenses Against Common - Mode Failure. United Kingdom Atomic Energy Authority, Report SRD R 196, January, 1981.

[25] NOGUEIRA, DIEGO PUPO, - Accidents During Work and Time of the Day. Industrial Medicine, Vol. 40, No 6: 28-30, 1971.

[26] ANDLAUER, P.; RUTENFRANZ, J.; KOGI, K.; THIERRY, H.; VIEUX, N.; DUVERNEUIL, G. - Organization of Night Shifts in Industries Where Public Safety is at Stake. International Archives of Occupational Environmental Health, 49:353-355, 1982.

[27] LAURIDSEN, OYVIND; TONNESEN, TOR - Injuries Related to the Aspects of Shift Working, A Comparison of Different Offshore Shift Arrangements, Journal of Occupational Accidents, Elsevier Science Publishers B.V., *12*:167-176, 1990.

[28] O'HARA, JOHN M.; HALL, ROBERT E. - Advanced Control Rooms and Crew Performance Issues: Implications for Human Reliability. IEEE Transactions on Nuclear Science, Vol. 39, No 4, 919-923.

[29] BARON, GROLLIER R. - Techniques for Improving Human Behavior with Respect to Safety and Quality. 6th International Loss Prevention Symposium, 30-1;30-17, Oslo, junho, 1989.

[30] GRIFFITHS, C. W.; LEES, ALAN - Training Needs Analysis: A Human Factors Analysis Tool. Quality and Reliability Engineering International, Vol. 11, 435-438, 1995.

[31] PARRY, GARETH W. - Suggestion for an Improved HRA Method for use in Probabilistic Safety Assessment. Reliability Engineering & System Safety, *49*: 1-12, No 1, 1995.

[32] DEMING, W. EDWARDS - Qualidade: A Revolução da Administração. Editora Marques Saraiva, XVII-XXV, 1990.

[33] KIRWAN, BARRY - A Guide to Practical Human Reliability Assessment. Taylor & Francis, 1994.

[34] VESELY, W. E.; GOLDBERG, F. F.; ROBERTS, N. H.; HAASL, D. F. - Fault Tree Handbook. NUREG-0492, Nuclear Regulatory Commission, Washington D.C., EUA. (1981)

[35] CENTER FOR CHEMICAL PROCESS SAFETY - Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples. American Institute of Chemical Engineers, 1985.

[36] PROCESS SAFETY MANAGEMENT, Reference Manual - Du Pont. Specialty Services Publications Group. Fabricated Products Department, E.I. du Pont de Memours & Co., Seventh Edition, 1987.

[37] ZOLLER, L.; ESPING, J. P. - Use "What If" method for process hazard analysis. Hydrocarbon Processing, 132B-132G, January, 1993.

[38] BRIDGES, WILLIAN G.; KIRKMAN, JOHN Q.; LORENZO, DONALD K. - Include Human Erros in Process Hazard Analysis. Chemical Engineering Progress, 74-82, maio 1994.

[39] GOYAL, R. K. - FMEA, the Alternative Process Hazard Method. Hydrocarbon Processing, 95-98, May, 1993.

[40] LAWLEY, H. G. - LOSS PREVENTION: Operability Studies And Hazard Analysis, Chemical Engineering Progress (vol 70, N° 4), 45-56, 1974

[41] KLETZ, TREVOR A. - HAZOP AND HAZAN, Identifying and Assessing Process Industry Hazards. 3° ed. Institution of Chemical Engineers, Cap. 2, 1992.

[42] GOYAL, R. K. - HAZOPS in Industry. Professional Safety, Vol 38, Part 8, 34-37, August, 1993.

[43] PRIMATECH - HAZOP-PC Version 2 User Guide. Personal Computer Software for Hazard Analysis of Industrial Facilities, 1990

[44] KLETZ, TREVOR A. - Organizations Have No Memory When it Comes to Safety. Hydrocarbon Processing, 88-95, June, 1993.

[45] KLETZ, TREVOR A. - Hazard Analysis: A Review of Criteria. Reliability Engineering, Vol. 3, Part 43, 325-338, 1982.

[46] COLLINS, ROBERT L. - Apply the HAZOP Method to Batch Operations. Chemical Engineering Progress, 48-51, abril, 1995.

[47] KELLY, W. J. - Oversights and Mythology in an HAZOP Program. Hydrocarbon Processing, 114-116, October, 1991.

[48] LARKIN, FELIN - HAZOP Study From Theory to Practice. Process Engineering, 26-27, March, 1996.

[49] BULLOCK, COLIN; MITCHELL, FRANK; SKELTON, BOB - Developments in the use of the Hazard and Operability Study Technique. Professional Safety, Vol. 36, Part 8, 33-40, August, 1991.

[50] TURNER, SIMON - Are your Hazops up to scratch ? The Chemical Engineer, 13-15, february, 1996.

[51] JONES, D. W. - Lessons from Hazop Experiences. Hydrocarbon Processing, April, 77-80, 1992.

[52] CURRY, FRANK H. - Prevent Accidents Before They Happen. Chemical Engineering, 80-82, June, 1995.

[53] WELLS, GEOFFREY LEONARD. - Safety in Process Plant Design. John Wiley & Sons, pág. 98, 1980.

[54] KLETZ, TREVOR A.- What Went Wrong ? Cases Histories of Process Plant Disasters. Gulf Publishing Company, Book Division, 1985

[55] KLETZ, TREVOR A. - HAZOP AND HAZAN, Identifying and Assessing Process Industry Hazards. 3° ed. Institution of Chemical Engineers, Cap. 3, 1992.

[56] NIMMO, L.; NUNNS, S. R.; EDDERSHAW, B. W. - Lessons Learned From the Failure of a Computer System Controlling a Nylon Polymer Plant. Safety & Reliability Society Symposium, November, 189-206, 1987.

[57] KLETZ, TREVOR A. - Human Problems With Computer Control: An Update. Plant/ Operation Progress, Vol. 10, No 1: 17-21, 1991.

[58] LEATHLEY, BRIDGET A. - Human-Computer Interaction in Safety Critical Systems. Quality and Reliability Engineering International, Vol. 11, 429-433, 1995.

[59] DRAKE, ELISABETH M.; THURSTON, CLARK W. - A Safety Evaluation Framework for Process Hazards Management in Chemical Facilities with PES-Based Controls. Process Safety Progress, Vol. 12, No 2, 92-103, 1993.

[60] COLLINS, ROBERT L. - Applying HAZOP to Control Systems. Professional Safety, Vol 40, Part 8, 23-26, August, 1995.

[61] FENCOTT, C.; HEBBRON, B. D. - The Application of HAZOP Studies to Integrated Requirements Models for Control Systems. ISA Transactions, *34*: 297-308, 1995.

[62] CURRY, FRANNK; HYATT, MICHAEL - DDM-HAZOP: A Software Package for Performing Process Hazards Analysis, Dyadem International Ltd.

[63] FREEMAN, RAYMOND A.; LEE, ROBERTO; McNAMARA, THIMOTHY P.- Plan HAZOP Studies With an Expert System. Chemical Engineering Progress, 28-32, agosto 1992.

[64] WHALLEY, S. P.; KIRWAN, BARRY - An Evaluation of Five Human Error Identification Techniques. 6th International Loss Prevention Symposium, 31-1;31-18, Oslo, junho, 1989.

[65] KIRWAN, BARRY - Human Error Identification in Human Reliability Assessment. Part 1: Overview of Approaches. Applied Ergonomics, Vol. 23, Part 5 : 299-317, 1992

[66] KIRWAN, BARRY - Human Error Identification in Human Reliability Assessment. Part 2: Comparison of Techniques. Applied Ergonomics, Vol. 23, Part 6 : 371-381, 1992

[67] KIRWAN, B.; SCANNALI, S.; ROBINSON, L. - Practical HRA in PSA, A CASE STUDY. PROCEEDINGS, ESREL '95 CONFERENCE, Vol II, 675-693, 1995.

[68] European Council Directive on the Major Accident Hazards of Certain Industrial Activities (82/501/EEC), 24 junho, 1982.

[69] HAWKSLEY, J. L. - Risk Analysis in Safety Reports Required by the Seveso Directive. Reliability Engineering and System Safety, *35*: 193-199, 1992.

[70] IEEE STD 500 - Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations. The Institute of Electrical and Electronic Engineers, Inc, 1984.

[71] CENTER FOR CHEMICAL PROCESS SAFETY - Guidelines for Process Equipment Reliability Data, With Data Tables. American Institute of Chemical Engineers, 1989.

[72] ROODBOL, H.G. - Risk Analysis Of The Six Potentially Hazardous Industrial Objects In The Rijnmond Area, A Pilot Study. A Report To The Rijnmond Authority (pag. 384), 1981

[73] BRADLEY, EDGAR A. - Determination of Human Error Patterns: The use of Published Results of Official Enquires into System Failures. Quality and Reliability Engineering International, Vol. II, 411-427, 1995

[74] REVISTA VEJA - O Mergulho na Selva. 13 setembro, 1989

[75] WALTON, MARY - O Método Deming de Administração. Editora Saraiva, 1986. 216

[76] GUROVITZ, HÉLIO - Piloto Podia Salvar o Fokker. Revista Exame, *24*: 20-21, 1996.