MICHIEL WICHERS SCHRAGE

RICARDO PIRES MENDES

PROGRAMA DE GERENCIAMENTO RISCOS APLICADO A UMA HIDROELÉTRICA NO ESTADO DE PERNAMBUCO - BRASIL

Monografia apresentada à Escola Politécnica da Universidade de São Paulo do Programa de Educação Continuada em Engenharia para a obtenção do título de Especialização em Engenharia de Segurança do Trabalho.

São Paulo

2005

MICHIEL WICHERS SCHRAGE

RICARDO PIRES MENDES

ANÁLISE PRELIMINAR DE RISCOS APLICADA A UMA HIDRELÉTRICA NO ESTADO DE PERNAMBUCO

Monografia apresentada à Escola Politécnica da Universidade de São Paulo do Programa de Educação Continuada em Engenharia para a obtenção do título de Especialização em Engenharia de Segurança do Trabalho.

São Paulo

2005

Às nossas famílias e amigos que nos apoiaram durante todo o curso.

AGRADECIMENTOS

Aos professores do PECE, por todos os ensinamentos e experiências transmitidos durante o curso.

Aos diretores, gerentes e técnicos da hidrelétrica envolvidos neste desafio, pelo interesse demonstrado neste trabalho contribuindo de forma importante para o alcance dos objetivos estabelecidos.

Aos amigos de classe, pelo bom convívio durante o curso e pela rica troca de experiências profissionais.

"Pense globalmente e atue localmente."

John Lennon

ANEXO B – Norma MIL STD 882D

RESUMO

Este trabalho apresenta a implantação de um Programa de Gerenciamento de Riscos utilizando o método da Análise Preliminar de Riscos. Mostra a implantação de um Programa de Gerenciamento de Riscos em uma usina hidroelétrica de grande porte, onde é possível verificar a necessidade de maior conhecimento e controle de seus riscos patrimoniais. O Programa é implantado com o auxílio de um experiente comitê interno de funcionários que, após um *workshop* de treinamento, realiza um levantamento dos riscos em campo. Os riscos foram levantados e classificados de acordo com a matriz de riscos que leva em conta índices de freqüência e gravidade. Os riscos classificados com Muito Graves e Graves foram merecedores de Planos de Ação que definiram a área responsável, prazo e medida para redução e controle do risco. Como resultados diretos deste trabalho, obteve-se uma equipe capaz de reconhecer e tratar riscos, assim como constatou-se a existência de riscos, que se não fossem detectados, poderiam trazer sérias perdas para a empresa hidrelétrica e para a sociedade.

ABSTRACT

This report presents a Risk Management Programme placement using the Preliminary Risks Analysis method. This shows a Risk Management Programme placement on a hydroelectric power station, where we can verify the necessity of more knowledge and control of its property risks. The Programme is placed under an experienced internal workers committee, which, after a training workshop, is able to recognize risks during a walking tour by the installations. The risks appointed were raised and classified accordingly a risks matrix that considers index of frequency and index of severity. Risks assorted as Very Severe or Severe received an Action Plan, which established the responsible sector, time limit and the action to reduce and control the risk. As a result of this work, it was possible to get a team able to recognize and mitigate risks, as it was possible to verify the risks presence, that if they were not found out they could cause serious losses to the hydroelectric plant and to the society.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

1 INTRODUÇÃO 1

1.1 Objetivo 2

1.2 Justificativa 3

2 REVISÃO BIBLIOGRÁFICA 4

2.1 Gerenciamento de Riscos 4

2.1.1 Introdução 4

2.2 Síntese do Processo 8

2.3 O Processo de Gerência de Riscos 8

2.4 Tipos de Técnicas Utilizadas na Análise de Riscos 9

2.4.1 What - If / Checklist 9

2.4.2 *Hazop* 10

2.4.3 Análise Preliminar de Riscos 11

3 METODOLOGIA 20

3.1 Apresentação Inicial – Formação e Preparação do Comitê 21

3.2 Identificação dos Riscos 22

3.3 Quantificação dos Riscos Inerentes com base nos conceitos de Freqüência e Gravidade (F/G); 22

3.4 Classificação dos Riscos (Inerentes); 23

3.5 Revisão 27

3.6 Quantificação dos Riscos Residuais (F/G) por meio de avaliação as proteções existentes 27

3.7 Focalizar os riscos classificados como 'Muito Grave' e 'Grave' 28

3.8 Planos de Ação 28

4 RESULTADOS 29

5 ANÁLISE DOS RESULTADOS 32

5.1 Planos de Ação estabelecidos 35

5 CONCLUSÃO 52

6 BIBLIOGRAFIA 54

6.1 REFERÊNCIAS BIBLIOGRÁFICAS 54

6.2 BIBLIOGRAFIA CONSULTADA 54

ANEXOS

ANEXO A – PLANILHA DE RISCOS 56
ANEXO B – NORMA MIL STD 882D 59

LISTA DE FIGURAS

Figura 1 - Riscos Inerentes Identificados em Campo 32
Figura 2 - Riscos Residuais Identificados após Análise pelo Comitê Avaliador 33

LISTA DE TABELAS

Tabela 1 - Categorias de Risco 13
Tabela 2 - Análise Preliminar de Riscos do exemplo da mitologia grega 15
Tabela 3 - Categorias de Severidade sugeridas 16
Tabela 4 - Categorias de Probabilidade sugeridas 17
Tabela 5: Exemplo de avaliação de riscos 18
Tabela 6: Exemplo de classificação final de um risco e definição do responsável 19
Tabela 7 - Freqüência 24
Tabela 8 - Gravidade 25
Tabela 9 - Matriz de Riscos 26
Tabela 10 - Tabela de Riscos a receberem Planos de Ação 34
Tabela 11 – Plano de Ação 1 36
Tabela 12 – Plano de Ação 2 37
Tabela 13 – Plano de Ação 3 38
Tabela 14 – Plano de Ação 4 39
Tabela 15 – Plano de Ação 5 40
Tabela 16 – Plano de Ação 6 41
Tabela 17 – Plano de Ação 7 42
Tabela 18 – Plano de Ação 8 43
Tabela 19 – Plano de Ação 9 44
Tabela 20 – Plano de Ação 10 46
Tabela 21 – Plano de Ação 11 47
Tabela 22 – Plano de Ação 12 49
Tabela 23 – Plano de Ação 13 50
Tabela 24 – Plano de Ação 14 51

LISTA DE ABREVIATURAS E SIGLAS

APP – Análise Preliminar de Perigos

APR – Análise Preliminar de Riscos

B – Baixo

CIPA – Comissão Interna de Prevenção de Acidentes

CFTV – Circuito Fechado de Televisão

EUA – Estados Unidos da América

G – Grave

HAZOP – Análise de Riscos e Operabilidade (*Hazard and Operability Studies*)

MB – Muito Baixo

MG – Muito Grave

NASA – National Aeronautics and Space Administration

NBR – Norma Brasileira Registrada

NR – Norma Regulamentadora

SE – Subestação

T – Tolerável

1 INTRODUÇÃO

É incontestável a importância da energia elétrica atualmente. Descoberta há pouco mais de um século, a eletricidade foi um dos fatores de maior impacto no notável desenvolvimento da humanidade desde então.

No Brasil, as usinas hidroelétricas tiveram papel de destaque na produção desta energia, vital para o progresso da economia e melhoria das condições de vida de seus habitantes. Apesar de já se dispor de algumas usinas termelétricas, eólicas e nucleares, as hidroelétricas ainda são responsáveis pela maior parte da produção consumida no país.

Devido ao fato de alguns centros industriais requererem uma demanda maior, usinas situadas em outros estados são chamadas a atender essa necessidade interligando seus sistemas por extensas linhas de transmissão. O abastecimento, de acordo com as necessidades de cada estado, está amparado por um sistema operacional de ações conjuntas entre diferentes usinas hidroelétricas.

Um sistema operacional conjunto e cadenciado entre diversas centrais hidroelétricas garante o fornecimento de energia de forma ininterrupta. Os recentes 'apagões' (paralisações abruptas de fornecimento de energia) quando decorrentes de sobrecarga, exemplificam bem a influência que uma única usina pode causar em todo o sistema, atingindo inclusive diversas regiões do país.

Os 'apagões' são causadores de grandes perdas financeiras para o país, sejam decorrentes dos danos causados aos aparelhos elétricos dos consumidores residenciais, sejam de perdas de equipamentos e interrupção de produção nas indústrias. Os danos podem se estender ainda para congestionamentos, acidentes de trânsito, tumultos e, durante a noite, ainda possibilitar o aumento da criminalidade.

Em alguns casos, as paradas de fornecimento de energia estão relacionadas a um sistema hidroelétrico nacional que tem apresentado sucessivos apagões, mostrando que o sistema tem problemas. Entretanto, esses podem ser minimizados com investimentos e construções de novas usinas a tempo para atender a demanda, sejam elas hidroelétricas, termoelétricas ou eólicas.

Em outros casos, as paradas podem estar relacionadas a danos de causa externa, como vandalismo, por exemplo, ou a falhas no gerenciamento dos sistemas operacionais e também à falta de um programa de manutenção mais rigoroso.

A fim de se reduzir a freqüência e os danos causados por situações que possam afetar a população em uma larga escala, devem ser estabelecidos procedimentos contínuos para se garantir um maior conhecimento e controle das operações. Esta é a base para um Programa de Gerenciamento de Riscos.

1.1 Objetivo

O objetivo deste trabalho é de apresentar a implantação de um Programa de Gerenciamento de Riscos que visa a proteção dos funcionários e patrimonial de uma hidroelétrica no estado de Pernambuco por meio da metodologia de Análise Preliminar de Riscos, na busca de prováveis riscos existentes. Também colabora para capacitar um grupo de funcionários a identificá-los e analisá-los.

1.2 Justificativa

A implantação de um programa de Gerenciamento de Riscos em uma empresa visa a prevenir situações que possam trazer sérios danos à saúde humana, danos materiais e financeiros para a empresa, assim como acidentes de trabalho.

Este estudo trata-se de uma situação real que irá revelar os benefícios diretos da metodologia de Análise Preliminar de Riscos.

No caso de uma hidroelétrica, por se tratar de uma companhia que presta serviços de geração e transmissão de energia, uma situação de risco desconhecida ou ignorada sua gravidade, pode trazer danos em grande escala para a população, já que o processo de fornecimento de energia não pode ser interrompido.

O uso dessa metodologia em uma usina hidroelétrica é um trabalho pioneiro no Brasil, segundo alguns profissionais da área consultados. Por esse motivo, foi solicitado pela empresa que possibilitou este trabalho o direito de sigilo sobre quaisquer informações que identificassem suas instalações e/ou características.

2 REVISÃO BIBLIOGRÁFICA

2.1 Gerenciamento de Riscos

2.1.1 Introdução

A idéia ou conceito de gerenciamento de riscos e de sistemas de gestão de segurança teve início no final dos anos 40, tendo sido a indústria bélica o primeiro setor a se preocupar de modo metodológico.

As indústrias de aviação e nuclear passam a considerar esse conceito somente no final dos anos 50. Até da década de 40, a técnica da 'tentativa e erro' era essencialmente utilizada entre projetistas e engenheiros na busca de um projeto mais seguro.

Esta técnica era relativamente boa numa época em que a complexidade de um sistema era relativamente simples, comparada com o desenvolvimento atual.

Como exemplo, na indústria aeronáutica esse processo de sistema de segurança era conhecido como "voa – arruma – voa", em relação aos problemas de um projeto. Um processo simples e rudimentar (TARALLI; SIMÕES, 2003).

Uma aeronave era projetada baseada nas já existentes ou com tecnologia já conhecida, depois voava até que os problemas começassem a aparecer ou no pior dos casos, até que caísse. Se a queda fosse causada por problemas do projeto e não por falhas humanas, estes eram arrumados e a aeronave voaria de novo.

Obviamente esse método de segurança funcionava bem quando as aeronaves voavam a baixa altitude, devagar e eram construídas de madeira, arame e pano. Porém, com o aumento da complexidade do sistema de vôo e das capacidades das aeronaves (transporte, autonomia, velocidade e maneabilidade), também cresceu a probabilidade de resultados desastrosos vindos de uma falha no sistema.

O início do programa espacial na metade dos anos 50 também contribuiu com a crescente necessidade de projetos mais seguros. Os foguetes e o desenvolvimento de programas espaciais se tornaram decisivamente uma força

impulsionadora no desenvolvimento da Engenharia de Segurança de Sistemas e de Gerenciamentos de Riscos (TARALLI; SIMÕES, 2003).

Aqueles sistemas em desenvolvimento no final dos anos 50 e início dos 60 precisavam de novas metodologias e técnicas de controle de falhas e acidentes, assim como aqueles ligados a armas e foguetes (por exemplo: componentes explosivos e pirotecnia, sistemas de propulsão instáveis e máquinas extremamente sensíveis).

O Foguete Balístico Intercontinental foi um dos primeiros sistemas a ter um programa de segurança de sistema formal, disciplinado e definido.

Em Julho de 1969, o Departamento de Defesa Americana formalizou a necessidade de um sistema de segurança publicando uma normativa intitulada "Necessidades de um Programa de Sistema de Segurança" (TARALLI; SIMÕES, 2003).

A NASA (National Aeronautics and Space Administration) rapidamente reconheceu a necessidade de um sistema de segurança e desde então tem mantido esta idéia como uma parte integral das atividades dos programas espaciais. Os primeiros anos dos programas de lançamento foram repletos de falhas catastróficas e dramáticas.

Durante aqueles anos, era sabido e falado que os foguetes simplesmente não voavam, eles explodiam.

A necessidade da busca pelo erro zero nos projetos e melhoras nos sistemas de gerenciamentos feitos pela NASA, face às vultosas somas de dinheiro investidas, contribuiu de forma importante no desenvolvimento e aprimoramento da qualidade dos produtos fabricados pelas indústrias (TARALLI; SIMÕES, 2003).

A fim de evitar novas perdas humanas e materiais, a indústria logo estaria absorvendo os conceitos de Gerenciamento de Riscos após o acontecimento de acidentes catastróficos (Bhopal, Chernobyl, entre outras).

A antecipação de uma possível falha e a tentativa de evitá-la, ou a correção e prevenção de uma já ocorrida, é o que faz o engenheiro de segurança normalmente quando analisa um projeto ou uma condição de operação, através de procedimentos e o uso de requisitos legais. Entretanto, sempre que possível, dever-se-ia usar o conceito de Gerenciamento de Riscos, que vai além desse modo de gerenciar e tenta administrar os riscos de um processo de maneira mais abrangente (ALMEIDA, 1996).

Nesse sentido, o método "voa – arruma – voa" deve ser transformado no método "Identificar, Analisar e Eliminar", atuando de modo a assegurar que trabalhos ou tarefas sejam realizados da maneira mais segura possível, reduzindo riscos de danos ou perdas inaceitáveis.

Para Almeida (1996), a Gerência de Riscos é um conjunto de procedimentos e técnicas que objetivam permitir que uma empresa conviva com as incertezas do futuro.

Sua premissa pode ser assim traduzida:

> "Gerenciar Riscos implica, necessariamente, em se conhecer bem o contexto que os caracteriza sobre seus objetos" (ALMEIDA, 1996).

A Gerência de Riscos é fundamental para viabilizar a elaboração e implantação de um programa global de prevenção de perdas, cuja eficácia tem como suporte o controle dos Riscos.

2.1.2) Gerenciamento de Riscos e os Seguros

Segundo Almeida (1996), identificar, avaliar, tratar e controlar riscos são as atividades que, basicamente, constituem o processo de Gerenciamento de Riscos. Analisar riscos é uma ação contínua.

A Gerência de Riscos não está ligada a somente reduzir os riscos de acidentes, mas também, na redução de custos de seguros patrimoniais. Várias filiais de multinacionais instaladas no Brasil são adeptas dessa cultura.

Segundo De Cicco (1994), essas empresas representaram 20% de todos os prêmios de seguros pagos no País, estimados em cerca de US$ 4 bilhões anuais em 1994.

Portanto, gerenciar riscos não é somente negociar boas apólices. Significa também traçar planos de ação para evitar erros, falhas e acidentes, ou pelo menos reduzi-los.

Tradicionalmente, os riscos que afetam uma organização podem ser divididos em riscos especulativos e riscos puros (DE CICCO, 1994).

Os riscos especulativos podem ser definidos como aqueles que envolvem uma possibilidade de ganho ou perda, já os riscos puros envolvem somente perdas, não existindo qualquer possibilidade de ganho ou lucro.

Para que uma organização funcione bem, é importante que ela identifique, classifique e avalie todos os seus riscos potenciais, definindo, a partir daí, quais as medidas de prevenção e proteção que devem ser adotadas, quais os riscos que podem ser assumidos pela empresa e quais os que devem ser transferidos a terceiros (normalmente a uma seguradora).

Segundo De Cicco (1994), na verdade, não existe um método ideal para identificar riscos. Na prática, a melhor estratégia é combinar as várias formas existentes (questionários, inspeções, roteiros, investigações de acidentes, fluxogramas, etc.), obtendo-se o maior número possível de informações sobre riscos, evitando-se que a companhia seja, inconscientemente, ameaçada por eventuais perdas e danos.

Os principais grupos em que os riscos puros podem ser classificados são:

- Riscos à Propriedade: incêndio, raio, explosão, vendaval, inundação, vandalismo, roubo, quebra de máquinas, colapso estrutural, etc;
- Riscos às Pessoas: doenças, incapacidade permanente, seqüestro, acidente do trabalho, morte, etc;

- Riscos por Responsabilidade: Prejuízos a terceiros decorrente de operações da empresa, danos causado ao meio ambiente, etc;

Os riscos devem ser então avaliados, tendo-se por base sua freqüência e gravidade.

Com essas informações em mãos a empresa consegue atingir um de seus principais objetivos, que são a redução das despesas com seguros e aumento do grau de proteção dos recursos materiais, humanos e financeiros.

2.2 Síntese do Processo

A identificação dos riscos aos quais um objeto está suscetível tem se apresentado polêmica. Tal fato se evidencia quando se questiona causas e efeitos. É comum, nos contextos nos quais os riscos se estabelecem, a inversão entre as causas e os efeitos.

Um sobreaquecimento pode vir a causar um curto-circuito e vice-versa, da mesma forma, invertem-se fogo e explosão, ou ainda, dano elétrico e dano mecânico.

O Risco não existe isolado do objeto e representa uma condição permanente de ameaça de perdas e danos a bens e componentes, à atividades, sistemas e pessoas, e se instala tanto no ambiente que os cerca, quanto na sua própria estrutura e função.

2.3 O Processo de Gerência de Riscos

O Gerenciamento de Riscos é definido a partir do conhecimento profundo do objeto em estudo, dos seus componentes, sistemas, funções e operacionalidade.

A chave para a identificação precisa dos riscos está no entendimento do objeto em estudo, considerando sua finalidade, modo de operação e detalhes estruturais, a partir do qual se pode investigar as possíveis causas de acidentes, considerando-se ainda as características do ambiente em que se encontra.

Como primeiro passo é necessário identificar quais os riscos potenciais que possam impedir a continuidade das operações.

Identificados os riscos, estes poderão ser graduados em razão de sua gravidade e de sua freqüência, devendo-se ater ao fato de que um componente pode vir a perder sua função sem necessariamente comprometer o processo no qual está inserido, ou mesmo o sistema.

2.4 Tipos de Técnicas Utilizadas na Análise de Riscos

Existem algumas técnicas que podem ser utilizadas na análise de riscos. O mais importante é escolher uma que se adapte melhor ao nível de profundidade em que se deseja chegar sobre o objeto em estudo ou que seja de melhor entendimento do grupo que irá analisá-lo.

2.4.1 What - If / Checklist

O *What-If / Check List* é um procedimento de revisão de riscos de processos que se desenvolve através de reuniões de questionamento sobre procedimentos, instalações, entre outros, gerando soluções para os problemas levantados (DE CICCO; FANTAZZINI, 1994).

Utiliza-se de uma sistemática envolvendo a área técnica e administrativa, que inclui princípios de dinâmica de grupos. O *What-If / Checklist*, uma vez aplicado, deve ser utilizado periodicamente.

É um excelente procedimento para uma primeira abordagem na análise de riscos de processos (como, por exemplo, processos de manufatura), inclusive na fase de projeto, possibilitando a revisão de um largo espectro de riscos e um consenso entre áreas de atuação (produção, processo e segurança) sobre a operação segura na planta. Gera um relatório detalhado, de fácil entendimento, que constitui por sua vez um material de treinamento e base para revisões futuras.

Segundo De Cicco; Fantazzini (1994), esta técnica apresenta uma estruturação e sistemática que o tornam um instrumento capaz de ser altamente exaustivo na detecção de riscos. Ideal para um primeiro trabalho da análise de uma situação, seja ela já operacional ou ainda não, sua utilidade não está limitada às empresas de processo.

2.4.2 *Hazop*

A técnica *Hazop* está baseada na identificação de perigos para estudar possíveis desvios (anomalias) de projeto ou na operação de uma instalação.

Segundo Taralli; Simões (2003), é uma técnica que utiliza um método sistemático de questionamento mais criativo e aberto. No Hazop, a "operabilidade" é tão importante quanto a "identificação de perigos". Na maioria das vezes, identificam-se muito mais problemas operacionais do que perigos.

Essa idéia pode ser melhor compreendida se levarmos em conta que a eliminação de problemas operacionais diminui a freqüência dos chamados erros humanos e, por conseguinte, o nível de riscos.

Em síntese, a técnica prevê uma descrição completa do processo, questionando-se sistematicamente toda e qualquer parte desse para levantar como poderiam ocorrer desvios e decidir o quanto estes podem gerar riscos.

Durante uma série de reuniões realizadas por uma equipe multidisciplinar, faz-se a revisão da instalação discutindo-se metodicamente o projeto a fim de verificar os perigos e/ou problemas de operabilidade.

O líder orienta o grupo através de um conjunto de palavras-guia que focalizam os parâmetros estabelecidos para o processo ou operação em análise.

O questionamento é focalizado em cima de qualquer componente da instalação. Submete-se esse componente a uma série de questões, utilizando-se as palavras-guia. Estas são utilizadas para assegurar que as questões que são levantadas para testar a integridade de cada componente da instalação explorarão qualquer

maneira possível na qual possa ocorrer o desvio de uma dada intenção prevista na instalação. Este questionamento resultará num certo número de desvios teóricos, e cada um deles é então considerado, analisando-se como ocorre (qual a causa?) e quais seriam as conseqüências.

As causas consideradas como irreais e triviais podem ser desconsideradas, entretanto, as potencialmente perigosas são merecedoras de ações de prevenção e/ou proteção. O processo é repetido em todos os componentes até ter se completado a análise de toda a instalação.

O sucesso dessa análise depende basicamente de:

a) Precisão dos documentos e outros dados utilizados como base para o estudo;

b) Competências e conhecimento da equipe;

c) Capacidade da equipe utilizar o método como uma ferramenta auxiliar de sua imaginação para visualizar desvios;

d) Capacidade da equipe em manter um senso de proporção, principalmente na avaliação dos perigos identificados.

2.4.3 Análise Preliminar de Riscos

A Análise Preliminar de Riscos é uma técnica de identificação de perigos que teve origem na área militar, mais especificamente no Departamento de Defesa dos EUA.

Surgiu na época do desenvolvimento de novos sistemas de mísseis, que continham alto grau de risco operacional. Como exemplo, de 72 silos de lançamento do míssil intercontinental Atlas, quatro foram destruídos em rápida sucessão. O custo de cada operação estava avaliado em 12 milhões de dólares.

A APR, como também é conhecida a Análise Preliminar de Riscos, é normalmente utilizada na revisão de problemas gerais de segurança. Por ser

superficial, outros detalhes dos objetos em estudo podem requerer uma análise mais profunda. Para análises mais detalhadas, outros métodos devem ser utilizados, (DE CICCO; FANTAZZINI, 1994).

A APR tem como princípio a revisão geral de aspectos por meio de um formato padrão. São levantadas as causas e efeitos de cada risco, as medidas de prevenção ou correção e a categorização dos riscos para priorização de ações.

Apesar de seu escopo básico de análise inicial, é muito útil como revisão geral de segurança em sistemas operacionais, revelando aspectos às vezes despercebidos.

De acordo com Taralli; Simões (2003), essa técnica tem por objetivo identificar os perigos presentes numa instalação que podem ser causados por eventos indesejáveis. Pode ser utilizada durante etapas de desenvolvimento, estudo básico, implantação e em estudos de revisão de segurança de uma instalação existente.

Para isso é constituído um grupo multidisciplinar que, baseado em sua competência e experiência, procura descrever e explorar as possíveis causas destes eventos, suas conseqüências ou efeitos. É desejável que o grupo seja composto de profissionais das áreas de engenharia de processo, manutenção, engenharia de segurança e operacional.

Como benefício direto, a técnica permite propor ações ou medidas de prevenção e/ou proteção para diminuir as probabilidades de ocorrência de um evento danoso. Pode também ser utilizada para estudar a influência de eventos externos (inundações, quedas de raio, temperatura, etc.).

Segundo Cardella (2004), a Análise Preliminar de Riscos (APR) é um técnica de identificação de perigos e análise qualitativa de riscos. É conhecida também como Análise Preliminar de Perigos (APP).

A APR tem aplicação na identificação de perigos nas fases iniciais dos projetos, daí a denominação preliminar, mas também é utilizada para análises de segurança nas fases operacionais.

Uma APR abrangente considera os eventos que causam danos ao homem, ao meio ambiente e ao patrimônio. E a identificação dos eventos não se restringe aos que provocam danos, mas também aos que levam a perdas de qualidade e produtividade.

O objeto de estudo da APR pode ser uma área, sistema, procedimento, projeto ou atividade. Aplica-se tanto a projetos das áreas aeronáutica, nuclear e química, como a eventos administrativos, seminários e solenidades, por exemplo.

Em uma adaptação simplificada da MIL-STD-882, norma americana sobre o assunto (ESTADOS UNIDOS, 2000), pode ser utilizada somente uma tabela que classifica os riscos em quatro categorias. A tabela 1 abaixo ilustra essa situação.

Tabela 1 - Categorias de Risco

CATEGORIA	NOME	CARACTERÍSTICAS
I	Desprezível	▪ Não degrada o sistema, nem seu funcionamento; ▪ Não ameaça os recursos humanos.
II	Marginal / Limítrofe	▪ Degradação moderada / danos menores; ▪ Não causa lesões; ▪ É compensável ou controlável.
III	Crítica	▪ Degradação crítica; ▪ Lesões; ▪ Dano substancial; ▪ Coloca o sistema em risco e necessita de ações corretivas imediatas para a sua continuidade e recursos humanos envolvidos.
IV	Catastrófica	▪ Séria degradação do sistema; ▪ Perda do sistema; ▪ Morte e lesões.

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

Exemplificando a aplicação da Tabela 1, foi escolhido uma caso bastante antigo e citado em diversas bibliografias referente a APR, como De Cicco; Fantazzini (1994) e Taralli; Simões (2003).

Segundo a mitologia grega, o Rei Minos, de Creta, mandou aprisionar Dédalo e seu filho Ícaro, na ilha de mesmo nome. Com o objetivo de escapar para a Grécia, Dédalo idealizou fabricar asas, como sendo sua única alternativa. Com penas, linho e cera de abelhas conseguiu fabricá-las. Entretanto, pouco antes de partir, seu pai Dédalo o advertiu que tomasse cuidado em sua jornada, pois se voasse muito baixo, as ondas molhariam suas penas e ele cairia no mar. Por outro lado, se voasse muito alto o sol poderia derreter a cera e ele também cairia no mar (DE CICCO; FANTAZZINI, 1994).

Como já é sabido, Ícaro assumiu o risco, voou muito alto, e sob essas circunstâncias de risco previsto, caiu no mar.

A tabela 2 a seguir sintetiza as informações desse exemplo de um modo mais técnico.

Tabela 2 - Análise Preliminar de Riscos do exemplo da mitologia grega

Sistema	Subsistema	Perigo	Causa	Efeito	Categoria Severidade	Medidas Preventivas ou Corretivas
Vôo Ded I	Asas	Radiação Térmica do Sol	Voar muito alto em presença de forte radiação.	Calor pode derreter cera de abelhas, que une as penas. Esta separação pode causar má sustentação aerodinâmica. Aeronauta pode morrer no mar.	IV	Providenciar advertência contra vôo muito alto e perto do Sol. Manter rígida supervisão sobre aeronauta. Prover trela de linho entre aeronautas para evitar que o jovem impetuoso, voe alto. Restringir a área da superfície aerodinâmica.
		Umidade	Voar muito perto da superfície do mar.	Asas podem absorver umidade, aumentando o peso e falhando. O poder de propulsão limitado pode não se adequado para compensar o aumento de peso. Resultado: perda da função e afogamento possível do aeronauta	IV	Advertir aeronauta para voar à meia altura, ou onde o sol manterá as asas secas, ou onde a taxa de acumulação de umidade é aceitável para a duração da missão.

(Fonte: DE CICCO; FANTAZZINI, 1994.)

Esse exemplo retrata uma das primeiras análises de risco e, de certa forma, define o conceito de Análise Preliminar de Riscos.

De acordo com a norma militar americana MIL-STD-882D (ESTADOS UNIDOS, 2000), uma Análise Preliminar de Riscos deve considerar aspectos de severidade e probabilidade.

As categorias de Severidade são definidas com o intuito de se prover medidas qualitativas de acordo com o cenário de dano mais provável de acontecer, isto é, é necessário pensar em termos de algo de possibilidades reais de ocorrer, conforme exemplificado na tabela 3, a seguir.

Tabela 3 - Categorias de Severidade sugeridas

Descrição	Categoria	Critério de análise
Catastrófico	IV	Pode resultar em morte, invalidez permanente ou danos ambientais irreversíveis que violam as leis.
Crítico	III	Pode resultar em invalidez parcial, lesões ou doenças ocupacionais que resultem em hospitalização de pelo menos três pessoas, ou danos ambientais reversíveis que ainda violam as leis.
Marginal	II	Pode resultar em resultar em lesão ou doença ocupacional que resulte em um ou mais dias de afastamento do trabalho, ou danos ambientais de pequenas proporções, sem violação da lei na qual as atividades de restauração podem ser realizadas.
Insignificante	I	Pode resultar em lesão ou doença sem resultar em afastamento do trabalho, ou mínimo dano ambiental sem violar a lei.

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

É importante notar que o as categorias de Severidade acima são guias para uma larga variedade de programas. Entretanto, essas categorias devem ser adaptadas de acordo o que está sendo analisado. Deve-se prever um bom entendimento dos termos usados nas definições de categorias.

Os aspectos de Probalidade estão ligados diretamente à probabilidade de algo acontecer dentro de um plano de expectativa de vida do sistema. Pode ser descrito em termos de ocorrências potenciais por unidade de tempo, evento, população, itens ou atividade. Está baseado também em dados estatísticos, conhecimentos e experiências do grupo envolvido.

A tabela 4 nos dá uma idéia de como podem ser as categorias de Probabilidades.

Tabela 4 - Categorias de Probabilidade sugeridas

Descrição	Nível	Probabilidade
Freqüente	A	Provável de ocorrer com freqüência na vida de um item, com probabilidade maior que 10^{-1} na vida
Provável	B	Irá ocorrer diversas vezes na vida do item, com probabilidade de ocorrência menor que 10^{-1} mas maior do que 10^{-2}
Ocasional	C	Provável de acontecer algumas vezes na vida do item, com probabilidade de ocorrência menor que 10^{-2} mas maior que 10^{-3}
Remoto	D	Improvável, mas possível de ocorrer na vida de um item, com probabilidade de ocorrência menor que 10^{-3} mas maior que 10^{-6}
Improvável	E	Muito improvável, pode se entendido que nunca ocorra, com a probalidade menor que 10^{-6} na vida.

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

Existem algumas considerações importantes sobre Probabilidade. Na avaliação de riscos, não há maiores dificuldades na determinação da severidade. A dificuldade está em avaliar a probabilidade de ocorrência.

A base dessa idéia está amparada pelo fato de as pessoas possuírem diferentes experiências de vida, fazendo com que alguns riscos pareçam mais reais que outros. Por exemplo, uma pessoa que vive no deserto tem uma visão diferente sobre afogamento do que aquela que vive perto de um lago ou oceano.

Cada um de nós tem diferentes sensibilidades a um mesmo risco. Uma pessoa que vê um acidente na rua a caminho do trabalho provavelmente irá avaliar esse risco como algo temporário. Uma pessoa que vive perto de uma entrada de

emergência de um hospital deve ter uma avaliação elevada de eventos de desastres humanos que ela até associa aos sons de sirenes.

Nenhuma dessas pessoas está errada. Trata-se apenas de uma questão de experiências e pontos de vista. Por este motivo, recomenda-se que um grupo realize o estudo para assegurar um resultado com a perspectiva o mais abrangente possível.

A avaliação dos riscos de severidade e probabilidade podem ser executadas por meio de uma matriz de avaliação de riscos. A tabela 5 mostra um exemplo de como pode ser traçada uma matriz de riscos.

Tabela 5: Exemplo de avaliação de riscos

Severidade Probabilidade	Insignificante	Marginal	Crítico	Catastrófico
Freqüente	1	3	7	13
Provável	2	5	9	16
Ocasional	4	6	11	18
Remoto	8	10	14	19
Improvável	12	15	17	20

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

Na tabela 6 pode se classificar os riscos em baixos, médios, sérios ou altos. A norma MIL-STD-882D (ESTADOS UNIDOS, 2000) utiliza esta mesma tabela para designar as áreas responsáveis para determinar ações cabíveis.

Tabela 6: Exemplo de classificação final de um risco e definição do responsável

Severidade do Risco (Tabela 5)	Categoria de Risco	Área Responsável
1 – 5	Baixo	Sem necessidade.
6 – 9	Médio	Gerente do Programa
10 – 17	Sério	Executivo do Programa
18 – 20	Alto	Diretor do Programa

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

3 METODOLOGIA

A metodologia utilizada neste estudo teve como base a Análise Preliminar de Riscos fundamentada na norma americana MIL-STD-882D (ESTADOS UNIDOS, 2000), por esta possuir a capacidade de identificar as principais situações de risco e estabelecer linhas de ação de controle em um ramo de atividade (energia) que apresenta pouco uso deste tipo de análise.

As tabelas de freqüência (tabela 7) e gravidade (tabela 8) foram adaptadas tomando-se por base a norma americana citada anteriormente. A tabela 05 (exemplo de avaliação de riscos) foi adaptada para o formato da tabela 09 (matriz de riscos) e a tabela 06 (exemplo de classificação final de um risco e definição do responsável) pode ser traduzida em Planos de Ação, conforme apresentado no item 5.1 deste trabalho.

As bibliografias consultadas (PRELIMINARY HAZARD ANALYSIS, 2002; ESTADOS UNIDOS, 2000; TARALLI; SIMÕES, 2003) exemplificam essas adaptações, nas quais são mantidos os conceitos de freqüência e gravidade.

Neste trabalho serão levantados e analisados aspectos que, de alguma forma, colocam em risco a segurança patrimonial e o sistema operacional da empresa. Dessa análise serão gerados 'Planos de Ação', para cada risco identificado, que fornecerão um panorama abrangente das principais medidas e práticas a serem adotadas no intuito de se garantir a continuidade dos negócios.

Para que sejam alcançados os objetivos estabelecidos, é necessário o seguir o seguinte ciclo de tarefas:

3.1 Apresentação Inicial – Formação e Preparação do Comitê;
3.2 Identificação de Riscos
3.3 Quantificação dos Riscos Inerentes com base nos conceitos de Freqüência e Gravidade (F/G);
3.4 Classificação dos Riscos (Inerentes);
3.5 Revisão;
3.6 Quantificação dos Riscos Residuais (IF/IG) por meio de avaliação das proteções existentes;

3.7 Focalizar os riscos classificados como 'Muito Grave' e 'Grave';

3.8 Definir Planos de Ações.

Para maior clareza apresenta-se a seguir o desenvolvimento de cada etapa.

3.1 Apresentação Inicial – Formação e Preparação do Comitê

Essa é a principal etapa de todo o processo. Ela é a responsável por garantir a conscientização de todos envolvidos e muni-los de conhecimento e motivação, fundamentais para garantir o sucesso do projeto.

Todo o processo de implantação de um Programa de Gerenciamento de Riscos deve ser conduzido por um profissional devidamente habilitado e experiente no assunto, que pode ser da própria empresa ou consultor externo.

É importante que se crie uma equipe multidisciplinar de profissionais formada por engenheiros e técnicos de todas as áreas da empresa (manutenção, elétrica, mecânica, produção, etc). Todos podem participar com opiniões, mesmo não pertencentes às suas especialidades, e todos devem ser ouvidos. Muitas vezes, essas opiniões inicialmente absurdas são base para a maturação de uma questão em análise.

Reunido o grupo, deve ser feita uma apresentação explicando-se o conceito e benefícios desse Programa. É importante abordar exemplos de empresas que utilizam esta ferramenta e apresentam sucesso em suas operações, assim como exemplos de empresas que poderiam ter evitado as perdas ocorridas se utilizassem este método, como Piper Alpha e Bhopal.

Os conceitos sobre a Análise Preliminar de Riscos devem ser explicados com profundidade ao grupo, fazendo com que seus integrantes sintam-se alertas quanto aos riscos quando da visita em campo e confiantes para fazerem suas análises.

Inicialmente o grupo deve localizar riscos tendo em mente seus riscos inerentes, como poderá ser visto próximo passo.

3.2 Identificação dos Riscos

Após o *wokshop* no qual o Comitê recebe instruções sobre todo o Programa de Gerenciamento de Riscos inicia-se a parte prática de todo o trabalho.

O grupo deve, então, percorrer toda a área do local em estudo em busca de situações que possam oferecer riscos levando-se em conta os riscos inerentes, isto é, sem considerar os sistemas protecionais de cada equipamento ou local visitado, ou ainda qualquer controle ou procedimento de prevenção, combate e/ou gerenciamento implantado.

O grupo deve ser motivado a anotar toda a quantidade possível de riscos inerentes observados durante a caminhada, independentemente de sua graduação de risco, como pode ser visto na Planilha de Riscos no ANEXO A. Destaca-se a importância de se relacionar o risco observado com o local no qual o mesmo encontra-se inserido.

Cada participante deve ser instruído a fazer anotações pessoais sobre riscos observados para serem utilizados no passo seguinte.

Nesta etapa tudo deve ser considerado para que nada, ou praticamente nada, deixe de ser analisado posteriormente.

3.3 Quantificação dos Riscos Inerentes com base nos conceitos de Freqüência e Gravidade (F/G);

Em um segundo *workshop*, o comitê deve ser reunido para quantificar todos os riscos levantados em campo.

Todos os riscos que foram anotados durante a visita pela empresa devem ser, nesta etapa, colocados em uma tabela denominada 'Planilha de Riscos' conforme exemplificado no ANEXO A, mais especificamente na coluna 'RISCO'.

A maior dificuldade nesse processo é identificar os riscos na sua forma inerente, isto é, não se levando em conta todos os sistemas, dispositivos e proteções de equipamentos. Muitas vezes os equipamentos já são instalados com seus sistemas protecionais no local de operação, o que dificulta ao integrante do grupo enxergar um risco.

Acrescenta-se o fato de que o grupo, sendo composto por funcionários que têm em mente manter toda a operação protegida da melhor forma possível, nesse momento de análise, deve se desprender totalmente da idéia de que seus equipamentos têm proteção, para então perceberem melhor a existência dos riscos.

A presença de uma equipe multidisciplinar, nessa fase, possibilita encontrar uma maior quantidade de riscos devido às diferentes experiências profissionais que levam à diversas percepções de risco.

3.4 Classificação dos Riscos (Inerentes);

Nesta etapa, após a quantificação dos riscos identificados em campo, os integrantes do grupo realizam o primeiro processo classificatório de análise de riscos.

Um cenário de risco consiste em um risco e no conjunto de impactos que podem ser causados por erros operacionais ou causas externas.

Para o grupo avaliador deve estar claro que risco inerente é o risco avaliado ignorando-se qualquer controle ou procedimento de prevenção, combate e/ou gerenciamento implantado.

Os riscos encontrados e listados na Planilha de Riscos elaborada (conforme exemplifica o ANEXO A) devem ser discutidos, um a um, avaliando-se a freqüência (a probabilidade de um risco ocorrer dentro de um determinado período), e a gravidade (qual seria o impacto se o mesmo vier a ocorrer), de acordo com as tabelas 07 e 08.

Tabela 7 - Freqüência

FREQÜÊNCIA

FREQÜÊNCIA	GRAU	DESCRIÇÃO*
5	Comum	O risco é quase certo de ocorrer mais de uma vez nos próximos 12 meses.
4	Provável	O risco é quase certo de ocorrer pelo menos uma vez nos próximos 12 meses.
3	Moderado	O risco é quase certo de ocorrer pelo menos uma vez nos próximos 2 a 10 anos.
2	Improvável	O risco é Quase certo de ocorrer pelo menos mais de uma vez nos próximos 10 a 100 anos.
1	Raro	Provavelmente o risco não ocorrerá, ou seja, menos de uma vez em 100 anos.

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

(*) O melhor julgamento poderá ser feito com base nas informações abaixo, mas também (com maior importância), levando-se em conta sua própria experiência e intuição.

Tabela 8 - Gravidade

GRAVIDADE

GRAVIDADE	GRAU	DESCRIÇÃO*
5	Catastrófico	Perda da capacidade de sustentar operações em andamento. Uma situação que causaria a interrupção da comercialização de um negócio, por exemplo: - Perda de capacidade de produção substancial (50% ou mais); - Redução maciça na credibilidade da empresa em relação a acionistas, consumidores, fornecedores, equipe e público em geral, por exemplo, após um incidente significativo; - Perda de uma oportunidade chave/vantagem competitiva; - Perda do suprimento de insumos chave dentro do processo.
4	Significativo	Redução da capacidade de atingir objetivos de negócios, por exemplo: - Perda de clientes importantes e oportunidades de vendas; - Perda de capacidade produtiva a curto prazo (de 3 a 6 meses) ou das cadeias de fornecimento / distribuição; - Sujeitar-se a custos excessivos que tenham impacto na lucratividade em andamento; - Redução permanente na qualidade do produto; - Perda ou apropriação errônea de bens significativos.
3	Moderado	Interrupção das operações normais com efeito limitado no cumprimento de estratégia da unidade de negócios e objetivos. Por exemplo: - Perda temporária (menos de 3 meses) de produção e das cadeias de distribuição e fornecimento, - Impacto corrigível na qualidade do produto; - Perda de ativos.
2	Pequeno	Não há impacto material sobre o cumprimento da estratégia de negócios e nos objetivos. Variância adversa exige a inclusão em relatórios mensais.
1	Insignificante	-

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

(*) Medir o nível que o risco afetaria a capacidade da empresa em cumprir com sua estratégia e objetivos. Por exemplo:

- Impacto sobre pessoas, inclusive consumidores e o público;
- Perda de vendas, lucratividade, fatia de mercado e vantagem competitiva, por exemplo, causada por evento repentinos ou um declínio a longo prazo no desempenho;
- Impacto sobre a reputação, por exemplo, devido a um incidente ambiental do produto.

Observação: Todas as descrições mencionados nas Tabelas 7 e 8 demonstram a magnitude de cada classificação de Freqüência e Gravidade, não havendo a intenção de proporcionar descrições definitivas.

Nas bibliografias consultadas (Estados Unidos, 2000; TARALLI; SIMÕES, 2003) foi possível verificar mais de um tipo de tabela que divide os tópicos Freqüência e Gravidade em quatro níveis, ao invés de cinco como utilizado neste trabalho. O mais importante nesse processo é adotar uma regra, familiarizar-se aos conceitos nela encontrados e aplicá-los aos cenários avaliados.

Com essas informações em mãos, o comitê discutiu ativamente sobre cada risco analisado. A partir das gradações de 'Freqüência (F)' e 'Gravidade (G)' definidas nas tabelas 7 e 8, foram transcritos para a coluna 'F' e 'G', dentro da coluna 'Inerente' da Planilha de Riscos no ANEXO A, a respectiva classificação de cada risco.

Através do auxílio da Matriz de Riscos (tabela 9), as gradações puderam ser consolidadas para determinar a classe do risco. Ver coluna 'Classe' dentro da coluna 'Inerente' na Planilha de Riscos no ANEXO A.

Tabela 9: Matriz de Riscos

Gravidade					
5 Catastrófico	T	G	MG	MG	MG
4 Significativo	T	T	G	MG	MG
3 Moderado	B	B	T	G	MG
2 Pequeno	MB	B	B	T	G
1 Insignificante	MB	MB	MB	B	T
	1 Raro	2 Improvável	3 Moderado	4 Provável	5 Comum
	Freqüência				

Fonte: ESTADOS UNIDOS, 2000 (adaptado)

Legenda:

MG – Muito Grave	-	Ações urgentes devem ser tomadas para reduzir o risco para o nível de, no mínimo, tolerável.
G – Grave	-	Necessário um plano de ação detalhado para reduzir o risco ao nível de, no mínimo, tolerável.
T – Tolerável	-	Gerenciar o risco para mantê-lo sob controle através de práticas adequadas.
B – Baixo	-	Gerenciar através de práticas adequadas.
MB – Muito Baixo	-	Nenhuma ação é necessária.

3.5 Revisão

Nessa fase, após a elaboração da 'Planilha de Riscos', tendo o grupo adquirido um maior entendimento e sedimentação sobre os conceitos abordados de Análise Preliminar de Riscos, é possível que nesse momento o grupo reflita sobre novos possíveis riscos antes não analisados com maior detalhamento.

3.6 Quantificação dos Riscos Residuais (F/G) por meio de avaliação as proteções existentes

Nessa fase o comitê deve ser instruído a considerar todos os sistemas protecionais e procedimentos de controles dos riscos listados na Planilha de Riscos (ANEXO A).

Os riscos devem ser reavaliados utilizando-se os quadros de 'Freqüência' (tabela 07) e 'Gravidade' (tabela 08) novamente.

Todas essa informações são então compiladas para a coluna 'Residual' da Planilha de Riscos (conforme exemplifica o ANEXO A).

Com isso, pode-se observar que muitos riscos poderão apresentar variação de classificação, passando de 'Graves' para 'Baixo', por exemplo, assim como outros podem permanecer com a mesma classificação inicial.

Deve estar claro para o comitê avaliador que risco residual é o risco avaliado considerando-se todo e qualquer controle ou procedimento de prevenção, combate e/ou gerenciamento implantado.

3.7 Focalizar os riscos classificados como 'Muito Grave' e 'Grave'

Com a 'Planilha de Riscos' em mãos, já contendo os riscos devidamente classificados, o grupo pode-se visualizar de modo satisfatório as prioridades, conforme coluna 'CLASSE' dentro da coluna 'RESIDUAL' da Planilha de Riscos (conforme exemplifica o ANEXO A). Isso possibilita o avanço à última etapa na elaboração de 'Planos de Ação'. Será adotado que somente os riscos classificados como 'Graves' e 'Muito Graves' serão tratados no formato de 'Planos de Ação'.

3.8 Planos de Ação

Os 'Planos de Ação', devem ser elaborados para todos os riscos classificados como 'Graves' e 'Muito Graves', por se tratarem de riscos que necessitam ação prioritária.

Esses 'Planos de Ação' devem conter informações sobre o risco, como localização, descrição, causa e impactos.

Devem apresentar também a descrição clara da ação a ser tomada para diminuição do risco, prazo para atendimento para a implantação das melhorias e área responsável para execução das mesmas.

4 RESULTADOS

O uso da metodologia de Análise Preliminar de Riscos em uma usina hidroelétrica é um trabalho pioneiro no Brasil, segundo alguns profissionais da área consultados. Por este motivo, foi solicitado pela empresa que possibilitou esse trabalho o direito de sigilo sobre quaisquer informações que identificassem suas instalações e/ou características.

O ciclo de tarefas para a implantação do Programa de Gerenciamento de Riscos em questão durou cerca de trinta dias, envolvendo profissionais de diversas áreas da própria empresa constituindo assim um grupo ou comitê multidisciplinar para este trabalho.

Reunido o grupo, foi feita uma apresentação explicando-se os conceitos e benefícios desse Programa. Foram abordados exemplos de empresas que utilizam esta ferramenta e apresentam sucesso em suas operações, assim como exemplos de empresas que poderiam ter evitado as perdas ocorridas se utilizassem este método relatados em acidentes como os de Piper Alpha e Bhopal.

Os conceitos sobre a análise preliminar de riscos foram explicados com profundidade ao comitê, fazendo seus integrantes sentirem-se alertas em suas análises quanto aos riscos quando da visita em campo.

Pelo fato do Comitê contar com quase quarenta pessoas, o que dificultaria a organização do trabalho de campo, optou-se por dividir o grupo em dois a fim de se evitar a falta de concentração do grupo e fazer com que os mesmos locais fossem visitados duas vezes, contribuindo para um levantamento de riscos mais apurado e para que uma menor quantidade de riscos passasse sem ser notado pelos seus integrantes.

Durante um dia e meio de trabalho em visita em campo os grupos percorreram toda a hidrelétrica na busca de situações que pudessem oferecer riscos levando-se em conta os riscos inerentes, isto é, não se levando em conta sistemas protecionais de equipamentos e instalações como também como qualquer procedimento de emergência ou segurança dos locais visitados.

Assim, durante a visita por toda empresa, destacam-se os seguintes locais:

- Na área externa: seus acessos até a área de transformação, passando pela área de comportas e instalações elétricas ao ar livre;
- Na área interna: salas de controle, manutenção e instalações elétricas;
- Na área subterrânea: passagens subterrâneas, geradores e instalações elétricas.

Foi observado que alguns riscos foram relatados por várias pessoas do grupo, enquanto que outros foram percebidos por somente uma pessoa. Daí a importância de um grupo multidisciplinar da empresa que foi decisivo para a colaboração na identificação de riscos, por dividirem diferentes pontos de vista.

De volta ao local de reunião do comitê, os riscos foram compilados e listados em uma planilha. Assim, os 32 riscos levantados apresentados na Planilha de Riscos no ANEXO A foram discutidos, um a um, avaliando-se a freqüência (a probabilidade de um risco ocorrer dentro de um determinado período), bem como a gravidade (qual seria o impacto se o mesmo viesse a ocorrer), de acordo com as tabelas 07 e 08.

Finda essa etapa, abriu-se, na fase de Revisão, uma nova discussão sobre os riscos levantados com a intenção de se verificar se, no entender comum do grupo, algum risco havia sido esquecido de ser relacionado, prova desse fato é de que alguns componentes do comitê trouxeram à luz do grupo novos riscos que foram incluídos, analisados, discutidos e classificados, resultando no acréscimo dos riscos de número 31 e 32 da Planilha de Riscos no ANEXO A.

Na etapa seguinte, os riscos foram reclassificados considerando-se agora todos os sistemas protecionais e procedimentos existentes. Assim, utilizando-se os quadros de 'Freqüência' (tabela 07) e 'Gravidade' (tabela 08) novamente, chegou-se à classificação de riscos residuais que podem ser encontrados na coluna 'Residual' da Planilha de Riscos (conforme exemplifica o ANEXO A).

Com isso, pôde-se observar que muitos riscos apresentaram variação de classificação, passando de 'Graves' para 'Baixo', por exemplo, assim como outros permaneceram com a mesma classificação inicial.

Os riscos com classificação residual em 'Muito Baixo', 'Baixo', e 'Tolerável' foram exaustivamente discutidos e considerados controlados no entender

do grupo. Já os riscos classificados como 'Graves' e 'Muito Graves' foram merecedores de atenção especial.

Estes últimos foram colocados em forma de Plano de Ação. Foram definidos os responsáveis, medidas necessárias para diminuir ou eliminar a classificação dos riscos e prazos para cumprimento dos mesmos.

5 ANÁLISE DOS RESULTADOS

Resumindo todo o processo, na primeira etapa da identificação e quantificação dos riscos os participantes foram instruídos a considerar os riscos na sua forma 'inerente', ou seja, ignorando-se todo e qualquer controle e procedimento de gerenciamento implantado. Nesta fase foram identificados os 32 riscos apresentados coluna 'Inerente' da Planilha de Riscos no ANEXO A. Segue abaixo o gráfico da figura 1 para melhor visualização da classificação após a primeira análise, considerando os riscos inerentes.

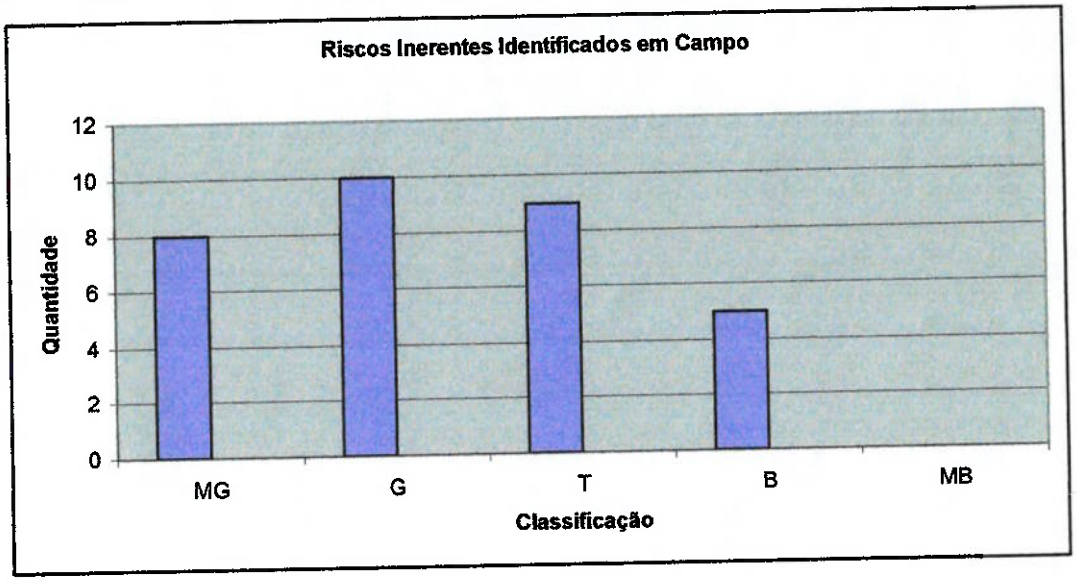

Figura 1 – Riscos Inerentes Identificados em Campo

Na Planilha de Riscos no ANEXO A, foram transcritos todos esses riscos. Para uma maior organização e clareza de informações, os riscos foram ordenados por 'Sistema' e 'Subsistema' (vide colunas de mesmo nome no ANEXO A), a fim de determinar sua localização dentro da empresa.

Na Planilha de Riscos no ANEXO A foram ainda inseridas as colunas 'Causas', 'Efeitos Imediatos' e 'Conseqüências/Impactos'. Essas informações permitiram uma melhor compreensão da classificação dos riscos.

Em seguida os riscos foram analisados considerando-se os sistemas protecionais e dispositivos de gerenciamento disponíveis. Foram utilizadas novamente as tabelas de freqüência e gravidade (tabelas 7 e 8, respectivamente). Dos 32 riscos apontados, 14 receberam a classificação de 'Muito Grave' ou 'Grave'.

Entre estes 14 riscos selecionados, apenas um risco classificado como 'Tolerável', que não seguiria adiante no processo de acordo a metodologia aplicada, foi mantido e analisado, sob consenso do comitê. Segue abaixo o gráfico da figura 2 para melhor visualização da classificação, considerando os riscos residuais.

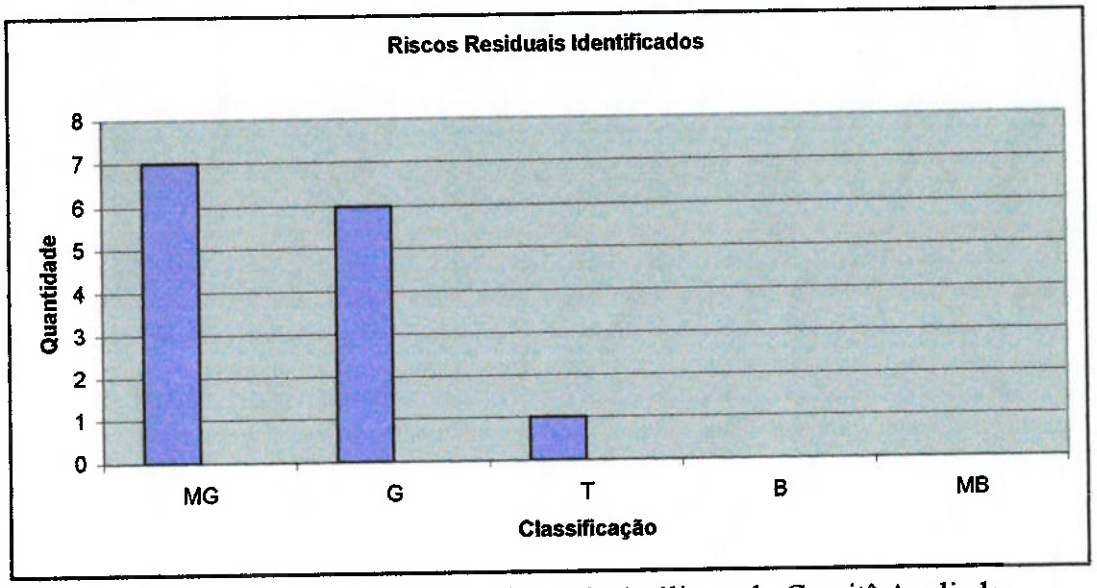

Figura 2 –Riscos Residuais Identificados após Análise pelo Comitê Avaliador

Como previsto no método da Análise Preliminar de Riscos, cada um dos 14 riscos levantados foi então merecedor de um Plano de Ação. Todos foram discutidos em profundidade pelo comitê no intuito de sanar os riscos através de medidas práticas.

A tabela 10 a seguir foi elaborada pelo grupo considerando os processos de controle e os procedimentos de gerenciamento já implantados (coluna 'Residual' no ANEXO A). Nela são relacionados os riscos que, pela graduação apresentada, foram submetidos a um processo de avaliação e elaboração dos 'Planos de Ação', item 4.1 deste trabalho.

Tabela 10: Tabela de Riscos a receberem Planos de Ação

Risco de acidente no barramento de neutro/excitação da unidade geradora.	Grave
Risco de choque elétrico no circuito e alimentação dos pórticos 375/270t.	Muito Grave
Risco de acidente / danos aos equipamentos durante o transporte através da ponte rolante interna.	Muito Grave
Risco de disparo das máquinas.	Muito Grave
Risco de indisponibilidade dos geradores por falha dos geradores de campo.	Grave
Risco de inundação quando do enchimento da sucção para montagem da plataforma.	Muito Grave
Risco de explosão das esferas de 240bar do ar comprimido do disjuntor de banco.	Grave
Risco de choque elétrico em partes do poço de turbina e sucção.	Muito Grave
Risco de acidente no acesso da antena de telecom e pára-raios na tomada d'água.	Grave
Risco de invasão/sabotagem/ocupação na tomada d'água da usina.	Muito Grave
Risco de agravamento de incêndio nos trafos da SE elevadora.	Muito Grave
Risco de acidente na oficina mecânica no hall de montagem.	Tolerável
Risco de incêndio nos painéis elétricos / casa de força / vertedouro da usina.	Muito Grave
Risco de roçamento do estator / rotor	Grave

O Plano de Ação tem como objetivo identificar o setor responsável pela execução e cumprimento do prazo no atendimento das medidas estabelecidas pelo comitê. O Plano de Ação traz ainda a informação da nova classificação do risco após avaliação das medidas tomadas.

Se ainda assim o risco não teve suas gradações de Gravidade e Freqüência reduzidas de forma a não representarem mais um risco 'Muito Grave' ou 'Grave', recomenda-se que um especialista no assunto seja consultado para então resolver o problema.

Cada um dos Planos de Ação elaborados poderá ser visto e melhor compreendido no item a seguir.

5.1 Planos de Ação estabelecidos

O item 08 da Planilha de Riscos no ANEXO A apresenta o risco de acidente por ausência de tela de proteção dos barramentos neutros na Unidade Geradora. Como efeitos imediatos pode haver a lesão de um funcionário e/ou o desligamento do gerador, tendo como conseqüências o afastamento ou morte do acidentado, além da perda de geração de energia.

O risco residual com Freqüência (F) igual a 2,0 e Gravidade (G) igual a 5,0, recebe a classificação de 'Grave'. Como Plano de Ação, após a aplicação de uma placa de celeron ou fibra de vidro com resina epóxi, dentro do prazo de execução de 12 meses, a ser cumprido pelo Setor de Produção, deverá haver redução da Freqüência (F) para 1,0 e Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) recebe classificação 'Muito Baixo'.

A tabela 11 a seguir resume essas informações.

Tabela 11 – Plano de Ação 1

Plano de Ação Nº 1 (Item 08 do ANEXO A)		
Risco: Acidente no barramento de neutro/excitação da unidade geradora.		
Causa: Ausência de tela de proteção no barramento do *air housing*.		
Impactos: Lesão / desligamento do gerador; Afastamento / morte / perda de geração de energia.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Proteção com placa de celeron, fibra de vidro com resina epóxi, etc.	12 meses	Setor de Produção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 12 da Planilha de Riscos no ANEXO A apresenta o risco de choque elétrico devido à presença de uma abertura no abrigo do barramento de 440Vac do circuito de alimentação dos pórticos de 375-270t. Como efeitos imediatos pode haver a lesão ou até morte de um funcionário, tendo como conseqüências o afastamento temporário ou definitivo, dependendo da situação.

O risco residual analisado gerou Freqüência (F) igual a 3,0 Gravidade (G) igual a 5,0 e classificação 'Muito Grave'. Como Plano de Ação, decidiu-se pelo desligamento do barramento quando fora de uso, sinalização quando em uso, estabelecimento de procedimentos operacionais e controle de intervenção. A responsabilidade cabe ao Setor de Produção, dentro do prazo de execução de 12 meses, e isso deverá reduzir a Freqüência (F) para 1,0 e Gravidade (G) para 5,0, que pela Matriz de Riscos (tabela 09) recebe a classificação 'Tolerável'.

A tabela 12 resume essas informações.

Tabela 12 – Plano de Ação 2

Plano de Ação Nº 2 (Item 12 do ANEXO A)		
Risco: Risco de choque elétrico no circuito e alimentação dos pórticos 375/270t.		
Causa: Abertura de abrigo no barramento de 440 Vac.		
Impactos: Lesão / Morte; Afastamento temporário / definitivo.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Desligamento do barramento quando o pórtico estiver fora do uso.	Imediato	Setor de Produção
Sinalizar quando o pórtico entrar em uso (ou quando o barramenro for energizado).	06 meses	
Colocação de bloqueio físico.		
Elaboração de procedimento operacional		
Controle de intervenção pelo órgão de intervenção.		
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 5 Matriz Final: Tolerável		

O item 13 da Planilha de Riscos no ANEXO A apresenta o risco de acidentes / danos aos equipamentos durante transporte por meio da ponte rolante situada na casa e maquinas, devido à deficiência do controle do sistema de frenagem e de procedimentos. Foi constatado ainda no local avarias no barramento de tensão. Como efeitos imediatos pode haver a queda de carga em transporte e perda do material, lesões e até morte de um funcionário tendo como conseqüências o afastamento temporário ou definitivo, dependendo da situação.

O risco residual analisado gerou Freqüência (F) igual a 4,0, Gravidade (G) igual a 5,0 e classificação 'Muito Grave'. Como Plano de Ação, decidiu-se pela substituição do sistema de barramento, frenagem, mancais, controle de levantamento / movimentação, etc. das pontes rolantes. A responsabilidade cabe ao Setor de Manutenção, dentro do prazo de execução de 12 meses, e isso deve reduzir a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) recebe a classificação 'Muito Baixo'.

A tabela 13 resume essas informações.

Tabela 13 – Plano de Ação 3

Plano de Ação Nº 3 (Item 13 da Relação ANEXO A)		
Risco: Acidente / danos aos equipamentos durante transporte através da ponte rolante interna		
Causa: Deficiência do controle do sistema de frenagem e de procedimentos. Barramento de tensão com avarias.		
Impactos: Lesão / Morte / Queda da carga /Afastamento temporário ou definitivo / Perda material.		
Risco Residual: Procedimento para acesso à cabine sem passar pelo trilho e sirene indicando a movimentação da ponte. Foram mantidos a Freqüência e Gravidade (4,0 x 5,0) estabelecidas para o risco inerente.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Substituição do sistema de barramento, frenagem, mancais, controle de levantamento / movimentação, etc das pontes rolantes.	12 meses	Setor de Manutenção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 14 da Planilha de Riscos no ANEXO A apresenta o risco disparo das máquinas nas comportas de adução na tomada d'água devido à ruptura da lagarta, travando a comporta na descida e defeito do distribuidor. Foi constatado ainda no local avarias no barramento de tensão. Como efeitos imediatos poderia haver inundação da casa de máquinas e até perda da total da geração de energia elétrica.

O risco residual analisado gerou Freqüência (F) igual a 3,0, Gravidade (G) igual a 5,0 e classificação 'Muito Grave'. Como Plano de Ação, decidiu-se pela substituição do sistema de barramento, frenagem, mancais, controle de levantamento / movimentação, etc das pontes rolantes. A responsabilidade cabe ao Setor de Manutenção (que deve rever periodicidade e procedimentos de manutenção) e ao Setor de Engenharia, que deve analisar o projeto e definir adequações se houver.

O prazo dado para ambos os casos foi de 06 meses, e isso deve reduzir a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) recebe a classificação 'Muito Baixo'.

A tabela 14 resume essas informações.

Tabela 14 – Plano de Ação 4

Plano de Ação Nº 4 (Item 14 da Relação ANEXO A)		
Risco: Disparo das máquinas		
Causa: Ruptura da lagarta travando a comporta na descida e defeito do distribuidor.		
Impactos: Inundação da casa de máquinas / Perda total da geração.		
Risco Residual: Foi realizada uma inspeção visual com substituição de elos e/ou componentes com defeitos e limpeza com freqüência não determinada. Foram mantidos a Freqüência e Gravidade)		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Analisar o projeto e definir adequações se houver.	06 meses	Setor de Engenharia
Rever a periodicidade e procedimentos de manutenção.	06 meses	Setor de Manutenção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 18 da Planilha de Riscos no ANEXO A apresenta o risco de indisponibilidade dos geradores por falha dos disjuntores de campo na unidade geradora, por quebra dos contatos auxiliares. Como efeitos imediatos poderia haver curto-circuito, bloqueio de retorno da unidade geradora ou sobretensão que poderiam acarretar em perda de geração de energia elétrica.

O risco residual analisado gerou Freqüência (F) igual a 4,0, Gravidade (G) igual a 3,0 e classificação 'Grave'. Como Plano de Ação, decidiu-se pela aquisição de conjuntos para troca e manutenção de reserva. A responsabilidade coube ao Setor de Produção para execução em até 06 meses. Isso poderia reduzir a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 15 resume essas informações.

Tabela 15 – Plano de Ação 5

Plano de Ação Nº 5 (Item 18 da Relação ANEXO A)		
Risco: Indisponibilidade dos geradores por falha dos disjuntores de campo.		
Causa: Quebra dos contatos auxiliares dos disjuntores de campo.		
Impactos: Sobretensão / curto-circuito / bloqueio de retorno da unidade geradora; Perda de geração.		
Risco Residual: Existência de contatos sobressalentes. Foram mantidos para o risco residual a Freqüência e Gravidade atribuídos ao risco inerente.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Aquisição de conjuntos para troca e manutenção de reserva.	03 meses	Setor de Produção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 19 da Planilha de Riscos no ANEXO A apresenta o risco de Inundação quando do enchimento da sucção para montagem da plataforma devido ao defeito no registro notado em campo, que impedia o fechamento do mesmo. Como efeito imediato, poderia haver inundação das galerias que poderia acarretar em perda da unidade geradora.

O risco residual analisado gerou Freqüência (F) igual a 4,0, Gravidade (G) igual a 3,0 e classificação 'Grave'. Como Plano de Ação, decidiu-se que quando da necessidade de encher / controlar o nível de sucção, será utilizada a válvula de *by-pass*[1] e *stop-log*[2] da própria unidade sob manutenção. A responsabilidade coube ao Setor de Produção para execução imediata. Isso poderia reduzir a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 16 resume essas informações.

Tabela 16 – Plano de Ação 6

Plano de Ação Nº 6 (Item 19 da Relação ANEXO A)		
Risco: Inundação quando do enchimento da sucção para montagem da plataforma.		
Causa: Defeito do registro, impedindo o seu fechamento.		
Impactos: Inundação das galerias;		
Risco Residual: Procedimento adotado: utilização do enchimento da sucção com controle da abertura do registro (aproximadamente 30%) da unidade geradora adjacente e com equipe reforçada (mais de um operador) e com controle de comunicação entre o operador e a equipe de manutenção. Com estes procedimentos, o risco residual foi avaliado em 01 de Freqüência e 02 de Gravidade. Apesar deste baixo *score*, o comitê decidiu elaborar um plano de ação complementar abaixo:		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Quando da necessidade de encher / controlar o nível de sucção, será utilizada a válvula de *by-pass* e *stop-log* da própria unidade sob manutenção.	Imediato	Setor de Produção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

[1] Sistema de proteção que, em caso de sobrecarga ou 'pane' do *nobreak*, alimenta as cargas diretamente com a energia da rede elétrica de entrada.

[2] Dispositivo de vedação emergencial do emboque de montante de tomada d'água.

O item 20 da Planilha de Riscos no ANEXO A, apresenta o risco de explosão das esferas de 250bar do ar comprimido do disjuntor de banco, por falta de critérios de inspeção e de teste hidrostático de acordo com a NR 13. Como efeito imediato poderia haver afastamento temporário ou definitivo (morte) de funcionário, perda de geração de energia elétrica e danos materiais.

O risco residual analisado gerou Freqüência (F) igual a 2,0, Gravidade (G) igual a 5,0 e classificação 'Grave'. Como Plano de Ação, decidiu-se por fazer manutenções e controle sobre o equipamento de acordo com NR-13. A responsabilidade coube ao Setor de Produção para respeitar a norma dentro do prazo de 12 meses. Isso poderia reduzir a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 17 resume essas informações.

Tabela 17 – Plano de Ação 7

Plano de Ação Nº 7 (Item 20 da Relação ANEXO A)		
Risco: Explosão das esferas de 250 bar do ar comprimido do disjuntor de banco		
Causa: Falta de critérios de inspeção e de teste hidrostático (NR 13).		
Impactos: Sobretensão / curto-circuito / bloqueio de retorno da unidade geradora; Perda de geração.		
Risco Residual: Existência de contatos sobressalentes. Foram mantidos para o risco residual a Freqüência e Gravidade atribuídos ao risco inerente.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Cumprir a NR 13	12 meses	Setor de Produção
Resultados Esperados: Redução da freqüência e gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 22 da Planilha de Riscos no ANEXO A, apresenta o risco de choque elétrico para o pessoal de manutenção no circuito de alimentação de 220V, em alguns locais do poço da turbina e sucção onde há uma grande presença de umidade.

Como efeito imediato poderia haver afastamento temporário ou definitivo (morte) de funcionário.

O risco residual analisado gerou Freqüência (F) igual a 3,0, Gravidade (G) igual a 5,0 e classificação 'Muito Grave'. Como Plano de Ação, decidiu-se por adquirir um kit de transformação de 220V para 12V para o sistema de iluminação de manutenção.

A responsabilidade coube ao Setor de Compras para aquisição do kit e ao Setor de Manutenção para instalá-lo, sendo o prazo de execução de 03 meses. Isso poderia reduzir a Freqüência (F) para 3,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 18 resume essas informações.

Tabela 18 – Plano de Ação 8

Plano de Ação Nº 8 (Item 22 da Relação ANEXO A)		
Risco: Choque elétrico em partes do poço de turbina e sucção.		
Causa: Presença de umidade elevada próximo à alimentação do circuito de iluminação, com tensão de 220V, durante atividade de manutenção,		
Impactos: Lesão / Morte / Afastamento temporário ou definitivo		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Aquisição de kit de transformação de 220V para 12V para o sistema de iluminação de manutenção.	03 meses	Setor de Compras / Setor de Manutenção
Resultados Esperados: Diminuição da Gravidade		
Classificação Final: Freqüência: 3 Gravidade: 1 Matriz Final: Muito Baixo		

O item 23 da Planilha de Riscos no ANEXO A apresenta o risco de acidente no acesso à antena de telecomunicação e pára-raio na tomada d'água, devido à ausência de guarda-corpo e de corrimão na escada, podendo assim, provocar o afastamento temporário do funcionário acidentado ou até mesmo sua morte.

O risco residual analisado gerou Freqüência (F) igual a 2,0, Gravidade (IG) igual a 5,0 e classificação 'Muito Grave'.

Como Plano de Ação, decidiu-se pela instalação de guarda-corpo e de corrimão na escada de acesso, a ser instalado pelo Setor de Produção dentro do prazo de execução de 03 meses.

Com isso, reduz-se a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'. A tabela 19 resume essas informações.

Tabela 19 – Plano de Ação 9

Plano de Ação Nº 9 (Item 23 da Relação ANEXO A)		
Risco: Acidente no acesso à antena de telecomunicação e pára-raio na tomada d'água.		
Causa: Ausência de guarda-corpo e de corrimão na escada.		
Impactos: Lesão /Afastamento / Morte.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Instalação de guarda-corpo e de corrimão na escada de acesso.	01 mês	Setor de Produção
Resultados Esperados: Diminuição da Gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 24 da Planilha de Riscos no ANEXO A apresenta o risco de invasão, sabotagem e ocupação da usina devido à vulnerabilidade da instalação por bloqueio de acesso ineficiente em ambos os lados da barragem (tomada d'água), que conta com um só posto de vigilância na parte central. Como efeitos imediatos podem previstos danos materiais, roubos, furtos, lesões e morte aos invasores e desligamentos de diversos equipamentos vitais à operação, que como conseqüências, podem levar à perda de geração e crime de responsabilidade civil.

O risco residual analisado gerou Freqüência (F) igual a 3,0, Gravidade (G) igual a 5,0 e classificação 'Muito Grave' na Matriz de Riscos.

Como Plano de Ação, decidiu-se pela implantação um plano de segurança física para bloqueio de acesso e de pessoas não autorizadas nas instalações. Entre outras ações: CFTV, guaritas, etc.

No caso de invasão por grupos, o Comitê sugeriu que a Diretoria estabelecesse um plano de ação preventivo e corretivo e buscasse soluções políticas e administrativas junto aos órgãos especializados. Foi estabelecido o prazo de 12 meses a ser atendido pelo Setor de Segurança e pela Diretoria.

Com isso, reduz-se a Freqüência (F) para 2,0, a Gravidade (G) para 5,0, que pela Matriz de Riscos (tabela 09) reduz para 'Grave'. Devido à essa classificação não ter sido reduzida de modo satisfatório, ficou estabelecido que este risco deverá ser revisto após a implantação das medidas sugeridas no plano de ação.

A tabela 20 resume essas informações.

Tabela 20 – Plano de Ação 10

Plano de Ação Nº 10 (Item 24 da Relação ANEXO A)		
Risco: Invasão/ sabotagem / ocupação da usina		
Causa: Vulnerabilidade da instalação por bloqueio de acesso ineficiente em ambos os lados da barragem, contando com um só posto de vigilância na parte central.		
Impactos: Danos Materiais / Roubo / Furto / Lesão / Morte / Desligamentos /		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Implantar um plano de segurança física para bloqueio de acesso e ação de pessoas não autorizadas nas instalações. Entre outras ações: CFTV, guaritas, etc. No caso de invasão por grupos, o Comitê sugere que a Diretoria estabeleça um plano de ação preventivo e corretivo e busque soluções políticas e administrativas junto aos órgãos especializados.	12 meses	Setor de Segurança / Diretoria
Resultados Esperados: Diminuição parcial da Freqüência		
Classificação Final: Freqüência: 2 Gravidade: 5 Matriz Final: Grave **(Este risco deverá ser revisto após a implantação das medidas sugeridas no plano de ação).**		

O item 27 da Planilha de Riscos no ANEXO A apresenta o risco de agravamento de incêndio nos trafos da SE elevadora devido a falha no sistema anti-incêndio por obstrução dos aspersores e de filtros d'água por algas e bactérias contribuindo assim para uma baixa confiabilidade no sistema, considerando a perda de função do equipamento que possibilita o agravamento de um incêndio. Os impactos diretos podem ser traduzidos no desligamento da linha e perda do trafo.

O risco residual analisado gerou Freqüência (F) igual a 3,0, Gravidade (G) igual a 5,0 e classificação 'Muito Grave'.

Como Plano de Ação, decidiu-se pela implantação de uma sistemática de testes com água para verificação da obstrução dos aspersores, a ser executado pelo Setor de Manutenção dentro de 03 meses.

Com isso, reduz-se a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'. A tabela 21 resume essas informações.

Tabela 21 – Plano de Ação 11

Plano de Ação Nº 11 (Item 27 da Relação ANEXO A)		
Risco: Agravamento de incêndio nos trafos da SE elevadora		
Causa: Falha no sistema anti-incêndio por obstrução dos aspersores e de filtros d'água por algas e bactérias / Baixa confiabilidade no sistema.		
Impactos: Perda de função / agravamento de incêndio; desligamento / perda do trafo.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Implantar o plano, já definido, que consiste em uma sistemática de testes com água para verificação da obstrução dos aspersores.	02 meses	Setor de Manutenção
Resultados Esperados: Diminuição da Gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 28 da Planilha de Riscos no ANEXO A apresenta o risco de acidente na oficina mecância do *hall* de montagem devido à presença de fumos de solda (gases) na área (que é confinada) podendo invadir a circulação interna e, como efeitos imediatos, podem causar intoxicação ou doenças crônico respiratórias a longo prazo. O afastamento pode ser caracterizado como o pior cenário nesta situação.

O risco residual analisado gerou Freqüência (F) igual a 2,0, Gravidade (G) igual a 4,0 e classificação 'Tolerável'.

Apesar de constituir um risco Tolerável, o comitê, por se tratar de um risco ocupacional, decidiu pela adequação dos sistemas de ventilação e exaustão do ambiente como Plano de Ação.

Devido a importância do risco, esta ação foi estendida para todos os ambientes confinados da usina em obediência à norma NBR 14787, a ser executado pelo Setor de Manutenção dentro de 06 meses, no caso da oficina, e dentro de 12 meses para demais espaços confinados.

Com isso, reduz-se a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 22 resume essas informações.

Tabela 22 – Plano de Ação 12

Plano de Ação Nº 12 (Item 28 da Relação ANEXO A)		
Risco: Acidente a oficina mecância do hall de montagem		
Causa: Fumos de solda (gases) na área, que é confinada, invadindo a circulação interna.		
Impactos: Intoxicação / doenças crônico-respiratórias; Afastamento.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Adequação dos sistemas de ventilação e exaustão do ambiente. Esta ação deverá ser estendida para todos os ambientes confinados da usina, em obediência à norma NBR 14787	06 meses para a oficina e 12 meses para os demais espaços confinados	Setor de Manutenção
Resultados Esperados: Diminuição da Gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

O item 31 da Planilha de Riscos no ANEXO A apresenta o risco de Incêndio nos painéis elétricos da casa de força e dos vertedores causado por um aquecimento numa situação de um curto-circuito, ocasionando em danos materiais e lesões. Os impactos diretos podem ser traduzidos em perda de bens e afastamento de funcionário.

O risco residual analisado gerou Freqüência (F) igual a 3,0, Gravidade (G) igual a 4,0 e classificação 'Grave'.

Como Plano de Ação, decidiu-se pela melhora do arranjo físico dos alames sonoros, permitindo que seja audível em qualquer local da usina, assim como a revisão do plano de ação da brigada de incêndio. Nos painéis elétricos mais importantes para a operação da usina, opto-se pela implantação de sistema de detecção e o combate automático.

O Setor de Segurança foi designado para a execução desses trabalhos dentro de 12 meses.

Com isso, reduz-se a Freqüência (F) para 3,0 e a Gravidade (G) para 3,0, que pela Matriz de Riscos (tabela 09) reduz para 'Tolerável'. A tabela 23 resume essas informações.

Tabela 23 – Plano de Ação 13

Plano de Ação Nº 13 (Item 31 da Relação ANEXO A)		
Risco: Incêndio nos painéis elétricos / casa de força e vertedores		
Causa: Aquecimento por curto-circuito		
Impactos: Danos Materiais / Lesões; Afastamento / Perda de Bens.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Melhorar a distribuição dos alarmes sonoros, permitindo que seja audível em qualquer local da usina.	12 meses	Setor de Segurança
Detecção/Combate automático nos painéis mais importantes para a operação da usina.		
Rever plano de ação da Brigada de Incêndio		
Resultados Esperados: Diminuição da Gravidade		
Classificação Final: Freqüência: 3 Gravidade: 3 Matriz Final: Tolerável		

O item 32 da Planilha de Riscos no ANEXO A apresenta o risco de roçamento no estator / rotor causado por de trincas no rotor podendo causar curto-circuito nas bobinas. As conseqüências podem ser traduzidas em perda de geração e perda do equipamento.

O risco residual analisado gerou Freqüência (F) igual a 2,0, Gravidade (G) igual a 5,0 e classificação 'Grave'.

O Setor de Manutenção foi designado a executar a instalação de sistema on-line de monitoramento do air-gap e encontrar especialistas para analisar a causa fundamental das trincas no rotor.

Com isso, reduz-se a Freqüência (F) para 1,0 e a Gravidade (G) para 1,0, que pela Matriz de Riscos (tabela 09) reduz para 'Muito Baixo'.

A tabela 23 resume essas informações.

Tabela 24 – Plano de Ação 14

Plano de Ação Nº 12 (Item 32 da Relação ANEXO A)		
Risco: Roçamento Estator / Rotor		
Causa: Trincas no rotor		
Impactos: Curto-circuito nas bobinas e no ferro / Perda de geração e do equipamento.		
AÇÃO	**PRAZO**	**RESPONSABILIDADE**
Instalação de sistema on-line de monitoramento do air-gap.	12 meses	Setor de Manutenção
Buscar a causa fundamental das trincas através de especialistas.		
Resultados Esperados: Diminuição da Freqüência e Gravidade		
Classificação Final: Freqüência: 1 Gravidade: 1 Matriz Final: Muito Baixo		

5 CONCLUSÃO

Baseando-se nos resultados apresentados, conclui-se que a implantação do Programa de Gerenciamento de Riscos utilizando o método da Análise Preliminar de Riscos na hidroelétrica atingiu seus objetivos.

O comitê de funcionários, após o entendimento dos conceitos abordados, pôde notar riscos importantes que, se não fossem percebidos e tratados a tempo, poderiam expor seus funcionários a acidentes de trabalho com maior freqüência e gravidade. Possibilitou ainda procurar melhorar os sistemas protecionais e de gerenciamento atuais.

Conforme a Planilha de Riscos no ANEXO A, foi possível verificar a existência de riscos até então desapercebidos ou erroneamente desprezados, que poderiam causar lesões aos funcionários, ao meio ambiente, à empresa ou ainda à sociedade. Alguns riscos inicialmente classificados como 'Muito Grave' chegaram ser reclassificados, como 'Muito Baixo' depois de uma análise técnica sobre o assunto, considerando-se as medidas propostas no plano de ação.

O comitê de funcionários passou a ter uma visão mais ampla e completa dos riscos aos quais eles mesmos estavam expostos no dia-a-dia, assim como aqueles da empresa com relação à sociedade, desde riscos classificados como 'Muito Baixo' a 'Muito Grave'.

Conclui-se também que a motivação conferida ao comitê por meio da apresentação de exemplos reais (acidente na P36, Piper Alpha, etc.) foi de fundamental importância. Constituiu-se numa ferramenta fundamental para manter o grupo sempre alerta na busca dos riscos em campo, bem como nas calorosas discussões técnicas sobre freqüência e gravidade entre todos.

Seguindo o conceito de 'Gerenciamento de Riscos', recomenda-se a continuidade do trabalho e assim estabelecer uma periodicidade, que pode ser anual,

no acompanhamento das ações definidas nos 'Planos de Ação'. Pode ser feito também o levantamento de novos riscos em campo, propiciando a criação de um hábito extremamente enriquecedor para empresa. Não menos importante é que sejam estabelecidos procedimentos de ação provisória enquanto que as ações determinadas nos 'Planos de Ação' sejam efetivamente implantadas.

A cada nova inspeção de campo, com um comitê cada vez mais amadurecido sobre os conceitos ensinados, aliado ao aumento da prática em campo, amplia-se o poder de análise em encontrar novos riscos e classificá-los.

6 BIBLIOGRAFIA

6.1 REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, R. R., **Gerência de riscos:** o desafio. Recife: Editora Universitária da UFPE, 1996.

APAGÕES Elétricos: estão controlados? **Gerência de Riscos e Seguros**, Madri, n.85, p.10, 2004.

CARDELLA, B. Análise Preliminar de Riscos: a APR tem aplicação na identificação de perigos nas fases iniciais dos projetos, mas também é utilizada para análises de segurança nas fases operacionais. **Revista CIPA**, São Paulo, n.297, p. 45-49, 2004.

DE CICCO, F. Gerenciamento de Riscos: uma abordagem eficaz para a otimização de despesas com seguros. **Revista CIPA**, São Paulo, n.172, p.68-69, 1994.

DE CICCO, F.; FANTAZZINI M.L. Gerência de riscos: a identificação e a análise de riscos. **Revista Proteção**, São Paulo, n.28, pt.2, p.1-8, abr. 1994. Suplemento Especial.

PRELIMINARY HAZARD ANALYSIS. Produced by R. R. Mohr, 2002. Disponível em: <http://www.sverdrup.com/safety/PHA.pdf. Acesso em: 03 dez. 2004.

ESTADOS UNIDOS. Department of Defense. **Standard Practice for Safety System – MIL STD 882D**. Febr. 2000. Disponível em <http://www.safetycenter.navy.mil/instructions/osh/milstd882d.pdf>. Acesso em: 05 dez. 2004.

TARALLI, G; SIMÕES, R. A. G. **Gerenciamento de riscos.** São Paulo: EPUSP/PECE, 2003. [Apostila do Curso de Especialização em Engenharia de Segurança do Trabalho].

6.2 BIBLIOGRAFIA CONSULTADA

CAMPOS, V. F. **Controle da qualidade total.** Rio de Janeiro: Bloch, 1992. 229 p

HAMMER, W. Handbook of system and product safety. Englewood Cliffs: 1972. 351 p.

LAPA, R. P. **Programa 5S.** Rio de Janeiro: Qualitymark, 1997. 81 p

SEGURANÇA e medicina do trabalho: Lei nº 6.514, de 22 de dez. 1977. 50. ed. São Paulo:Atlas, 2002. (Manuais de Legislação Atlas).

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Espaço confinado – Prevenção de acidentes, procedimentos e medidas de proteção - NBR 14787.** Rio de Janeiro, 2001.

ANEXO A – Planilha de Riscos

PLANILHA DE RISCOS

ITEM	SISTEMA	SUBSISTEMA	RISCO	CAUSAS	EFEITOS IMEDIATOS	CONSEQÜÊNCIAS/ IMPACTOS	INERENTE			RESIDUAL			APOS PLANO DE AÇÃO		
							IF	IG	CLASSE	IF	IG	CLASSE	IF	IG	CLASSE
1	SE elevadora	pára-raios e chave de aterramento	danos ao transformador	queda pára-raios ou chave / explosão pára-raios	desligamento do transformador	perda de geração (dues máquinas)	2.0	3.0	B						
2	SE elevadora	tirante se sustentação do LINK do trafo	queda do LINK	rompimento dos tirantes	desligamento do transformador	perda de geração (duas máquinas)	2.0	3.0	B						
3	SE elevadora	caixa coletora de óleo dos trafos	contaminação ambiental	válvula de saída da caixa coletora na posição aberta	poluição do rio	multa por crime ambiental	3.0	4.0	G	1.0	1.0	MB			
4	SE elevadora	sistema anti-incêndio	desligamento / curto circuito	atuação indevida por manobra acidental da válvula de dreno do ar comprimido e/ou quebra da ampola por choque mecânico e drenagem d'água	desligamento do transformador	perda de geração (duas máquinas)	2.0	3.0	B						
5	SE elevadora	armários de comando dos trafos regul. 01R1/01R2	curto circuito / desligamento dos trafos	falha de vedação, permitindo entrada de animais	perda de uma das fontes dos serviços auxiliares	perda de confiabilidade	3.0	3.0	T						
6	SE elevadora	sistema anti-incêndio	choque elétrico por indução	falta de aterramento	lesão / morte	afastamento temporário ou definitivo	1.0	5.0	T						
7	SE elevadora	transformador	desligamento indevido	deficiência no controle do 50BF do disjuntor do Gerador	desligamento do transformador	perda de geração (duas máquinas)	3.0	4.0	G	2.0	4.0	T			
8	Unidade Geradora	barramento de neutro / excitação	acidente	ausência de tela de proteção barramentos no air housing	lesão / desligamento do gerador	afastamento / morte / perda geração	2.0	5.0	G	2.0	5.0	G	1.0	1.0	MB
9	sala de comando	central de ar condicionado	vazamento d'água sobre painéis e equipamentos	rompimento da tubulação de refrigeração	curto circuito	perda de função / desligamentos	3.0	3.0	T						
10	SE elevadora	reatores limitadores CDJ 1 e 2	curto circuito	inexistência de vedação sob a porta	desligamento do transformador	perda de geração (duas máquinas)	3.0	3.0	T						
11	geradores	rotores de geradores	queda durante o transporte	falhas de procedimentos ou dos mecanismos do pórtico 375t	danos aos rotores e/ou danos às unidades em operação	perda de geração / perdas materiais /lesões / mortes	2.0	5.0	G	2.0	4.0	T			
12	circuito de alimentação dos pórticos	pórticos 375 / 270t	choque elétrico	abertura no abrigo do barramento de 440Vac	lesão / morte	afastamento temporário ou definitivo	3.0	5.0	MG	3.0	5.0	MG	1.0	5.0	T
13	casa de máquinas	ponte rolante interna	acidente / danos equipamentos durante transporte	deficiência do controle, do sistema de frenagem e de procedimentos / barramento de tensão com avarias	lesão / morte / queda de carga	afastamento temporário ou definitivo / perda material	4.0	5.0	MG	4.0	5.0	MG	1.0	1.0	MB
14	tomada d'água	comportas de adução	disparo das máquinas	ruptura da lagarta, travando a comporta na descida e defeito no distribuidor	inundação da casa de máquinas	perda total da geração	3.0	5.0	MG	3.0	5.0	MG	1.0	1.0	MB
15	unidade geradora	turbina	acidente	fechamento indevido do distribuidor, quando em manutenção	lesão / morte	afastamento temporário ou definitivo	1.0	5.0	T						
16	unidade geradora	gerador	sobrevelocidade	travamento das paletas do distribuidor quando de atuação da proteção	danos à unidade geradora	perda de geração	1.0	5.0	T						

PLANILHA DE RISCOS

ITEM	SISTEMA	SUBSISTEMA	RISCO	CAUSAS	EFEITOS IMEDIATOS	CONSEQÜÊNCIAS/ IMPACTOS	INERENTE			RESIDUAL			APOS PLANO DE AÇÃO		
							IF	IG	CLASSE	IF	IG	CLASSE	IF	IG	CLASSE
17	unidade geradora	curto circuito no estator / rotor, por umidade	desligamento da unidade	rompimento do cooler / outros vazamentos	desligamento da unidade geradora	perda de geração	3.0	4.0	G	2.0	3.0	B			
18	unidade geradora	disjuntor de campo	indisponibilidade dos geradores	quebra dos contatos auxiliares dos disjuntores de campo	sobretensão / curto circuito / bloqueio de retorno da unidade geradora	perda de geração	4.0	3.0	G	4.0	3.0	G	1.0	1.0	MB
19	sucção	esvaziamento	inundação quando do enchimento da sucção para montagem da plataforma	defeito do registro, impedindo o fechamento do mesmo	inundação das galerias	perda da unidade geradora	3.0	5.0	MG	1.0	2.0	MB	1.0	1.0	MB
20	ar comprimido do disjuntor de banco	esferas de 250 Bar	explosão	falta de critérios de inspeção e de teste hidrostático (NR13)	lesão / morte / desligamentos	afastamento temporário ou definitivo / perda de geração / danos materiais	2.0	5.0	G	2.0	5.0	G	1.0	1.0	MB
21	serviços auxiliares	Subestação Abaixadora 16,0/13,8/0,44kV	perda de alimentação	durante comutação dos SA, queima das bobinas dos disjuntores siemens de 13,8kV	desligamento da unidade geradora	perda de geração	2.0	4.0	T						
22	turbina	partes do poço da turbina e sucção	choque elétrico	presença de umidade elevada próximo à alimentação do circuito de iluminação com tensão de 220V, durante atividade de manutenção	lesão / morte	afastamento temporário ou definitivo	3.0	5.0	MG	3.0	5.0	MG	3.0	1.0	MB
23	tomada dágua	acesso antena telecom e pára-raios	acidente	ausência de guarda-corpo e de corrimão, na escada	lesão	afastamento / morte	2.0	5.0	G	2.0	5.0	G	1.0	1.0	MB
24	usina	tomada dágua	invasão / sabotagem / ocupação	vulnerabilidade da instalação, por bloqueio de acesso ineficiente, em ambos os lados da barragem, contando com um só PV, na parte central	danos materiais / roubo / furto / lesão / morte / desligamentos	perda de geração / perda material / crime de responsabilidade civil	3.0	5.0	MG	3.0	5.0	MG	2.0	5.0	G
25	hall de montagem	sala de estoque de inflamáveis, sob a sala de comando	incêndio	curto circuito e centelhamento no sistema de iluminação (fluorescentes em luminárias comuns), atingindo óleos lubrificantes e estopas / sala com pouca aeração	sobretemperatura nos cabos da sala de comando	curto circuitos / desligamentos / perda material	2.0	3.0	B						
26	SE elevadora	trafos	curto circuiro nas buchas	descargas parciais de alta energia no isolamento	explosão	incêndio / desligamento do trafo / perda de geração	2.0	5.0	G	1.0	5.0	T			
27	SE elevadora	trafo	agravamento de incêndio	falha do sistema anti-incêndio por obstrução dos aspersores e de filtros de água por algas e bactérias / baixa confiabilidade do sistema	perda de função / agravamento de incêndio	desligamento/perda do trafo	3.0	5.0	MG	3.0	5.0	MG	1.0	1.0	MB
28	hall de montagem	oficina mecânica	acidente	fumos de soldas (gases) na área, que é confinada, invadindo a circulação interna	intoxicação / doenças cronico-respiratórias	afastamento	2.0	4.0	T	2.0	4.0	T	1.0	1.0	MB
29	poço de drenagem	bombas de sucção	crime ambiental	redução do nível dágua e sucção do óleo em suspensão	dano ao meio ambiente	crime inafiançável	2.0	3.0	B						
30	geradores	painéis de excitação	curto circuito	vazamento dágua no sistema de refrigeração das máquinas	desligamento / inundação	perda de geração	2.0	4.0	T						
31	usina	painéis elétricos / casa de força + vertedores	Incêndio	Aquecimento por curto circuito	Danos Materiais / Lesões	Afastamento / Perda de bens	3.0	5.0	MG	3.0	4.0	G	3.0	3.0	T
32	unidade geradora	rotor do gerador (unidadesa II e III)	Roçamento Estator/Rotor	Trincas no rotor	Curto circuito nas bobinas e no ferro	Perda de geração e do equipamento	2.0	5.0	G	2.0	5.0	G	1.0	1.0	MB

NOT MEASUREMENT SENSITIVE

MIL-STD-882D
10 February 2000

SUPERSEDING
MIL-STD-882C
19 January 1993

DEPARTMENT OF DEFENSE

STANDARD PRACTICE FOR SYSTEM SAFETY

AMSC N/A

AREA SAFT

FOREWORD

1. This standard is approved for use by all Departments and Agencies within the Department of Defense (DoD).

2. The DoD is committed to protecting: private and public personnel from accidental death, injury, or occupational illness; weapon systems, equipment, material, and facilities from accidental destruction or damage; and public property while executing its mission of national defense. Within mission requirements, the DoD will also ensure that the quality of the environment is protected to the maximum extent practical. The DoD has implemented environmental, safety, and health efforts to meet these objectives. Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations. A key objective of the DoD system safety approach is to include mishap risk management consistent with mission requirements, in technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation. The DoD goal is zero mishaps.

3. This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified mishap risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority, and compliant with federal laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. Residual mishap risk associated with an individual system must be reported to and accepted by the appropriate authority as defined in DoD Regulation 5000.2-R. When MIL-STD-882 is required in a solicitation or contract and no specific references are included, then only those requirements presented in section 4 are applicable.

4. This revision applies the tenets of acquisition reform to system safety in Government procurement. A joint Government/Industrial process team oversaw this revision. The Government Electronic and Information Technology Association (GEIA), G-48 committee on system safety represented industry on the process action team. System safety information (e.g., system safety tasks, commonly used approaches, etc.) associated with previous versions of this standard are in the *Defense Acquisition Deskbook* (see 6.8). This standard practice is no longer the source for any safety-related data item descriptions (DIDs).

5. Address beneficial comments (recommendations, additions, and deletions) and any pertinent information that may be of use in improving this document to: HQ Air Force Materiel Command (SES), 4375 Chidlaw Road, Wright-Patterson AFB, OH 45433-5006. Use the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter or electronic mail.

CONTENTS

PARAGRAPH PAGE

FOREWORD ii

1. SCOPE 1
1.1 Scope 1

2. APPLICABLE DOCUMENTS 1

3. DEFINITIONS 1
3.1 Acronyms used in this standard 1
3.2 Definitions 1
3.2.1 Acquisition program 1
3.2.2 Developer 1
3.2.3 Hazard 1
3.2.4 Hazardous material 1
3.2.5 Life cycle 2
3.2.6 Mishap 2
3.2.7 Mishap risk 2
3.2.8 Program manager 2
3.2.9 Residual mishap risk 2
3.2.10 Safety 2
3.2.11 Subsystem 2
3.2.12 System 2
3.2.13 System safety 2
3.2.14 System safety engineering 2

4. GENERAL REQUIREMENTS 3
4.1 Documentation of the system safety approach 3
4.2 Identification of hazards 3
4.3 Assessment of mishap risk 3
4.4 Identification of mishap risk mitigation measures 4
4.5 Reduction of mishap risk to an acceptable level 4
4.6 Verification of mishap risk reduction 4
4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority 4
4.8 Tracking of hazards and residual mishap risk 4

5. DETAILED REQUIREMENTS 4

6. NOTES 5
6.1 Intended use 5
6.2 Data requirements 5
6.3 Subject term (key words) listing 5

6.4 Definitions used in this standard 6
6.5 International standardization agreements 6
6.6 Explosive hazard classification and characteristic data 6
6.7 Use of system safety data in certification and other specialized safety approvals .. 6
6.8 DoD acquisition practices 7
6.9 Identification of changes 7

APPENDIXES
A Guidance for implementation of system safety efforts 8

CONCLUDING MATERIAL 26

TABLES

TABLE PAGE
A-I. Suggested mishap severity categories 18
A-II. Suggested mishap probability levels 19
A-III. Example mishap risk assessment values 20
A-IV. Example mishap risk categories and mishap risk acceptance levels 20

1. SCOPE

1.1 Scope. This document outlines a standard practice for conducting system safety.

The system safety practice as defined herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. When requiring MIL-STD-882 in a solicitation or contract and no specific paragraphs of this standard are identified, then apply only those requirements presented in section 4.

2. APPLICABLE DOCUMENTS

Sections 3, 4, and 5 of this standard contain no applicable documents. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples.

3. DEFINITIONS

3.1 Acronyms used in this standard. The acronyms used in this standard are defined as follows:

a.	AMSDL	Acquisition Management System & Data Requirement List
b.	ANSI	American National Standard Institute
c.	DID	Data Item Description
d.	DoD	Department of Defense
e.	ESH	Environmental, Safety, and Health
f.	GEIA	Government Electronic & Information Technology Association
g.	MAIS	Major Automated Information System
h.	MDAP	Major Defense Acquisition Program
i.	USAF	United States Air Force

3.2 Definitions. Within this document, the following definitions apply (see 6.4):

3.2.1 Acquisition program. A directed, funded effort designed to provide a new, improved, or continuing system in response to a validated operational need.

3.2.2 Developer. The individual or organization assigned responsibility for a development effort. Developers can be either internal to the government or contractors.

3.2.3 Hazard. Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

3.2.4 Hazardous material. Any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage.

3.2.5 Life cycle. All phases of the system's life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.

3.2.6 Mishap. An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.7 Mishap risk. An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

3.2.8 Program Manager (PM). A government official who is responsible for managing an acquisition program. Also, a general term of reference to those organizations directed by individual managers, exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated systems. This term will normally be used in lieu of any other titles, e.g.; system support manager, weapon program manager, system manager, and project manager.

3.2.9 Residual mishap risk. The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence (see 4.4).

3.2.10 Safety. Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.11 Subsystem. A grouping of items satisfying a logical group of functions within a particular system.

3.2.12 System. An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

3.2.13 System safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

3.2.14 System safety engineering. An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

4. GENERAL REQUIREMENTS

This section defines the system safety requirements to perform throughout the life cycle for any system, new development, upgrade, modification, resolution of deficiencies, or technology development. When properly applied, these requirements should ensure the identification and understanding of all known hazards and their associated risks; and mishap risk eliminated or reduced to acceptable levels. The objective of system safety is to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management. This document delineates the minimum mandatory requirements for an acceptable system safety program for any DoD system. When MIL-STD-882 is required in a solicitation or contract, but no specific references are included, then only the requirements in this section are applicable. System safety requirements consist of the following:

4.1 Documentation of the system safety approach. Document the developer's and program manager's approved system safety engineering approach. This documentation shall:

a. Describe the program's implementation using the requirements herein. Include identification of each hazard analysis and mishap risk assessment process used.

b. Include information on system safety integration into the overall program structure.

c. Define how hazards and residual mishap risk are communicated to and accepted by the appropriate risk acceptance authority (see 4.7) and how hazards and residual mishap risk will be tracked (see 4.8).

4.2 Identification of hazards. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application. Consider and use historical hazard and mishap data, including lessons learned from other systems. Identification of hazards is a responsibility of all program members. During hazard identification, consider hazards that could occur over the system life cycle.

4.3 Assessment of mishap risk. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential negative impact of the hazard on personnel, facilities, equipment, operations, the public, and the environment, as well as on the system itself. The tables in Appendix A are to be used unless otherwise specified.

4.4 Identification of mishap risk mitigation measures. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority. The system safety design order of precedence for mitigating identified hazards is:

a. Eliminate hazards through design selection. If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection.

b. Incorporate safety devices. If unable to eliminate the hazard through design selection, reduce the mishap risk to an acceptable level using protective safety features or devices.

c. Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.

d. Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid using warning, caution, or other written advisory as the only risk reduction method.

4.5 Reduction of mishap risk to an acceptable level. Reduce the mishap risk through a mitigation approach mutually agreed to by both the developer and the program manager. Communicate residual mishap risk and hazards to the associated test effort for verification.

4.6 Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. Report all new hazards identified during testing to the program manager and the developer.

4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. Unless otherwise specified, the suggested tables A-I through A-III of the appendix will be used to rank residual risk. The program manager shall ensure that remaining hazards and residual mishap risk are reviewed and accepted by the appropriate risk acceptance authority (ref. table A-IV). The appropriate risk acceptance authority will include the system user in the mishap risk review. The appropriate risk acceptance authority shall formally acknowledge and document acceptance of hazards and residual mishap risk.

4.8 Tracking of hazards, their closures, and residual mishap risk. Track hazards, their closure actions, and the residual mishap risk. Maintain a tracking system that includes hazards, their closure actions, and residual mishap risk throughout the system life cycle. The program manager shall keep the system user advised of the hazards and residual mishap risk.

5. DETAILED REQUIREMENTS

Program managers shall identify in the solicitation and system specification any specific system safety engineering requirements including risk assessment and acceptance, unique classifications and certifications (see 6.6 and 6.7), or any mishap reduction needs unique to their program. Additional information in developing program specific requirements is located in Appendix A.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use. This standard establishes a common basis for expectations of a properly executed system safety effort.

6.2 Data requirements. Hazard analysis data may be obtained from contracted sources by citing DI-MISC-80508, Technical Report - Study/Services. When it is necessary to obtain data, list the applicable Data Item Descriptions (DIDs) on the Contract Data Requirements List (DD Form 1423), except where the DoD Federal Acquisition Regulation Supplement exempts the requirement for a DD Form 1423. The developer and the program manager are encouraged to negotiate access to internal development data when hard copies are not necessary. They are also encouraged to request that any type of safety plan required to be provided by the contractor, be submitted with the proposal. It is further requested that any of the below listed data items be condensed into the statement of work and the resulting data delivered in one general type scientific report.

Current DIDs, that may be applicable to a system safety effort (check DoD 5010.12-L, Acquisition Management Systems and Data Requirements Control List (AMSDL) for the most current version before using), include:

DID Number	DID Title
DI-MISC-80043	Ammunition Data Card
DI-SAFT-80101	System Safety Hazard Analysis Report
DI-SAFT-80102	Safety Assessment Report
DI-SAFT-80103	Engineering Change Proposal System Safety Report
DI-SAFT-80104	Waiver or Deviation System Safety Report
DI-SAFT-80105	System Safety Program Progress Report
DI-SAFT-80106	Occupational Health Hazard Assessment
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-MISC-80508	Technical Report - Study Services
DI SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-ADMN-81250	Conference Minutes
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-ILSS-81495	Failure Mode, Effects, Criticality Analysis Report

6.3 Subject term (key word) listing.

Environmental
Hazard
Mishap
Mishap probability levels
Mishap risk
Mishap severity categories
Occupational Health
Residual mishap risk
System safety engineering

6.4 Definitions used in this standard. The definitions at 3.2 may be different from those used in other specialty areas. One must carefully check the specific definition of a term in question for its area of origination before applying the approach described in this document.

6.5 International standardization agreements. Certain provisions of this standard are the subject of international standardization agreements (AIR STD 20/23B, *Safety Design Requirements for Airborne Dispenser Weapons*, and STANAG No. 3786, *Safety Design Requirements for Airborne Dispenser Weapons*). When proposing amendment, revision, or cancellation of this standard that might modify the international agreement concerned, the preparing activity will take appropriate action through international standardization channels, including departmental standardization offices, to change the agreement or make other appropriate accommodations.

6.6 Explosive hazard classification and characteristic data. Any new or modified item of munitions or of an explosive nature that will be transported to or stored at a DoD installation or facility must first obtain an interim or final explosive hazard classification. The system safety effort should provide the data necessary for the program manager to obtain the necessary classification(s). These data should include identification of safety hazards involved in handling, shipping, and storage related to production, use, and disposal of the item.

6.7 Use of system safety data in certification and other specialized safety approvals. Hazard analyses are often required for many related certifications and specialized reviews. Examples of activities requiring data generated during a system safety effort include:

a. Federal Aviation Agency airworthiness certification of designs and modifications
b. DoD airworthiness determination
c. Nuclear and non-nuclear munitions certification
d. Flight readiness reviews
e. Flight test safety review board reviews
f. Nuclear Regulatory Commission licensing
g. Department of Energy certification

Special safety-related approval authorities include USAF Radioisotope Committee, Weapon System Explosive Safety Review Board (Navy), Non-Nuclear Weapons and Explosives Safety Board (NNWESB), Army Fuze Safety Review Board, Triservice Laser Safety Review

Board, and the DoD Explosive Safety Board. Acquisition agencies should ensure that appropriate service safety agency approvals are obtained prior to use of new or modified weapons systems in an operational or test environment.

6.8 DoD acquisition practices. Information on DoD acquisition practices is presented in the *Defense Acquisition Deskbook* available from the Deskbook Joint Program Office, Wright-Patterson Air Force Base, Ohio. Nothing in the referenced information is considered additive to the requirements provided in this standard.

6.9 Identification of changes. Due to the extent of the changes, marginal notations are not used in this revision to identify changes with respect to the previous issue.

GUIDANCE FOR IMPLEMENTATION OF A SYSTEM SAFETY EFFORT

A.1 SCOPE

A.1.1 Scope. This appendix provides rationale and guidance to fit the needs of most system safety efforts. It includes further explanation of the effort and activities available to meet the requirements described in section 4 of this standard. This appendix is not a mandatory part of this standard and is not to be included in solicitations by reference. However, program managers may extract portions of this appendix for inclusion in requirement documents and solicitations.

A.2 APPLICABLE DOCUMENTS

A.2.1 General. The documents listed in this section are referenced in sections A.3, A.4, and A.5. This section does not include documents cited in other sections of this appendix or recommended for additional information or as examples.

A.2.2 Government documents.

A.2.2.1 Specifications, standards, and handbooks. This section is not applicable to this appendix.

A.2.2.2 Other Government documents, drawings, and publications. The following other Government document forms a part of this document to the extent specified herein. Unless otherwise specified, the issue is that cited in the solicitation.

DoD 5000.2-R	Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs

(Copies of DoD 5000.2-R are available from the Washington Headquarters Services, Directives and Records Branch (Directives Section), Washington, DC or from the DoD Acquisition Deskbook).

A.2.3 Non-Government publications. This section is not applicable to this appendix.

A.2.4 Order of precedence. Since this appendix is not mandatory, in event of a conflict between the text of this appendix and the reference cited herein, the text of the reference takes precedence. Nothing in this appendix supersedes applicable laws and regulations unless a specific exemption has been obtained.

A.3 DEFINITIONS

A.3.1 Acronyms used in this appendix. No additional acronyms are used in this appendix.

A.3.2 Definitions. Additional definitions that apply to this appendix:

A.3.2.1 Development agreement. The formal documentation of the agreed-upon tasks that the developer will execute for the program manager. For a commercial developer, this agreement usually is in the form of a written contract.

A.3.2.2 Fail-safe. A design feature that ensures the system remains safe, or in the event of a failure, causes the system to revert to a state that will not cause a mishap.

A.3.2.3 Health hazard assessment. The application of biomedical knowledge and principles to identify and eliminate or control health hazards associated with systems in direct support of the life-cycle management of materiel items.

A.3.2.4 Mishap probability. The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap.

A.3.2.5 Mishap probability levels. An arbitrary categorization that provides a qualitative measure of the most reasonable likelihood of occurrence of a mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.6 Mishap risk assessment. The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

A.3.2.7 Mishap risk categories. An arbitrary categorization of mishap risk assessment values often used to generate specific action such as mandatory reporting of certain hazards to management for action, or formal acceptance of the associated mishap risk.

A.3.2.8 Mishap severity. An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard.

A.3.2.9 Mishap severity category. An arbitrary categorization that provides a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.10 Safety critical. A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component).

A.3.2.11 System safety management. All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the development, test, acquisition, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities.

A.4 GENERAL REQUIREMENTS

A.4.1 General. System safety applies engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle. It draws upon professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the environmental, safety, and health mishap risk associated with a system. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given. The program manager and the developer must apply this emphasis during all phases of the system's life cycle. A safe design is a prerequisite for safe operations, with the goal being to produce an inherently safe product that will have the minimum safety-imposed operational restrictions.

A.4.1.1 System safety in environmental and health hazard management. DoD 5000.2-R has directed the integration of environmental, safety, and health hazard management into the systems engineering process. While environmental and health hazard management are normally associated with the application of statutory direction and requirements, the management of mishap risk associated with actual environmental and health hazards is directly addressed by the system safety approach. Therefore, environmental and health hazards can be analyzed and managed with the same tools as any other hazard, whether they affect equipment, the environment, or personnel.

A.4.2 Purpose (see 1.1). All DoD program managers shall establish and execute programs that manage the probability and severity of all hazards for their systems (DoD 5000.2-R). Provision for system safety requirements and effort as defined by this standard should be included in all applicable contracts negotiated by DoD. These contracts include those negotiated within each DoD agency, by one DoD agency for another, and by DoD for other Government agencies. In addition, each DoD in-house program will address system safety.

A.4.2.1 Solicitations and contracts. Apply the requirements of section 4 to acquisitions. Incorporate MIL-STD-882 in the list of contractual compliance documents, and include the potential of a developer to execute section 4 requirements as source selection evaluation criteria. Developers are encouraged to submit with their proposal a preliminary plan that describes the system safety effort required for the requested program. When directed by the program manager, attach this preliminary plan to the contract or reference it within the statement of work; so it becomes the basis for a contractual system safety program.

A.4.3 System safety planning. Before formally documenting the system safety approach, the program manager, in concert with systems engineering and associated system safety

professionals, must determine what system safety effort is necessary to meet program and regulatory requirements. This effort will be built around the requirements set forth in section 4 and includes developing a planned approach for safety task accomplishment, providing qualified people to accomplish the tasks, establishing the authority for implementing the safety tasks through all levels of management, and allocating appropriate resources to ensure that the safety tasks are completed.

A.4.3.1 System safety planning subtasks. System safety planning subtasks should:

a. Establish specific safety performance requirements (see A.4.3.2) based on overall program requirements and system user inputs.

b. Establish a system safety organization or function and the required lines of communication with associated organizations (government and contractor). Establish interfaces between system safety and other functional elements of the program, as well as with other safety and engineering disciplines (such as nuclear, range, explosive, chemical, and biological). Designate the organizational unit responsible for executing each safety task. Establish the authority for resolution of identified hazards.

c. Establish system safety milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

d. Establish an incident alerting/notification, investigation, and reporting process, to include notification of the program manager.

e. Establish an acceptable level of mishap risk, mishap probability and severity thresholds, and documentation requirements (including but not limited to hazards and residual mishap risk).

f. Establish an approach and methodology for reporting to the program manager the following minimum information:

(1) Safety critical characteristics and features.

(2) Operating, maintenance, and overhaul safety requirements.

(3) Measures used to eliminate or mitigate hazards.

(4) Acquisition management of hazardous materials.

g. Establish the method for the formal acceptance and documenting of residual mishap risks and the associated hazards.

h. Establish the method for communicating hazards, the associated risks, and residual mishap risk to the system user.

i. Specify requirements for other specialized safety approvals (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) as necessary (reference 6.6 and 6.7).

A.4.3.2 Safety performance requirements. These are the general safety requirements needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate them into the system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of: a hazard category developed through a mishap risk assessment matrix; an overall system mishap rate; demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable mishap risk assessment procedures. Listed below are examples of safety performance statements.

a. Quantitative requirements. Quantitative requirements are usually expressed as a failure or mishap rate, such as "The catastrophic system mishap rate shall not exceed x.xx X 10^{-y} per operational hour."

b. Mishap risk requirements. Mishap risk requirements could be expressed as "No hazards assigned a Catastrophic mishap severity are acceptable." Mishap risk requirements could also be expressed as a level defined by a mishap risk assessment (see A.4.4.3.2.3), such as "No Category 3 or higher mishap risks are acceptable."

c. Standardization requirements. Standardization requirements are expressed relative to a known standard that is relevant to the system being developed. Examples include: "The system will comply with the laws of the State of XXXXX and be operable on the highways of the State of XXXXX" or "The system will be designed to meet ANSI Std XXX as a minimum."

A.4.3.3 Safety design requirements. The program manager, in concert with the chief engineer and utilizing systems engineering and associated system safety professionals, should establish specific safety design requirements for the overall system. The objective of safety design requirements is to achieve acceptable mishap risk through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources. Review these for safety design parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. Expand these requirements and criteria for inclusion in the associated follow-on or lower level specifications. See general safety system design requirements below.

a. Hazardous material use is minimized, eliminated, or associated mishap risks are reduced through design, including material selection or substitution. When using potentially hazardous materials, select those materials that pose the least risk throughout the life cycle of the system.

b. Hazardous substances, components, and operations are isolated from other activities, areas, personnel, and incompatible materials.

c. Equipment is located so that access during operations, servicing, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous substances, high voltage, electromagnetic radiation, and cutting and puncturing surfaces).

d. Protect power sources, controls, and critical components of redundant subsystems by physical separation or shielding, or by other acceptable methods.

f. Consider safety devices that will minimize mishap risk (e.g., interlocks, redundancy, fail safe design, system protection, fire suppression, and protective measures such as clothing, equipment, devices, and procedures) for hazards that cannot be eliminated. Make provisions for periodic functional checks of safety devices when applicable.

g. System disposal (including explosive ordnance disposal) and demilitarization are considered in the design.

h. Implement warning signals to minimize the probability of incorrect personnel reaction to those signals, and standardize within like types of systems.

i. Provide warning and cautionary notes in assembly, operation, and maintenance instructions; and provide distinctive markings on hazardous components, equipment, and facilities to ensure personnel and equipment protection when no alternate design approach can eliminate a hazard. Use standard warning and cautionary notations where multiple applications occur. Standardize notations in accordance with commonly accepted commercial practice or, if none exists, normal military procedures. Do not use warning, caution, or other written advisory as the only risk reduction method for hazards assigned to Catastrophic or Critical mishap severity categories.

j. Safety critical tasks may require personnel proficiency; if so, the developer should propose a proficiency certification process to be used.

k. Severity of injury or damage to equipment or the environment as a result of a mishap is minimized.

l. Inadequate or overly restrictive requirements regarding safety are not included in the system specification.

m. Acceptable risk is achieved in implementing new technology, materials, or designs in an item's production, test, and operation. Changes to design, configuration, production, or mission requirements (including any resulting system modifications and upgrades, retrofits, insertions of new technologies or materials, or use of new production or test techniques) are accomplished in a manner that maintains an acceptable level of mishap risk. Changes to the environment in which the system operates are analyzed to identify and mitigate any resulting hazards or changes in mishap risks.

A.4.3.3.1 Some program managers include the following conditions in their solicitation, system specification, or contract as requirements for the system design. These condition statements are used optionally as supplemental requirements based on specific program needs.

A.4.3.3.1.1 Unacceptable conditions. The following safety critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the mishap risk associated with these situations to a level acceptable to the program manager.

a. Single component failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical mishap severity catagories.

b. Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of Catastrophic or Critical mishap severity catagories.

c. Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

d. Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.

e. Hazard categories that are specified as unacceptable in the development agreement.

A.4.3.3.1.2 Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigating actions are implemented and verified.

a. For non-safety critical command and control functions: a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

b. For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors.

c. System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.

d. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

e. System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

f. System designs that provide an approved safety factor, or a fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

g. System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).

h. System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin.

i. System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction has been provided.

j. System designs that limit or control the use of hazardous materials.

A.4.3.4 Elements of an effective system safety effort. Elements of an effective system safety effort include:

a. Management is always aware of the mishap risks associated with the system, and formally documents this awareness. Hazards associated with the system are identified, assessed, tracked, monitored, and the associated risks are either eliminated or controlled to an acceptable level throughout the life cycle. Identify and archive those actions taken to eliminate or reduce mishap risk for tracking and lessons learned purposes.

b. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

c. Environmental protection, safety, and occupational health, consistent with mission requirements, are designed into the system in a timely, cost-effective manner. Inclusion of the appropriate safety features is accomplished during the applicable phases of the system life cycle.

d. Mishap risk resulting from harmful environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration) and human error in system operation and support is minimized.

e. System users are kept abreast of the safety of the system and included in the safety decision process.

A.4.4 System safety engineering effort. As stated in section 4, a system safety engineering effort consists of eight main requirements. The following paragraphs provide further descriptions on what efforts are typically expected due to each of the system safety requirements listed in section 4.

A.4.4.1 Documentation of the system safety approach. The documentation of the system safety approach should describe the planned tasks and activities of system safety management

and system engineering required to identify, evaluate, and eliminate or control hazards, or to reduce the residual mishap risk to a level acceptable throughout the system life cycle. The documentation should describe, as a minimum, the four elements of an effective system safety effort: a planned approach for task accomplishment, qualified people to accomplish tasks, the authority to implement tasks through all levels of management, and the appropriate commitment of resources (both manning and funding) to ensure that safety tasks are completed. Specifically, the documentation should:

a. Describe the scope of the overall system program and the related system safety effort. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.

b. Describe the safety tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety and reference where they are specified or described. Include the organizational relationships between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization including the review and approval authority of those tasks.

c. Describe specific analysis techniques and formats to be used in qualitative or quantitative assessments of hazards, their causes, and effects.

d. Describe the process through which management decisions will be made (for example, timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, and program deviations). Include a description on how residual mishap risk is formally accepted and this acceptance is documented.

e. Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability levels, and the system safety design order of precedence that should be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for mishap risk assessment including a description of the acceptable and unacceptable risk levels (if applicable). Include system safety definitions that modify, deviate from, or are in addition to those in this standard or generally accepted by the system safety community (see *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook)* (see A.6.1).

f. Describe how resolution and action relative to system safety will be implemented at the program management level possessing resolution authority.

g. Describe the verification (e.g., test, analysis, demonstration, or inspection) requirements for ensuring that safety is adequately attained. Identify any certification requirements for software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).

h. Describe the mishap or incident notification, investigation, and reporting process for the program, including notification of the program manager.

i. Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned data. Include a description on how a system hazard log is developed and kept current (see A.4.4.8.1).

j. Describe how the user is kept abreast of residual mishap risk and the associated hazards.

A.4.4.2 Identification of hazards. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended usage or application. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

A.4.4.2.1 Approaches for identifying hazards. Numerous approaches have been developed and used to identify system hazards. A key aspect of many of these approaches is empowering the design engineer with the authority to design safe systems and the responsibility to identify to program management the hazards associated with the design. Hazard identification approaches often include using system users in the effort. Commonly used approaches for identifying hazards can be found in the *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook* (see A.6.1)

A.4.4.3 Assessment of mishap risk. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential impact of the hazard on personnel, facilities, equipment, operations, the public, or environment, as well as on the system itself. Other factors, such as numbers of persons exposed, may also be used to assess risk.

A.4.4.3.1 Mishap risk assessment tools. To determine what actions to take to eliminate or control identified hazards, a system of determining the level of mishap risk involved must be developed. A good mishap risk assessment tool will enable decision makers to properly understand the level of mishap risk involved, relative to what it will cost in schedule and dollars to reduce that mishap risk to an acceptable level.

A.4.4.3.2 Tool development. The key to developing most mishap risk assessment tools is the characterization of mishap risks by mishap severity and mishap probability. Since the highest system safety design order of precedence is to eliminate hazards by design, a mishap risk assessment procedure considering only mishap severity will generally suffice during the early design phase to minimize the system's mishap risks (for example, just don't use hazardous or toxic material in the design). When all hazards cannot be eliminated during the early design phase, a mishap risk assessment procedure based upon the mishap probability as well as the mishap severity provides a resultant mishap risk assessment. The assessment is used to establish priorities for corrective action, resolution of identified hazards, and notification to management of the mishap risks. The information provided here is a suggested tool and set of definitions that can be used. Program managers can develop tools and definitions appropriate to their individual programs.

A.4.4.3.2.1 Mishap severity. Mishap severity categories are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table A-I. The dollar values shown in this table should be established on a system by system basis depending on the size of the system being considered to reflect the level of concern.

TABLE A-I. **Suggested mishap severity categories.**

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

NOTE: These mishap severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the program manager and the developer as to the meaning of the terms used in the category definitions. Other risk assessment techniques may be used provided that the user approves them.

A.4.4.3.2.2 Mishap probability. Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be

derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table A-II.

TABLE A-II. **Suggested mishap probability levels.**

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

*Definitions of descriptive words may have to be modified based on quantity of items involved.
**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

A.4.4.3.2.3 Mishap risk assessment. Mishap risk classification by mishap severity and mishap probability can be performed by using a mishap risk assessment matrix. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is then often used to rank different hazards as to their associated mishap risks. An example of a mishap risk assessment matrix is shown at Table A-III.

TABLE A-III. **Example mishap risk assessment values.**

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

A.4.4.3.2.4 Mishap risk categories. Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table A-IV includes an example listing of mishap risk categories and the associated assessment values. In the example, the system management has determined that mishap risk assessment values 1 through 5 constitute "High" risk while values 6 through 9 constitute "Serious" risk.

TABLE A-IV. **Example mishap risk categories and mishap risk acceptance levels.**

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

*Representative mishap risk acceptance levels are shown in the above table. Mishap risk acceptance is discussed in paragraph A.4.4.7. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

A.4.4.3.2.5 Mishap risk impact. The mishap risk impact is assessed, as necessary, using other factors to discriminate between hazards having the same mishap risk value. One might discriminate between hazards with the same mishap risk assessment value in terms of mission capabilities, or social, economic, and political factors. Program management will closely consult with the using organization on the decisions used to prioritize resulting actions.

A.4.4.3.3 Mishap risk assessment approaches. Commonly used approaches for assessing mishap risk can be found in the *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook* (see A.6.1)

A.4.4.4 Identification of mishap risk mitigation measures. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority.

A.4.4.4.1 Prioritize hazards for corrective action. Hazards should be prioritized so that corrective action efforts can be focused on the most serious hazards first. A categorization of hazards may be conducted according to the mishap risk potential they present.

A.4.4.4.2 System safety design order of precedence (see 4.4). The ultimate goal of a system safety program is to design systems that contain no hazards. However, since the nature of most complex systems makes it impossible or impractical to design them completely hazard-free, a successful system safety program often provides a system design where there exist no hazards resulting in an unacceptable level of mishap risk. As hazard analyses are performed, hazards will be identified that will require resolution. The system safety design order of precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk are evaluated so that an acceptable method for mishap risk reduction can be agreed to.

A.4.4.5 Reduction of mishap risk to an acceptable level. Reduce the system mishap risk through a mitigation approach mutually agreed to by the developer, program manager and the using organization.

A.4.4.5.1 Communication with associated test efforts. Residual mishap risk and associated hazards must be communicated to the system test efforts for verification.

A.4.4.6 Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. The program manager must ensure that the selected mitigation approaches will result in the expected residual mishap risk. To provide this assurance, the system test effort should verify the performance of the mitigation actions. New hazards identified during testing must be reported to the program manager and the developer.

A.4.4.6.1 Testing for a safe design. Tests and demonstrations must be defined to validate selected safety features of the system. Test or demonstrate safety critical equipment and procedures to determine the mishap severity or to establish the margin of safety of the design. Consider induced or simulated failures to demonstrate the failure mode and acceptability of safety critical equipment. When it cannot be analytically determined whether the corrective action taken will adequately control a hazard, conduct safety tests to evaluate the effectiveness of the controls. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation. Integrate testing of safety systems into appropriate system test and demonstration plans to the maximum extent possible.

A.4.4.6.2 Conducting safe testing. The program manager must ensure that test teams are familiar with mishap risks of the system. Test plans, procedures, and test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation should be reviewed to ensure that:

a. Safety is adequately demonstrated.

b. The testing will be conducted in a safe manner.

c. All additional hazards introduced by testing procedures, instrumentation, test hardware, and test environment are properly identified and controlled.

A.4.4.6.3 Communication of new hazards identified during testing. Testing organizations must ensure that hazards and safety discrepancies discovered during testing are communicated to the program manager and the developer.

A.4.4.7 Review and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. For long duration programs, incremental or periodic reporting should be used.

A.4.4.7.1 Residual mishap risk. The mishap risk that remains after all planned mishap risk management measures have been implemented is considered residual mishap risk. Residual mishap risk is documented along with the reason(s) for incomplete mitigation.

A.4.4.7.2 Residual mishap risk management. The program manager must know what residual mishap risk exists in the system being acquired. For significant mishap risks, the program manager is required to elevate reporting of residual mishap risk to higher levels of appropriate authority (such as the Program Executive Officer or Component Acquisition Executive) for action or acceptance. The program manager is encouraged to apply additional resources or other remedies to help the developer satisfactorily resolve hazards providing significant mishap risk. Table A-IV includes an example of a mishap risk acceptance level matrix based on the mishap risk assessment value and mishap risk category.

A.4.4.7.3 Residual mishap risk acceptance. The program manager is responsible for formally documenting the acceptance of the residual mishap risk of the system by the appropriate authority. The program manager should update this residual mishap risk and the associated hazards to reflect changes/modifications in the system or its use. The program manager and using organization should jointly determine the updated residual mishap risk prior to acceptance of the risk and system hazards by the risk acceptance authority, and should document the agreement between the user and the risk acceptance authority.

A.4.4.8 Tracking hazards and residual mishap risk. Track hazards, their closures, and residual mishap risk. A tracking system for hazards, their closures, and residual mishap risk must be maintained throughout the system life cycle. The program manager must keep the system user apprised of system hazards and residual mishap risk.

A.4.4.8.1 Process for tracking of hazards and residual mishap risk. Each system must have a current log of identified hazards and residual mishap risk, including an assessment of the residual mishap risk (see A.4.4.7). As changes are integrated into the system, this log is updated to incorporate added or changed hazards and the associated residual mishap risk. The Government must formally acknowledge acceptance of system hazards and residual mishap risk. Users will be kept informed of hazards and residual mishap risk associated with their systems.

A.4.4.8.1.1 Developer responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The developer (see 3.2.2) is responsible for communicating information to the program manager on system hazards and residual mishap risk, including any unusual consequences and costs associated with hazard mitigation. After attempting to eliminate or mitigate system hazards, the developer will formally document and notify the program manager of all hazards breaching thresholds set in the safety design criteria. At the same time, the developer will also communicate the system residual mishap risk.

A.4.4.8.1.2 Program manager responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The program manager is responsible for maintaining a log of all identified hazards and residual mishap risk for the system. The program manager will communicate known hazards and associated risks of the system to all system developers and users. As changes are integrated into the system, the program manager shall update this log to incorporate added or changed hazards and the residual mishap risk identified by the developer. The program manager is also responsible for informing system developers about the program manager's expectations for handling of newly discovered hazards. The program manager will evaluate new hazards and the resulting residual mishap risk, and either recommend further action to mitigate the hazards, or formally document the acceptance of these hazards and residual mishap risk. The program manager will evaluate the hazards and associated residual mishap risk in close consultation and coordination with the ultimate end user, to assure that the context of the user requirements, potential mission capability, and the operational environment are adequately addressed. Copies of the documentation of the hazard and risk acceptance will be provided to both the developer and the system user. Hazards for which the program manager accepts responsibility for mitigation will also be included in the formal documentation. For example, if the program manager decides to execute a special training program to mitigate a potentially hazardous situation, this approach will be documented in the formal response to the developer. Residual mishap risk and hazards must be communicated to system test efforts for verification.

A.5 SPECIFIC REQUIREMENTS

A.5.1 Program manager responsibilities. The program manager must ensure that all types of hazards are identified, evaluated, and mitigated to a level compliant with acquisition management policy, federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. The program manager should:

A.5.1.1 Establish, plan, organize, implement, and maintain an effective system safety effort that is integrated into all life cycle phases.

A.5.1.2 Ensure that system safety planning is documented to provide all program participants with visibility into how the system safety effort is to be conducted.

A.5.1.3 Establish definitive safety requirements for the procurement, development, and sustainment of the system. The requirements should be set forth clearly in the appropriate system specifications and contractual documents.

A.5.1.4 Provide historical safety data to developers.

A.5.1.5 Monitor the developer's system safety activities and review and approve delivered data in a timely manner, if applicable, to ensure adequate performance and compliance with safety requirements.

A.5.1.6 Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

A.5.1.7 Evaluate new lessons learned for inclusion into appropriate databases and submit recommendations to the responsible organization.

A.5.1.8 Establish system safety teams to assist the program manager in developing and implementing a system safety effort.

A.5.1.9 Provide technical data on Government-furnished Equipment or Government-furnished Property to enable the developer to accomplish the defined tasks.

A.5.1.10 Document acceptance of residual mishap risk and associated hazards.

A.5.1.11 Keep the system users apprised of system hazards and residual mishap risk.

A.5.1.12 Ensure the program meets the intent of the latest MIL-STD 882.

A.5.1.13 Ensure adequate resources are available to support the program system safety effort.

A.5.1.14 Ensure system safety technical and managerial personnel are qualified and certified for the job.

A.6 NOTES

A.6.1 DoD acquisition practices and safety analysis techniques. Information on DoD acquisition practices and safety analysis techniques is available at the referenced Internet sites. Nothing in the referenced information is considered binding or additive to the requirements provided in this standard.

A.6.1.1 *Defense Acquisition Deskbook.* Wright-Patterson Air Force Base, Ohio: Deskbook Joint Program Office.

A.6.1.2 *System Safety Analysis Handbook.* Unionville, VA: System Safety Society.

CONCLUDING MATERIAL

Custodians:
Army - AV
Navy - AS
Air Force – 40

Reviewing activities:
Army - AR, AT, CR, MI
Navy - EC, OS, SA, SH
Air Force - 10, 11, 13, 19

Preparing activity:
Air Force - 40

Project SAFT - 0038

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7, and send to preparing activity.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-STD-882	2. DOCUMENT DATE (YYYYMMDD) 20000210

3. DOCUMENT TITLE
System Safety

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER		
a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include zip code)*	d. TELEPHONE *(Include Area Code)* (1) Commercial (2) DSN *(if applicable)*	7. DATE SUBMITTED *(YYYYMMDD)*

8. PREPARING ACTIVITY	
a. NAME Headquarters, Air Force Materiel Command System Safety Division	b. TELEPHONE *(Include Area Code)* (1) Commercial (937) 257-6007 (2) DSN 787-6007
b. ADDRESS *(Include Zip Code)* HQ AFMC/SES 4375 Chidlaw Road Wright Patterson AFB, Ohio 45433-5006	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Standardization Program Office (DLSC-LM) 8725 John J. Kingman Road, Suite 2533 Fort Belvoir, Virginia 22060-6621 Telephone 703 767-6888 DSN 427-6888

DD Form 1426, FEB 1999 (EG) PREVIOUS EDITION IS OBSOLETE. WHS/DIOR, Feb 99