Faculdade de Engenharia da Universidade do Porto

Análise dos Modos de Avaria de um Sistema de Alimentação de Emergência para um Centro de Informática

Maria Luísa Soares de Azevedo Vaz Matos

Dissertação realizada no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Automação

Orientador: Prof. Dr. Paulo José Lopes Machado Portugal
Co-orientador: Prof. Dr. António José de Pina Martins

Julho de 2009

Resumo

Esta dissertação pretende analisar os modos de avaria do Sistema de Alimentação de Emergência de um Centro de Informática.

A partir do conhecimento do funcionamento deste sistema e dos elementos que o constituem, fez-se uma análise de fiabilidade qualitativa recorrendo a uma Análise dos Modos e Efeitos de Avaria (FMEA). Este é um método indutivo que permite avaliar, a partir de um determinado modo de avaria, as respectivas causas e efeitos. Com estes dados, é possível fazer uma análise da criticalidade dos modos de avaria e caracterizar o seu impacto no funcionamento do sistema.

Como complemento do método supracitado, fez-se também uma análise por Árvore de Falhas. Ao contrário da Análise dos Modos e Efeitos de Avaria, este é um processo dedutivo que partindo de um evento indesejado, investiga as sucessivas combinações de falhas dos componentes até atingir as suas causas básicas.

Com os resultados obtidos, foi possível identificar os elementos mais críticos do sistema e propor medidas de redução de risco.

Abstract

This dissertation aims the failure modes analysis of a Data Center Emergency Power System.

From the knowledge of the system's functioning and the elements which constitute it, a qualitative reliability analysis was made recurring to a Failure Mode and Effects Analysis (FMEA). This is an inductive method which allows the evaluation, starting from a determined failure mode, of its causes and effects. With this information it's possible to perform a criticality analysis of the failure modes and characterize its impact on the system's functioning.

In addition to the above method, a Fault Tree Analysis was also developed. Unlike the Failure Mode and Effects Analysis, this is a deductive process which starts with an unwanted event and investigates the successive combinations of failures of a component until arriving at its basic causes.

With the obtained results, it was possible to identify the most critical elements of the system and propose measures to reduce the risk.

Agradecimentos

Aproveito para agradecer aos meus pais, irmã e amigos por todo o apoio, compreensão e carinho que me deram ao longo da vida.

Agradeço também a todas as pessoas que colaboraram neste trabalho, muito especialmente ao meu orientador, o Prof. Dr. Paulo José Lopes Machado Portugal, e co-orientador, Prof. Dr. António José de Pina Martins.

Índice

Lista de figuras

Lista de tabelas

Abreviaturas e Símbolos

ALARP	As Low As Reasonably Practicable
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FTA	Fault Tree Analysis
MT	Média Tensão
NASA	National Aeronautics and Space Administration
PT	Posto de Transformação
QGBT	Quadro Geral de Baixa Tensão
QTC	Quadro de Transferência de Cargas
RPN	Risk Priority Number
SMS	Short Message Service
UPS	Uninterruptable Power Supply

Capítulo 1

Introdução

A presente dissertação tem por tema: Análise dos Modos de Avaria de um Sistema de Alimentação de Emergência para um Centro de Informática. Trata-se de uma temática bastante actual, em virtude da crescente e justificada preocupação que todos os sectores e organismos têm com a fiabilidade e disponibilidade dos sistemas informáticos.

Neste contexto, a fiabilidade e disponibilidade assumem um papel extremamente importante. A fiabilidade está associada à continuidade de serviço, isto é, a capacidade de um sistema ou equipamento cumprir a função requerida, em condições de utilização e durante um determinado período de tempo. Já a disponibilidade relaciona-se com a capacidade de o sistema estar pronto a ser utilizado.

Um Centro de Informática é uma estrutura, composta por diversos equipamentos, que oferece recursos de processamento e armazenamento de dados em larga escala. No conjunto dos componentes de um Centro de Informática, os servidores são os elementos mais críticos, já que exigem não só uma elevada fiabilidade mas também uma elevada disponibilidade.

O processamento de dados pode ser afectado quando os servidores sofrem perturbações derivadas de falhas do sistema de alimentação. Assim, para que o Sistema de Alimentação de Emergência seja totalmente capaz de suportar estas cargas críticas do Centro de Informática e de assegurar a continuidade de serviço, deve providenciar-se a garantia de que este é fiável e capaz de actuar rapidamente.

A situação abordada neste trabalho tem a ver com a importância de garantir a disponibilidade das três Salas de Servidores - A, B e C, do Centro de Informática em estudo, no âmbito do sistema de alimentação. O objectivo deste estudo centrava-se em encontrar os pontos mais problemáticos do Sistema de Alimentação de Emergência de modo a que se pudesse elaborar um plano de acções tendente a minimizar avarias com potenciais consequências críticas no funcionamento do Centro de Informática.

Numa primeira fase, tomou-se conhecimento dos componentes existentes e procedeu-se ao estudo do funcionamento global do Sistema de Alimentação de Emergência. Nesta etapa, pretendeu-se adquirir os conhecimentos necessários para se poder investigar os modos de avaria dos componentes do sistema, assim como, as suas causas e efeitos. Posteriormente, com os dados entretanto obtidos, foi analisada a criticalidade do risco associado a cada modo de avaria. Finalmente, numa terceira e última fase, propuseram-se soluções que permitissem

a diminuição ou eliminação da ocorrência das avarias, bem como o aumento da disponibilidade do sistema e melhoraria do seu desempenho.

Atendendo aos pressupostos da análise, optou-se por uma abordagem de resolução do problema recorrendo ao uso combinado de duas metodologias qualitativas de análise de fiabilidade e disponibilidade: a Análise dos Modos e Efeitos de Avaria (FMEA) e a análise por Árvores de Falhas.

A Análise dos Modos e Efeitos de Avaria foi utilizada por ser um método que permite reconhecer e avaliar os modos de avaria de um sistema, as suas causas e consequências. Com base no estudo dos parâmetros da criticalidade, ou seja, a severidade e a ocorrência, que vão sendo associados a cada avaria e analisando os Números de Prioridade do Risco obtidos pelo produto destes dois índices, é possível detectar quais os componentes do sistema que exigem um plano de acções de mitigação do risco.

Como a Análise dos Modos e Efeitos de Avaria considera as avarias dos componentes de forma individual, não permite analisar avarias que tenham origem na combinação de eventos. Por isso, como complemento desta metodologia, optou-se por fazer, também, uma Análise por Árvore de Falhas, permitindo assim suprir esta lacuna.

O relatório desta dissertação está dividido em 7 capítulos.

No primeiro capítulo apresenta-se uma introdução do assunto tratado, com a apresentação do tema, objectivos e referência das metodologias utilizadas no seu desenvolvimento.

O segundo capítulo apresenta a descrição do Sistema de Alimentação de Emergência do Centro de Informática, abordando o seu funcionamento geral e sua constituição através da descrição dos principais elementos que o constituem e as suas funções.

No Capítulo 3 expõe-se a abordagem proposta para o desenvolvimento deste trabalho. São ainda apresentadas as duas metodologias usadas, a Análise dos Modos e Efeitos de Avaria (FMEA) e a análise por Árvores de Falhas, e é feita uma fundamentação teórica sobre os dois métodos.

No Capítulo 4 é apresentada a Análise dos Modos e Efeitos de Avaria (FMEA) do Sistema de Alimentação de Emergência do Centro de Informática. Aqui são descritas as etapas de planeamento e os critérios usados para a análise de risco. São ainda expostos alguns dos resultados obtidos e retiradas as conclusões inerentes.

No Capítulo 5 é feita a apresentação dos resultados obtidos pela análise por Árvore de Falhas com as respectivas conclusões.

No Capítulo 6 abordam-se as soluções propostas para diminuir o risco dos pontos mais críticos do Sistema de Alimentação de Emergência do Centro de Informática.

No sétimo e último capítulo, são apresentadas as conclusões a que se chegou após a realização deste trabalho.

Capítulo 2

Sistema de Alimentação de Emergência

Num Sistema de Alimentação, em especial sistemas com cargas críticas que exigem uma elevada disponibilidade, a continuidade do fornecimento de energia eléctrica deve ser sempre assegurada. Os subsistemas e/ou componentes que o constituem são, por isso, divididos em dois grupos – cargas prioritárias e cargas não prioritárias. Esta divisão é determinada de acordo com a importância inerente e pelo impacto crítico que a sua indisponibilidade provoca no sistema global. Deste modo, o fornecimento de energia dos grupos é assegurado por barramentos diferentes e as cargas prioritárias, quando há uma falha de tensão da rede, são alimentadas a partir de um Sistema de Alimentação de Emergência.

A definição de Sistema de Alimentação de Emergência pode ser dada da seguinte forma:

> "Uma fonte de energia eléctrica de reserva e independente que, após a falha ou interrupção da fonte normal, fornece automaticamente energia eléctrica fiável dentro de um de tempo específico para dispositivos e equipamentos críticos cujas falhas de operação satisfatória poderiam comprometer a saúde e segurança de pessoas ou resultar em danos na propriedade." [1]

Neste capítulo apresenta-se a constituição e funcionamento de um Sistema de Alimentação de Emergência, no âmbito do Centro de Informática em estudo.

Na primeira parte é dada uma visão geral do Sistema de Alimentação, sendo a segunda à apresentação e breve descrição dos subsistemas que o constituem.

2.1 - Funcionamento geral

Neste Centro de Informática, as cargas prioritárias são três conjuntos de servidores, dispostos em três salas distintas – Sala de Servidores A, B e C - com requisitos de disponibilidade respectivamente decrescentes.

A Figura 2.1 apresenta um diagrama simplificado do Sistema de Alimentação de Emergência do Centro de Informática.

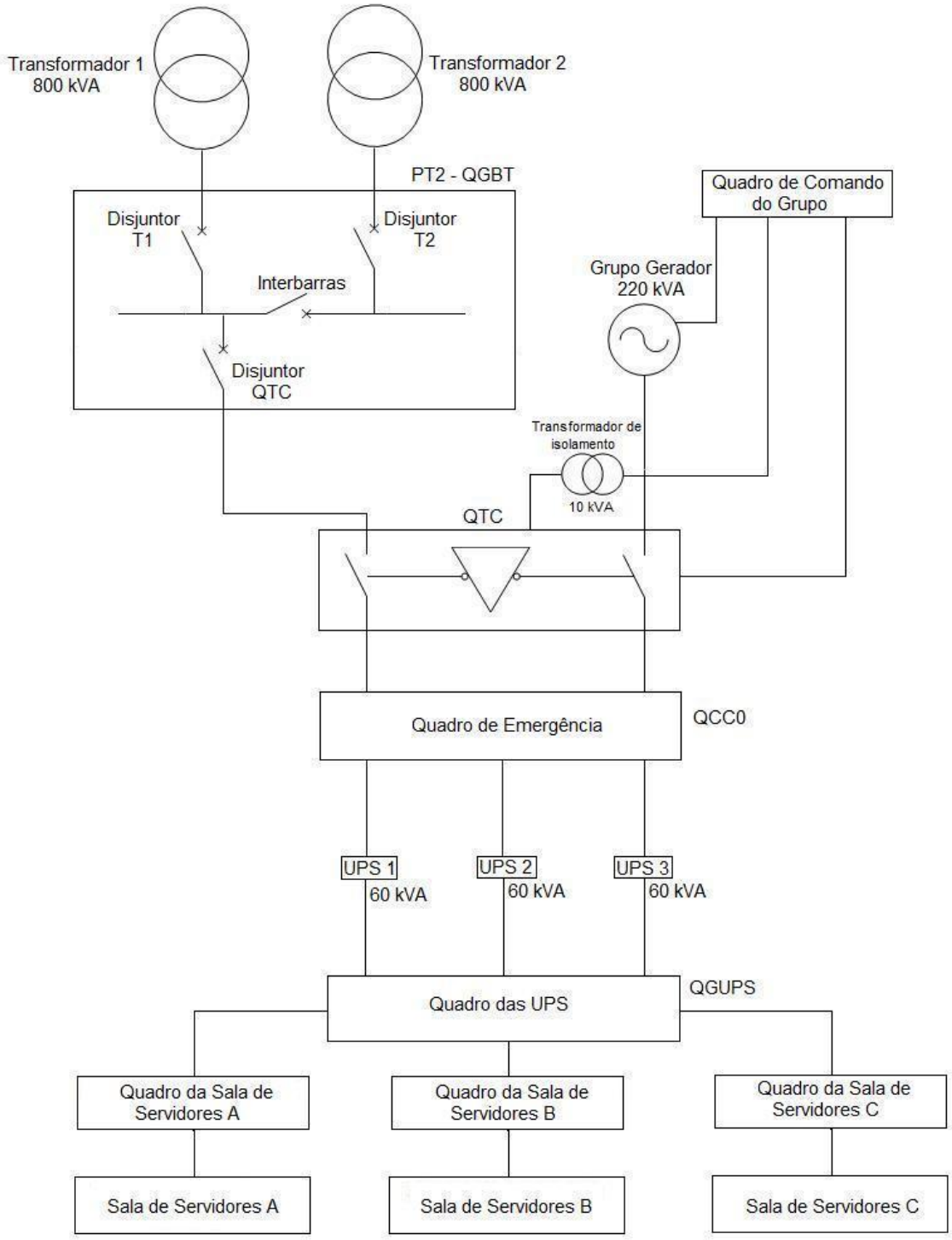


Figura 2.1 – Representação esquemática do Sistema de Alimentação de Emergência

Em funcionamento normal, quando existe tensão na rede de Média Tensão (MT), a alimentação das três salas é proveniente do Posto de Transformação (PT), mais concretamente do Transformador 1. Existe também um segundo transformador, Transformador 2, que tem por função a alimentação de outros edifícios. Normalmente, os dois transformadores não estão em paralelo para que as correntes de curto-circuito não sejam duplicadas. Só quando existe uma avaria do Transformador 1 é que os dois transformadores são, então, ligados em paralelo, de modo a garantir a continuidade da alimentação das

cargas. A comutação dos transformadores é feita de forma manual, através de um disjuntor interbarras.

Em caso de avaria dos dois transformadores ou se existir ausência de tensão da rede, o Sistema de Alimentação de Emergência activa automaticamente a sequência de ligação a um Grupo Gerador de Emergência, na rede eléctrica interna, por meio do inversor de rede do Quadro de Transferência de Cargas (QTC).

No Quadro de Transferência de Cargas é feita uma monitorização contínua do estado das tensões da rede e do Grupo Gerador. Quando detecta ausência de tensão da rede, envia um sinal para o Quadro de Comando do Grupo de forma que o gerador inicie a sua sequência de arranque.

Quando a tensão da rede voltar a ser detectada, o Quadro de Transferência de Cargas devolve as cargas para a rede eléctrica externa. O gerador é colocado fora do circuito e, após um ciclo de arrefecimento, é automaticamente desligado e colocado novamente em posição de emergência.

Durante o período de inicialização do gerador, três UPS (*Uninterruptable Power Supply*) garantem a alimentação das cargas críticas.

Num caso extremo, correspondente a um corte de energia simultâneo do Posto de Transformação e do Grupo Gerador, a alimentação do Centro de Informática é transferida para o Quadro de Emergência. As salas de servidores passam a receber tensão através das UPS, dispostas numa configuração em redundância 2+1. Isto é, para que forneçam tensão pelo menos duas delas têm de estar operacionais. A comutação entre as UPS é automática: ao sair uma UPS do circuito, uma outra, desde que operacional, substitui-a imediatamente.

O tempo de autonomia das UPS é um aspecto que não deve ser descurado. No caso do Centro de Informática, as UPS garantem, no máximo, uma autonomia do sistema de 30 minutos. Caso não seja possível efectuar a reparação da anomalia do Grupo Gerador e/ou do Posto de Transformação durante esse período de tempo, as Salas de Servidores deixam de receber tensão e o sistema fica indisponível.

2.2 – Constituição do Sistema

Nesta secção é feita a apresentação dos principais elementos do Sistema de Alimentação de Emergência e a descrição sumária das suas funções.

2.2.1 – Posto de Transformação

O Posto de Transformação é uma instalação eléctrica que tem como função reduzir de Média Tensão para Baixa Tensão (BT), o nível de tensão usualmente utilizado pelo consumidor final. Os principais elementos que o constituem são os transformadores, os órgãos de corte e protecção e o Quadro Geral de Baixa Tensão (QGBT).

Como foi referido anteriormente, o Posto de Transformação do Sistema de Alimentação de Emergência do Centro de Informática dispõe de dois transformadores, apresentados na Figura 2.2. O transformador 1, localizado no lado esquerdo, é o responsável por fornecer tensão ao Centro, enquanto o transformador 2, do lado direito, alimenta outros edifícios.

Figura 2.2 – Transformadores 1 e 2 do Posto de Transformação

Os órgãos de corte e protecção estão inseridos dentro do Quadro Geral de Baixa Tensão, ilustrado no Figura 2.3. Dentro da aparelhagem de protecção, merecem especial destaque os disjuntores de protecção dos transformadores 1 e 2 e o disjuntor do Quadro de Transferência de Cargas, referidos na Figura 2.1 como disjuntor T1, disjuntor T2, e disjuntor QTC, respectivamente.

No anexo A, é possível a consulta dos esquemas eléctricos do Quadro Geral de Baixa Tensão.

É também no interior do Quadro Geral de Baixa Tensão que se situa o Interbarras. Este disjuntor, que funciona como um órgão de seccionamento, encontra-se aberto por defeito. Ao ser fechado, coloca os dois transformadores em paralelo, permitindo assim a alimentação do Centro de Informática pelo transformador 2. Isto quando ocorre uma avaria no transformador 1. É importante referir que não existe selectividade entre os disjuntores de protecção dos transformadores e o Interbarras.

Figura 2.3 - Quadro Geral de Baixa Tensão

Na Figura 2.4 pode-se ver o disjuntor de protecção do transformador 1 e o disjuntor interbarras, respectivamente.

Figura 2.4 - Disjuntor de protecção do transformador (a) e Interbarras (b)

2.2.2 – Grupo Gerador

O Grupo Gerador, apresentado na Figura 2.5, corresponde ao conjunto do motor de combustão a Diesel e do alternador que produz a energia eléctrica.

A protecção do alternador, contra sobrecargas e curto-circuitos, é assegurada por um disjuntor de saída.

O motor é responsável pelo arranque do Grupo Gerador.

No interior do gerador, existe um sistema de refrigeração que tem como função manter a temperatura do motor, monitorizada a partir de um termóstato, dentro dos limites predefinidos.

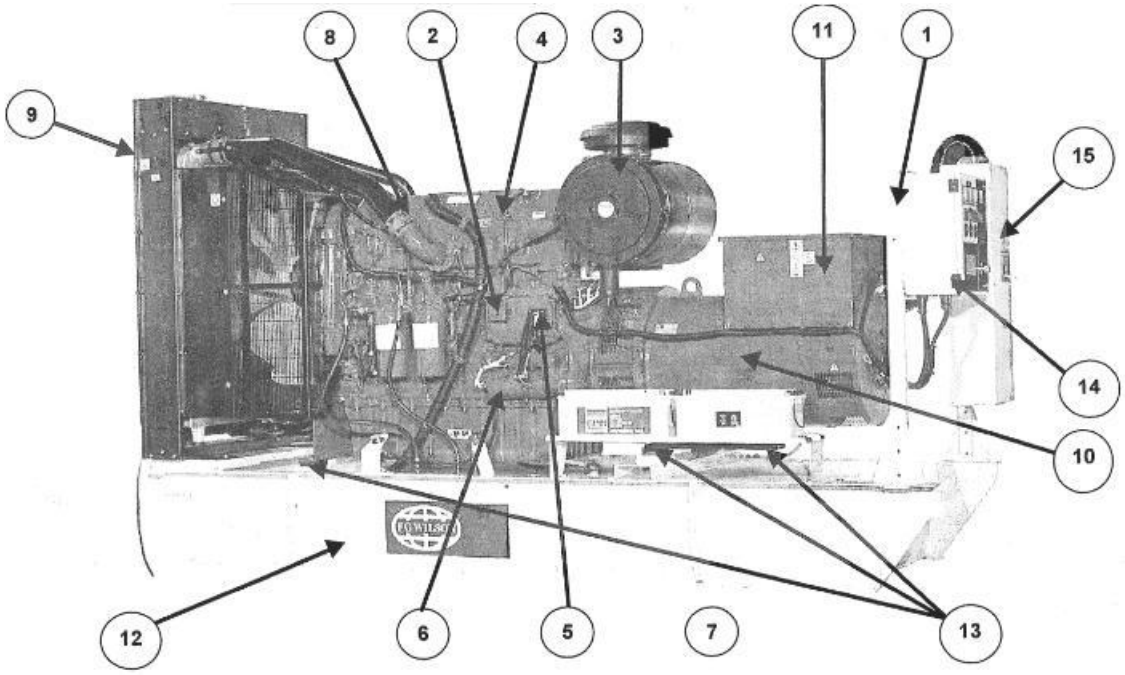
O Grupo Gerador dispõe de um Painel de Controlo corresponde ao sistema de supervisão e controlo do Quadro de Comando do Grupo. Aí são monitorizados vários parâmetros fundamentais do gerador, nomeadamente a tensão no alternador, a frequência de saída do grupo, a pressão do óleo do motor e a tensão da bateria, entre outras. Se for detectada alguma condição crítica durante o funcionamento do grupo, por exemplo, temperatura elevada do motor ou baixa pressão do óleo do motor, este painel desliga automaticamente o gerador.

Figura 2.5 – Grupo Gerador

O Painel de Controlo é um autómato que, consoante a informação que recebe do estado da rede, dá ordem de arranque ou paragem do grupo. Esta ordem pode ser efectuada de modo manual ou automático.

A alimentação do Painel de Controlo é feita a partir de uma bateria. É indispensável que esta bateria tenha sempre a tensão adequada. Caso contrário não é possível activar a sequência de arranque do gerador, pois o painel não é alimentado.

Uma representação da constituição interna do Grupo Gerador e alguns dos seus componentes pode ser vista na Figura 2.6.



Item	Descrição
1.	Etiqueta do Grupo Gerador
2.	Motor Diesel
3.	Filtro de Ar
4.	Turbocompressor (caso exista)
5.	Regulador do Motor (localizado no lado oposto)

Item	Descrição
6.	Motor de Arranque (localizado no lado oposto)
7.	Bateria/Porta-bateria
8.	Alternador de Carga da Bateria
9.	Radiador
10.	Alternador

Item	Descrição
11.	Caixa de Bornes
12.	Estrutura Base e Reservatório de Combustível
13.	Isoladores de Vibração
14.	Painel de Controle
15.	Disjuntor de Saída

Figura 2.6 – Constituição do Grupo Gerador [2]

2.2.3 – Quadro de Transferência de Cargas (QTC)

De uma forma geral, todas as instalações que utilizem um grupo gerador como fonte alternativa de energia necessitam, obrigatoriamente, de um Quadro de Transferência de Cargas. Este tem como finalidade comutar entre a alimentação normal da rede e a alimentação via gerador de emergência. Ao ser detectada um falha na alimentação da rede, o autómato do Grupo Gerador retira-a do circuito e substitui o gerador de emergência como fonte de alimentação.

No interior do Quadro de Transferência de Cargas existem dois contactores: o contactor de rede e o contactor do gerador. O contactor de rede é responsável pela comutação para a alimentação normal, enquanto o contactor do gerador acciona a alimentação de emergência por meio do Grupo Gerador.

Quando é dada a ordem de arranque do grupo, uma resistência de aquecimento do Quadro de Transferência de Cargas, ajusta a temperatura do motor para que o Grupo Gerador entre em funcionamento mais rapidamente possível.

Um encravamento mecânico entre os dois contactores impede que estes sejam fechados em simultâneo e que, assim, as duas redes fiquem em paralelo no momento da permuta. A ausência de encravamento pode resultar num curto-circuito entre a rede e o gerador e, consequentemente, na actuação das respectivas protecções.

No interior do quadro existe ainda um interruptor geral. Este aparelho de corte actua como medida de protecção na eventualidade de surgir uma tensão intempestiva, oriunda do gerador.

A Figura 2.7 apresenta o interior do Quadro de Transferência de Cargas, onde se podem ver os dois contactores e o interruptor referidos.

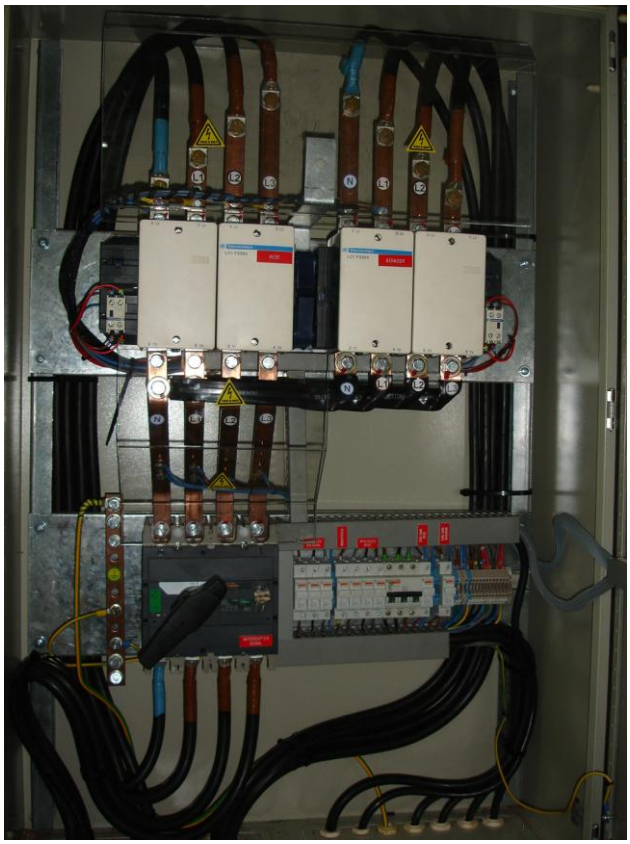


Figura 2.7 - Interior do Quadro de Transferência de Cargas

Seguidamente, na Figura 2.8 pode ver-se, na parte superior, o Quadro de Transferência de Cargas e, na parte inferior, um Transformador de Isolamento. Este transformador foi instalado para evitar que o autómato do Quadro de Comando do Grupo receba informações erradas do estado da rede, provocadas pela distorção harmónica que pode ser introduzida pelo envio de telecomandos da rede de Média Tensão.

Figura 2.8 - Quadro de Transferência de Cargas e Transformador de Isolamento

Apesar de, por defeito, a ligação ao gerador de emergência ser automática, existe a possibilidade ligar o gerador manualmente.

O esquema eléctrico do Quadro de Transferência de Cargas está representado no anexo B.

2.2.4 – Quadro de Emergência

O Quadro de Emergência, que se pode ver na Figura 2.9, é alimentado a partir do Quadro de Transferência de Cargas. Este quadro fornece a tensão das três UPS, que garantem a autonomia das cargas prioritárias durante o arranque do gerador, e alimenta os sistemas de ar condicionado das três salas de servidores. O ar condicionado, por sua vez, tem a função de controlar a temperatura e humidade destas salas.

Figura 2.9 - Quadro de Emergência

Os componentes de maior importância no Quadro de Emergência são, deste modo, os disjuntores de protecção das três UPS e do ar condicionado.

O esquema eléctrico do Quadro de Emergência é apresentado no anexo C.

2.2.5 – UPS

A função das UPS (*Uninterruptable Power Supply*) é assegurar a disponibilidade dos três conjuntos de servidores durante o período de arranque do gerador ou, no pior cenário, em caso de ausência de tensão proveniente da rede e do gerador. A Figura 2.10 mostra um exemplo de uma UPS utilizada no Centro de informática.

Uma UPS é constituída por um rectificador, um inversor e um sistema de armazenamento de energia a baterias. Durante o funcionamento normal da UPS, a tensão alternada é convertida em tensão contínua através do rectificador e usada para carregar um sistema de baterias. Após este processo, o inversor converte a tensão contínua em tensão alternada regulada. É o nível de carregamento da bateria que vai definir o tempo de autonomia da UPS.

Numa situação de emergência, quando não existe tensão da rede, as UPS fornecem toda a energia para as cargas prioritárias. Uma vez que as UPS estão numa configuração on-line, o tempo de transferência das cargas é nulo.

As UPS estão dispostas numa configuração com redundância 2+1. Para que a alimentação das cargas seja garantida pelo menos duas UPS têm, obrigatoriamente, de estar operacionais. Caso uma destas avarie, um interruptor de *by-pass*, localizado no Quadro das UPS, coloca a terceira UPS, normalmente em standby, no circuito e retira a UPS com defeito. Desta maneira, uma configuração das UPS redundante resulta num aumento da disponibilidade.

Figura 2.10 – Exemplo de uma UPS

2.2.6 – Quadro das UPS

O Quadro das UPS, que pode ser visto na Figura 2.11, é alimentado a partir das UPS e fornece a tensão de entrada dos Quadros das Salas de Servidores A, B e C.

Os componentes de maior relevância deste quadro são, deste modo, os disjuntores de protecção destes três quadros.

O esquema eléctrico do Quadro das UPS pode ser consultado no Anexo D.

Figura 2.11 - Quadro das UPS

2.2.7 – Quadro das Salas de Servidores

Os Quadros da Salas de Servidores, fornecem a tensão de entrada das Salas de Servidores e contêm os disjuntores diferenciais de protecção dos vários servidores.

A Figura 2.12 apresenta um exemplo de um Quadro da Sala de Servidores. Como se pode observar no lado direito da figura, cada quadro dispõe de um amperímetro por cada circuito de alimentação, de modo optimizar e facilitar a distribuição das cargas. Também possui sinalização geral da corrente por fase, visível no lado esquerdo da figura.

É fundamental ter em consideração que, apesar do objectivo do Sistema de Alimentação de Emergência ser a garantia a alimentação das três salas, estas têm requisitos de disponibilidade diferentes.

Como o Centro de Informática não especificou com exactidão os valores a tomar como referência, este foram definidos de forma qualitativa:

- A Sala de Servidores A é o ponto mais crítico do sistema e pode suportar uma indisponibilidade máxima de alguns minutos/ano, inferior a 10 minutos;

- A Sala de Servidores B é um ponto crítico do sistema e pode ter uma indisponibilidade máxima de algumas horas/ano, inferior a 2 horas;

- A Sala de Servidores C, com uma indisponibilidade máxima de alguns minutos/dia, inferior a 10 minutos, constitui o ponto menos crítico do sistema.

Assim, o disparo intempestivo de um disjuntor na Sala de Servidores A terá um nível de criticalidade consideravelmente superior ao disparo de um disjuntor da Sala de Servidores C.

Figura 2.12 - Exemplo de Quadro da Sala de Servidores

Capítulo 3

Abordagem Proposta

Como já se referiu, objectivo desta dissertação consiste em analisar os modos de avaria do Sistema de Alimentação de Emergência do Centro de Informática que foi proposto para, assim, determinar as suas causas e consequências, de modo que possam ser tomadas medidas no sentido de as remover e aumentar a disponibilidade do sistema.

A primeira decisão a tomar foi a escolha das ferramentas adequadas para desenvolver este estudo. Após alguma pesquisa obteve-se os elementos necessários para considerar que a Análise dos Modos e Efeitos de Avarias (FMEA) era um método amplamente usado por diversos sectores, tais como a indústria automóvel, a aeronáutica e a engenharia civil. Também, porque não existiam muitos dados quantitativos das taxas de avaria dos componentes a ser analisados, exigidas noutros métodos de análise.

Apesar das várias vantagens da FMEA, esta ferramenta possui algumas limitações, a mais notória a incapacidade de analisar modos de avaria combinados. Assim, para se obterem resultados mais efectivos, optou-se por complementar a FMEA com uma análise por Árvores de Falhas.

Neste capítulo será feita uma breve descrição dos seus fundamentos teóricos.

3.1 - FMEA - *Failure Mode and Effects Analysis*

3.1.1 – Introdução

A Análise dos Modos e Efeitos de Avarias, mais conhecida como FMEA, é um método de análise de risco qualitativo que permite avaliar os possíveis modos de avaria de um sistema, as causas que lhes deram origem e os efeitos por elas gerados. Assim, este processo sistemático visa a redução ou eliminação do risco associado a cada potencial modo de avaria, através da identificação do impacto no funcionamento do sistema e da proposta de soluções que permitam melhorar o seu desempenho. O método FMECA, Análise dos Modos de Avaria, Efeitos e Criticalidade, é uma extensão da FMEA em que a criticalidade das avarias é analisada mais detalhadamente.

O aparecimento da FMEA, como ferramenta de análise formal, data do final dos anos 40 com a introdução do standard MIL-P-1629A e actualmente designado MIL-STD-1629A.

Desenvolvido pelo Departamento de Defesa dos Estados Unidos com o nome *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. Neste método, os efeitos das avarias nos sistemas e equipamentos eram identificados e classificados de acordo com o impacto que tinham no sucesso de uma missão e na segurança de pessoas/equipamentos. [3]

O grande avanço da prevenção de falhas teve início na década de 60, quando a FMEA começou a ser utilizada no âmbito da pesquisa e desenvolvimento aeroespacial, nomeadamente no projecto Apollo. No entanto, o apogeu surgiu já no final dos anos 70 com introdução desta técnica na indústria automóvel pela Ford Motor Company, com os objectivos de obter de melhores resultados ao nível da produção/concepção e estabelecer critérios regulamentares e de segurança. [4]

Nos anos 80, a indústria automóvel americana começou a incorporar a FMEA no desenvolvimento dos seus novos produtos. Com o intuito de criar um padrão dos seus sistemas de qualidade, uma equipa formada por elementos da "Chrysler Corporation", "Ford Motor Company" e "General Motors" desenvolveu a norma QS-9000 [5], cujo princípio base era a obrigatoriedade de utilização da FMEA no processo de planeamento da qualidade. Em 1994, este standard expandiu-se a todos os fabricantes da indústria com o aparecimento da SAE J-1739 [6], desenvolvido pela Society of Automotive Engineers.

Actualmente, existe uma vasta gama de aplicação da FMEA que incluiu, além das já mencionadas indústrias automóvel e aeroespacial, áreas como a electrónica, a medicina, engenharia civil, gestão, engenharia de qualidade e avaliação do impacto ambiental, entre outras.

3.1.2 – Normas associadas à FMEA

Como já foi mencionado, ao longo do tempo várias indústrias foram estabelecendo as suas próprias normas FMEA em conformidade com os requisitos próprios da sua área. Em seguida será feita uma breve apresentação das normas mais utilizadas na actualidade.

- MIL-STD-1629A - "*Procedures for Performing a Failure Mode, Effects and Criticality Analysis*" [6]

O MIL-STD-1629A estabelece os requisitos e procedimentos necessários à realização de uma FME(C)A que permitem avaliar e documentar, de modo sistemático e por ordem de itens correspondentes a cada modo de avaria de um componente, o potencial impacto de cada falha funcional ou de hardware no sucesso de uma missão, na segurança de pessoas e sistemas, no desempenho do sistema, na sua durabilidade e requisitos de manutenção. Cada potencial modo de avaria é classificado de acordo com a severidade dos seus efeitos, a fim de que sejam tomadas medidas de correcção adequadas para controlar ou eliminar o risco dos itens de risco mais elevado.

- SAE J1739 - "*Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and assembly Processes (Process FMEA) Reference Manual*" [6]

Desenvolvida em conjunto pela Chrysler, Ford e General Motors, a SAE J1739 introduz o tópico da FMEA e dá uma orientação geral de como aplicá-la. Nesta norma, a FMEA é descrita como um grupo de actividades sistemáticas destinadas a reconhecer e avaliar o potencial da

avaria de um produto ou processo e seus efeitos, identificar as acções que possam eliminar ou reduzir a hipótese da potencial falha ocorrer e documentação do processo.

- IEC 60812 - "*Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*" [6]

O IEC 60812, publicado pelo IEC (International Electrotechnical Commission), descreve não só a FMEA (Análise dos Modos de Avaria e Efeitos) mas também a FMECA (Análise dos Modos de Avaria, Efeitos e Criticalidade) e dá orientações de como os objectivos da análise podem ser alcançados utilizando-as como ferramentas de análise de risco. Inclui ainda os passos necessários ao desenvolvimento da análise, a identificação dos termos apropriados, pressupostos e medidas de criticalidade, um exemplo de formulário de documentação da FMEA/FMECA e uma matriz de criticalidade para avaliar os efeitos das avarias.

No desenvolvimento da FMEA do Sistema de Alimentação de Emergência do Centro de Informática, esta norma foi usada como referência.

3.1.3 – Metodologia da FMEA

A FMEA deve ser iniciada com a hierarquização do sistema, ou seja, a sua divisão em sistemas mais simples. Este podem ser subsistemas e/ou componentes, dependendo do nível de detalhe pretendido para a análise e devem ser representados através de diagramas simples mas que realcem as funções essenciais do sistema. [8]

A informação disponível e a experiência de utilização do sistema são alguns dos critérios a ter em consideração na definição dos limites e do nível de detalhe da análise. Um subsistema que se saiba ser fiável ou cujo histórico de utilização não revele problemas maiores, poderá não justificar uma análise muito detalhada. Do mesmo modo, devem ser analisados mais minuciosamente os subsistemas mais recentes ou subsistemas que já tenham dado origem a problemas, e ainda subsistemas cuja fiabilidade ainda não é completamente conhecida.

Depois de um subsistema ser escolhido, a etapa seguinte é a sua análise funcional. Nesta fase, deve ser feita uma lista das suas funções e do comportamento esperado em várias etapas de funcionamento como, por exemplo, durante a operação ou em manutenção.

Tendo conhecimento das funções desempenhadas, procede-se ao levantamento dos potenciais modos de avaria. O modo de avaria caracteriza o processo ou mecanismo de avaria que ocorre no subsistema/componente ao descrever o afastamento em relação à sua função. O grau de especificação definido na hierarquização e análise funcional do sistema é fundamental para se conseguir identificar de forma transparente os modos de avaria.

Para cada potencial modo de avaria, devem listar-se os efeitos a que a sua ocorrência pode dar origem e as causas que podem ter estado na origem do seu aparecimento. Os efeitos traduzem o modo como a avaria se manifesta e as consequências que produz no sistema global ou no próprio subsistema/componente dependendo se a análise é global ou local, respectivamente. As causas correspondem às razões pelas quais a função do subsistema/componente não é cumprida. Dado que um potencial modo de avaria pode ser originado por causas diferentes e, tipicamente, independentes entre si estas devem ser todas devidamente identificadas e descritas.

A última etapa da FMEA consiste na proposta de métodos de detecção e prevenção das avarias, tendo em conta a forma e os meios através dos quais são detectadas as suas ocorrências. Estes métodos devem garantir que a ocorrência dos modos de avaria que ponham em causa a segurança de pessoas ou equipamentos é eliminada ou, pelo menos, mitigada.

Como já foi referido, a FMECA (*Failure Mode, Effects and Criticality Analysis*) é uma extensão da metodologia FMEA, pelo que o seu processo de desenvolvimento exige alguns detalhes adicionais.

A grande diferença entre as duas análises reside no grau de profundidade com que a criticalidade é estudada. Assim, às etapas descritas junta-se uma outra – a análise de risco. Esta análise engloba a avaliação da severidade e da frequência de ocorrência do modo de avaria em estudo para determinação da criticalidade.

A severidade avalia o impacto dos efeitos do modo de avaria no sistema que está a ser analisado e pode ter em conta inúmeros factores, tais como o impacto no desempenho funcional do sistema ou na segurança das pessoas e equipamentos. Para facilitar a avaliação, é atribuída uma classificação à severidade, denominada índice de severidade (S). A escala deste índice tem uma amplitude variável, dependendo do nível de detalhe estabelecido. No entanto, a classificação 1 corresponde sempre ao nível de severidade mais insignificante e a classificação de fim de escala a um grau de severidade que pode ter consequências catastróficas. A Tabela 3.1 ilustra uma hipotética escala do índice de severidade.

Tabela 3.1 - Exemplo de classificação do índice de severidade (S) [8]

Classe	Nível de Severidade	Consequências para as pessoas ou o ambiente
IV	Catastrófica	Um modo de avaria que poderia eventualmente resultar no falha das principais funções do sistema e, consequentemente, provocar sérios danos ao sistema e ao seu ambiente e/ou ferimentos em pessoas.
III	Crítica	Um modo de avaria que poderia eventualmente resultar na falha das principais funções do sistema e, portanto, causar um prejuízo considerável para o sistema e o seu ambiente, mas que não constitui uma ameaça grave para a vida ou lesão
II	Marginal	Um modo de avaria que poderia potencialmente degradar o desempenho das funções do sistema mas sem lhe causar danos apreciáveis, nem representar ameaça de vida ou lesão.
I	Insignificante	Um modo de avaria que poderia potencialmente degradar as funções do sistema, mas que não lhe causa danos, nem constitui uma ameaça de vida ou lesão.

A ocorrência avalia a frequência ou probabilidade de um modo avaria ocorrer. Tal como ocorre com a severidade, a classificação da frequência de ocorrência é feita com recurso a uma escala, na qual o patamar inferior corresponde um nível de ocorrência improvável e o patamar superior corresponde a ocorrências muito frequentes. A tabela 3.2 fornece um exemplo de classificação do nível de ocorrência.

Tabela 3.2 - Exemplo de classificação do índice de ocorrência (O) [8]

Ocorrência do Modo de Avaria	Classificação, O	Frequência	Probabilidade
Remota: Avaria improvável	1	≤ 0,010 por mil veículos/items	$\leq 1x10^{-5}$
Baixa: Avarias pouco frequentes	2	0,1 por mil veículos/items	$1x10^{-4}$
	3	0,5 por mil veículos/items	$5x10^{-4}$
Moderada: Avarias ocasionais	4	1 por mil veículos/items	$1x10^{-3}$
	5	2 por mil veículos/items	$2x10^{-3}$
	6	5 por mil veículos/items	$5x10^{-3}$
Elevada: Avarias frequentes	7	10 por mil veículos/items	$1x10^{-2}$
	8	20 por mil veículos/items	$2x10^{-2}$
Muito elevada: Avarias quase inevitáveis	9	50 por mil veículos/items	$5x10^{-2}$
	10	≥100 em mil veículos/items	$\geq 1x10^{-1}$

Para além da severidade e da ocorrência, a análise de risco pode também recorrer a um terceiro critério, o índice de detecção (D), que corresponde à probabilidade do modo de avaria ser ou não detectado.

A determinação quantitativa do risco pode ser obtida através do Número de Prioridade do Risco, RPN. Este número corresponde ao produto dos índices descritos anteriormente e é calculado para cada um dos potenciais modos de avaria:

$$RPN = S \times O$$

Os valores de RPN permitem definir a prioridade dos modos de avaria e hierarquizá-los por ordem de necessidade de tomada de acções correctivas. Deste modo, valores de RPN muito elevados correspondem a um nível de risco intolerável e implicam, de uma maneira geral, a elaboração imperativa de um plano de resposta ao risco com várias propostas de acções correctivas que levem à sua diminuição. Pelo contrário, a valores de RPN muito pequenos correspondem, habitualmente, modos de avarias cujos efeitos são negligenciáveis ou que não põem em risco o funcionamento normal do sistema.

Uma forma alternativa de representar o risco é através de uma matriz de risco, como a da tabela 3.3. Esta matriz dá o risco associado a um potencial modo de avaria como função do nível de severidade e da frequência de ocorrência da avaria.

Tabela 3.3 - Exemplo de uma matriz de risco [8]

Frequência de ocorrência do efeito da avaria	Nível de Severidade			
	1 Insignificante	2 Marginal	3 Crítica	4 Catastrófica
5: Frequente	Indesejável	Intolerável	Intolerável	Intolerável
4: Provável	Tolerável	Indesejável	Intolerável	Intolerável
3: Ocasional	Tolerável	Indesejável	Indesejável	Intolerável
2: Remota	Negligenciável	Tolerável	Indesejável	Indesejável
1: Improvável	Negligenciável	Negligenciável	Tolerável	Tolerável

A FMEA deve ter como apoio um formulário, com a forma de uma tabela como a que está representada Figura 3.1. Este formulário deve ser preenchido de maneira sistemática e respeitando a ordem as várias etapas de desenvolvimento, de modo a agrupar a toda a informação que vai sendo reunida.

As fases de desenvolvimento da FME(C)A, de acordo com a norma IEC 60812, estão resumidas e no fluxograma da Tabela 3.4.

Tabela 3.4 - Exemplo de formulário da FMEA [8]

Período de oeração:			Item: Revisão:					Preparada por: Data:			
Ref. do item	Descrição do item e sua função	Modo de Avaria	Código do Modo de Avaria	Possíveis causas da Avaria	Efeito local	Efeito global	Método de detecção	Medidas para mitigação da Avaria	Classe de Severidade	Frequência ou probabilidade de ocorrência	Comentários

Este formulário deve identificar o subsistema/componente que está em análise e incluir informações como o seu nome, a função que desempenha, os modos de avarias, as possíveis causas e efeitos que provocam no sistema, valores numéricos dos índices de severidade, ocorrência e detecção e algumas considerações e/ou comentários relevantes.

O aspecto gráfico do formulário da FME(C)A não está completamente padronizado, sofrendo algumas variações dependendo da aplicação. Apesar disso, as colunas devem ser sempre preenchidas de forma clara e concisa para que a informação aí presente não suscite qualquer tipo de dúvida.

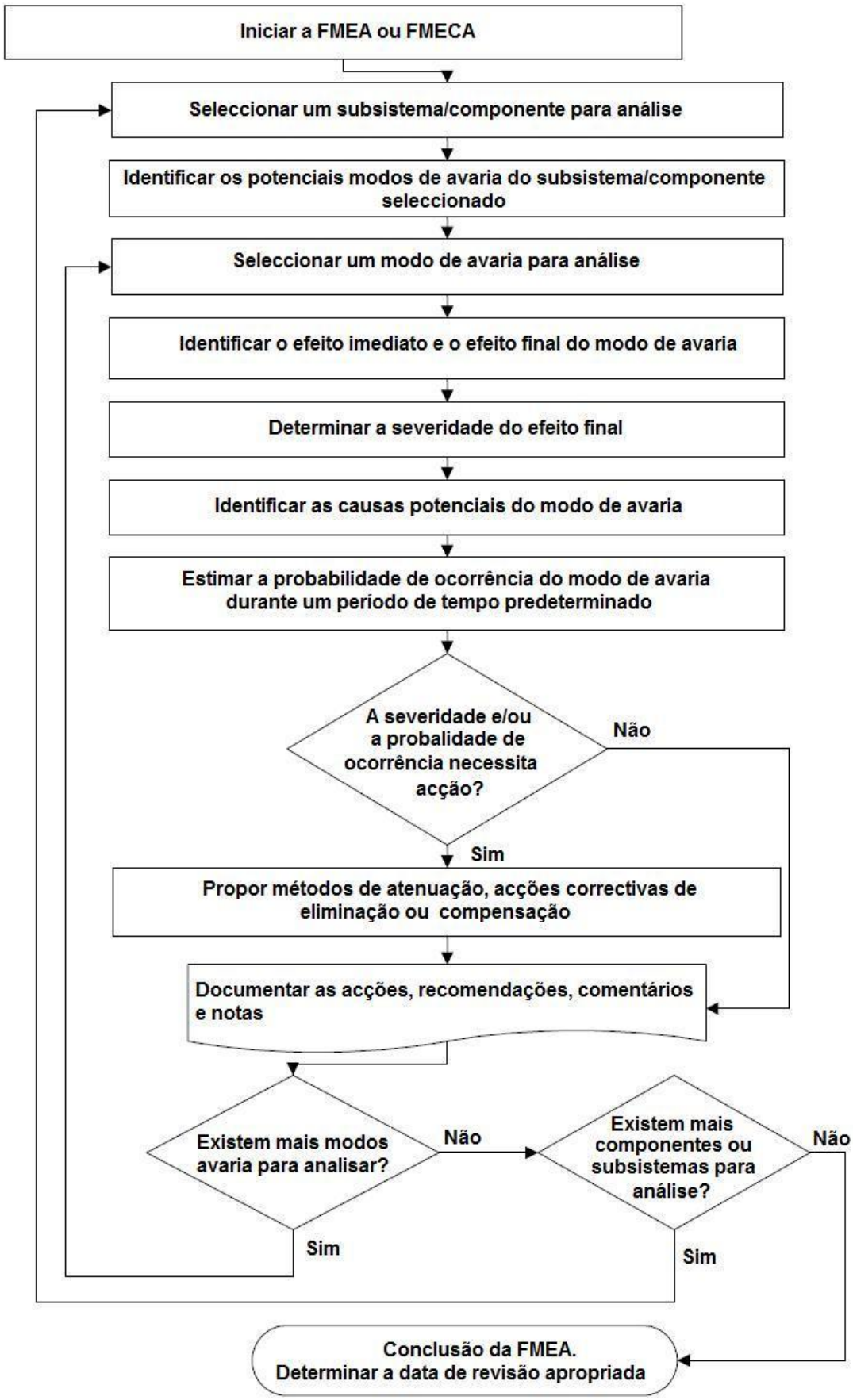


Figura 3.1 - Fluxograma da análise da FME(C)A [8]

3.2 – Árvores de Falhas (*FTA – Fault Tree Analysis*)

3.2.1 – Introdução

O conceito fundamental das FTA (Fault Tree Analysis), Árvores de Falhas, consiste em estudar, detalhadamente, o modo como as falhas de um sistema podem ser alcançadas através da combinação lógicas de eventos primários. Assim, a análise consiste na construção de um diagrama lógico, a árvore de falhas, através de um processo dedutivo que parte de um evento indesejado predefinido, denominado evento de topo, e procura as possíveis causas desse evento. O processo vai sendo consecutivamente desenvolvido até se atingirem os eventos independentes básicos ou eventos sobre os quais não se possui mais informação, que constituem o limite de resolução da análise. As Árvores de Falhas também permitem identificar combinações de falhas que levam ao evento de topo, ao contrário da FMEA.

Esta técnica foi desenvolvida início dos anos 60 por H. A. Watson, nos laboratórios Bell, a pedido da Força Aérea dos Estados Unidos, para avaliar a fiabilidade do sistema de controlo do míssil Minuteman. Em 1963, foi reconhecida e aperfeiçoada pela Boeing como uma importante ferramenta de análise de segurança passando a ser usada frequentemente por esta companhia.

Em Junho de 1965, a Boeing e a Universidade de Washington organizaram um simpósio de análise de segurança e de sistemas de segurança em Seattle, onde as primeiras publicações técnicas sobre Árvores de Falhas foram apresentadas.

A partir dos anos 70, com o desenvolvimento de novos algoritmos de avaliação, o uso das Árvores de Falhas foi abrangendo cada vez mais áreas de aplicação, nomeadamente sistemas de alimentação, robótica e aviação. [9]

3.2.1 – Metodologia das Árvores de Falhas

A análise de Árvore de Falhas é uma boa prática quando se pretende estudar os factores que podem causar um evento indesejável, normalmente uma avaria do sistema. Este método pode ser desenvolvido através das seguintes etapas que estão representadas esquematicamente na Figura 3.2 [10]:

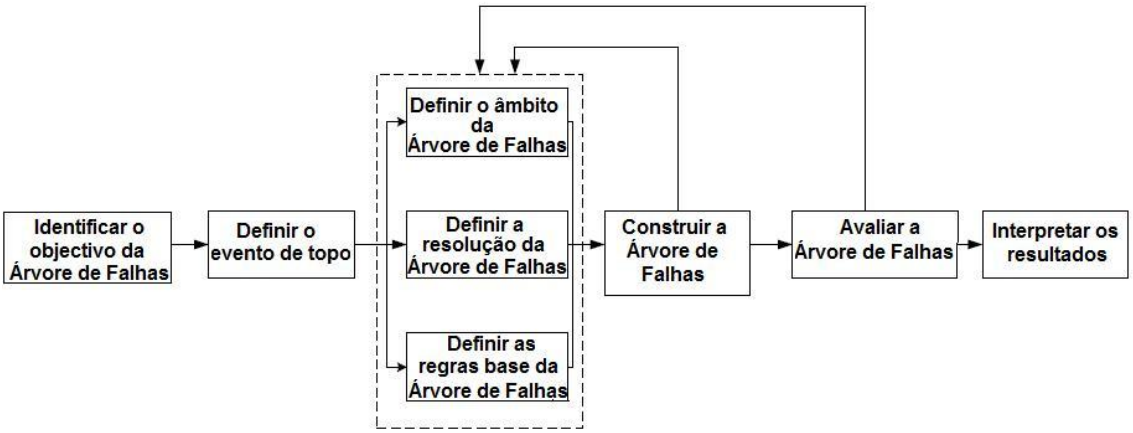


Figura 3.2 - Diagrama do processo de desenvolvimento da Árvore de Falhas

1. Identificar o objectivo da Árvore de Falhas

O objectivo da Árvore de Falhas consiste em fazer a formulação do problema do sistema que vai ser estudado.

2. Definir o evento de topo

O evento de topo corresponde à raiz da Árvore de Falhas. Este evento define o modo de avaria do sistema que vai ser analisado, isto é, o acontecimento indesejável. Caso existam vários modos de avaria do sistema em estudo, é conveniente definir um evento de topo para cada um.

3. Definir o âmbito da Árvore de Falhas

Nesta etapa, deve indicar-se quais as falhas e componentes que vão ser incluídos na análise e quais vão ser desprezados. Devem também ser definidas as condições fronteira que incluem os estados iniciais dos componentes e o levantamento das entradas do sistema.

4. Definir a resolução da Árvore de Falhas

A resolução da Árvore de Falhas corresponde ao nível de detalhe com que se vão desenvolver as causas das falhas do evento de topo. O nível de detalhe depende do conhecimento do analista e da informação disponível sobre o sistema.

5. Definir as regras base da Árvore de Falhas

Para que a Árvore de Falhas seja coerente, a nomenclatura e o modo como os eventos e as portas lógicas são identificados deve estar bem definida. Por este motivo, antes de se iniciar a construção da Árvore, devem ser estabelecidas as regras base.

6. Construir a Árvore de Falhas

A através de diagramas sequenciais que envolvem os eventos ou falhas, de modo sistemático, mostrando o relacionamento entre os mesmos e o acontecimento indesejável em análise.

O processo tem início com a identificação dos eventos que directamente relacionados ao evento de topo e, assim, vai-se avançando, sucessivamente até atingir os eventos ou falhas básicas. A relação entre eventos é feita através de portas lógicas.

7. Avaliar a Árvore de Falhas

Após a construção da Árvore de Falhas a etapa seguinte é sua avaliação, que pode ter duas abordagens: qualitativa e quantitativa.

A avaliação qualitativa tem como finalidade representar a ocorrência da avaria através de uma forma lógica equivalente, mostrando através do diagrama as combinações de eventos básicos, erros operacionais ou outros defeitos que podem dar origem ao evento de topo.

A avaliação quantitativa tem como objectivo analisar a probabilidade de ocorrência do evento de topo em função das probabilidades de ocorrência dos eventos básicos. Nem sempre se procede a esta avaliação, uma vez que podem não estar disponíveis informações relativas às probabilidades de ocorrência dos eventos.

8. Interpretar os resultados

A análise de uma Árvore de Falhas termina com a interpretação dos resultados obtidos pela avaliação qualitativa e/ou quantitativa e a decisão das acções a tomar para melhorar o desempenho do sistema e eliminar o(s) evento(s) indesejável(eis).

3.2.3 – Simbologia utilizada nas Árvores de Falhas

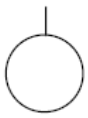
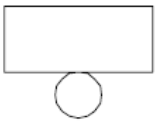
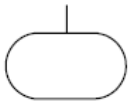
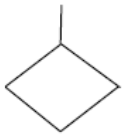
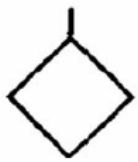
Nesta secção será feita uma breve descrição dos símbolos mais utilizados na construção da Árvore de Falhas.

3.2.3.1 – Eventos básicos

Os eventos básicos de uma Árvore de Falhas correspondem aos acontecimentos que não foram mais desenvolvidos, por uma razão ou por outra.

Existem quatro tipos de eventos básicos:

Tabela 3.5 - Eventos básicos de uma Árvore de Falhas [11]

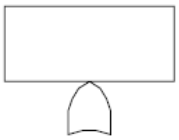
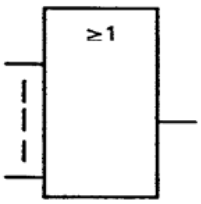
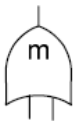
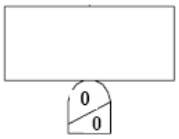
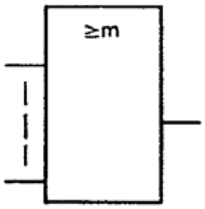
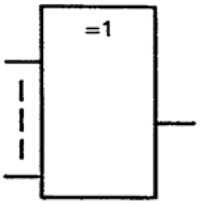
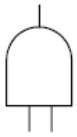
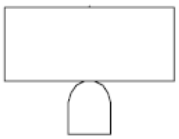
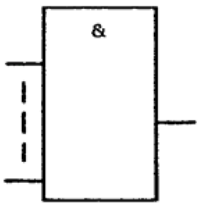
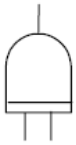
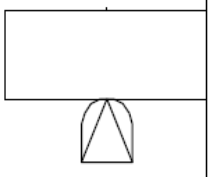
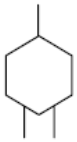
	Símbolo		Nome	Descrição
			EVENTO BÁSICO	O nível mais baixo do evento para o qual a informação da probabilidade de ocorrência ou fiabilidade está disponível
			EVENTO CONDICIONAL	Evento que é uma condição de ocorrência de um outro evento, quando ambos têm de ocorrer para a saída ocorrer
			EVENTO NÃO DESENVOLVIDO	Um evento primário que representa uma parte do sistema ainda não desenvolvida
			EVENTO EXTERNO	Evento que ou já ocorreu ou vai, com certeza, ocorrer

3.2.3.2 – Portas lógicas

Os dois tipos básicos de portas lógicas são as portas *AND* e as portas *OR*.

As portas *AND* devem ser utilizadas quando o evento de saída só ocorre quando todos os eventos de entrada ocorrem. As portas *OR* associam-se a eventos de saída que ocorrem se um ou mais eventos de entrada ocorrem.

Tabela 3.6 - Portas lógicas de uma Árvore de Falhas [11]

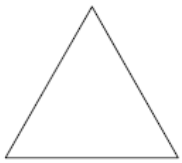
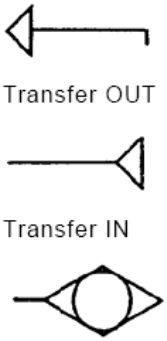
	Symbols		Name	Description
			Porta OU	O evento de saída só ocorre se um ou mais dos eventos de entrada ocorrerm
			Porta votadora	O evento de saída ocorre se de m entradas pelo menos n ocorrem
			Porta OU EXCLUSIVO	O evento de saída só ocorre se exactamente um dos eventos de entrada ocorre
			Porta E	O evento de saída só ocorre se todos os eventos de entrada ocorrerm
			Porta E PRIORIDADE	O evento de saída só ocorre se todos os eventos de entrada ocorrerm dentro de uma sequência ordenada específica
			Porta inibidora	O evento de saída só ocorre quando ambos os eventos de entrada ocorrem, um deles condicional

Existem também alguns casos particulares, por exemplo a porta *OR* Exclusivo onde o evento de saída ocorre somente se exactamente um dos eventos de entrada ocorrer ou a por *AND* Prioridade cujo evento de saída ocorre somente se todos os eventos de entrada ocorrem de acordo com uma sequência específica.

3.2.3.3 – Transferência

Um símbolo de transferência é utilizado para indicar que a análise do evento em questão vai ser continuada noutra parte da árvore. Estes símbolos têm como principal objectivo indicar a continuidade da análise e, de uma maneira geral, são utilizados quando se atinge o final de uma página. Caso a Árvore de Falhas ocupe múltiplas páginas, deve ser indicado no símbolo o número da página para onde o diagrama foi transferido (*Transfer In*), de modo a facilitar o acompanhamento da sua evolução. Do mesmo modo, no destino, deve ser incluída a informação da página inicial (*Transfer Out*).

Tabela 3.7 - Símbolo de transferência de uma Árvore de Falhas [11]

	Símbolo		Nome	Descrição
			Transferência	Porta que indica que esta parte do sistema é desenvolvida noutra parte ou página do diagrama

Capítulo 4

Análise FMEA

A ferramenta Análise dos Modos e Efeitos de Avarias (FMEA: *Failure Mode and Effects Analysis*)[1] tem como objectivo a identificação dos modos de avaria, as suas causas e as suas consequências. A sua aplicação permite obter uma visão geral do sistema e o estabelecer um plano de acções de prevenção e/ou mitigação do risco.

Esta análise permite reconhecer o potencial da avaria de um subsistema, ou componente, e avaliar sua repercussão no sistema. Este processo é encarado de maneira global e sistemática. As avarias são hierarquizadas, através determinação do Número de Prioridade do Risco (RPN) que é atribuído a cada uma, e as que apresentarem maior índice de risco deverão ser objecto de planos de acção específicos.

Neste capítulo apresenta-se a FMEA do Sistema de Alimentação de Emergência do Centro de Informática.

Na primeira parte são descritas, sinteticamente, as etapas do planeamento da FMEA e são expostos os critérios utilizados na análise de risco. A segunda parte é feita a apresentação de algumas tabelas com resultados obtidos e, com base nestes, são retiradas algumas conclusões preliminares acerca dos elementos mais críticos do Sistema de Alimentação de Emergência.

4.1 – Planeamento da FMEA

Em sistemas complexos, como o sistema em estudo, a FMEA é tipicamente executada por uma equipa multidisciplinar, de modo a garantir que a análise é o mais exaustiva possível. Com esse intuito, foi constituída uma equipa responsável pela FMEA do Sistema de Alimentação do Centro de Informática. Esta equipa era formada por seis elementos, alguns das áreas envolvidas no processo, nomeadamente um coordenador do Centro de Informática e um responsável pelos Serviços Técnicos e de Manutenção, para melhor apoiar o desenvolvimento deste estudo com a contribuição da sua experiência e conhecimento do sistema.

[1] A Análise dos Modos e Efeitos de Avarias passará a ser referida através da sigla em inglês, FMEA, dado ser mais perceptível para o leitor.

A equipa reunia-se semanalmente e em cada reunião era discutido um subsistema. O planeamento da FMEA abrangeu os seguintes passos:

1. Descrição dos objectivos e abrangência da análise, isto é, a identificação dos processo a serem analisados;

2. Divisão e hierarquização do Sistema de Alimentação de Emergência em subsistemas;

3. Listagem dos potenciais modos de avaria dos subsistemas considerados;

4. Discussão das causas dos modos de avaria;

5. Estudo das consequências dos modos de avaria;

6. Análise do risco associado a cada avaria;

7. Recomendação de medidas que permitam mitigar o risco da avaria e/ou diminuir a sua ocorrência, tendo em conta os modos de avaria mais críticos.

4.2 – Análise de Risco

A Análise de Risco deve ser iniciada após a equipa possuir o conhecimento dos modos de avarias, dos seus efeitos e das suas causas. Nesta etapa devem ser definidos os índices de severidade (S), ocorrência (O).

A Severidade (S) é o índice que reflecte a gravidade do efeito da avaria sobre o sistema global. Aliás, a severidade é sempre aplicada ao efeito do modo de avaria e existe uma relação directa entre os dois: por exemplo, se o efeito é crítico, a severidade é alta. Por outro lado, se o efeito não é crítico, a severidade é baixa. Deste modo, quanto maior for o grau na escala do índice de severidade mais grave é o impacto do efeito da avaria. Na avaliação da severidade dos modos de avaria do Sistema de Alimentação de Emergência do Centro de Informática, a classificação foi feita com base na escala de 1 (um) a 5 (cinco) apresentada na Tabela 4.1. Na escala proposta, o número 5 (nível de severidade catastrófico) é o caso mais grave e corresponde a uma avaria que afecte a Sala de Servidores A, a carga mais crítica do sistema e que exige uma disponibilidade muito elevada.

A Ocorrência (O) representa a frequência ou probabilidade de aparecimento de cada modo de avaria e tem como base o histórico de utilização do sistema ou o estudo de casos semelhantes. Quando as taxas de avaria são conhecidas, o índice de ocorrência dos modos de avaria é, usualmente, representado pela probabilidade da sua ocorrência. Uma vez que não existiam dados suficientes acerca dos componentes do sistema para proceder a este tipo de avaliação, optou-se por classificar o índice de acordo com a frequência, hipotética, das avarias. A escala de classificação proposta para qualificar o índice de ocorrência é, como no caso da Severidade, de 1 (um) a 5 (cinco). O nível de ocorrência mais baixo corresponde a uma avaria com frequência improvável, enquanto o mais elevado representa um evento frequente, como se pode observar na Tabela 4.2.

Tabela 4.1 - Classificação da Severidade (S)

Severidade (S)		
Classificação	Nível de severidade	Descrição
1	Insignificante	Sem influência no funcionamento global do sistema
2	Pouco significativa	Afecta alguns subsistemas (não críticos)
3	Significativa	Afecta a Sala de Servidores C
4	Crítico	Afecta a Sala de Servidores B
5	Catastrófico	Afecta a Sala de Servidores A

Tabela 4.2 - Classificação da Ocorrência (O)

Ocorrência (O)		
Classificação	Frequência	Descrição
1	Improvável	Superior a 10 anos
2	Remota	De 5 em 5 anos
3	Ocasional	Todos os anos
4	Provável	De 6 em 6 meses
5	Frequente	Todos os meses

A partir dos índices de severidade e ocorrência é possível avaliar a criticalidade do risco de cada modo de avaria através de uma matriz de risco. Como se pode ver na tabela 4.3, a Matriz de Risco proposta categoriza o risco em quatro regiões distintas. Estas quatro regiões podem ser definidas como: região negligenciável (a verde), duas regiões ALARP (*As Low As Reasonably Practicable)* - "risco tão baixo quanto razoavelmente praticável" (a amarelo, em casos de pouca gravidade, e a laranja, para situações graves) e região de risco intolerável (a vermelho).

Quando o risco é negligenciável, o processo de redução de risco não é necessário, uma vez que este é considerado aceitável. Nos casos em que o risco está num patamar acima do negligenciável, a região ALARP, mas em que ainda é possível a convivência com o mesmo devido aos benefícios associados ou à inviabilidade de reduzi-lo, pode-se considerá-lo como risco tolerável ou indesejável. A distinção entre risco tolerável e risco indesejável baseia-se no facto de que o primeiro é aceitável mas com potencial de melhoria enquanto no segundo o risco já é inaceitável mas as medidas adicionais ainda não obrigatórias, somente recomendadas.

Se um modo de avaria adquire uma classificação de severidade e ocorrência que o coloque no patamar superior da Matriz de Risco, correspondente à zona de risco intolerável, é obrigatório tomar medidas de segurança adicionais, sob pena de por em causa a disponibilidade do sistema.

O produto entre os índices de severidade e ocorrência permite obter, como já foi referido, o Número de Prioridade do Risco (RPN). De acordo com esta classificação, o risco dos vários modos de avaria deve ser hierarquizado. A Tabela 4.4 apresenta a classificação utilizada para a prioritização do risco.

Tabela 4.3 - Matriz de Risco

Matriz de risco					
Frequência de ocorrência	**Severidade**				
	1: Insignificante	2: Pouco significativa	3: Significativa	4: Crítica	5: Catastrófica
5: Frequente	Tolerável	Indesejável	Intolerável	Intolerável	Intolerável
4: Provável	Tolerável	Indesejável	Indesejável	Intolerável	Intolerável
3: Ocasional	Tolerável	Tolerável	Indesejável	Indesejável	Intolerável
2: Remota	Negligenciável	Tolerável	Tolerável	Indesejável	Indesejável
1:Improvável	Negligenciável	Negligenciável	Tolerável	Tolerável	Tolerável

Tabela 4.4 - Classificação do Número de Prioridade do Risco

Número de Prioridade do Risco (RPN)	
Nível de Risco	Descrição
Negligenciável $1 \leq RPN \leq 2$	Risco aceitável
Tolerável $3 \leq RPN \leq 6$	Risco aceitável mas que pode ser sujeito a melhorias
Indesejável $8 \leq RPN \leq 12$	Risco inaceitável - é conveniente tomar medidas de segurança adicionais
Intolerável $15 \leq RPN \leq 25$	Risco absolutamente inaceitável - obrigatório tomar medidas de segurança adicionais

4.3 - Apresentação de resultados

Nesta secção são apresentadas as tabelas da FMEA desenvolvida para os vários subsistemas. Dado que o conteúdo das tabelas é bastante extenso, para cada subsistema serão apresentados somente os modos de avaria com maior índice de severidade ou com um maior número de prioridade do risco, RPN.

As tabelas da FMEA do Sistema de Alimentação do Centro de Informática podem ser consultadas na íntegra no anexo E.

4.3.1 – Subsistema Posto de Transformação

O subsistema do Posto de Transformação decompõe-se em três níveis hierárquicos, como se pode observar na figura 4.1. No topo, encontra-se o Posto de Transformação; no nível intermédio estão os dois transformadores e o Quadro Geral de Baixa Tensão. No interior deste quadro, encontram-se os componentes que foram considerados relevantes neste subsistema: os disjuntores de protecção dos transformadores, o disjuntor interbarras que permite a comutação dos transformadores e o disjuntor associado ao Quadro de Transferência de Cargas.

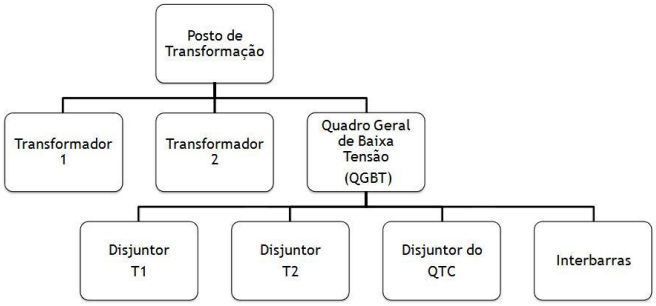


Figura 4.1 - Hierarquia do Subsistema Posto de Transformação

A Tabela 4.5 expõe o extracto da FMEA do Posto de Transformação relativo aos modos de avaria do Transformador 1. Como se pode observar, os três modos de avaria apresentados para este componente – Sobretensão, Subtensão e Sem Tensão – encontram-se na região de risco tolerável (cor amarela) e têm o mesmo Número de Prioridade do Risco. Apesar de este número corresponder ao limite superior da gama de valores de risco tolerável, pode afirmar-se, à partida, que o Transformador 1 não é um componente crítico do sistema. Isto porque, apesar do índice de Severidade (S) de qualquer uma das avarias ser significativo, o índice de Ocorrência (O) indica que sua a frequência é remota, isto é, espera-se que ocorram uma vez em cada cinco anos.

Os modos de avaria do Transformador 2, que podem ser consultados no anexo E, são muito semelhantes aos do Transformador 1. A única diferença reside no RPN, que é ligeiramente inferior para o Transformador 2. O motivo desta diferença é que, uma vez que o Transformador 2 não é a alimentação principal das Salas de Servidores, apesar do índice de Ocorrência das avarias ser o mesmo, o índice de Severidade é ligeiramente inferior.

Tabela 4.5 - Extracto da FMEA do Transformador

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Transformador 1	Fornecer tensão	Sobretensão (tensão superior a U_n)	• Descarga atmosférica • Sobreintensidades	Potencial perda da tensão do transformador 1	3	2	6	*Actuação de protecções*
		Subtensão (tensão inferior a U_n)	• Problema de isolamento • Curto-circuito	Potencial perda da tensão do transformador 1	3	2	6	
		Sem tensão	• Problema de isolamento • Curto-circuito • Interrupção da alimentação da Média Tensão (MT)	O transformador não fornece tensão	3	2	6	

A tabela 4.2 apresenta os modos de avaria mais críticos de dois componentes do Quadro Geral de Baixa Tensão: o disjuntor de protecção do transformador 1 (Disjuntor T1) e o Interbarras. No caso do Disjuntor T1 o pior caso corresponde à sua abertura intempestiva e consequente corte, desnecessário, da tensão proveniente do Transformador 1. Já para o Interbarras, as avarias mais críticas estão directamente associadas a um cenário de avaria do Transformador 1 e a à incapacidade de comutação das cargas por ele alimentadas para o Transformador 2.

Pode observar-se que, assim como no caso do Transformador 1, todos os modos de avaria destes componentes estão na região de risco tolerável (cor amarela). Contudo, os valores de RPN correspondem ao nível inferior da gama de valores da região tolerável. Apesar de o nível de Severidade ser o mesmo, os disjuntores são componentes muito fiáveis, o que baixa a expectativa de uma potencial avaria de um período de cinco anos para um período de dez anos.

Tabela 4.6 - Extracto da FMEA do Quadro Geral de Baixa Tensão

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Interbarras	Colocar em paralelo os transformadores 1 e 2	Ao fechar	Avaria interna (mecânica) do disjuntor	Não é possível colocar os transformadores em paralelo	3	1	3	*Por defeito o interbarras está aberto mas, em caso de avaria do transformador 1, o transformador 2 não pode fornecer tensão ao sistema*
		Não operação	• Avaria interna do disjuntor • Causas humanas • Abertura intempestiva do disjuntor	O interbarras é fechado mas não há condução da corrente	3	1	3	*Em caso de avaria do transformador 1, o transformador 2 não fornece tensão ao sistema*
Disjuntor T1	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	A tensão do transformador 1 é cortada	3	1	3	

Os restantes modos de avaria destes componentes, assim como os modos de avaria dos disjuntores de protecção do transformador 2 e quadro de transferência de cargas podem ser consultados nas tabelas do anexo E.

4.3.2 – Subsistema Grupo Gerador

Os componentes considerados no subsistema do Grupo Gerador foram: o alternador, o motor, o disjuntor de saída de protecção do alternador, o sistema de refrigeração do motor, a bateria e o quadro de controlo ou comando do grupo. O Quadro de Controlo foi, ainda, decomposto em três elementos de nível inferior: o painel de controlo e monitorização do

grupo, o transformador de isolamento e o seu disjuntor de protecção. A hierarquia destes componentes pode ser vista na Figura 4.2.

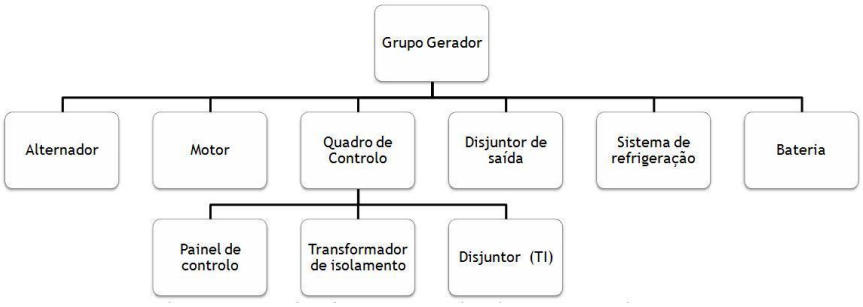


Figura 4.2 - Hierarquia do Subsistema Grupo Gerador

Na Tabela 4.7. estão expostos os modos de avaria dos componentes mais críticos do subsistema do Grupo Gerador. De facto, analisando os Números de Prioridade do Risco dos modos de avaria do Motor e da Bateria de alimentação do Painel de Controlo é possível concluir que estes se encontram na região de risco indesejável (cor laranja). Os índices de Severidade e Ocorrência indicam que não só estas avarias são significativas como podem ter uma frequência anual.

Tabela 4.7 - Extracto da FMEA do Grupo Gerador

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Motor	Arranque do Grupo Gerador	Não arranca	• Falta de combustível • Obstrução do radiador • Botão de paragem de emergência premido • Interruptor de controlo ligado • Obstrução do filtro de ar	O grupo gerador não arranca	3	3	9	*Redundância do Grupo Gerador*
		Arranca mas pára intempestivamente	• Motor sobrecarregado • Sobrevelocidade • Temperatura do motor demasiado elevada • Pressão do óleo demasiado baixa • Sobretensão ou subtensão • Nível do líquido de refrigeração demasiado baixo • Combustível inadequado	Potencial paragem do gerador	3	3	9	
Bateria	Alimentação do Painel de Controlo	Subtensão/Sem tensão	• Falha do sistema de carga da bateria • Bateria no fim de vida • Bateria sulfatada • Ligações incorrectas ou danificadas	Painel de Controlo não é alimentado	3	3	9	

Deste modo, ao contrário do subsistema do Posto de Transformação, cujas avarias tinham um nível de risco aceitável, no subsistema do Grupo Gerador já é aconselhada a implementação de medidas de segurança adicionais.

Os modos de avaria dos restantes componentes do subsistema Grupo Gerador não são aqui apresentados, por terem níveis de RPN consideravelmente inferiores aos modos de avaria do motor e da bateria, mas podem ser consultados nas tabelas do anexo E.

4.3.3 – Subsistema Quadro de Transferência de Cargas

A hierarquia do subsistema do Quadro de Transferência de Cargas está ilustrada na Figura 4.3. Os componentes considerados neste subsistema foram os dois contactores - rede e gerador, o encravamento mecânico, a resistência de aquecimento e o interruptor. Os contactores e a resistência de aquecimento incluem um nível de detalhe adicional. Os contactores foram subdivididos em contactos, bobina e fusível de protecção, enquanto o subnível da resistência de aquecimento inclui a resistência e o fusível de protecção.

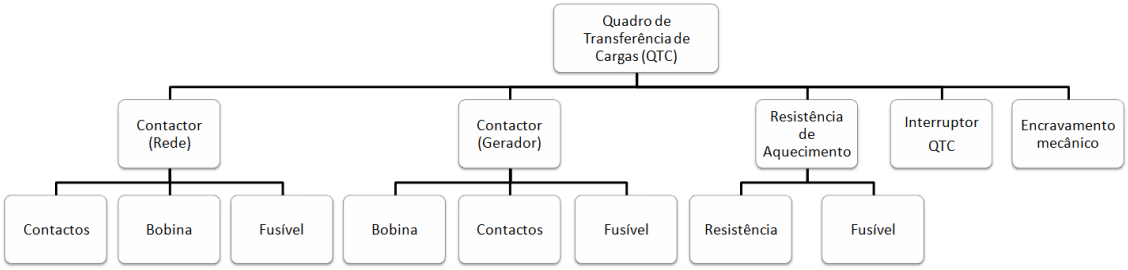


Figura 4.3 - Hierarquia do Subsistema Quadro de Transferência de Cargas

As tabelas 4.8 e 4.9 apresentam um extracto da FMEA do Quadro Transferência de Cargas. Na primeira tabela encontra-se o modo de avaria do encravamento mecânico e na segunda os modos de avaria dos componentes constituintes do contactor de rede.

Como se pode observar, o modo de avaria do encravamento mecânico apresenta um nível de Severidade muito elevado. Este valor reflecte o facto de uma avaria deste componente resultar na impossibilidade de alimentar as Salas de Servidores através do Posto de Transformação e do Grupo Gerador. Contudo, como já ocorreu noutros componentes, um baixo nível do índice de Ocorrência permite situar este modo de avaria na região de risco tolerável (cor amarela).

Tabela 4.8 - Extracto da FMEA do Quadro de Transferência de Cargas

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Encravamento mecânico	Impedir a ligação simultânea dos contactores de rede e gerador	Contactos do encravamento colados	Falha dos componentes mecânicos	A rede e o gerador ficam ligados em paralelo	4	1	4	*Actuação das protecções: não há energia proveniente da rede e do gerador*

Tabela 4.9 - Extracto da FMEA do Contactor de Rede do Quadro de Transferência de Cargas

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Bobina	Produzir campo magnético que atrai o núcleo do contactor	Curto-circuito	• Aquecimento excessivo • Corte de fios na bobina • Sobrecargas • Falha nos terminais devido a vibração do circuito	Não há comutação entre a rede e o grupo gerador	3	2	6	*Actuação do fusível de protecção da rede*
Contactos	Fecho/abertura do circuito	Mecanicamente em aberto	• Aquecimento excessivo • Desgaste prematuro • Pressão fraca • Contactos colados	O contacto não consegue fechar	3	2	6	
		Mecanicamente fechado		O contacto não consegue abrir				
Fusível	Dispositivo de corte e protecção contra sobreintensidades	Falha em aberto	• Sobreaquecimento • Queima intempestiva do elemento fusível (sobreintensidade)	A bobina do contactor de rede não é ligada	3	2	6	

Os modos de avaria dos componentes do contactor de rede inserem-se na região de risco tolerável da Matriz de Risco (cor amarela). Apesar do nível de Severidade ser significativo, como já ocorreu anteriormente, uma frequência de ocorrência remota torna o impacto destas avarias no sistema global aceitável. O elevado valor do índice de Severidade é justificado pelo facto de uma avaria do contactor de rede ter implicações na comutação entre a rede e o grupo gerador. O mesmo acontece com o contactor do gerador, cuja FMEA é muito semelhante à do contactor de rede

As tabelas com os modos de avaria dos restantes componentes do Quadro de Transferência de Cargas podem ser consultadas no anexo E.

4.3.4 – Subsistema Quadro de Emergência

No subsistema do Quadro de Emergência os componentes em análise são os disjuntores de protecção das três UPS e do sistema de Ar Condicionado, como se pode constatar a partir da Figura 4.4.

Uma vez que os disjuntores das UPS são equivalentes entre si, no extracto da FMEA do Quadro de Emergência apresentada na Tabela 4.10 só são apresentados os disjuntores de protecção da UPS 1 e do sistema de Ar Condicionado. A FMEA completa do Quadro de Emergência está presente no anexo E.

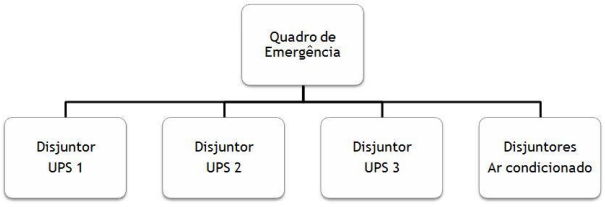


Figura 4.4 - Hierarquia do Subsistema Quadro de Emergência

Tabela 4.10 - Extracto da FMEA do Quadro de Emergência

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Disjuntor UPS1	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	UPS 1 não é alimentada	4	1	4	*As UPS têm redundância 2 em 3, pelo que a falha da UPS 1 só será crítica se a UPS 2 ou a UPS 3 também estiver avariada*
		Não abre na ocorrência de um defeito	• Contactos colados • Falha no sensor de corrente • Problema no mecanismo de abertura	Potencial falha de alimentação da UPS 1	3	1	3	
Disjuntor Ar condicionado	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	O ar condicionado não é alimentado	4	1	4	*Potencial sobreaquecimento das salas de servidores*
		Não abre na ocorrência de um defeito	• Contactos colados • Falha no sensor de corrente • Problema no mecanismo de abertura	Potencial falha de alimentação do ar condicionado	3	1	3	

A análise de criticalidade dos modos de avaria destes dois disjuntores permite concluir que o Quadro de Emergência não possui componentes críticos do sistema. Apesar do índice de Severidade classificar o modo de avaria de abertura indevida como uma avaria crítica, a elevada fiabilidade dos disjuntores leva a um factor de Ocorrência improvável. Deste modo, todos os componentes do Quadro de Emergência pertencem à região de risco tolerável da Matriz de Risco.

4.3.5 – Subsistema Ar Condicionado

A FMEA do subsistema Ar Condicionado pode ser vista na Tabela 4.11. Dos dois modos de avaria considerados – temperatura não é regulada e humidade excessiva – ambos apresentam o valor máximo de índice de Ocorrência. Isto indica-nos que estas avarias têm uma frequência de ocorrência mensal.

No que diz respeito à Severidade, o modo de avaria associado à temperatura é classificado como sendo pouco significativo. Deste modo, o risco que lhe está associado ainda se insere na região indesejável (cor laranja) da Matriz de Risco. Já o modo de avaria de humidade excessiva, que tem um índice de Severidade considerado significativo, pertence à região intolerável (cor vermelha) da Matriz de Risco.

Os resultados obtidos na análise da criticalidade do subsistema do Ar Condicionado permitem, assim, constatar uma forte necessidade de implementação medidas de segurança adicionais.

Tabela 4.11 - FMEA do Ar Condicionado

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Ar Condicionado	Controlo da temperatura e humidade das salas de servidores	Temperatura não é regulada	• Falha de ventilação • Falha do condensador • Filtro obstruído • Falha de alimentação de água para o humidificador • Falha do sensor de caudal de ar • Falha do sensor de temperatura e humidade • Temperatura da água fria elevada • Baixa pressão do compressor • Alta pressão do compressor • Não é alimentado	Potencial inoperacionalidade da estrutura das redes	2	5	10	*Sobreaquecimento das salas de servidores*
		Humidade excessiva		Potencial inoperacionalidade da estrutura das redes	3	5	15	*Actuação de protecções*

4.3.6 – Subsistema UPS

O subsistema UPS, cuja hierarquia é ilustrada na Figura 4.5, é constituído pelas três UPS do Sistema de Alimentação de Emergência. Dado que as características das UPS são idênticas e, por consequência, também os seus modos de avaria, na Tabela 4.12 da FMEA deste subsistema só são apresentados os modos de avaria da UPS1.

Como se pode comprovar na Tabela 4.12, todos os modos de avaria da UPS1 apresentam um índice de Severidade significativo. Como os modos de avaria relativos ao tempo de autonomia da UPS apresentam um valor baixo de Ocorrência, ainda pertencem à região de risco tolerável (cor amarela) da Matriz de Risco. Todavia, tendo em conta que o Número de Prioridade de Risco é relativamente elevado, não deve ser completamente descartada a hipótese de introduzir acções de redução do risco.

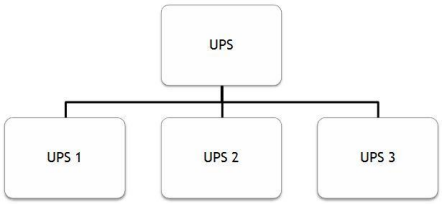


Figura 4.5 - Hierarquia do Subsistema UPS

Tabela 4.12 - FMEA do Subsistema UPS

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
UPS 1	Fornecer alimentação às cargas no caso de falha da rede de alimentação	Tempo de autonomia reduzido	• Sobrecarga • Bateria em descarga • Bateria no fim de vida	Em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	
		Tempo de autonomia nulo	Sobrecarga da UPS	UPS fora do circuito, em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	*Deslastragem de cargas*
		Distorção da tensão de saída	• Falha do rectificador • Falha do inversor	Pode resultar em danificação de componentes do sistema	3	3	9	
		Sem tensão	• Bateria em descarga • Bateria no fim de vida • Curto-circuito • Não tem tensão de entrada • Rectificador em aberto	Cargas não podem ser alimentadas pela UPS	3	3	9	

Os modos de avaria "Sem tensão" e "Distorção da tensão de saída" que, devido a uma frequência de Ocorrência ocasional, já pertencem à região da Matriz de Risco na qual o risco é considerado indesejável (cor laranja), reforçam a necessidade de implementação de acções de redução do risco.

4.3.7 – Subsistema Quadro das UPS

O Quadro das UPS fornece tensão aos quadros das salas de servidores. Por este motivo, os elementos deste subsistema considerados na FMEA são os disjuntores de protecção das Salas de Servidores A, B e C. A hierarquia deste subsistema é apresentada na Figura 4.6.

Tendo em conta que as características dos disjuntores das salas de servidores são iguais, na Tabela 4.13 é apresentado um extracto da FMEA do subsistema Quadro das UPS na qual apenas surge o disjuntor de protecção da sala de servidores A. Os modos de avaria dos outros dois disjuntores podem ser consultadas nas tabelas do anexo E.

Figura 4.6 - Hierarquia do Subsistema Quadro das UPS

Tabela 4.13 - Extracto da FMEA do Subsistema Quadro das UPS

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Disjuntor Quadro da Sala de Servidores A	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	O Quadro da Sala de Servidores A não recebe tensão	4	1	4	
		Não abre na ocorrência de um defeito	• Contactos colados • Falha no sensor de corrente • Problema no mecanismo de abertura	Potencial falha de tensão no Quadro da Sala de Servidores A	4	1	4	

Os disjuntores de protecção das salas de servidores não podem ser considerados elementos críticos do sistema como se pode ver pelo exemplo da Tabela 4.13. Apesar de apresentarem níveis de Severidade muito elevados, que classificam os modos de avaria como críticos, a improbabilidade da sua Ocorrência coloca-os na região de risco tolerável (cor amarela) da Matriz de Risco.

4.3.8 – Subsistemas Quadro das Salas de Servidores

Os componentes dos Quadros das Salas de Servidores A, B e C considerados na FMEA foram somente os disjuntores dos servidores. Apesar de cada sala constituir um subsistema diferente, na Tabela 4.14 os disjuntores das salas de servidores A e B são apresentados como um subsistema único, de modo a realçar a diferença dos índices de Severidade. A frequência de Ocorrência é a mesma para todos os modos de avaria considerados. Dado que o disjuntor é um componente fiável, a Ocorrência está classificada como improvável.

Tabela 4.14 - Extracto da FMEA dos Subsistemas Quadro das Salas de Servidores

Componente	Função	Modo (s) de Avaria	Causa (s)	Efeito (s)	S	O	RPN	Comentários e Soluções
Disjuntor Servidores A	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	Estrutura da rede inoperacional	5	1	5	
		Não abre na ocorrência de um defeito	• Contactos colados • Falha no sensor de corrente • Problema no mecanismo de abertura	Potencial inoperacionalidade da estrutura de rede	5	1	5	
Disjuntor Servidores B	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	• Falha no sensor de corrente • Falha interna do disjuntor • Causas humanas	Estrutura da rede inoperacional	4	1	4	
		Não abre na ocorrência de um defeito	• Contactos colados • Falha no sensor de corrente • Problema no mecanismo de abertura	Potencial inoperacionalidade da estrutura de rede	4	1	4	

Como se pode observar, os modos de avaria do disjuntor de protecção do conjunto de servidores A são classificados com um índice de Severidade catastrófico. Por outro lado, aos modos de avaria do disjuntor de protecção do conjunto de servidores B só foi atribuída um nível de Severidade crítico. Esta diferença deve-se ao facto de ser exigida ao conjunto de servidores A uma disponibilidade superior à do conjunto de servidores B.

Apesar dos elevados valores de Severidade, estes componentes pertencem à região de risco tolerável (cor amarela) da Matriz de Risco. Uma vez que o Número de Prioridade de Risco é baixo, não se justifica a aplicação de acções de redução de risco.

4.4 – Conclusões

No decorrer do presente capítulo foi-se analisando a criticalidade associada aos modos de avaria de alguns componentes. Detectou-se que os maiores números de prioridade do risco estavam associados aos subsistemas Grupo Gerador, Ar Condicionado e UPS. Dado que estes valores são bastante elevados, são recomendáveis acções de prevenção do risco.

Capítulo 5

Análise por Árvore de Falhas

As Árvores de Falhas são modelos gráficos que permitem mostrar o encadeamento de diferentes eventos relacionados com uma determinada falha. Partindo de um modo de avaria, denominado evento de topo, procuram-se as causas directas da ocorrência do evento. O objectivo fundamental é a identificação de todas as possíveis causas dessa avaria principal.

Uma análise quantitativa das Árvores de Falhas possibilita a estimativa da probabilidade com que determinada falha pode ocorrer. Embora o objectivo inicial fosse uma avaliação quantitativa da Árvore de Falhas, a falta de dados relativos às taxas de avaria dos componentes tornou esta abordagem inviável. Deste modo, fez-se uma somente avaliação qualitativa.

A Árvore de Falhas do Sistema de Alimentação de Emergência do Centro de Informática, apresentada neste capítulo, é um complemento da FMEA que foi desenvolvida. A análise da Árvore de Falhas também permite eliminar uma das principais desvantagens da FMEA, que corresponde à impossibilidade de avaliar uma avaria que tenha origem em eventos combinados.

De modo a facilitar a consulta dos eventos da Árvore de Falhas do Centro de Informática, esta foi repartida em árvores mais pequenas.

A Figura 5.1 representa o diagrama principal da Árvore de Falhas. Neste pode ser visto o evento de topo, ou seja, o evento indesejado que ocupa o topo da Árvore de Falhas e é o ponto de partida para sua elaboração. No caso do Centro de Informática, o evento de topo corresponde à inoperacionalidade da estrutura das redes A, B e C. Na verdade, devia existir uma árvore para cada uma das salas de servidores, sendo o evento de topo a inoperacionalidade da rede que lhe está associada. No entanto como são todas iguais isso não é necessário.

Como se pode observar, este evento pode ser originado por falhas em dois sistemas principais: o sistema de alimentação e o sistema térmico de protecção das salas de servidores. Assim, a partir da ramificação do evento de topo, a árvore começa a dividir-se em falhas originadas pelo sistema de alimentação e falhas originadas pelo sistema de ar condicionado.

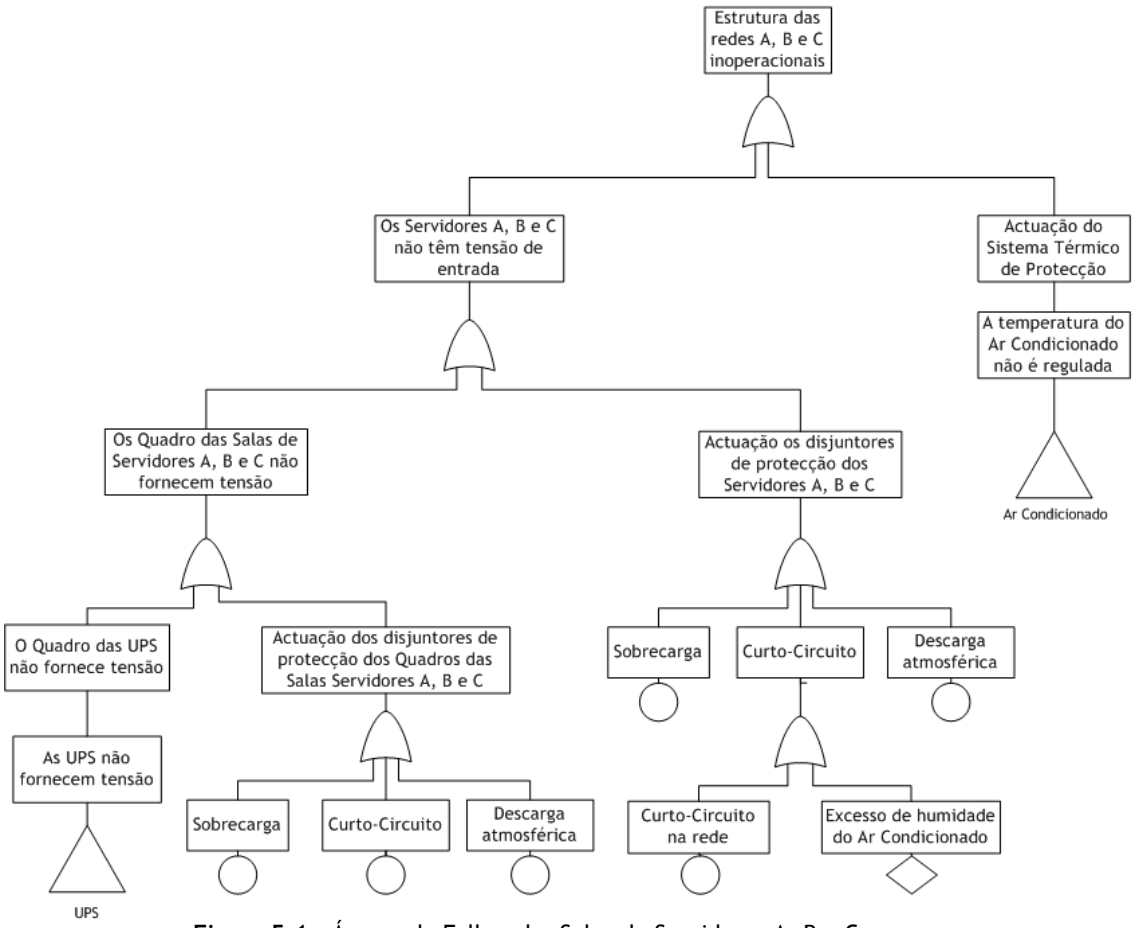


Figura 5.1 - Árvore de Falhas das Salas de Servidores A, B e C

A falha do sistema de alimentação directamente ligada ao evento de topo corresponde à ausência de tensão nos Servidores A, B e C. Este evento pode ter duas origens:

1. Os Quadros das Salas de Servidores A, B e C não fornecem tensão.

Este evento pode derivar da ausência de tensão das UPS e, por consequência, no Quadro das UPS ou da actuação dos disjuntores de protecção dos Quadros das Salas de Servidores. As causas da primeira situção serão desenvolvidas num diagrama posterior, conforme é indicado pelo símbolo de transferência no canto inferior esquerdo da Figura 5.1. O disparo dos disjuntores pode ser justificado pela ocorrência de uma sobrecarga, descarga atmosférica ou curto-circuito.

2. Actuaram os disjuntores de protecção dos Servidores A, B e C.

O disparo dos disjuntores de protecção dos servidores tem três causas possíveis: sobrecargas, descargas atmosféricas ou curto-circuitos. Como se pode ver na mesma figura, um curto-circuito nos servidores pode ter origem na rede ou ser provocado pelo excesso de humidade derivado de uma anomalia do ar condicionado.

As falhas com origem no sistema de Ar Condicionado estão expostas no diagrama da Figura 5.2. Como se pode observar, o evento "temperatura do Ar Condicionado não é regulada" pode ter diversas causas directas, entre as quais o filtro obstruído, pressão desregulada do compressor, falha dos sensores de temperatura e humidade e do caudal de ar, entre outras. Este elevado número de eventos básicos vem, assim, reforçar a conclusão retirada pela FMEA de que o Ar Condicionado é um componente crítico do sistema.

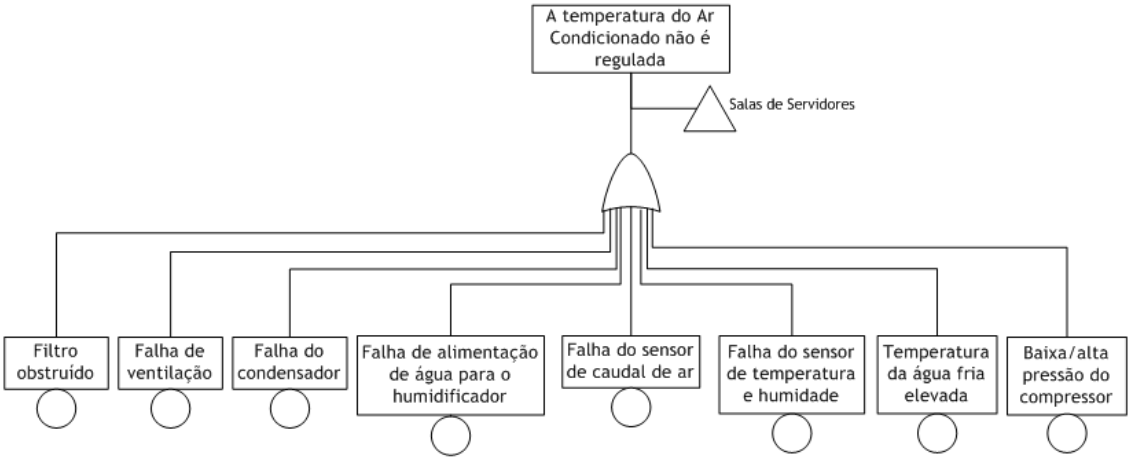


Figura 5.2 - Árvore de Falhas do Ar Condicionado

O diagrama da Figura 5.3 corresponde à secção da Árvore de Falhas relativa às UPS. Neste, pode ver-se que os eventos directamente ligados ao facto das UPS não fornecerem tensão são: actuação dos seus disjuntores de protecção por sobrecarga, curto-circuito ou descarga atmosférica ou o falha no fornecimento de tensão de pelo menos duas das três UPS.

A redundância das UPS está explícita através do uso de uma *gate* votadora, identificada com o número dois, que corresponde ao número mínimo de UPS que devem falhar para que o evento, acima referido, ocorra. A redundância das UPS é um exemplo de eventos combinados que não podem ser avaliados na FMEA. Nesta análise cada UPS é considerada individualmente, ao passo que na Árvore de Falhas pode considera-se a hipótese de falha simultânea de uma ou mais UPS. Consequentemente, é previsível que o índice de ocorrência das avarias com origem em falhas das UPS diminua.

Na sequência do diagrama surgem, ainda, o motivo do não fornecimento de tensão da UPS1, 2 e 3, analisadas individualmente. As causas que estão directamente na origem deste evento são o tempo reduzido da autonomia da UPS, devido à sua sobrecarga ou a uma falha da bateria e ausência da tensão proveniente do Quadro de Emergência. Como é possível ver pelos três símbolos de transferência, as causas deste evento serão exploradas num diagrama à parte.

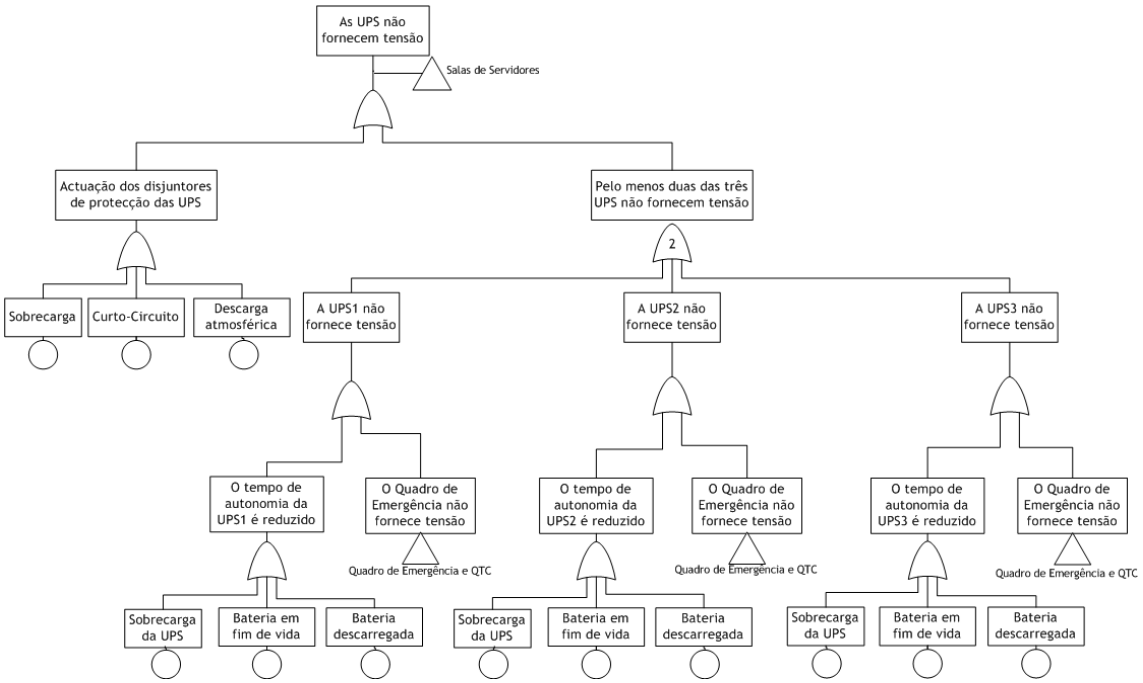


Figura 5.3 - Árvore de Falhas das UPS

Como se pode observar na Figura 5.4, o evento que está na origem da ausência de tensão no Quadro de Emergência é: "o Quadro de Transferência de Cargas não fornece tensão". Este, por sua vez, pode derivar de quatro situações distintintas:

1. O interruptor do Quadro de Transferência de Cargas foi aberto, devido a causas humanas;

2. O Quadro de Transferência de Cargas não recebe tensão do Posto de Transformação nem do Grupo Gerador.

Este evento só ocorre quando os disjuntores de protecção do alternador e transformadores actuam ou o Posto de Transformação e o Grupo Gerador não fornecem tensão ao Quadro de Transferência de Cargas. Neste último caso, a falha tem origem numa combinação de eventos. Tal como no caso das UPS, a FMEA não considera esta situação já que o Grupo Gerador e o Posto de Transformação são vistos como subsistemas independentes.

A ausência de tensão do Posto de Transformação resulta do facto desta não ser fornecida pelo Quadro Geral de Baixa Tensão. As causas na origem deste evento serão desenvolvidas, posteriormente, no diagrama referente ao Posto de Transformação. O mesmo se aplica ao evento "o Grupo Gerador não fornece tensão" que será desenvolvido no diagrama Grupo Gerador.

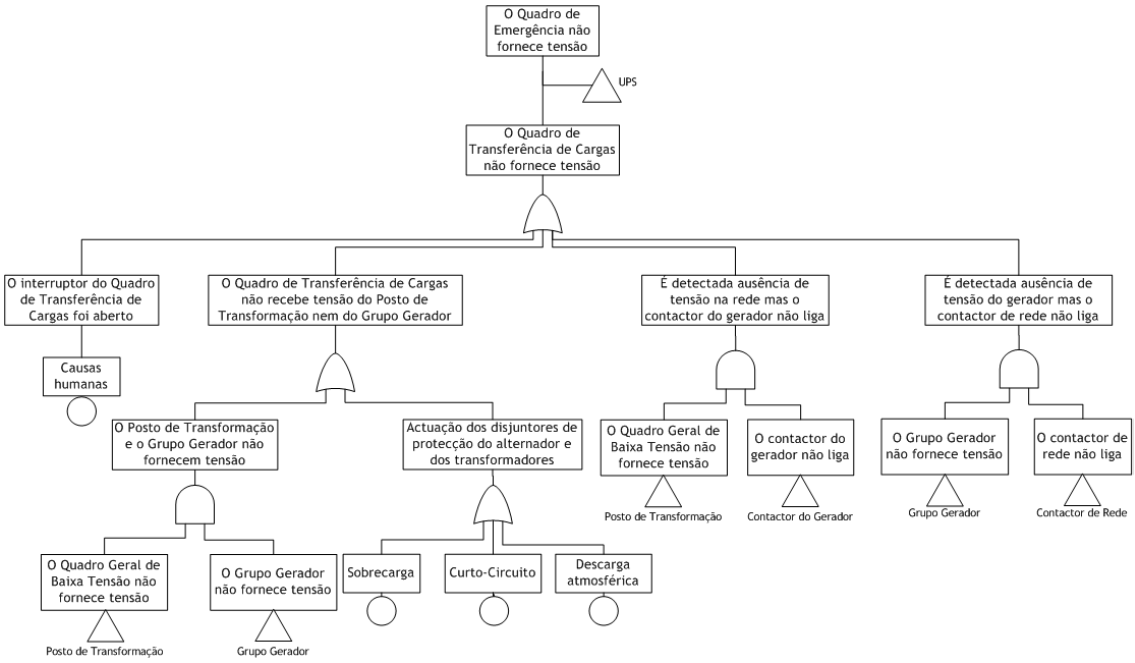


Figura 5.4 - Árvore de Falhas do Quadro de Transferência de Cargas

3. É detectada ausência de tensão na rede mas o contactor do gerador não liga.

As causas directas da origem desta falha são: "o contactor do gerador não liga" e "o Quadro Geral de Baixa Tensão não fornece tensão". Estes eventos serão desenvolvidos nos diagramas Contactor do Gerador e Posto de Transformação, respectivamente.

4. É detectada ausência de tensão do gerador mas o contactor de rede não liga.

Quando o Grupo Gerador não fornece tensão e o contactor de rede não liga, situações que serão exploradas mais adiante, ocorre este evento. Mais uma vez, trata-se de uma combinação e a obrigatoriedade da ocorrência destas duas causas para que ocorra o evento está representada através do uso de uma *gate AND*.

As Figuras 5.5 e 5.6 apresentam os diagramas das Árvores de Falhas dos contactores do gerador e da rede, respectivamente. Como se pode constatar, as falhas são muito semelhantes. A origem destas pode ser devida aos contactos do contactor estarem colados ou ao curto-circuito da bobina. Por sua vez, este evento pode decorrer de sobreaquecimento, sobrecargas, corte nos fios da bobina ou actução do fusível de protecção.

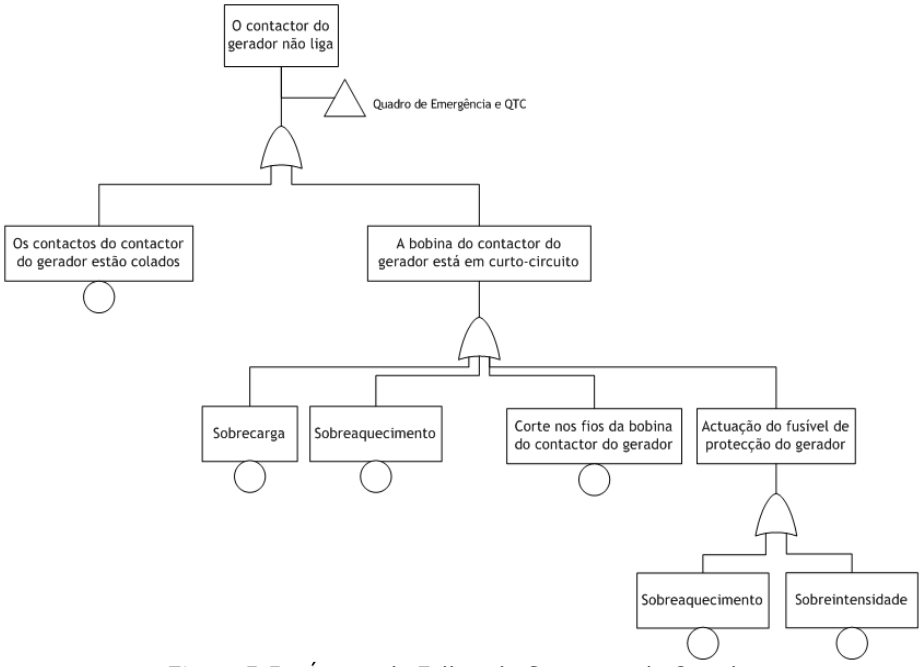


Figura 5.5 - Árvore de Falhas do Contactor do Gerador

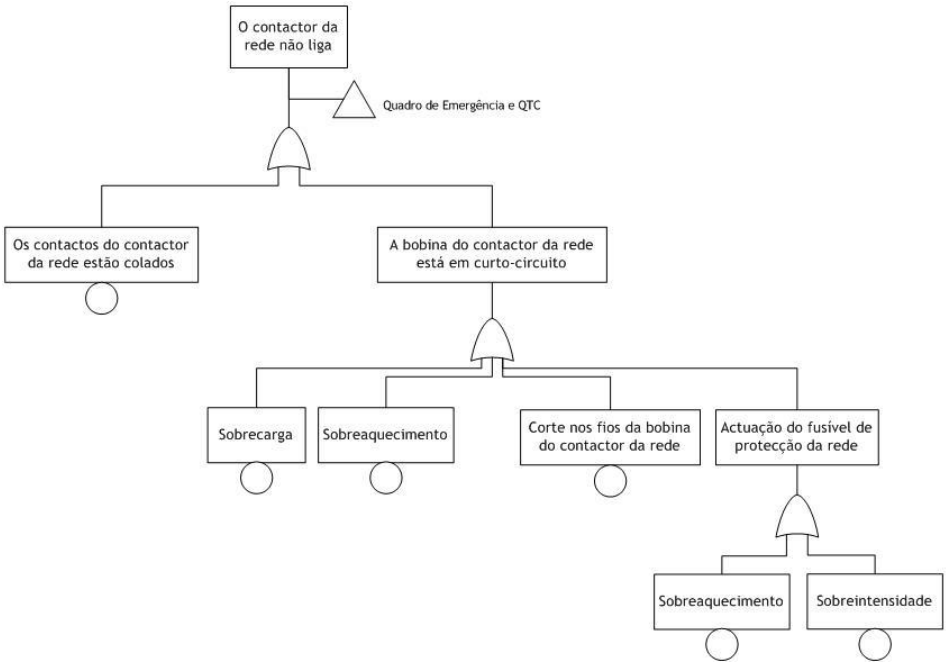


Figura 5.6 - Árvore de Falhas do Contactor da Rede

As falhas que estão na origem do, já referido, evento “o Grupo Gerador não fornece tensão” podem ser analisadas na Figura 5.7. Como se pode verificar, a árvore possui duas ramificações, uma associada ao falha do arranque do Grupo Gerador e a outra à quebra da sua produção de energia eléctrica.

No que diz respeito à quebra da produção de energia eléctrica, esta pode resultar de uma falha do alternador ou da actuação do seu disjuntor de protecção, devido a uma sobrecarga ou curto-circuito. As causas directas da falha do alternador são: o alternador não tem tensão e a tensão do alternador falha subitamente. Os seus eventos básicos podem ser consulta na parte inferior da supramencionada.

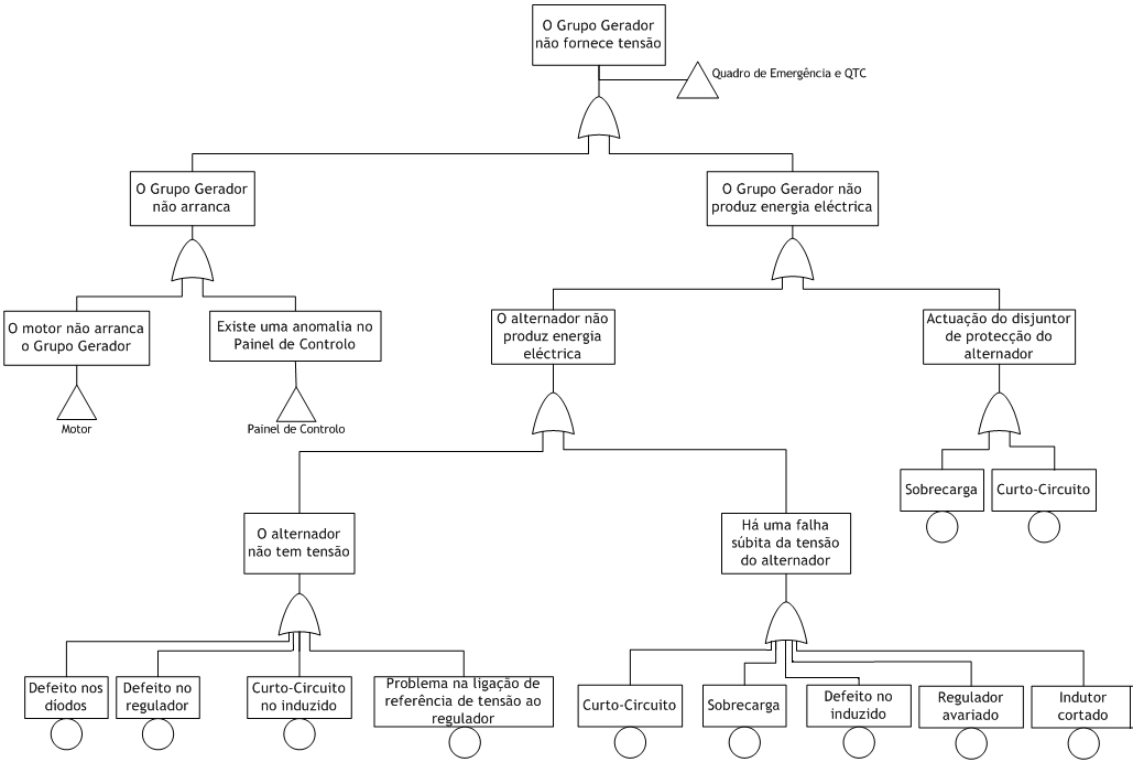


Figura 5.7 - Árvore de Falhas do Grupo Gerador

A falha do arranque do gerador pode resultar da incapacidade do motor o realizar ou de uma anomalia no Painel de Controlo. As causas na origem destas duas situações estão presentes nos diagramas das Figuras 5.8 e 5.9, respectivamente.

O evento “o motor não arranca o Grupo Gerador “ pode ser motivado pelas três seguintes causas: o motor não consegue arrancar, o motor sobreaquece e o motor pára intempestivamente. Os eventos básicos na sua origem podem ser consultados na Figura 5.8. É de realçar que a falha “o motor pára intempestivamente” pode ser originada, também, por uma falha no sistema de refrigeração do motor, representada pelo evento “temperatura do motor está fora dos limites”.

Como se pode ver na Figura 5.9, a falha correspondente à anomalia no Painel de Controlo pode derivar de informações inadequadas do acerca do estado da rede pelo transformador de isolamento ou de uma falha da sua alimentação, por ausência de tensão da bateria. As informações do transformador de isolamento, por sua vez, podem ser influenciadas pela ausência de tensão ou subtensão do transformador e ainda pelo disparo do seu disjuntor de protecção.

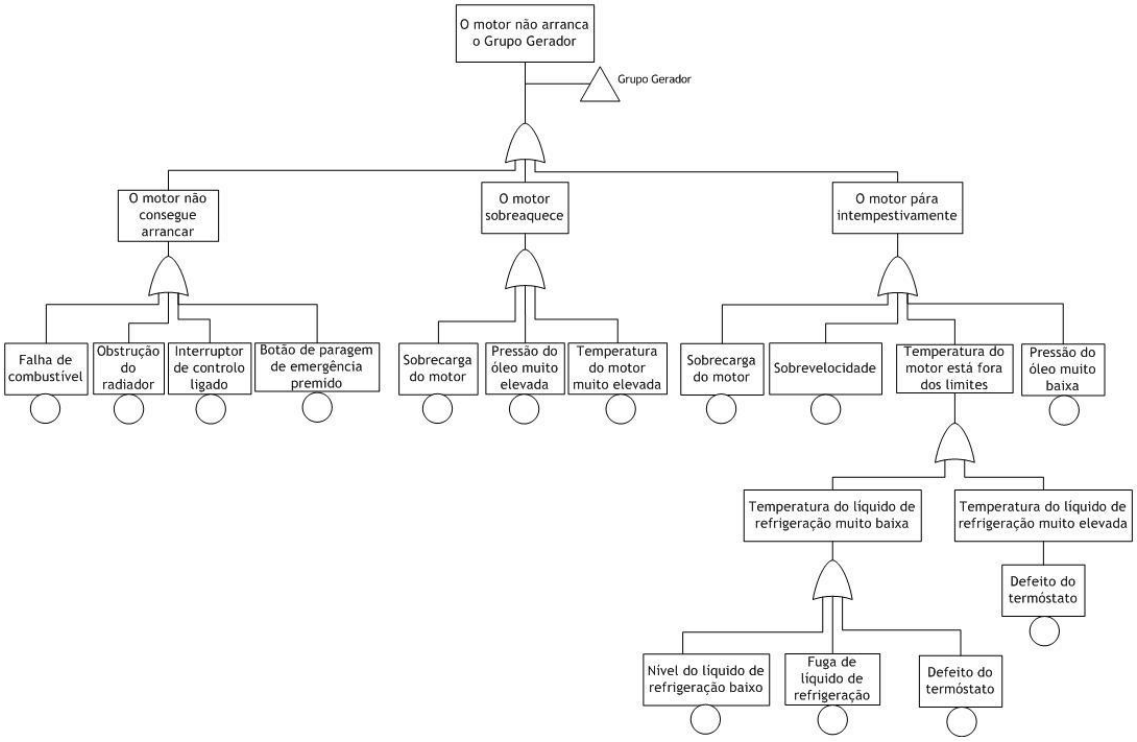


Figura 5.8 - Árvore de Falhas do Motor

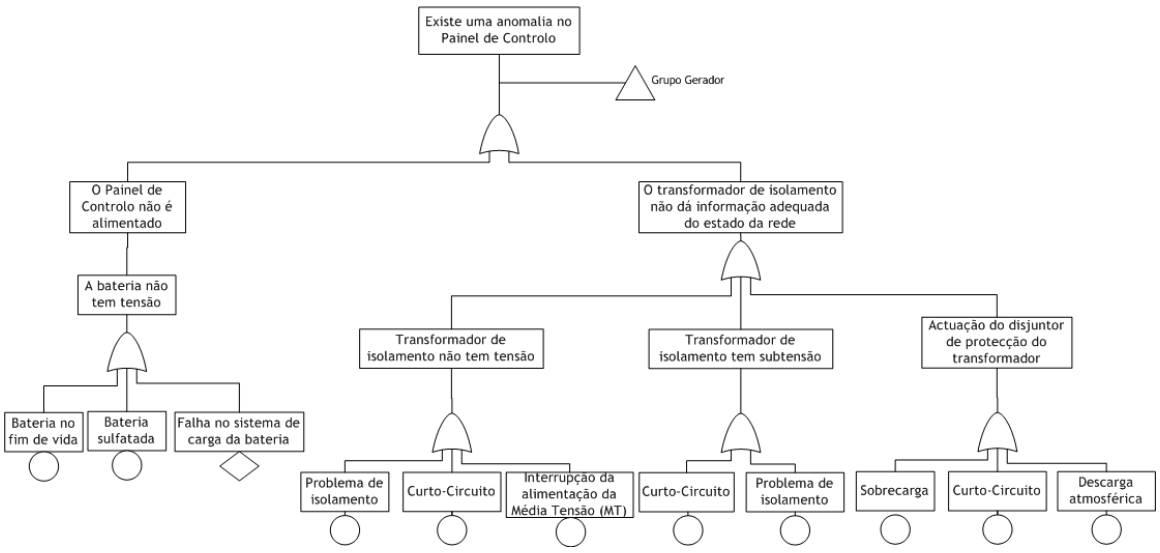


Figura 5.9 - Árvore de Falhas do Painel de Controlo

O diagrama da Figura 5.10 apresenta as combinações de falhas que resultam no evento “o Quadro Geral de Baixa Tensão não fornece tensão”. As causas directas na sua origem correspondem à actuação dos disjuntores de protecção, evento que está desenvolvido no diagrama da Figura 5.11, e a ausência de tensão proveniente dos transformadores.

A falha com a descrição “os transformadores não fornecem tensão” pode derivar dos eventos “nenhum dos transformadores fornece tensão” ou “o transformador 1 não fornece tensão e o interbarras não conduz corrente”. É de notar que ambos derivam da combinação de eventos: para que o primeiro ocorra é obrigatório que os dois transformadores não forneçam tensão e o segundo exige que não só que o transformador 1 não forneça tensão mas também que haja uma falha do disjuntor Interbarras. As potenciais causas do evento “o transformador 1 não fornece tensão” são mostradas no diagrama da Figura 5.12.

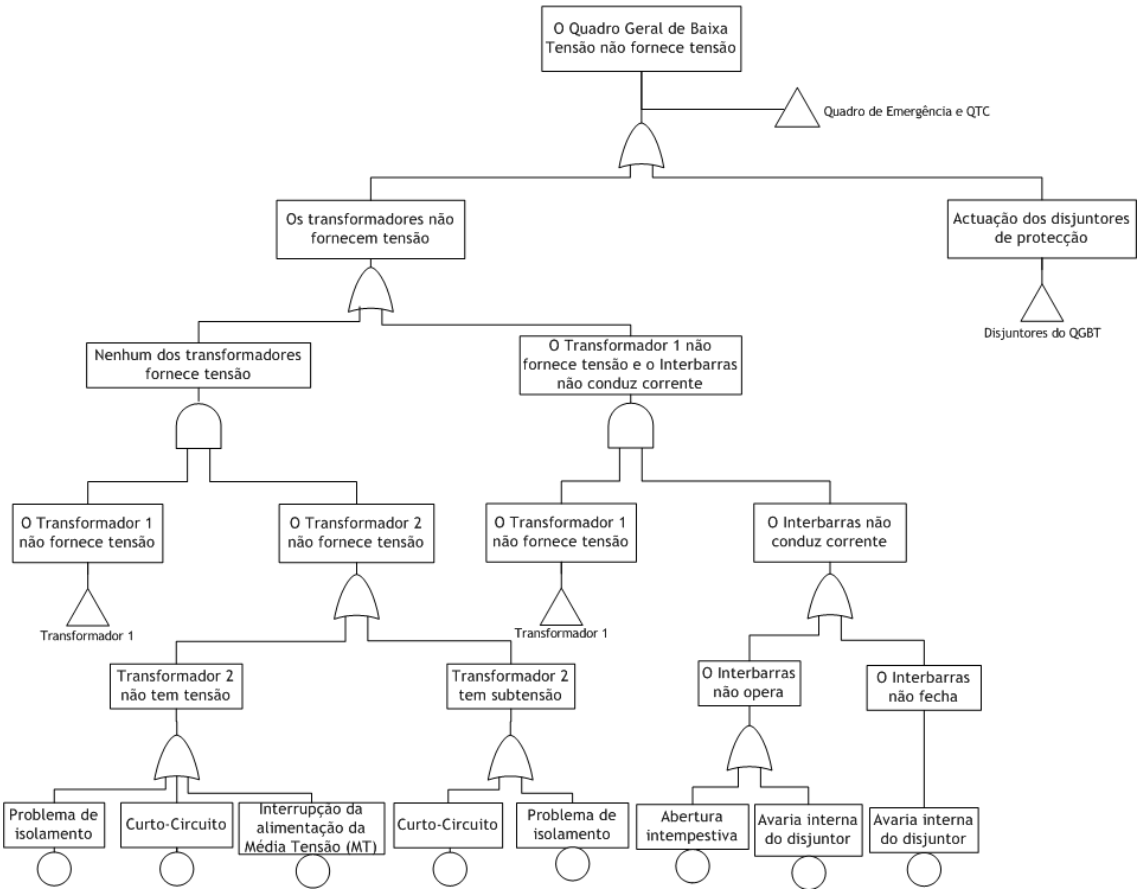


Figura 5.10 - Árvore de Falhas do Posto de Transformação

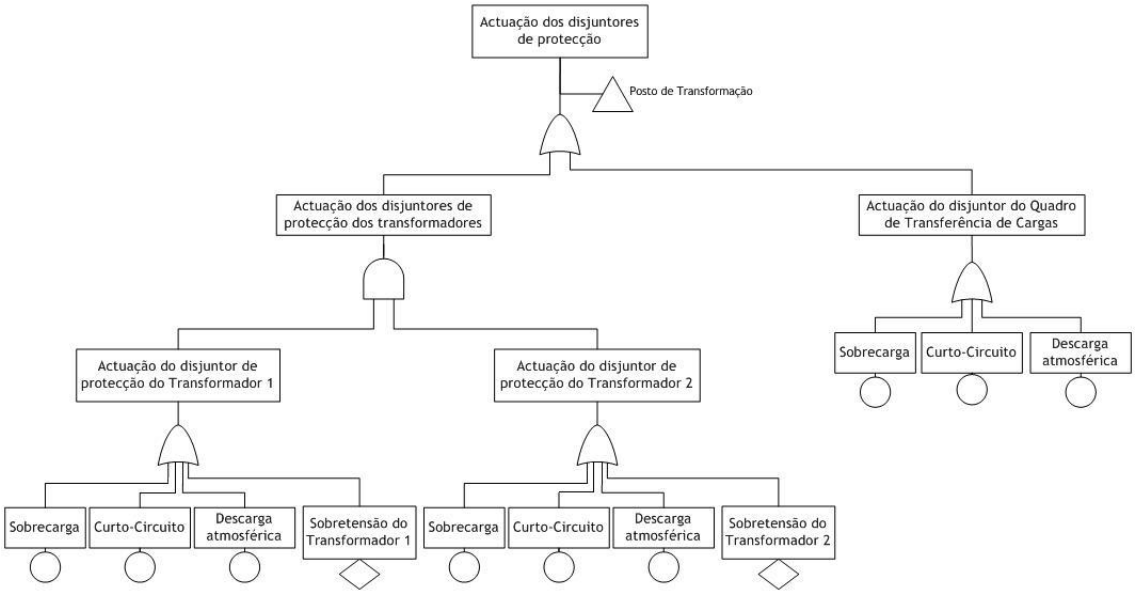


Figura 5.11 - Árvore de Falhas do Quadro Geral de Baixa Tensão

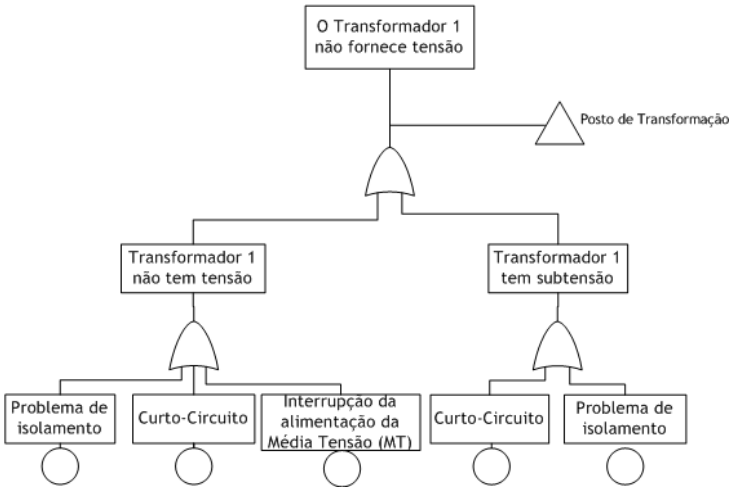


Figura 5.12 - Árvore de Falhas do Transformador 1

Capítulo 6

Soluções Propostas

Neste capítulo, será apresentado o plano de acções recomendado para minorar os riscos dos componentes considerados mais críticos do sistema.

A tabela 6.1 expõe a hierarquização dos Números de Prioridade do Risco dos modos de avaria, obtidos pela FMEA e analisados no Capítulo 4, que obtiveram as classificações mais elevadas.

Tabela 6.1 - Hierarquização dos Números de Prioridade do Risco

Subsistema	Componente	Função	Modo(s) de Avaria	Efeito(s)	RPN
Ar condicionado	Ar condicionado	Controlo da temperatura e humidade das salas de servidores	Humidade excessiva	Potencial inoperacionalidade da estrutura das redes	15
			Temperatura não é regulada	Potencial inoperacionalidade da estrutura das redes	10
Grupo Gerador	Motor	Arranque do gerador	Não arranca	O Grupo Gerador não arranca	9
			Arranca mas pára intempestivamente	Potencial paragem do gerador	9
	Bateria	Alimentação do painel de controlo (autómato)	Subtensão / sem tensão	O Painel de Controlo não é alimentado	9
UPS	UPS 1	Fornecer alimentação às cargas no caso de falha da rede de alimentação	Distorção da tensão de saída	Pode resultar em danos nos componentes do sistema	9
			Sem tensão	Cargas não podem ser alimentadas pela UPS	9
			Tempo de autonomia reduzido	Em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	6
			Tempo de autonomia nulo	UPS fora do circuito, em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	6

Como se pode constatar a partir da tabela, os modos de avaria do ar condicionado apresentam os Números de Prioridade do Risco mais elevados, seguido pelos modos de avaria do motor e bateria do subsistema Grupo Gerador e UPS1. É de notar que, na análise FMEA, os modos de avaria obtidos para as três UPS são os mesmos. Optou-se por só apresentar os modos de avaria da UPS1 na tabela 6.1 por uma questão de simplificação.

Na análise por Árvore de Falhas desenvolvida no capítulo 5, detectou-se que os eventos mais importantes na origem do evento de topo – estrutura das redes A, B e C inoperacionais – derivavam de falhas em dois sistemas: o sistema de alimentação e o sistema de ar condicionado.

Na ramificação da árvore correspondente ao sistema de ar condicionado observou-se que a falha de regulação de temperatura é o evento mais relevante e pode ser originada por um elevado número de causas básicas.

No que diz respeito à ramificação da árvore relativa ao sistema de alimentação, a falha que surge directamente ligada ao evento de topo corresponde à ausência de tensão nos Servidores A, B e C. Analisando esta secção da Árvore de Falhas, detectou-se que esta situação pode ocorrer pela actuação dos disjuntores de protecção dos servidores ou por ausência de tensão nos quadros das salas de servidores. Este último evento, por sua vez, pode ser originado por uma falha de tensão do Quadro das UPS e, por consequência, pela falha da tensão proveniente das UPS. Depreende-se, assim, que uma falha neste subsistema pode contribuir, de forma relevante para a ocorrência do evento de topo.

Deste modo, a partir dos resultados obtidos através das análises FMEA e por Árvore de Falhas, concluiu-se que o Ar Condicionado, o Grupo Gerador e as UPS são os elementos mais críticos do sistema.

A FMEA das UPS permitiu concluir que seria aconselhável tomar algumas medidas de redução do risco inerente a este subsistema. No entanto, a partir da análise da Árvore de Falhas observou-se que uma falha de tensão do subsistema das UPS está dependente da ocorrência do evento combinado da falha de pelo menos duas UPS. Assim, provavelmente, a ocorrência dos modos de avaria não será tão elevada como a determinada na FMEA, que analisa as avarias de cada UPS individualmente. Mesmo assim, propõe-se medidas que contribuirão para melhorar o seu desempenho, tendo em conta a importância destes componentes no Sistema de Alimentação de Emergência:

1º. Monitorizar, online, o sistema de baterias das UPS e implementar um sistema de deslastragem das cargas.

O principal objectivo da monitorização contínua do sistema de baterias das UPS, através de um computador remoto, consiste em poder reduzir a ocorrência dos modos de avaria destes equipamentos derivados de tempo de autonomia reduzido através do aumento do seu tempo de vida útil.

Ao longo do tempo, factores como condições adversas, temperatura incorrecta e um regime fraco de carregamento diminuem a performance da bateria e podem dar origem a falhas prematura nos sistemas de bateria. Ao monitorizar estes parâmetros, possível identificar previamente as causas da falha antes de se produzir qualquer dano e ocorrer uma falha na bateria.

Tipicamente, os fabricantes fornecem o software necessário para a instalação desta funcionalidade.

No que diz respeito ao sistema de deslastragem das cargas, este deve fazer uma divisão dos equipamentos existentes nas salas de servidores em cargas prioritárias e cargas não prioritárias, de modo a aumentar o tempo de funcionamento das UPS. A deslastragem de cargas permite, ainda, evitar picos de consumo ao fazer uma gestão por prioridades dos consumos máximos dos equipamentos. A implementação desta medida requer, contudo, que sejam adquiridos dispositivos que permitam efectuar a monitorização e o corte automático das cargas, de acordo com a sua prioridade.

2º. Avaliar a possibilidade de aumentar a redundância das UPS, para 3+1, ou colocar uma UPS como alimentação de emergência da sala de servidores A.

Esta medida foi sugerida uma vez que existe uma quarta UPS disponível, actualmente sem ser utilizada, pelo que não seria necessária a aquisição de um novo equipamento.

Uma configuração das UPS com redundância 3+1 significa que, para que as UPS forneçam tensão, pelo menos três têm de estar operacionais. Prevê-se que a utilização desta configuração aumente o tempo de autonomia das UPS e, por consequência, a autonomia das salas de servidores.

Por outro lado, dado que a Sala de Servidores A apresenta maiores requisitos de disponibilidade, a quarta UPS pode ser utilizada para alimentação exclusiva desta sala. Por exemplo, em caso de ausência da tensão do Posto de Transformação, Grupo Gerador ou das restantes UPS, esta seria responsável por fornecer tensão para a Sala de Servidores A, de modo a garantir a sua autonomia.

3º. Instalar o software disponibilizado pelo fabricante das UPS que permite monitorizar continuamente o seu estado e fazer *shutdown* controlado.

A monitorização contínua do estado das UPS permite um maior controlo da ocorrência das suas avarias e, consequentemente, uma reparação e manutenção mais rápida.

O controlo do *shutdown*, por sua vez, tem como objectivo a possibilidade de estabelecer prioridades para as várias aplicações. Isto é, deve-se começar por fazer o *shutdown* das aplicações de menor importância e finalizar com as aplicações mais críticas.

4º. Implementar um sistema que faça a notificação periódica do estado das UPS via SMS.

O sistema de notificação do estado das UPS funcionaria como um complemento da medida acima sugerida, com o intuito de aumentar a eficácia de detecção de potenciais avarias nestes equipamentos. Para que seja enviada a notificação periódica, por este método, tem de ser adquirido um modem SMS.

Na FMEA do subsistema Grupo Gerador os modos de avaria do motor e da bateria obtiveram uma classificação elevada do Número de Prioridade do Risco (9) e correspondente a um nível de criticalidade indesejável. Assim, é altamente recomendável a execução de acções de redução do risco.

Como se observa na Árvore de Falhas, a falha do arranque do gerador pode derivar de uma avaria do motor ou de uma anomalia do painel de controlo. De facto, uma avaria do motor que impeça o arranque do grupo pode ser muito crítica porque as UPS só conseguem garantir a disponibilidade das Salas de Servidores por um período máximo de trinta minutos.

Contudo, como se pode constatar uma avaria da bateria resulta na falha de alimentação do Painel de Controlo. Caso esta situação ocorra, o grupo não só não arranca, porque não é enviado sinal ao motor, como as informações importantes por ele monitorizadas ficam indisponíveis. Assim, a mitigação do risco associado à avaria da bateria de alimentação do painel deve ser considerada prioritária. Portanto, as recomendações para melhorar o desempenho do Grupo Gerador são as seguintes:

1º. Implementar um sistema de monitorização remota do grupo que permita o controlo do estado das principais variáveis do gerador, nomeadamente a tensão da bateria que alimenta o painel de controlo e o nível de combustível do gerador, pela gestão técnica centralizada. Envio de um alarme (por exemplo via SMS ou email) em caso de detecção de qualquer anomalia;

O sistema de monitorização remota do grupo é montado à parte do gerador e permite a consulta, à distância, do funcionamento do grupo ou de condições de alarme. A implementação desta medida requer a aquisição de um indicador remoto de falhas, disponibilizado pelo fabricante, e de um modem SMS para o envio de notificações.

2º. Uma vez que existe um outro gerador de emergência que pode ser disponibilizado apesar de estar adstrito a outros edifícios, deve considera-se a hipótese da redundância dos geradores;

Para ser possível a comutação entre os dois geradores seria necessário acrescentar um Quadro de Transferência de Cargas, com funcionamento idêntico ao descrito no Capítulo 2.

3º. Adicionar um sistema de detecção de presença, no Posto de Transformação e Grupo Gerador, de modo a prevenir potenciais actos de vandalismo. Envio de um SMS a um segurança quando detectada uma intrusão indesejada.

O sistema de detecção de presença tem como principal objectivo evitar acções de má-fé que possam por em causa o funcionamento do Posto de Transformação e do Grupo Gerador. Para esse efeito, devem ser adquiridos sensores que permitam a detecção de presenças, tais como, detectores de infravermelho, detectores de microondas ou sensores de detecção perimétrica. O envio do alarme à segurança exige, ainda, a aquisição de um modem SMS.

Os dois modos de avaria do sistema de ar condicionado obtiveram os mais elevados Número de Prioridade de Risco da análise FMEA. Um deles, a falha de regulação da temperatura, possui um nível de risco indesejável e o outro, humidade excessiva, tem um nível de risco intolerável. De acordo com os critérios estabelecidos para a análise da criticalidade, um modo de avaria considerado intolerável na FMEA é o suficiente para serem obrigatórias medidas de mitigação do risco adicionais. Por outro lado, observando os resultados da análise por Árvore de Falhas, constata-se que existe um número bastante significativo de causas directas na origem da falha de regulação da temperatura. Esta constatação reforça os resultados da FMEA. O plano de acções que se julga adequado para mitigar os riscos associados ao sistema de ar condicionado é:

1º. O ar condicionado, alimentado pelo Quadro de Emergência, deverá também ser ligado às UPS, dado ser uma carga crítica;

2º. Acrescentar sensores de humidade, pelo menos um por equipamento, e ainda sensores de nível para prevenção de potenciais excessos de humidade ou fugas de água nas salas de servidores;

A aquisição dos sensores de humidade e de nível é bastante importante devido à ocasional queda de condensação proveniente do ar condicionado. O excesso de humidade pode dar origem a curto-circuitos nalguns servidores e, por consequência, à actuação das suas protecções. Caso esta situação ocorra, estes servidores ficam, temporariamente, indisponíveis.

3º. Instalar um sistema de insuflação para melhor aproveitamento dos caudais de ar, através de grelhas adicionais no pavimento falso. Também é recomendável a instalação de um sistema de exaustão ou de ventiladores que permitam a extracção do ar quente;

A instalação de um sistema de insuflação e exaustão tem como principal objectivo a prevenção de excessos de temperatura nas salas de servidores, que podem resultar na actuação do sistema de protecção térmico do Ar Condicionado e na inoperacionalidade dos equipamentos.

4º. Estudar a aplicabilidade de redundância do ar condicionado correspondente a estruturas de refrigeração do tipo N+1, ou seja, para cada equipamento, há outro de reserva e pronto para uso imediato.

A implementação desta medida requer a aquisição de um outro sistema de ar condicionado de modo que, caso haja uma avaria no ar condicionado, este esteja pronto a entrar em funcionamento, sem permitir o sobreaquecimento das salas de servidores.

Apesar de as estruturas de refrigeração redundante serem bastante utilizadas em grandes Centros de Informática, esta solução pode tornar-se dispendiosa.

Uma vez que se prevê que a implementação das outras medidas seja suficiente para reduzir, de forma eficaz, os modos de avaria associados ao ar condicionado, esta sugestão só deve ser considerada se a relação entre o custo e o benefício for bastante vantajosa.

No decorrer do estudo do Sistema de Alimentação de Emergência do Centro de Informática foi detectado o problema do acesso das salas de servidores, resultante de um eventual corte de energia. Como esse acesso é feito através da leitura de um cartão, de banda magnética, este implicaria não só que o cartão não seria lido mas também que a base de dados com a lista de utilizadores com permissões de acesso não seria consultada. Nesta situação, a única maneira de aceder ao interior das salas de servidores seria por abertura manual da porta, através de uma chave mestra. Portanto, o referido acesso ficaria condicionado, não podendo ser feito com a rapidez expectável.

Apesar de não pertencer ao âmbito da análise FMEA e da análise por Árvore de Falhas, deixa-se a recomendação final de repensar este acesso das salas de servidores, em especial o modo de alimentação do sistema de cartões.

Capítulo 7

Conclusões

No culminar desta dissertação, retiram-se conclusões que se julgam importantes. Em primeiro lugar que a escolha das duas metodologias utilizadas para o desenvolvimento deste trabalho foi adequada. Na realidade, só com a conjugação da análise FMEA e da análise por Árvore de Falhas é que se pôde examinar com maior precisão quais são os modos de avaria que necessitam de acções prioritárias de mitigação do risco.

A análise FMEA não considera avarias simultâneas de componentes, apenas os modos de avaria individuais de cada elemento. Por isso, verificou-se que alguns dos componentes considerados críticos nesta análise não são tão críticos para o sistema como seria esperado, visto existirem componentes em redundância ou falhas que dependem de outros eventos. Estas situações só foram detectadas através da análise por Árvore de Falhas. Concluiu-se que o uso conjunto destas ferramentas resultou numa mais-valia porque uma ferramenta beneficia-se com a utilização da outra.

Embora a realização deste trabalho tenha sido feita unicamente de forma qualitativa e com base no conhecimento do funcionamento do sistema, por não estar disponível o histórico de avarias de alguns dos seus componentes, julga-se que, mesmo assim, se obtiveram resultados bastante aceitáveis.

A partir destas análises, pôde-se assim determinar qual era o elemento mais crítico do sistema - o Ar Condicionado. Atendendo à importância que os subsistemas Grupo Gerador e UPS têm, apesar de não possuírem um nível de criticalidade tão elevado como o elemento supracitado, devem ser também considerado elementos muito críticos do sistema.

Detectados os elementos mais críticos do sistema e, com base no conhecimento que foi sendo adquirido ao longo da elaboração deste trabalho, foi proposto um conjunto de medidas de redução do risco que se considera adequado, tendo em conta as características do Sistema de Alimentação de Emergência do Centro de Informática.

Espera-se que a implementação de algumas destas medidas origine uma diminuição da ocorrência de alguns dos modos de avaria considerados mais críticos, melhorando assim o desempenho e disponibilidade do sistema.

Referências

[1] *IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*.

[2] Grupo gerador: Manual técnico de operação e manutenção, Dezembro 2002.

[3] Clifton A. Ericson. (2005) *Hazard analysis techniques for system safety*. Edição de John Wiley and Sons

[4] Quality Associates International, http://www.quality-one.com/services/fmea.php. Acesso em Maio de 2009.

[5] SGS, http://www.sgs.com/qs_9000-2?serviceId=13425&lobId=24178. Acesso em Maio de 2009.

[6] Society of Automotive Engineers, http://www.sae.org/technical/standards/J1739_200901. Acesso em Maio de 2009.

[7] FMEA Info Center, http://www.fmeainfocentre.com/standards.htm. Acesso em Maio de 2009.

[8] IEC 60812: 1985, *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*.

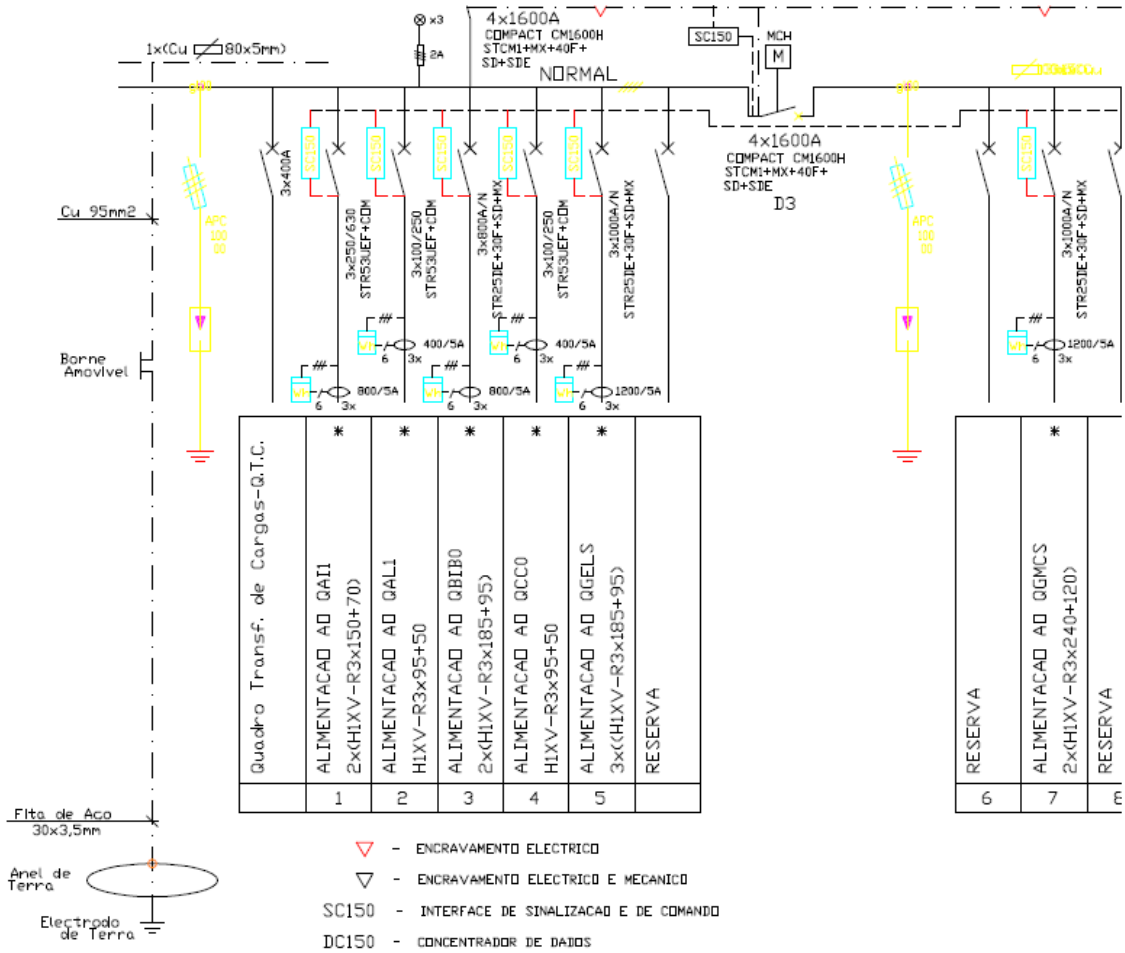
[9] Clifton A. Ericson, *"Fault Tree Analysis – A History"*, 1999. Disponível em http://www.fault-tree.net/papers/ericson-fta-history.pdf

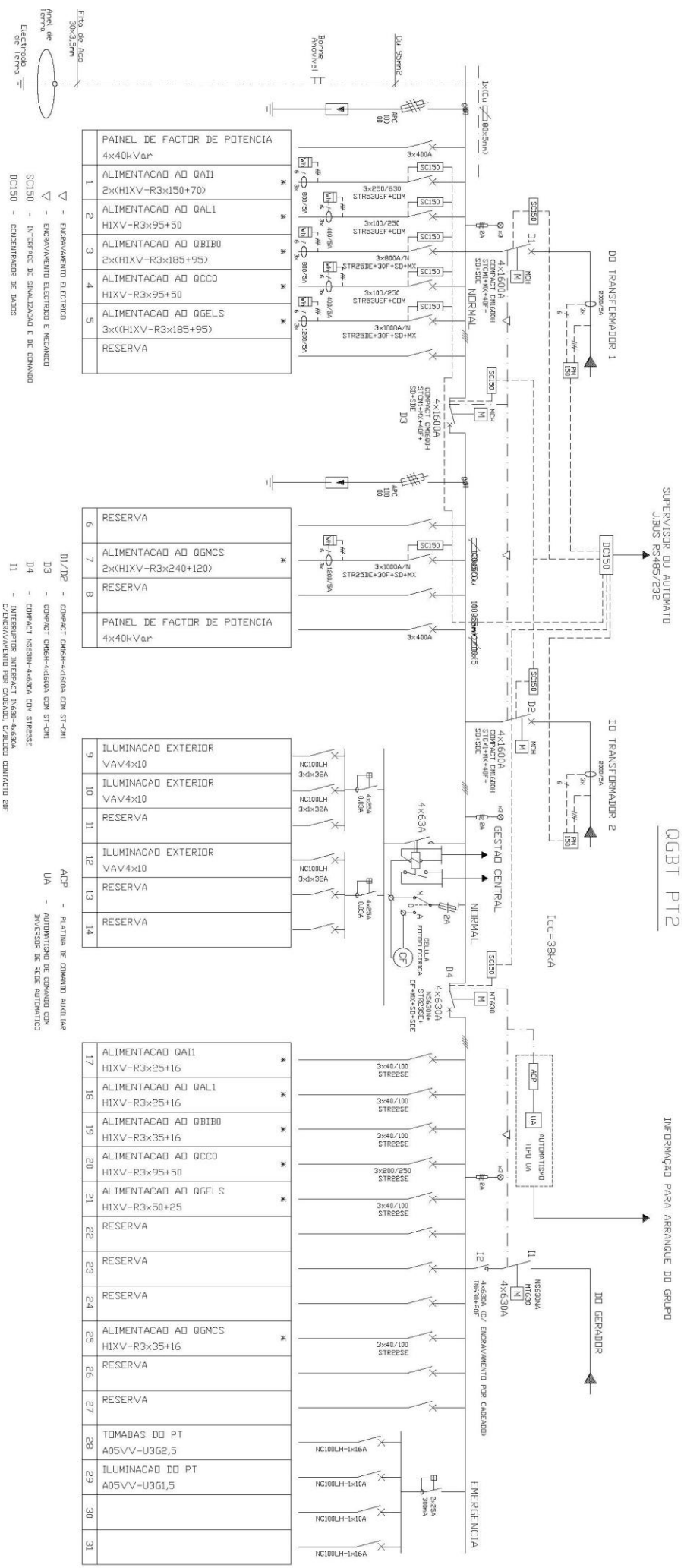
[10] NASA. *Fault Tree Handbook with Aerospace Applications*, NASA Office of Safety and Mission Assurance, Washington DC, 2002

[11] IEC 61025: 2006, *Fault Tree Analysis (FTA)*

Anexo A

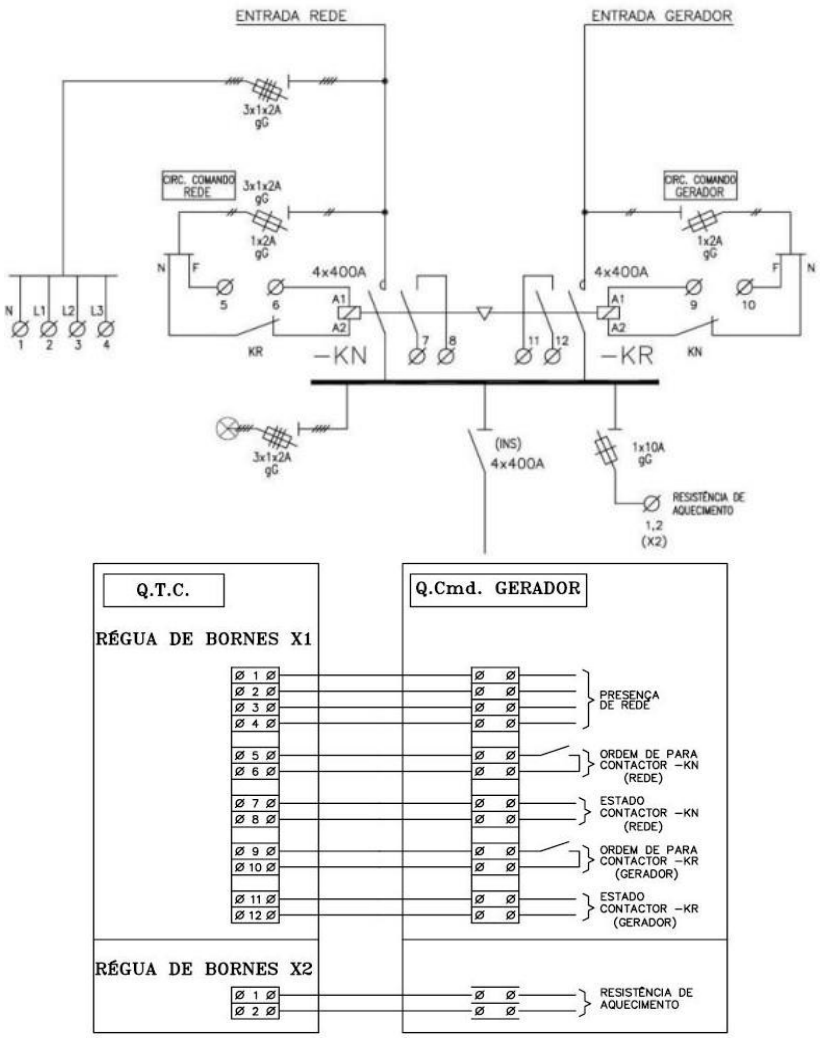
Esquema eléctrico do Quadro Geral de Baixa Tensão




QGBT PT2
Icc=38kA
Eléctrodo de Terra
Anel de terra
Fita de Aço 30x3,5mm
Borne Amovível
Cu 95mm2
1x(Cu 80x5mm)
PAINEL DE FACTOR DE POTENCIA 4x40kVar
ALIMENTACAO AO QAI1 2x(H1XV-R3x150+70)
ALIMENTACAO AO QAL1 H1XV-R3x95+50
ALIMENTACAO AO QBIB0 2x(H1XV-R3x185+95)
ALIMENTACAO AO QCC0 H1XV-R3x95+50
ALIMENTACAO AO QGELS 3x((H1XV-R3x185+95)
RESERVA
DO TRANSFORMADOR 1
DO TRANSFORMADOR 2
SUPERVISOR OU AUTOMATO JBUS RS485/232
DC150
NORMAL
GESTAO CENTRAL
EMERGENCIA
DO GERADOR
INFORMAÇÃO PARA ARRANQUE DO GRUPO
ALIMENTACAO AO QGMCS 2x(H1XV-R3x240+120)
ILUMINACAO EXTERIOR VAV4x10
ALIMENTACAO QAI1 H1XV-R3x25+16
ALIMENTACAO AO QAL1 H1XV-R3x25+16
ALIMENTACAO AO QBIB0 H1XV-R3x35+16
ALIMENTACAO AO QCC0 H1XV-R3x95+50
ALIMENTACAO AO QGELS H1XV-R3x50+25
ALIMENTACAO AO QGMCS H1XV-R3x35+16
TOMADAS DO PT A05VV-U3G2,5
ILUMINACAO DO PT A05VV-U3G1,5
ENCRAVAMENTO ELECTRICO
ENCRAVAMENTO ELECTRICO E MECANICO
INTERFACE DE SINALIZACAO E DE COMANDO
CONCENTRADOR DE BARRAS
D1/D2 - COMPACT CM16H+4x1600A COM ST-CM1
D3 - COMPACT CM16H+4x1600A COM ST-CM1
D4 - COMPACT NS630N+4x630A COM STR23SE
I1 - INTERRUPTOR INTERPACT INS38+4x630A C/ENCRAVAMENTO POR CADEADO, C/BLOCO CONTACTO PRF
ACP - PLATINA DE COMANDO AUXILIAR
UA - AUTOMATISMO DE COMANDO COM INVERSOR DE REDE AUTOMATICO

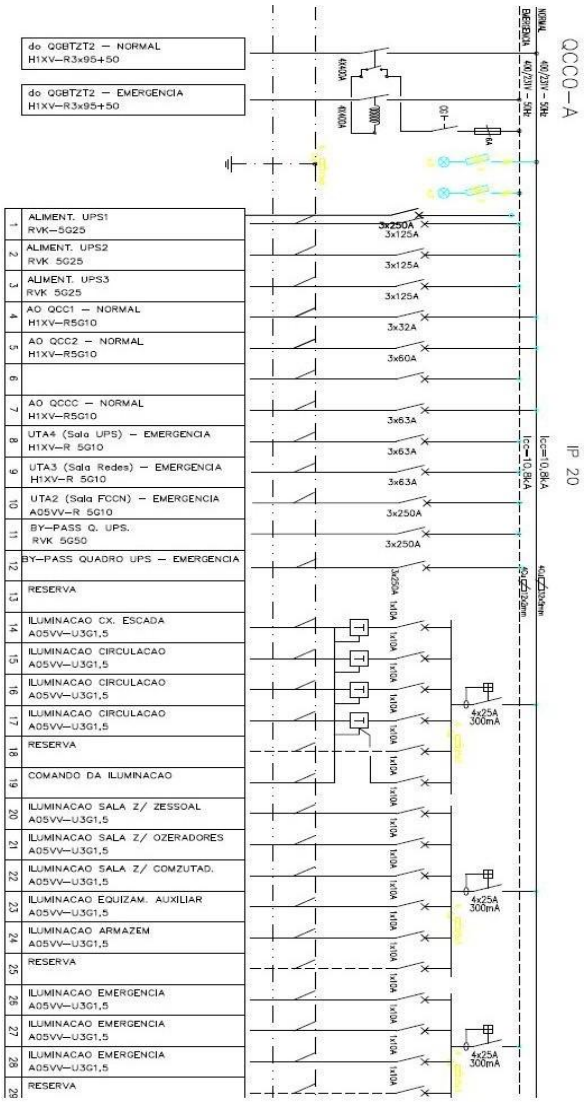
Anexo B

Esquema eléctrico do Quadro de Transferência de Cargas



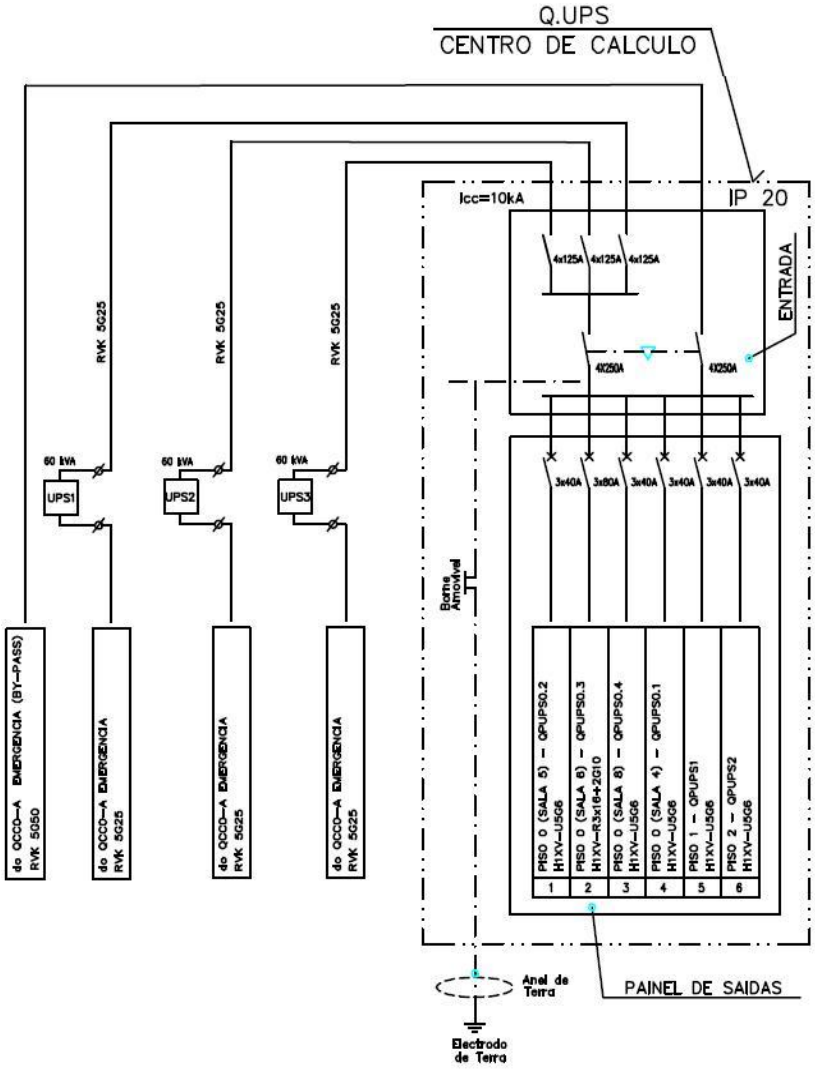
Anexo C

Esquema eléctrico do Quadro de Emergência



Anexo D

Esquema eléctrico do Quadro Geral das UPS



Anexo E

Tabelas da FMEA

- Posto de Transformação

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Transformador 1	Fornecer tensão	Sobretensão (tensão superior a U_n)	- Descarga atmosférica -Sobreintensidades	Potencial perda da tensão do transformador 1	3	2	6	*Actuação de protecções*
		Subtensão (tensão inferior a U_n)	- Problema de isolamento - Curto-circuito	Potencial perda da tensão do transformador 1	3	2	6	
		Sem tensão	- Problema de isolamento - Curto-circuito - Interrupção da alimentação da Média Tensão (MT)	O transformador não fornece tensão	3	2	6	
		Aquecimento	- Sobrecargas	Potencial perda da tensão do transformador 1	3	1	3	*Actuação de protecções*
Transformador 2	Fornecer tensão	Sobretensão (tensão superior a U_n)	- Descarga atmosférica -Sobreintensidades	Potencial perda da tensão do transformador 2	2	2	4	*Actuação de protecções*
		Subtensão (tensão inferior a U_n)	- Problema de isolamento - Curto-circuito	Potencial perda da tensão do transformador 2	2	2	4	*O transformador 2 só é utilizado na alimentação das salas de servidores quando há avaria no transformador 1. A comutação entre transformadores é feita através do Interbarras*
		Sem tensão	- Problema de isolamento - Curto-circuito - Interrupção da alimentação da Média Tensão (MT)	O transformador não fornece tensão	2	2	4	
		Aquecimento	- Sobrecargas	Potencial perda da tensão do transformador 2	2	1	2	

Quadro Geral de Baixa Tensão (QGBT)								
Interbarras	Colocar em paralelo os transformadores 1 e 2	Ao fechar	- Avaria interna (mecânica) do disjuntor	Não é possível colocar os transformadores em paralelo	3	1	3	*Por defeito o interbarras está aberto mas, em caso de avaria do transformador 1, o transformador 2 não pode fornecer tensão ao sistema*
		Ao abrir	- Avaria interna (mecânica) do disjuntor	Duplicação das correntes e curto-circuito e consequente aumento das perdas	2	1	2	*Caso ambos os transformadores estiverem operacionais*
		Não operação	- Avaria interna do disjuntor - Causas humanas - Abertura intempestiva do disjuntor	O interbarras é fechado mas não há condução da corrente	3	1	3	*Em caso de avaria do transformador 1, o transformador 2 não fornece tensão ao sistema*
Disjuntor (T1)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	A tensão do transformador 1 é cortada	3	1	3	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial corte da tensão do transformador 1	2	1	2	
Disjuntor (T2)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	A tensão do transformador 2 é cortada	2	1	2	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial corte da tensão do transformador 2	2	1	2	
Disjuntor do Quadro de Transferência de Cargas	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	A tensão dos dois transformadores é cortada	3	1	3	*Ao ser detectada falha de tensão dos transformadores, há comutação para o gerador no quadro de transferência de cargas*
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial corte da tensão dos transformadores	3	1	3	

- Grupo Gerador

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Motor	Arranque do gerador	Não arranca	- Falta de combustível - Obstrução do radiador - Botão de paragem de emergência premido - Interruptor de controlo ligado - Obstrução do filtro de ar	O Grupo Gerador não arranca	3	3	9	*Redundância do gerador*
		Arranca mas pára intempestivamente	- Motor sobrecarregado - Sobrevelocidade - Temperatura do motor demasiado elevada - Pressão do óleo demasiado baixa - Sobretensão ou subtensão - Nível do líquido de refrigeração demasiado baixo - Combustível inadequado	Potencial paragem do gerador	3	3	9	
		Sobreaquecimento	- Motor sobrecarregado - Temperatura do líquido de refrigeração demasiado elevada - Pressão do óleo demasiado elevada - Obstrução do radiador	Potencial paragem do gerador	2	2	4	
Alternador	Produzir energia eléctrica	Sem tensão	- Defeito dos díodos - Curto-circuito no induzido - Defeito do regulador - Problema na ligação de referência de tensão ao regulador	Não é produzida energia eléctrica	3	1	3	
		Falha súbita de tensão	- Actuação da protecção interna - Curto-circuito - Sobrecarga - Regulador avariado - Defeito no induzido - Indutor cortado	Potencial falha na produção de energia eléctrica	3	1	3	
		Sobretensão	- Defeito do regulador	Potencial falha na produção de energia eléctrica	3	1	3	*Actuação das protecções*

Sistema de refrigeração	Manter a temperatura do motor dentro de limites aceitáveis	Temperatura do líquido de refrigeração muito elevada	- Defeito do termóstato	Potencial paragem do motor	2	1	2	*Sobreaquecimento do motor*
		Temperatura do líquido de refrigeração muito baixa	- Defeito do termóstato - Fuga do líquido de refrigeração - Nível do líquido de refrigeração baixo	Potencial paragem do motor	2	1	2	
Bateria	Alimentação do painel de controlo (autómato)	Subtensão / sem tensão	- Falha do sistema de carga da bateria - Bateria no fim de vida - Bateria sulfatada - Ligações incorrectas ou danificadas	Painel de Controlo não é alimentado	3	3	9	*Apesar de haver controlo diário da tensão da bateria recomenda-se ligação à gestão técnica centralizada*
Disjuntor de saída	Proteger o alternador de sobrecargas e curto-circuitos	Abre indevidamente	- Falha no sensor de corrente - Erro de operação - Causas humanas	Corte da alimentação do alternador	3	1	3	
		Não abre quando ocorre um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial corte da alimentação do alternador	2	1	2	
Quadro de Controlo								
Painel de controlo	Monitorização e controlo do grupo gerador	Não controla	- Não é alimentado	O grupo gerador não arranca	3	2	6	*Falha da bateria*
Transformador de Isolamento (TI)	Evitar a perturbação do painel de controlo, pela distorção harmónica introduzida pelo envio de telecomandos pela EDP através da média tensão	Sobretensão (tensão superior a U_n)	- Descarga atmosférica Sobreintensidades	O painel de controlo não recebe a informação adequada da rede	3	2	6	
		Subtensão (tensão inferior a U_n)	- Problema de isolamento - Curto-circuito					
		Sem tensão	- Problema de isolamento - Curto-circuito - Interrupção da alimentação da Média Tensão (MT)					
		Aquecimento	- Sobrecargas					
Disjuntor (TI)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	Corte da alimentação do transformador de isolamento	3	1	3	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial corte da alimentação do transformador de isolamento	2	1	2	

- Quadro de Transferência de Cargas

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Encravamento mecânico	Impedir a ligação simultânea dos contactores de rede e emergência	Contactos do encravamento colados	- Falha dos componentes mecânicos	A rede e o gerador ficam ligados em paralelo	4	1	4	*Actuação das protecções - não há energia da rede nem do gerador, as salas de servidores são alimentados pelas UPS*
Interruptor QTC	Impedir o aparecimento intempestivo de tensão a partir do grupo gerador	Abre indevidamente	- Causas humanas	Não há protecção contra eventuais tensões intempestivas do grupo gerador	2	1	2	
Contactor da Rede								
Bobina	Produzir campo magnético que atrai o núcleo do contactor	Curto-circuito	- Aquecimento excessivo - Corte de fios na bobina - Sobrecargas - Falha nos terminais devido a vibração do circuito	Não há comutação rede-grupo gerador	3	2	6	*Actuação do fusível de protecção da rede*
Contactos	Fecho/abertura do circuito	Mecanicamente em aberto	- Aquecimento excessivo - Desgaste prematuro - Pressão fraca - Contactos colados	O contacto não consegue fechar	3	2	6	
		Mecanicamente fechado		O contacto não consegue abrir				
Fusível (Rede)	Dispositivo de corte e protecção contra sobreintensidades	Falha em aberto	Sobreaquecimento - Queima intempestiva do elemento fusível (sobreintensidade)	A bobina do contactor de rede não é ligada	3	2	6	
Contactor do Gerador								
Bobina	Produzir campo magnético que atrai o núcleo do contactor	Curto-circuito	- Aquecimento excessivo - Corte de fios na bobina - Sobrecargas - Falha nos terminais devido a vibração do circuito	Não há comutação rede-grupo gerador	3	2	6	*Actuação do fusível de protecção do gerador*
Contactos	Fecho/abertura do circuito	Mecanicamente em aberto	- Aquecimento excessivo - Desgaste prematuro - Pressão fraca - Contactos colados	O contacto não consegue fechar	3	2	6	
		Mecanicamente fechado		O contacto não consegue abrir				
Fusível (Gerador)	Dispositivo de corte e protecção contra sobreintensidades	Falha em aberto	- Sobreaquecimento - Queima intempestiva do elemento fusível (sobreintensidade)	A bobina do contactor de rede não é ligada	3	2	6	

Resistência de aquecimento								
Resistência	Tornar mais rápido o arranque do grupo gerador	Em aberto	- Mau contacto - Falta de alimentação - Curto-circuito - Falha nas conexões	Falha no grupo gerador	2	2	4	*Actuação das protecções*
		Fuga de corrente	- Mau contacto - Baixa de isolamento - Falha nas conexões	Falha no grupo gerador	2	2	4	*Actuação das protecções*
Fusível (Resistência)	Dispositivo de corte e protecção contra sobreintensidades	Falha em aberto	Sobreaquecimento - Queima intempestiva do elemento fusível (sobreintensidade)	Falha no grupo gerador	2	2	4	

- Quadro de Emergência

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Disjuntor (UPS1)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	UPS 1 não é alimentada	4	1	4	*As UPS têm redundância 2 em 3, pelo que a falha da UPS 1 só será crítica se a UPS 2 ou a UPS 3 também estiver avariada*
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de alimentação da UPS 1	3	1	3	
Disjuntor (UPS2)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	UPS 2 não é alimentada	4	1	4	*As UPS têm redundância 2 em 3, pelo que a falha da UPS 2 só será crítica se a UPS 1 ou a UPS 3 também estiver avariada*
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de alimentação da UPS 2	3	1	3	
Disjuntor (UPS3)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	UPS 3 não é alimentada	4	1	4	*As UPS têm redundância 2 em 3, pelo que a falha da UPS 3 só será crítica se a UPS 1 ou a UPS 2 também estiver avariada*
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de alimentação da UPS 3	3	1	3	
Disjuntor (Ar condicionado)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	O ar condicionado não é alimentado	4	1	4	*Potencial sobreaquecimento das salas de servidores*
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de alimentação do ar condicionado	3	1	3	

- Ar Condicionado

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Ar-condicionado	Controlo da temperatura e humidade das salas de servidores	Temperatura não é regulada	- Falha de ventilação - Falha do condensador - Filtro obstruído - Falha de alimentação de água para o humidificador - Falha do sensor de caudal de ar - Falha do sensor de temperatura e humidade - Temperatura da água fria elevada - Baixa pressão do compressor - Alta pressão do compressor - Não é alimentado	Potencial inoperacionalidade da estrutura das redes	2	5	10	*Sobreaquecimento das salas de servidores*
		Humidade excessiva		Potencial inoperacionalidade da estrutura das redes	3	5	15	*Actuação de protecções*

- UPS

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
UPS 1	Fornecer alimentação às cargas no caso de falha da rede de alimentação	Tempo de autonomia reduzido	- Sobrecarga - Bateria em descarga - Bateria no fim de vida	Em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	
		Tempo de autonomia nulo	- Sobrecarga	UPS fora do circuito, em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	*Deslastragem de cargas*
		Distorção da tensão de saída	- Falha do rectificador - Falha do inversor	Pode resultar em danos nos componentes do sistema	3	3	9	
		Sem tensão	- Bateria em descarga - Bateria no fim de vida - Curto-circuito - Não tem tensão de entrada - Rectificador em aberto	Cargas não podem ser alimentadas pela UPS	3	3	9	

UPS 2	Fornecer alimentação às cargas no caso de falha da rede de alimentação	Tempo de autonomia reduzido	- Sobrecarga - Bateria em descarga - Bateria no fim de vida	Em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	
		Tempo de autonomia nulo	- Sobrecarga	UPS fora do circuito, em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	*Deslastragem de cargas*
		Distorção da tensão de saída	- Falha do rectificador - Falha do inversor	Pode resultar em danos nos componentes do sistema	3	3	9	
		Sem tensão	- Bateria em descarga - Bateria no fim de vida - Curto-circuito - Não tem tensão de entrada - Rectificador em aberto	Cargas não podem ser alimentadas pela UPS	3	3	9	
UPS 3	Fornecer alimentação às cargas no caso de falha da rede de alimentação	Tempo de autonomia reduzido	- Sobrecarga - Bateria em descarga - Bateria no fim de vida	Em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	
		Tempo de autonomia nulo	- Sobrecarga	UPS fora do circuito, em caso de falha de rede a UPS pode não conseguir garantir a autonomia do sistema	3	2	6	*Deslastragem de cargas*
		Distorção da tensão de saída	- Falha do rectificador - Falha do inversor	Pode resultar em danos nos componentes do sistema	3	3	9	
		Sem tensão	- Bateria em descarga - Bateria no fim de vida - Curto-circuito - Não tem tensão de entrada - Rectificador em aberto	Cargas não podem ser alimentadas pela UPS	3	3	9	

- Quadro das UPS

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Disjuntor (Quadro da Sala de Servidores A)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	O Quadro da Sala de Servidores A não recebe tensão	4	1	4	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de tensão no Quadro da Sala de Servidores A	4	1	4	

Disjuntor (Quadro da Sala de Servidores B)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	O Quadro da Sala de Servidores B não recebe tensão	5	1	5	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de tensão no Quadro da Sala de Servidores B	5	1	5	
Disjuntor (Quadro da Sala de Servidores C)	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	O Quadro da Sala de Servidores C não recebe tensão	4	1	4	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial falha de tensão no Quadro da Sala de Servidores C	4	1	4	

- Quadro da Sala de Servidores A

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Disjuntor Servidores A	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	Estrutura da rede inoperacional	5	1	5	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial inoperacionalidade da estrutura de rede	5	1	5	

- Quadro da Sala de Servidores B

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários e Soluções
Disjuntor Servidores B	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	Estrutura da rede inoperacional	4	1	4	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial inoperacionalidade da estrutura de rede	4	1	4	

- Quadro da Sala de Servidores C

Componente	Função	Modo(s) de Avaria	Causa(s)	Efeito(s)	S	O	RPN	Comentários
Disjuntor Servidores C	Aparelho de corte e protecção que actua em situação de defeito	Abre indevidamente	- Falha no sensor de corrente - Falha interna do disjuntor - Causas humanas	Estrutura da rede inoperacional	4	1	4	
		Não abre na ocorrência de um defeito	- Contactos colados - Falha no sensor de corrente - Problema no mecanismo de abertura	Potencial inoperacionalidade da estrutura de rede	4	1	4	