SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GGH-08
19 a 24 Outubro de 2003
Uberlândia - Minas Gerais

GRUPO I
GRUPO DE ESTUDO DE GERAÇÃO HIDRÁULICA - GGH

CONFIABILIDADE E DISPONIBILIDADE EM SISTEMAS DE AUTOMAÇÃO DE USINAS HIDRELÉTRICAS

Alexandre Nogueira Machado*
Voith Siemens Hydro Power Generation

Eduardo H. V. Gorga
Voith Siemens Hydro Power Generation

RESUMO

No contexto atual as agências reguladoras e a opinião pública vem exigindo índices mais altos de qualidade de energia enquanto os investidores pressionam por custos mais baixos de produção e maior competitividade . A automação da geração de energia vem surgindo como resposta a tais necessidades. Como o cerne do comando e controle da usina o sistema digital desempenha um papel capital e tem grande impacto nos índices de disponibilidade . Este trabalho tem como objetivo discutir os conceitos utilizados no projeto de Sistemas de Automação para Usinas Hidrelétricas , visando a disponibilidade e a confiabilidade da usina.

PALAVRAS-CHAVE

Hidrogeração. Automação. Confiabilidade. Disponibilidade.

1.0 - INTRODUÇÃO

Os sistemas de automação de usinas hidrelétricas evoluíram para a arquitetura conhecida hoje como Sistema Digital de Supervisão e Controle (SDSC) que é hierarquizado e distribuído , como mostrado na figura 1. Tal sistema , assim como qualquer outro , está sujeito a falhas. Tais falhas influenciam no funcionamento da usina , podendo levar até a sua total indisponibilidade , consequentemente com a perda da geração . No entanto , é possível , reduzir de forma efetiva a possibilidade de ocorrência destas falhas se forem levadas em conta certos conceitos e recursos , que hoje apresentam os equipamentos eletrônicos , quando da concepção do projeto . De maneira geral , o rápido avanço da tecnologia digital e a redução dos custos dos equipamentos permitem a utilização de técnicas como:

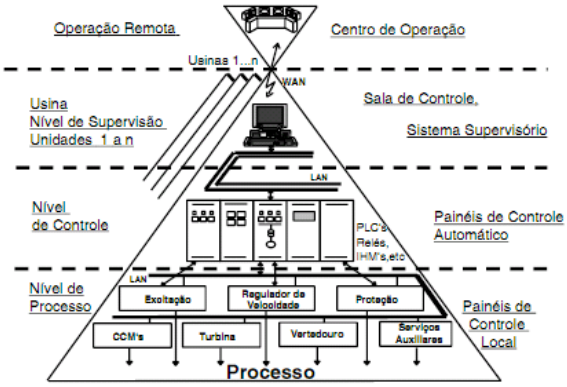

FIGURA 1 – SISTEMA DIGITAL DE SUPERVISÃO E CONTROLE

- Distribuição de funções em elementos de hardware cada vez menores . Como conseqüência , a falha de um elemento fica restrita a uma parte dos sistema, permitindo , mesmo com restrições , a operação segura do sistema . Características como auto-diagnose e possibilidade de troca a "quente" são altamente desejáveis a tais elementos , influenciando diretamente em grandezas como o MTTR(Mean Time to Repair- tempo médio para reparo)
- Redundância ou duplicação/realocação de recursos para execução de uma dada função . Qualquer elemento que possua uma função crítica no sistema ou que tenha um MTBF (mean time between failure – tempo médio entre falhas) inaceitável podem ser

*Rua Friedrich von Voith, 825 - CEP 02995-000 - São Paulo - SP - BRASIL
Tel.: (011) 3944-5179 - Fax: (011) 3944-5182 - E-MAIL: alexandre.machado@vs-hydro.com

considerados como sujeitos a aplicação de técnicas de redundância. A característica mais relevante para equipamentos redundantes é o chaveamento perfeito , ou “bumpless” . Tal característica permite que o processo não sofra qualquer alteração no momento da comutação , causada por falha , de um equipamento para outro.

É importante notar que nenhum sistema atinge 100% de disponibilidade . Tal grandeza deve ser corretamente estudada face aos seguintes requisitos:

- investimentos necessários
- custos das paradas de máquina
- redução de manutenção e custos operacionais.
- requisitos das agências reguladoras

Tais requisitos influenciam diretamente na configuração dos elementos do sistema . A experiência acumulada em vários projetos e os avanços na área de tecnologia da informação permitiram o desenvolvimento de soluções mais confiáveis e que podem ser aplicadas em todos os níveis hierárquicos do SDSC.

2.0 - SISTEMA SUPERVISÓRIO

O Sistema Supervisório de uma usina é composto de uma estrutura cliente/servidor e tem as seguintes funcões básicas:
-Operação(Base de Dados em tempo Real)
-Arquivamento Histórico
-Treinamento
-Engenharia
-Comunicação com outros Sistemas

2.1 Arquitetura Centralizada

Dependendo dos requisitos do sistema , tais funcões podem ser concentradas em uma única estação ,como mostrado na figura 2.

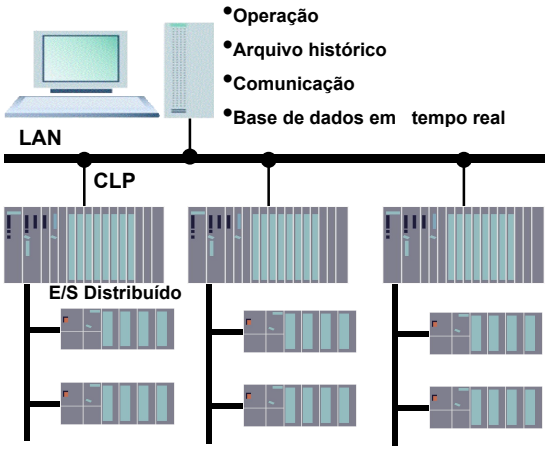

FIGURA 2 –ESTAÇÃO COM FUNÇÕES CENTRALIZADAS

O hardware deverá possuir um índice suficiente de disponibilidade pois quando a estação falha , a singularidade da arquitetura causa a indisponibilidade do Sistema de Automação.

Uma alternativa a esta situação seria a utilização de painéis de IHM’s(Interface homem-máquina) nos painéis de controle local , com chaveamento automático (hot stand-by) ou chaveamento manual , executado pelo operador. Quando do evento de falha , a operação poderia ser executada através da IHM .

Tabela 1 - DISPONIBILIDADE TÍPICA DE ESTAÇÕES

Tipo	Disponibilidade (%)	Indisponibilidade (horas/ano)
PC’s para uso doméstico	99%	87 hs
Servidores de alta confiabilidade	99,9% a 99,99%	8,8 hs a 53 minutos
Servidores tolerante a falhas	99,999% a 99,9999%	5 minutos a 32 segundos

Fonte:Intel

2.2 Arquitetura Distribuída

A distribuição das funções como mostrada na figura 3 aumenta a confiabilidade do sistema como um todo e permite que sejam aplicadas soluções específicas para o aumento da confiabilidade de cada componente.

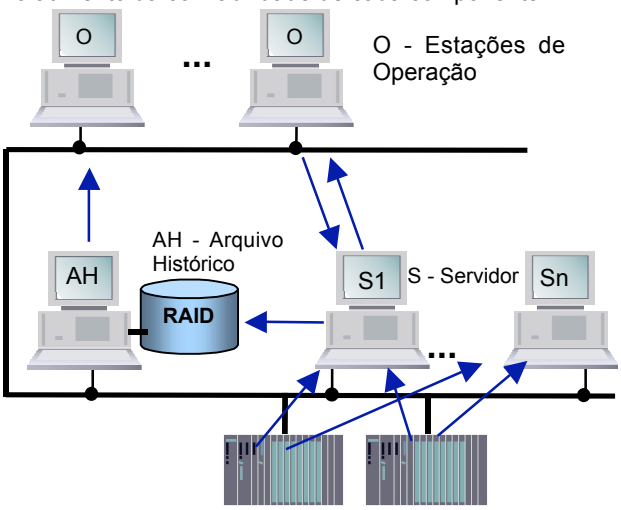

FIGURA 3 –ARQUITETURA DISTRIBUÍDA

O servidor é responsável pelas tarefas de aquisição da imagem de processo(base de dados em tempo real) , prover as estações de operação(clientes) com os dados de processo , curvas de tendência , arquivos de mensagens , arquivamento histórico , comunicação com os clientes e outros sistemas remotos. Devido a sua importância , normalmente se aplicam técnicas de redundância no hardware do servidor. No entanto apenas a redundância de hardware não garante que o sistema seja tolerante a falhas , é necessário também estratégias no software instalado no servidores com o objetivo de :

- Identificar qual estação é a principal e qual é a backup e o status de ambas
- Sincronização dos arquivos entre as estações primária e backup (histórico,eventos,alarmes)
- Redirecionar os clientes para o servidor apropriado no evento de falha
- Redirecionar a rota de comunicação entre clientes e servidores através de rotas alternativas

As estações de operação tem a função permitir o monitoramento e o controle da planta , também podendo ser aplicada a redundância nestas estações . Quando existem múltiplas estações elas normalmente são identicas e têm as mesmas prioridades de acesso ao servidores.

O Arquivamento Histórico é responsável pelo armazenamento de informações de longa duração , que servem para fins de informação administrativa , construção de gráfico de tendências , registros de horas de operação dos equipamentos. Um conjunto de discos rigidos normalmente é utilizado para o armazenamento dos dados .

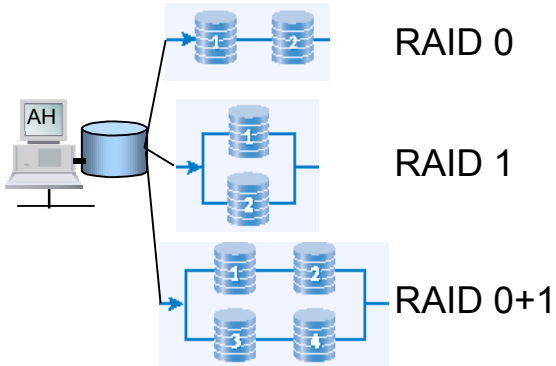

FIGURA 4 - CONFIGURAÇÕES DE RAID

A forma como estes discos são configurados normalmente é chamada de RAID (redundant array of independent disks) e pode variar desde RAID 0 até RAID 10 , de acordo com a sua configuração. O RAID 0 faz apenas a distribuição de dados entre os 'n' discos do conjunto, aumentando a performance de transferência de dados , enquanto a configuração RAID 1 apresentam um espelhamento dos dados em discos redundantes.

Tabela 2 - DISPONIBILIDADE DE ALGUNS ARRANJOS DE RAID

Tipo	Disponibilidade A do conjunto	Número de discos	Disponibilidade com A_i=0,999942
RAID 0	A_i^2	1	99,9884003%
RAID 1	$1-[(1-A_i)]^2$	2	99,9999997%
RAID 0+1	$1-[(1-(A_i)^2)^2]$	4	99,9999987%

Ai = disponibilidade individual do disco Fonte: Dell

A configuração RAID 0+1 apresenta as duas características , a distribuição dos dados entre os discos do conjunto e o espelhamento em discos redundantes e representa , como pode ser observado na Tabela 2, um bom compromisso entre confiabilidade e desempenho .

3.0 - CONTROLADORES LÓGICOS PROGRAMÁVEIS

Os Controladores Lógicos Programáveis(CLP) são responsáveis pelo controle do processo e pela aquisição dos dados dos instrumentos de campo e atuadores via módulos discretos ou fieldbus. Normalmente são montados em racks ou gabinetes que se compõe basicamente de fonte , CPU , módulos de I/O , módulos de comunicação ,etc . Para avaliação dos índices de confiabilidade do conjunto , todos estes elementos podem ser considerados como uma estrutura em série como mostrado na figura 5:

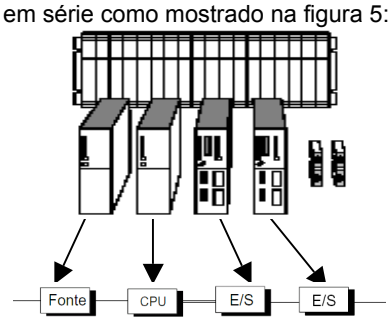

FIGURA 5 – REPRESENTAÇÃO DO BASTIDOR DE CLP

A confiabilidade de cada componente , assumindo que apresentem uma taxa constante de falha pode ser calculada através da seguinte equação:

$$R(t) = e^{-\frac{t}{MTBF}} \qquad (1)$$

Na estrutura em série o MTBF do sistema todo ,se este for constituído por n componentes , é calculado pela seguinte equação, derivada da equação 1:

$$\frac{1}{MTBF} = \frac{1}{MTBF_1} + \frac{1}{MTBF_2} + .. + \frac{1}{MTBF_n} \qquad (2)$$

Cada componente tem tipicamente, um valor de MTBF. A tabela abaixo ilustra alguns valores típicos para componentes do CLP :

Tabela 3 –VALORES TÍPICOS DE MTBF e MTTR

Tipo	MTBF (ANOS)	MTTR (horas)
Fonte	103	2
CPU	23	1,5
Módulo de Comunicação(CP)	16	1,5
Módulo de E/S	68	1,5
Rack	204	2

Para ilustrar os procedimentos adotados na busca da otimização dos índices de confiabilidade será utilizado uma configuração básica de um bastidor mostrada na figura 6:

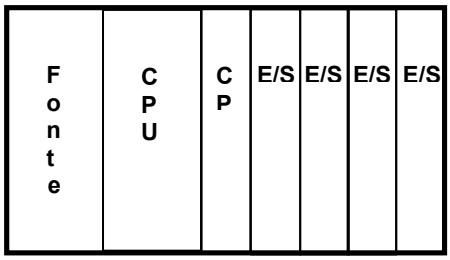

FIGURA 6 – EXEMPLO DE CONFIGURAÇÃO DE BASTIDOR

Utilizando-se dos índices da tabela 3 e as equações (1) e (2) pode-se calcular o $MTBF_i$ do bastidor da figura 5 :

$$\frac{1}{MTBF_i} = \frac{1}{103} + \frac{1}{23} + \frac{1}{16} + \frac{4}{68} + \frac{1}{204}$$

$MTBF_i$=5,57 (anos)

O MTTR do conjunto é calculado levando-se em conta a taxa de falha de cada componente e o tempo necessário para o seu reparo :

$$MTTR = \frac{\sum_{j=1}^{n} \frac{MTTR_j}{MTBF_j}}{\sum_{j=1}^{n} \frac{1}{MTBF_j}} \qquad (3)$$

Calculando-se o valor para o bastido da figura 6 temos:

$$MTTR = \frac{\frac{2}{103} + \frac{1,5}{23} + \frac{1,5}{16} + \frac{4x1,5}{68} + \frac{2}{204}}{\frac{1}{103} + \frac{1}{23} + \frac{1}{16} + \frac{4}{68} + \frac{1}{204}}$$

$MTTR_i$ = 1,54 (horas)

A indisponibilidade do bastidor é calculada através do MTBF e MTTR :

$$U_i = \frac{MTTR_i}{MTTR_i + MTBF_i} = \frac{1,54}{1,54 + 8760x5,57}$$

***U_i* = 3,1 x 10^{-5} = 0,0031% = 16,6 min/ano**
***A_i* = 1-U_i = 99,9968%**

Com o objetivo de otimizar tais resultados , pode ser aplicada a distribuição dos módulos de E/S e a redundância do bastidor . No entanto , como no caso dos servidores ,a CPU deverá possuir algumas características essenciais para a operação redundante , dentre as quais :

- Chaveamento Perfeito , isto é , no evento de falha de uma CPU , a outra CPU assumiria o processamento sem causar qualquer alteração ao sistema
- Detecção de Erro e Localização da Falhas
- Reparo durante a Operação
- Sincronização entre as CPU's

Com estas características , a aplicação da redundância aumenta consideravelmente os valores do MTBF apesar da inclusão de um novo bastidor. A alteração da confiabilidade do sistema como um todo pode ser visto pelo exemplo da figura 7 :

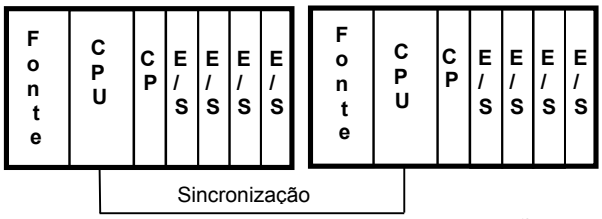

FIGURA 7 – EXEMPLO DE CONFIGURAÇÃO DE BASTIDOR REDUNDANTE

A equação que representa a disponibilidade de um sistema com n elementos em paralelo em que apenas um necessita funcionar para o sucesso do sistema pode ser escrita como:

$$A\left[\frac{1}{n}\right] = 1 - (1 - A_i)^n \qquad (3)$$

onde
A[1/n] é a confiabilidade do sistema redundante
$A_i(t)$ é a disponibilidade do elemento
n é o número de elementos em paralelo
Reescrevendo a equação (3) em função dos resultados encontrados para o bastidor singular , teremos :

$$A\left[\frac{1}{2}\right] = 1 - (1 - 0,999968)^2$$

***A* = 99,999999989%**
U = 1,024 x 10^{-9}= 0,24 seg/ano

Ou seja , comparando os dois valores de disponibilidade nota-se que o sistema redundante tem uma disponibilidade extremamente alta em comparação ao sistema com bastidor singular.

4.0 - REDES DE COMUNICAÇÃO

As redes de comunicação interligam todos os níveis do processo , tanto o sistema supervisório com os CLP's , normalmente através de redes Ethernet , assim como entre os PLC's e os instrumentos de processo através das redes fieldbus. A disponibilidade do sistema de comunicação pode ser otimizada por redundância do meio, duplicação de subcomponentes, ou duplicação de todos os componentes do barramento. A missão da rede de comunicação é interconectar dois ou mais sistemas de maneira que estes interoperem .Esta função pode ser modelada como o sistema da figura 8.

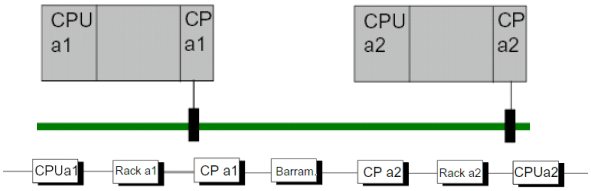

FIGURA 8 – MODELO BASE DE COMUNICAÇÃO ENTRE CPU'S

Considerando o MTBF do Barramento infinito e os valores da tabela 3 temos :

$$\frac{1}{MTBF} = \frac{2}{103} + \frac{2}{16} + \frac{2}{204} \Rightarrow MTBF = 6,48 \text{(anos)}$$

$$MTTR = \frac{\frac{2x1,5}{103} + \frac{2x1,5}{16} + \frac{2x2}{204}}{6,48^{-1}} \Rightarrow MTTR = 1,53 \text{(horas)}$$

$$U = \frac{1,53}{1,53 + 8760x6,48} \Rightarrow U = 2,69x10^{-5}$$

U = 2,35 (horas/ano)
A=1-U = 99,9973%

O método mais simples de aumentar a disponibilidade de sistemas interconectados é a utilização de um barramento redundante conjugado ao sistema de bastidor redundante analisado anteriormente. O monitoramento e os mecanismos de sincronização asseguram que no caso da falha de um componente, outro assumirá as funções e manterá pelo menos uma rota ativa. A figura 9 ilustra tal modelo:

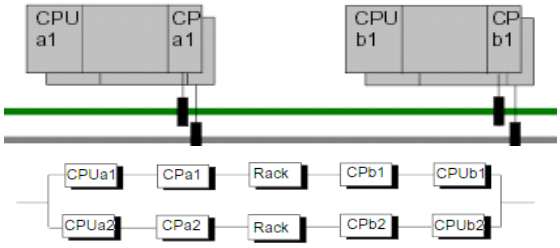

FIGURA 9 – BARRAMENTO REDUNDANTE

Utilizando a equação 3 , podemos calcular a disponibilidade do sistema da figura 9:

$$A_{\left(\frac{1}{2}\right)} = 1-(1-0{,}9999731)^2$$

A = 99,9999999276%
U=1-A = 7,24x10^{-10} = 0,022 seg/ano

De maneira geral , os PC's não tem um hardware tolerante a falha , no entanto eles podem ser montados e configurados para que acessem a rede de comunicação de uma forma confiável. A disponibiliidade do sistema supervisório e o gerenciamento das rotas de comunicação pode ser assegurada pelo uso de software específico para essas aplicações. A figura 10 ilustra basicamente a conexão entre CLP e PC sem qualquer característica especial:

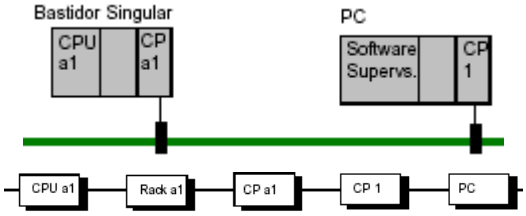

FIGURA 10 – COMUNICAÇÃO ENTRE PC E CLP

O MTBF da conexão do sistema da figura 10 , considerando o MTBF do barramento infinito e o MTBF tipíco de um PC(Servidor) igual a 5,5 anos é:

$$\frac{1}{MTBF} = \frac{1}{23}+\frac{2}{16}+\frac{1}{204}+\frac{1}{5{,}5} \Rightarrow \textbf{MTBF} = \textbf{2,82(anos)}$$

O MTTR do PC(servidor) tem um valor típico de 5 horas , e o MTTR do sistema pode ser calculado :

$$MTTR = \frac{\frac{1{,}5}{23}+\frac{2x1{,}5}{16}+\frac{5}{5{,}5}+\frac{2}{204}}{\frac{1}{23}+\frac{2}{16}+\frac{1}{204}+\frac{1}{5{,}5}} \Rightarrow \textbf{MTTR} = \textbf{3,30(hora)}$$

A indisponibilidade do sistema é

$$U = \frac{MTTR}{MTTR+MTBF} = \frac{3{,}30}{3{,}30+8760x2{,}82}$$

U= 1,34x10^{-4} =0,013% = 70 minutos/ano

A duplicação do barramento , criando rotas alternativas de comunicação torna a conexão entre o PC(servidor) e o CLP mais confiável , aumentando a disponibilidade do sistema :

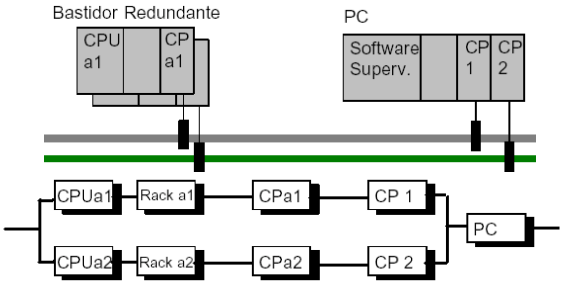

FIGURA 11 – COMUNICAÇÃO REDUNDANTE ENTRE PC E CLP

O modelo acima pode ser simplificado para o cálculo da disponibilidade do sistema , resultando em dois sistemas em paralelo , idênticos , em série com o PC como mostra a figura abaixo:

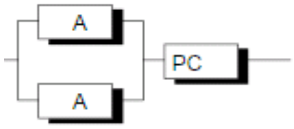

FIGURA 12 – MODELO SIMPLIFICADO

O MTBF e o MTTR do sistema A são :

$$\frac{1}{MTBF_A} = \frac{1}{23}+\frac{2}{16}+\frac{1}{204} \Rightarrow \textbf{MTBF}_{\textbf{A}} = \textbf{5,77(ano}$$

$$MTTR_A = \frac{\frac{1{,}5}{23}+\frac{2x1{,}5}{16}+\frac{2}{204}}{\frac{1}{23}+\frac{2}{16}+\frac{1}{204}} \Rightarrow \textbf{MTTR}_{\textbf{A}} = \textbf{1,51(hora)}$$

A indisponibilidade do sistema A será :

$$U_A = \frac{MTTR_A}{MTTR_A+MTBF_A} = \frac{1{,}51}{1{,}51+8760x5{,}77}$$

U_A= 2,99x10^{-5}

Um sistema com dois componentes em paralelo se torna indisponível quando ambos os componentes estiverem indisponíveis e este valor pode ser calculado da seguinte forma:

$$U = U_A x U_A = U_A^2 \qquad (4)$$

E a disponibililidade do sistema inteiro pode ser calculada considerando a disponibilidade do PC da seguinte forma :

$$A = (1-U_A^2)x(A_{PC}) \qquad (5)$$

$$A = (1-(2{,}99x10^{-5})^2)x(1-\frac{5}{5+8760x5{,}5})$$

A = 99,9896%
U=1-A = 1,03x10^{-4} = 55 minutos /ano

Podemos notar pelos cálculos anteriores que o fator limitante em relação a otimização da indisponibilidade deste sistema é a confiabilidade do PC. Tal fato, aliado a importância da função do servidor , leva comumente a aplicação da técnica de redundância de hardware nesta estação como pode ser visto na figura abaixo:

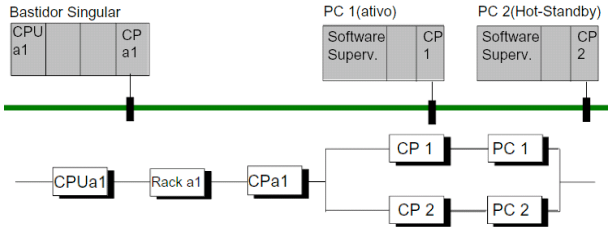

FIGURA 13 – COMUNICAÇÃO ENTRE CLP E PC'S REDUNDANTES

O sistema acima pode ser simplificado até se reduzir a um sistema série e então se calcula a sua disponibilidade.

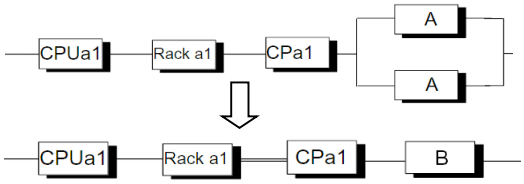

FIGURA 14– SIMPLIFICAÇÕES DO MODELO DA FIG.13

A simplificação é útil para se calcular o MTBF e MTTR de A , como mostrado na Figura 14:

$$\frac{1}{MTBF_A} = \frac{1}{16} + \frac{1}{5{,}5} \Rightarrow MTBF_A = 4{,}10(\text{ano}$$

$$MTTR_A = \frac{\frac{1{,}5}{16} + \frac{5}{5{,}5}}{\frac{1}{16} + \frac{1}{5{,}5}} \Rightarrow MTTR_A = 4{,}11(\text{horas})$$

A indisponibilidade do bloco A será :

$$U_A = \frac{MTTR_A}{MTTR_A + MTBF_A} = \frac{4{,}11}{4{,}11 + 8760x4{,}10}$$

U_A= 1,14x10^{-4}

Utilizando a equação 4 temos a indisponibilidade do bloco B:

U_B = (1,14x10^{-4})^2 = **U_B = 1,3x10^{-8}**

Calculando a disponibilidade total do sistema temos:

$$A = (1 - U_{CPUa1})(1 - U_{Racka1})(1 - U_{Cpa1})(1 - U_B)$$

$$A = 0{,}999993x0{,}999999x0{,}999989x0{,}999999$$

A = 0,999980
U= 1,999989x10^{-5}= 10,5 (min/ano)

Comparando esta indisponibilidade com a configuração anterior ,percebe-se que houve uma grande diminuição ,pelo fato da utilização de redundância nos PC's , que tem um valor de MTBF e MTTR incompatível com os valores dos outros equipamentos do sistema de automação.

5.0 - CONCLUSÕES

Os métodos e conceitos aqui discutidos provaram a sua eficácia através dos projetos executados e na busca de solução otimizada para alcançar os índices previstos nas normas operativas das agências reguladoras . É importante notar que os sistemas foram analisados separadamente , o que resultou , de maneira geral , nos elevados valores de disponibilidade . O que não impede a adoção dos mesmos conceitos e procedimentos para sistemas mais complexos , levando-se em consideração que quanto maior a complexidade do sistema , piores serão os seus indíces de confiabilidade e consequentemente a sua disponibilidade. Com base nos valores teóricos de disponibilidade e confiabilidade apresentados neste trabalho, a VOITH SIEMENS HYDRO vem aprimorando suas soluções para automação de usinas hidrelétricas, mantendo-as compatíveis com as exigências operacionais e normativas vigentes. Recomenda-se adotar alternativas (sub-automatismos distribuídos e autônomos, sistemas de retaguarda independentes, etc.) para a supervisão e controle do processo em função do custo da indisponibilidade do SDSC para o empreendedor.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) VOITH SIEMENS HYDRO POWER GENERATION. Cálculo de Disponibilidade dos Sistemas Digitais de Supervisão e Controle das UHE's Emborcação , Volta Grande e Jaguara. Relatório Técnico A576.592-0/002. São Paulo, 1997-06-06;

(2) SIEMENS A. G. – ANL A 45 – Reliability Engineering – Introduction to the methods of reliability assessment of systems – 05/96;

(3) SIEMENS A. G. Manual S7-400H Programmable Controller Fault Tolerant Systems - 07/2001

(4) Department of Defense U.S.A. . Eletronic Reliability Design Handbook MIL-HDBK-338B. 1998-10-01.