



Journal homepage:
www.arvore.org.br/seer

DEPENDABILIDADE EM REDE DE COMPUTADORES: UMA ANÁLISE BASEADA EM IMPORTÂNCIA PARA CONFIABILIDADE

RESUMO

Este artigo tem por objetivo o estudo de aspectos relativos à dependabilidade de redes de computadores corporativas, com vistas a que se garanta um melhor tempo de atividade e se alcance os objetivos organizacionais. Serão utilizados RBD e FT como abordagem de modelagem para avaliação analítica de cenários complexos. Uma combinação de modelos de dependabilidade será utilizada para análise da confiabilidade do sistema em função dos componentes mais importantes.

PALAVRAS-CHAVES: Dependabilidade; Confiabilidade; RBD; FT; Redes de Computadores.

DEPENDABILITY IN COMPUTER NETWORK: AN ANALYSIS BASED ON RELIABILITY IMPORTANCE

ABSTRACT

This article has as objective the study of the relative aspects of corporative computer network dependability to guarantee better time performance, and to reach the organizational goals. To perform the analytic evaluation of the complex scenarios it will be used the RBD and FT as a modeling approach. To analyze the reliability of the system regarding the most important components it will be used a combination of dependability models.

KEYWORDS: Dependability; Reliability; Availability; Modeling; Computer Networks.

*Revista Brasileira de
Administração Científica,
Aquidabã, v.4, n.2, Ago 2013.*

ISSN 2179-684X

SECTION: *Articles*
TOPIC: *Sistemas e Tecnologia da
Informação*



*Anais do Simpósio Brasileiro de
Tecnologia da Informação (SBTI 2013)*



DOI: 10.6008/ESS2179-684X.2013.002.0007

Eduardo Rodrigues de Carvalho

Universidade Federal de Alagoas, Brasil
<http://lattes.cnpq.br/9988689413005523>
eduardo.carvalho@arapiraca.ufal.br

Almir Pereira Guimarães

Universidade Federal de Alagoas, Brasil
<http://lattes.cnpq.br/3181745681718312>
almir@arapiraca.ufal.br

Received: 07/07/2013

Approved: 05/08/2013

Reviewed anonymously in the process of blind peer.

Referencing this:

CARVALHO, E. R.; GUIMARÃES, A. P.. Dependabilidade em rede de computadores: uma análise baseada em importância para confiabilidade. *Revista Brasileira de Administração Científica*, Aquidabã, v.4, n.2, p.96-106, 2013. DOI: <http://dx.doi.org/10.6008/ESS2179-684X.2013.002.0007>

INTRODUÇÃO

Em um mundo ideal, a eficiência das redes de comunicação deveria ser uma constante. Entretanto, no mundo real isto não se aplica. Falhas aleatórias afetam a rede e podem ser causadas por falhas físicas, como ruptura em fibra, falha no fornecimento de energia, incêndios e terremotos, falhas de software ou falhas resultantes de erros humanos não intencionais. A possibilidade de evitar falhas, as quais podem colocar os negócios em risco, é uma expectativa possível, e deve ser uma política a ser observada pelas organizações, pois a correta operação destes sistemas tem impacto significativo tanto na integração de negócios como na qualidade do serviço prestado aos clientes. O projeto, desenvolvimento e gerenciamento das redes corporativas deve atender a essas exigências (GUIMARÃES, 2011).

Este trabalho realiza análise da dependabilidade em redes corporativas utilizando técnicas de modelagem não baseado em espaço de estados, tais como diagrama de blocos de confiabilidade (RBD, em inglês *Reliability Block Diagram*) e Árvore de Falhas (FT, em inglês *Fault-Tree*). Além disso, será utilizado o mecanismo de "importância para confiabilidade (em inglês *Reliability Importance*) para uma análise do sistema em função de seus componentes mais importantes em termos de confiabilidade" (WANG, 2004). Desta maneira, pode-se tanto prever possíveis falhas em pontos da rede, e conseqüentemente melhorar a qualidade de seus serviços, como incrementar a atividade de planejamento destes sistemas.

REVISÃO TEÓRICA

Dependabilidade

Segundo (AVIZIENIS, 2004) "a dependabilidade de um sistema de computadores deve ser entendida como a habilidade de se evitar falhas em serviços que são mais frequentes e mais severas do que seria tolerável". "Considerando que, as exigências de dependabilidade englobam os conceitos de disponibilidade, confiabilidade, integridade, manutenibilidade e segurança" (AVIZIENIS, 2004). Para este trabalho, com relação à dependabilidade, iremos tratar principalmente dos conceitos de confiabilidade e disponibilidade.

"A confiabilidade é a probabilidade de que um sistema esteja operacional em um dado intervalo de tempo $[0, t]$, desde que estava operacional no tempo $t=0$ (PRADHAN, 1996). Um sistema de alta confiabilidade é aquele que mais provavelmente continuará a funcionar sem interrupção durante um período de tempo relativamente longo. Este atributo mede a correta continuidade de um serviço, a partir de um tempo de referência inicial: $R(t) = 1 - F(t)$, onde $F(t)$ é a função de distribuição cumulativa a qual pode ser considerada como não confiabilidade.

Por sua vez, a disponibilidade "é a probabilidade de que o sistema esteja operacional, isto é, a porcentagem de tempo na qual o sistema está executando seus serviços" (Trivedi, 2001) (Ver abaixo a equação da Disponibilidade):

$$\text{Disponibilidade} = \text{UpTime} / (\text{UpTime} + \text{DownTime})$$

onde UpTime e DownTime representam o período operacional e não operacional respectivamente. Por outro lado, a indisponibilidade pode ser obtida por:

$$A' = 1 - A$$

Segundo Weber (2011, p.13-14):

As medidas mais conhecidas na prática para avaliação de dependabilidade são: Tempo Médio para Falha (*Mean Time To Failure* - MTTF), Tempo Médio para Reparo (*Mean Time To Repair* - MTTR) e Tempo Médio entre Falhas (*Mean Time Between Failure* - MTBF). O MTTF é fornecido pelo fabricante e representa o tempo médio para a falha de um componente. O MTTR é diretamente relacionado à política de manutenção adotada pela organização. Por sua vez, o MTBF é a soma dos tempos de MTTF e MTTR.

RBD

RBD é considerado um modelo tipo combinatorial, não baseado em espaço de estados. Ele representa a estrutura lógica de um sistema com relação à forma de como a confiabilidade de seus componentes afeta a confiabilidade do sistema. Os componentes são combinados em blocos, em configurações do tipo série e/ou em paralelo. Todos estes construtores podem ser utilizados juntos em um único diagrama de blocos. Eles mapeiam a dependência operacional de um sistema em relação a seus componentes. O subsistema representando os componentes em série, implica que a falha de qualquer componente resulta em uma falha daquele subsistema. Por outro lado, o subsistema representando os componentes em paralelo, implica que apenas a falha de todos os componentes resulta na falha daquele subsistema. Por fim um subsistema representando os componentes em k-of-n implica que o subsistema é operacional se k ou mais dos n componentes estão trabalhando.

Configurações em série e em paralelo são casos especiais de configuração tipo k-of-n. Uma estrutura em série é do tipo n-of-n e uma estrutura em paralelo é do tipo 1-of-n. A Figura 1 mostra um exemplo de RBD que modela o fornecimento de energia para um circuito eletrônico tolerante a falhas com redundância no fornecimento de energia das redes elétricas (RdElet01 e RdElet02), que é compartilhado, garantindo que o sistema é operacional se ao menos um dos RedElet falhar. O circuito conta com uma redundância da fonte, se ocorrer defeito ou queima da fonte principal a fonte redundante assumirá tornando o circuito sempre operacional.

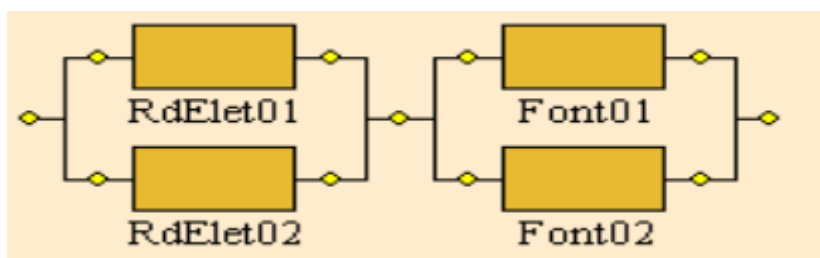


Figura 1: Exemplo de um modelo RBD.

FT

FT é um tipo de modelo combinatorial que mapeia a dependência operacional de um sistema em relação a seus componentes" (SAHNER & TRIVEDI, 2002). FT é um dos modelos mais comumente utilizados para análise de dependabilidade. Ele representa todas as possíveis sequências de falhas em componentes que poderão acarretar a interrupção no sistema. O ponto de partida desta análise é a definição de um único evento indesejado, o qual é a raiz de uma estrutura em árvore. O FT é uma representação da combinação de eventos que podem causar a ocorrência deste evento indesejado. Um evento num nível i é reduzido a uma combinação de eventos de mais baixo nível por meio de portas lógicas. Portas tipo *AND* e portas tipo *OR* são os dois tipos de portas mais comumente utilizadas. A saída de uma porta *AND* é um valor lógico de 1 se e apenas se todas as suas entradas assumem o valor lógico de 1. A saída de uma porta tipo *OR* é o valor lógico 1 se e apenas se uma ou mais de suas entradas assumem o valor lógico 1.

O FT poderá também incluir portas tipo *k-out-of-n* e portas tipo *NOT*. Para portas tipo *k-out-of-n*, a saída assume o valor lógico 1 se k ou mais entradas assumem o valor lógico 1 e 0 de modo contrário. Por fim, a saída de uma porta *NOT* é o valor lógico 1 se a entrada é o valor lógico 0. Outras portas podem ser representadas pela combinação de portas lógicas *AND*, *OR* e *NOT*.

A Figura 2 mostra um exemplo de FT que modela um fornecimento de energia para um circuito eletrônico tolerante a falhas com redundância no fornecimento de energia das redes elétricas (RdElet01 e RdElet02) compartilhados garantindo que o sistema é operacional se ao menos um dos RedElet falhar. O circuito conta com uma redundância da fonte, se ocorrer algum defeito ou queima da fonte principal a fonte redundante assumirá deixando o circuito sempre operacional. Neste modelo, a estrutura mostra quando o sistema tem falhado.

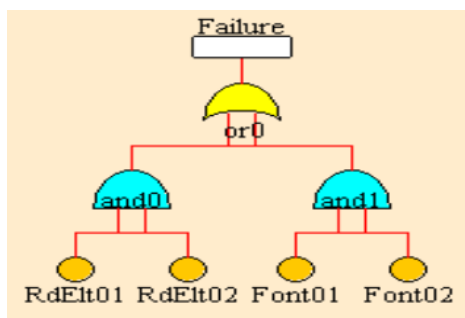


Figura 2: Exemplo de um modelo em FT.

RI

Kuo e Zuo (2003, p. 193):

A Importância para Confiabilidade, I_i^B , também conhecida como importância de Birnbaum (B-importância) de um componente, é independente da confiabilidade do componente em si. Pode-se dizer que a importância para confiabilidade de um componente i é igual à quantidade do aumento (no tempo t) na confiabilidade do sistema quando a confiabilidade do componente i é melhorada em uma unidade. Esta medida prevê uma classificação numérica para determinar quais componentes

são mais importantes para a melhoria da confiabilidade do sistema. De acordo com a importância para confiabilidade de um componente i é definida por:

$$I_i^B = \frac{\partial R_s(\mathbf{p})}{\partial p_i}$$

Onde p_i é a confiabilidade do componente i , \mathbf{p} é o vetor de confiabilidade dos componentes, como o R_s é a confiabilidade do sistema. Esta medida de importância fornece uma classificação numérica para determinar quais componentes são mais importantes para a melhoria do sistema. Neste artigo, vamos usar I_i^B para analisar o comportamento do sistema de acordo com a disponibilidade dos componentes mais importantes, tendo em vista o que se determina como importância para confiabilidade.

Ferramenta SHARPE

A ferramenta SHARPE é um modelador, porque contém suporte para múltiplos tipos de modelos e fornece mecanismos legíveis para combinação de resultados. Com isso, auxilia na escolha de boas abstrações de cenários de redes de computadores, ficando uma parametrização mais prática na validação dos modelos. O modelador SHARPE permite construir e analisar o desempenho, a confiabilidade, disponibilidade e modelos de performance. Os três tipos de modelos que são comumente usados para análise de confiabilidade e disponibilidade, são diagramas de blocos de confiabilidade(RBD), árvores de falhas(FT), e gráficos de confiabilidade(RG).

METODOLOGIA

A metodologia para avaliação da dependabilidade do sistema consiste em quatro etapas: A primeira é a apresentação das características do sistema e o escopo do estudo a ser realizado. A segunda etapa refere-se a coleta dos dados que foram utilizados na parametrização do modelo. A terceira etapa corresponde a modelagem e validação do modelo do sistema em estudo. Por fim, a quarta etapa consiste dos métodos de avaliação, da definição dos cenários que foram avaliados e interpretados e os seus resultados. A primeira etapa trata ainda da caracterização do sistema que foi avaliado, onde foram identificados os componentes relevantes do sistema e a interface entre eles. Para a segunda etapa, foi necessário definir as métricas a serem observadas, como por exemplo as informações de dependabilidade que são relacionadas às seguintes variáveis: MTTF e MTTR. Sendo importante salientar que o MTTF é fornecido pelo fabricante e representa o tempo médio para a falha de um componente. O MTTR é relacionado à política de manutenção da organização. A terceira etapa, que corresponde à modelagem do sistema, considera tanto RBD e FT como modelos formais de representação, e também o estudo da importância para confiabilidade na análise da disponibilidade do sistema, em função dos componentes mais

importantes. A última etapa do processo configura-se na escolha dos métodos de avaliação a serem conduzidos (análise ou simulação, estacionária ou transiente).

DISCUSSÃO

O sistema estudado é baseado na rede de computadores de uma indústria alimentícia localizada no Nordeste do Brasil. Esta rede apresenta uma topologia em estrela (Figura 3), aonde os nós folha são interligados ao um nó central (Core). Para o acesso à rede WAN é proporcionado um enlace L1. Esta conexão é realizada através de um firewall. Além disso, esta rede possui dois servidores (Protheus1 e Dominio1) que estão também interligados ao nó central. Na Figura 3 consideramos uma arquitetura de rede sem redundância.

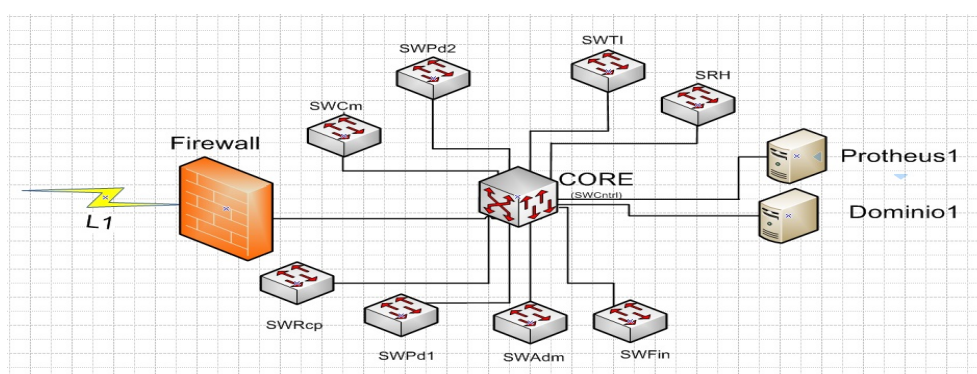


Figura 3: Arquitetura sem redundância.

Na Figura 4 e 5 mostramos modelos de dependabilidade da arquitetura apresentada. Estes modelos podem ser avaliados utilizando ferramentas tais como SHARPE¹.

Na Figura 4 mostramos um modelo RBD. Os blocos desses modelos estão em uma estrutura em série. Segundo esse modelo para que o sistema esteja operacional é necessário que não ocorra nenhuma falha em qualquer um dos blocos.

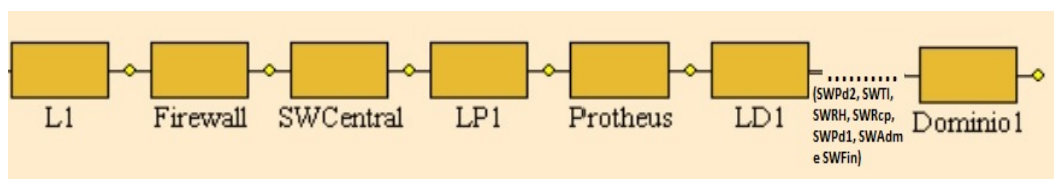


Figura 4: Modelo em RBD sem redundância.

Além disso, foi criado um modelo baseado em FT (Figura 5) para a avaliação de dependabilidade (confiabilidade e disponibilidade) e determinar o comportamento dos pontos críticos dentro desta rede através de análise dos resultados obtidos. Neste modelo, verificamos que para ocorrer o evento-topo (*Failure*), deve ocorrer a falha de um dos componentes da porta lógica OR (or1), ou um dos componentes da porta lógica OR (or2), ou uma falha em um dos componentes SWCm, SWPd2, SWTI, SRH, SWRcp, SWPd1, SWAdm, SWFin, SWCntrl, Firewall,

¹ <http://people.ee.duke.edu/~kst>

L1, LP1 e LD1. Todos os componentes são representados por uma árvore de falhas. As portas or1 e or2, junto com os componentes SWCm, SWPd2, SWTI, SRH, SWRcp, SWPd1, SWAdm, SWFin, SWCntrl, Firewall, LP1 e LD1 estão interligados à porta or0.

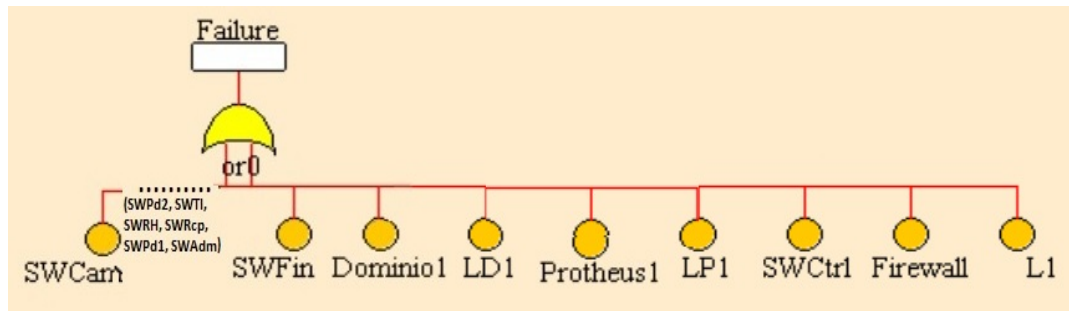


Figura 5: Modelo em FT sem redundância.

Estudo de Caso

Nesta seção consideramos a arquitetura mostrada na Seção 4. Será utilizado o mecanismo de importância para confiabilidade, a fim de auxiliar no processo de incremento da dependabilidade do sistema, através da elaboração de uma nova arquitetura. Além disso, iremos utilizar modelos RBD para o cálculo tanto dos valores importância para confiabilidade quanto da métrica de confiabilidade do sistema. Para estes cálculos será utilizada a ferramenta Sharpe utilizando os valores mostrados na Tabela 1.

Desta forma, devemos desprender ações tanto para adição de redundância quanto para um aumento do MTTF em relação aos componentes com maior impacto na dependabilidade do sistema em detrimento aos demais componentes do sistema.

Tabela 1: MTTF dos equipamentos.

Equipamentos	MTTF
Firewall	15.778h
SRVs(Protheus1/Dominio1)	79.165h
SRVs-Virtuais(Protheus2/Dominio2)	4.320h
SWCentral(Core)	94.194h
SWFolha	16.666h
Enlace	796h
EnlaceRd	396h
EnlaceUTP	87600h

Então, a partir da Tabela 2 selecionamos os componentes com os maiores valores de importância para confiabilidade (L1, Protheus1 e Dominio1). Considerando estes componentes iremos propor uma nova arquitetura (ver Figura 6) através tanto da adição de um enlace redundante para a rede WAN (L2) quanto da adição de servidores redundantes (Protheus1/Protheus2 e Dominio1/Dominio2, ver Figura 6). As mudanças nestes componentes tiveram um grande impacto sobre a dependabilidade do sistema.

É interessante observar que estes servidores redundantes pertencem a uma estrutura virtualizada, através de um servidor de virtualização. Esta arquitetura é representada pelo modelo RBD mostrado na Figura 7.

Tabela 2. Importância valores de confiabilidade

Mod	$I_i^B(\text{SwPd2})$	$I_i^B(\text{SwT1})$	$I_i^B(\text{SwRcp})$	$I_i^B(\text{SwCm})$	$I_i^B(\text{SwRH})$	$I_i^B(\text{LP1})$	$I_i^B(\text{LP2})$	$I_i^B(\text{LD1})$	$I_i^B(\text{LD2})$
1	0,0059	0,0059	0,0059	0,0059	0,0059	0,0055	--	0,0055	--
Mod	$I_i^B(\text{L1})$	$I_i^B(\text{L2})$	$I_i^B(\text{Firew})$	$I_i^B(\text{Core})$	$I_i^B(\text{Pth})$	$I_i^B(\text{Dom})$	$I_i^B(\text{SwAdm})$	$I_i^B(\text{SwFin})$	$I_i^B(\text{SwPd1})$
1	0,0403	--	0,0059	0,0055	0,0169	0,0169	0,0059	0,0059	0,0059

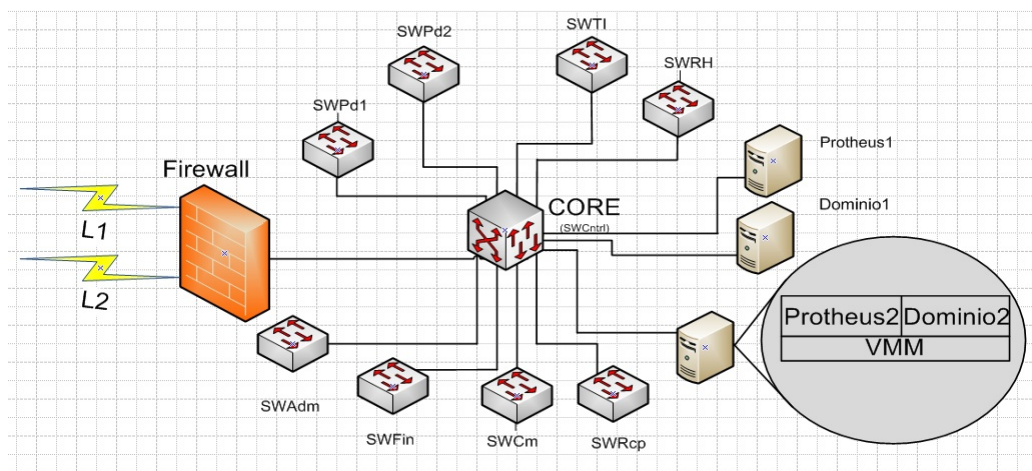


Figura 6: Arquitetura com Redundância.

Figura 7 mostra um modelo representando a segunda arquitetura considerando redundância de enlace e de servidores. Neste modelo foi incluído o componente redundante (L2) ao enlace principal (L1) e adicionado dois servidores redundantes numa estrutura virtualizada (Protheus2 e Dominio2) aos servidores principais (Protheus1 e Dominio1). Segundo este modelo, o sistema estará operacional mesmo que ocorra falha em um dos blocos representando os enlaces (L1 ou L2) e os servidores ((Protheus1 ou Protheus2) e (Dominio1 ou Dominio2)).

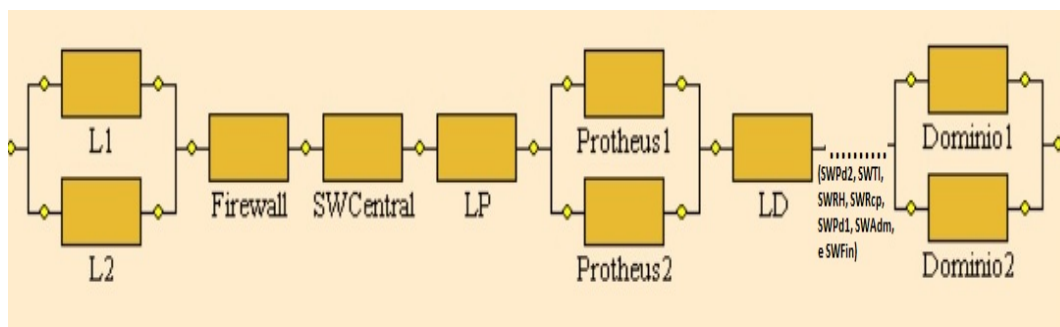


Figura 7. Modelo em RBD com redundância.

A Figura 8 trata com aspectos de dependabilidade relativos aos componentes SWCm, SWPd2, SwT1, SRH, SWRcp, SWPd1, SWAdm, SWFin, SWCntrl, Firewall, L1, L2, Protheus1,

Protheus2, Dominio1 e Dominio2. Este modelo representa dois Links(L1 e L2), dois servidores com redundância((Protheus1 e Protheus2) e (Dominio1 e Dominio2)). A análise do modelo é realizada da seguinte forma: o evento topo (*failure*) quando obtém como saída o valor lógico 1, diagnosticamos a ocorrência de falha na rede. A porta lógica or0 determinará a entrada de tal componente, sendo que esta porta retornará como saída 1 se SWCm, SWPd2, SWTI, SRH, SWRcp, SWPd1, SWAdm, SWFin, SWCntrl ou Firewall falharem ou se a porta lógica and0 apresentar o valor 1 em sua saída. Para que a porta and0 apresente o valor lógico de 1 em sua saída, os enlaces (L1 e L2) e dos servidores ((Protheus1 e Protheus2) e (Dominio1 e Dominio2)), que são entradas desta porta, terão de falhar simultaneamente.

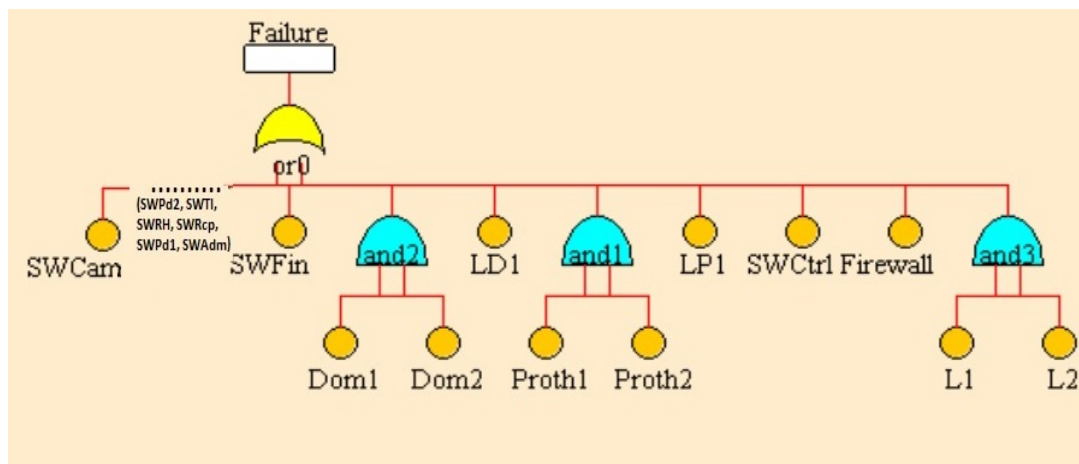


Figura 8. Modelo em FT com Redundância.

Os modelos RBD e FT, foram utilizados para a avaliação da confiabilidade do sistema. Figura 9 mostra o gráfico que representa os resultados da confiabilidade em função do tempo obtidos a partir da primeira arquitetura (sem redundância).

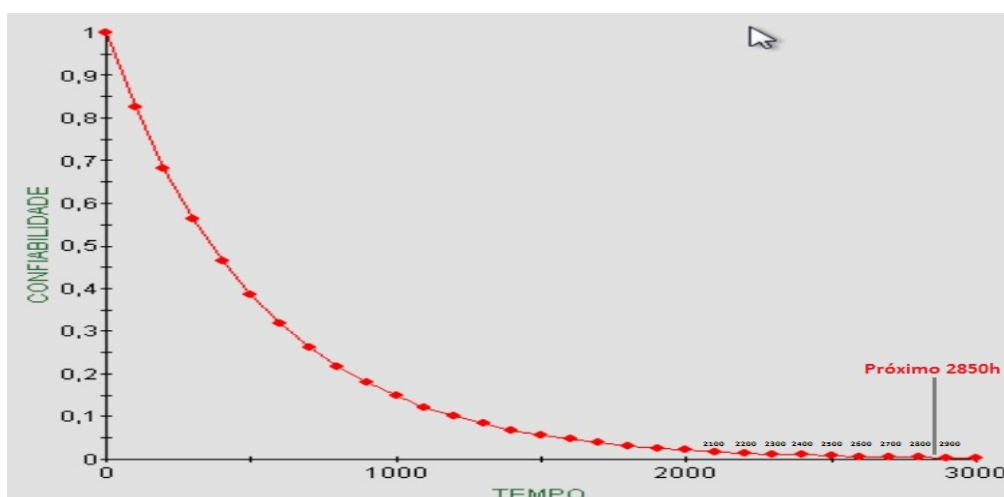


Figura 9. Gráfico sem redundância.

O gráfico mostrado na Figura 10 corresponde aos resultados obtidos a partir de uma rede com redundância nos enlaces L1 e dos servidores Protheus1 e Dominio1.

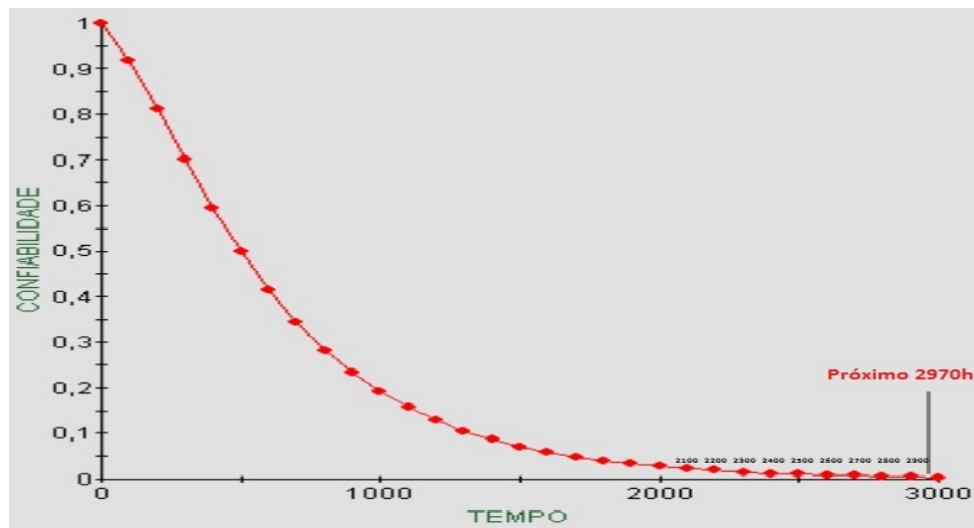


Figura 10. Gráfico de uma rede com redundância.

Por fim, comparando as arquiteturas descritas neste estudo de caso (ver Figuras 9 e 10), percebemos que na arquitetura sem redundância a confiabilidade da rede decresce de maneira acentuada, alcançando um valor próximo a zero, em um tempo aproximadamente de 2850 horas. Além disso, esta arquitetura possui um valor relativo ao MTTF do sistema de 523.24 horas. Por outro lado, na Figura 10 a confiabilidade do sistema é aumentada, alcançando um valor próximo a zero em um tempo próximo a 2970 horas. Esta arquitetura possui um valor de MTTF do sistema de 636.64 horas.

CONCLUSÕES

Neste trabalho, onde foram apresentados modelos baseados em FT, RBD para avaliar a dependabilidade de redes de computadores, os resultados obtidos ajudam a compreender o seu comportamento em relação a alguns cenários, considerando-se a variação em diversos parâmetros de seus principais componentes. Por adequação, a medida RI foi utilizada para analisar o sistema de acordo com a disponibilidade dos componentes mais importantes.

No que diz respeito a FT e RBD foi possível provar através de estudo teórico, que sua aplicação como suporte para simulação é viável e está alinhada com os objetivos que se pretendia alcançar.

Numa sequencia deste estudo, pode-se estender esses modelos e incluir um maior número de redundâncias além de aumentar a quantidade de componentes. É também possível a utilização de *Stochastic Petri Nets (SPN)* para o cálculo de diversos parâmetros das redes de computadores.

REFERÊNCIAS

GUIMARÃES, A. P.; MACIEL, P. R.; OLIVEIRA, H. M. N.; BARROS, R.. Availability analysis of redundant computer networks: a strategy based on reliability importance. In: IEEE INTERNATIONAL CONFERENCE ON COMMUNICATION SOFTWARE AND NETWORKS (ICCSN). **Anais**. p.328-332, 2011.

AVIZIENIS, A.; LAPRIE, J. C.; RANDELL, B.; LANDWEHR C.. Basic concepts and taxonomy of dependable and secure computing. In: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. **Anais**. p.11-33, 2004.

PRADHAN, K. **Fault tolerant computer system design**. Prentice Hall, 1996.

SAHNER, R.; TRIVEDI, K. S.; PULIAFITO, A.. **Performance and reliability analysis of computer systems**. Kluwer Academic Publishers Group, 2002.

TRIVEDI, K. S.. **Probability and statistics with reliability: queuing, and computer science**. New York: John Wiley and Sons, 2001.

KUO, W.; ZUO, M.J.. **Optimal reliability modeling: principles and applications**. Hoboken: John Wiley & Sons, 2003.

WANG, W.; LOMAN, J.; VASSILIOU, P.. **Reliability importance of components in a complex system**. Los Angeles: Institute of Electrical and Electronics Engineers, 2004.

WEBER, T. S.. **Um roteiro para exploração dos conceitos básicos de tolerância a falhas**. Disponível: <http://www.inf.ufrgs.br/~taisy/disciplinas/textos/Dependabilidade.pdf> . Acesso: 2011.