

Sensitivity Analysis of *Data Center* Electrical Infrastructures Considering Aspects of Dependability and Cost

F. F. L. Melo, E. T. G. Sousa and G. R. A. Callou

Abstract—In the last years, the demand and use of *data center* have increased greatly due to the services offered by them. There must be a concern with *data centers* to allow the infrastructure to be available most of the time. Considering this need, this work has the objective of conducting a sensitivity analysis in the electrical infrastructure of the *data center*, thus finding the most sensitive equipment, taking into account the availability, reliability and cost. After obtaining the most sensitive equipment, it applies *warm standby* and *hot standby* replication techniques. The present work makes use of a hybrid modeling approach that considers the advantages of Stochastic Petri Nets (SPN) and Reliability Block Diagrams (RBD) to evaluate the dependability and cost of equipment acquisition.

Index Terms—Reliability block diagrams, dependability, sensitivity analysis, Stochastic Petri net, *warm standby*, *hot standby*.

I. INTRODUÇÃO

Ao longo dos últimos anos, o número, o tamanho e o poder computacional dos *data centers* vêm aumentando consideravelmente devido aos serviços ofertados pela computação em nuvem, redes sociais e comércio eletrônico [1] [2].

Os *data centers* são formados por equipamentos e sistemas responsáveis pelo processamento e armazenamento de informações cruciais e de grande valia para a continuidade e funcionamento de diferentes aplicações e serviços [3]. Os *data centers* são recursos de missão crítica, pois abrigam muitos serviços que são cruciais para as empresas. Por exemplo, eles podem ser utilizados como *host* de sites para processar transações comerciais e proteger dados bancários, registros financeiros e histórico médico de pacientes. Tais sistemas demandam que seus serviços estejam em operação 24 horas por dia, durante os 7 dias da semana [4]. Por se tratar de ambientes de missão crítica, os *data centers* devem estar sempre aptos a operar ininterruptamente. Portanto, é essencial manter a disponibilidade e confiabilidade sempre elevados para permitir que o ambiente funcione conforme a necessidade [5].

Dado o contexto acima, este trabalho tem como objetivo propor uma estratégia que faz uso da análise de sensibilidade [6] com o intuito de identificar qual equipamento da infraestrutura elétrica do *data center* mais impacta na disponibilidade

do sistema. Assim que identificado o dispositivo mais sensível, um novo equipamento pode ser adicionado para melhorar tal ponto de falha. Este trabalho considera a replicação de um equipamento como a adição de um dispositivo com a mesma configuração do equipamento já presente na arquitetura. Os mecanismos de redundância evitam a ocorrência de um único ponto de falha e, sendo assim, proporcionam uma elevação na disponibilidade e confiabilidade do sistema [7]. Além da análise da disponibilidade e confiabilidade, este trabalho também tem como objetivo o de estimar o custo de aquisição dos componentes, e os custos necessários para o pleno funcionamento da infraestrutura elétrica do *data center*. Dessa forma, para se obter melhores resultados ao verificar tais métricas, se faz necessária a utilização de uma análise de sensibilidade com o intuito de apontar os equipamentos mais sensíveis às métricas de disponibilidade e custo, e confiabilidade e custo.

Foi utilizado uma técnica de modelagem híbrida e hierárquica que considera as vantagens das redes de Petri estocásticas (SPN) [8] e diagramas de bloco de confiabilidade (RBD) [9] para avaliar a disponibilidade e confiabilidade das infraestruturas de *data centers*. Além disso, modelos também foram propostos para representar duas abordagens distintas de replicação para os equipamentos (redundância *hot standby* e *warm standby*).

O restante do artigo está organizado conforme descrito a seguir. A Seção II apresenta os trabalhos relacionados. A Seção III apresenta conceitos fundamentais sobre disponibilidade, confiabilidade e análise de sensibilidade que será aplicada às infraestruturas de *data centers*. A Seção IV detalha os modelos propostos. A Seção V explica a estratégia de modelagem utilizada. A Seção VI apresenta um estudo de caso e, por fim, a Seção VII conclui este trabalho e apresenta trabalhos futuros.

II. TRABALHOS RELACIONADOS

Callou et al. [10] apresentam uma abordagem de modelagem integrada para avaliar e otimizar a sustentabilidade, a disponibilidade e o custo de *data centers*. Uma técnica de modelagem formal híbrida que considera as vantagens de redes de Petri estocásticas, diagramas de blocos de confiabilidade e fluxo de energia (EFM) foi proposta. No entanto, nenhuma técnica de análise de sensibilidade foi empregada.

Figueirêdo et al. [11] apresentam uma análise sobre a importância de confiabilidade e o custo de aquisição para infraestruturas de energia de *data centers*. Uma abordagem que

F. F. L. Melo, Universidade Federal Rural de Pernambuco, Recife-PE, Brazil, e-mail: (felipe.lmelo@ufrpe.br).

E. T. G. SOUSA, Universidade Federal Rural de Pernambuco, Recife-PE, Brazil, e-mail: (erica.sousa@ufrpe.br).

G. R. A. CALLOU, Universidade Federal Rural de Pernambuco, Recife-PE, Brazil, e-mail: (gustavo.callou@ufrpe.br Corresponding).

Author: Felipe Fernandes de Lima Melo.

combina a importância da confiabilidade e índices com TCA (custo total de aquisição) para avaliar infraestruturas elétricas de *data center* foi proposta no artigo. No entanto, um estudo sobre técnicas de redundâncias *hot* e *warm standby* não foi o foco da pesquisa.

Rocha et al. [12] apresentam uma análise referente ao impacto das falhas na infraestrutura de energia e na disponibilidade de aplicações localizadas em *data centers*. O artigo faz uso da análise de sensibilidade para definir quatro arquiteturas de infraestrutura de energia e analisar o impacto das falhas da infraestrutura de energia em serviços hospedados em um *data center*.

Os autores em [13] propõem um mecanismo eficiente de recuperação de falhas para sistemas de multiprocessadores em tempo real com o uso de redundância *cold standby*. Também foi proposto um agendador de tolerância a falhas, chamado FT-FS (Fault Tolerant Fair Scheduler), com o propósito de minimizar as finalizações / rejeições de trabalho durante a recuperação e redistribuindo criteriosamente um subconjunto de tarefas, melhorando desempenho no processo. Não foi o foco da pesquisa as infraestruturas elétricas dos *data centers*.

Zhu et al. [14] apresentam um método de análise de sensibilidade para redes de distribuição desequilibrada com base no modelo de fluxo de energia linearizado. Foi apresentado um método para utilização dos dados de medição com o intuito de construir um modelo de fluxo de potência linearizado, onde os dados de sensibilidade foram obtidos diretamente através da resolução de equações lineares. A análise de diferentes técnicas de redundância para se melhorar a disponibilidade do sistema analisado não foi o foco desse artigo.

Uma contribuição desse trabalho é que nele utiliza-se uma modelagem híbrida e hierárquica, com auxílio da técnica de redes de Petri estocásticas [15] e [16] e diagramas de bloco de confiabilidade [17], diferente das outras abordagens, que usam apenas uma destas técnicas. Uma modelagem híbrida e hierárquica utilizada neste trabalho para avaliar a disponibilidade, confiabilidade e custos dos equipamentos que compõem a infraestrutura elétrica do *data center*, aplicando redundâncias (*hot* e *warm standby*, por exemplo) conforme indicada pela técnica de análise de sensibilidade adotada.

III. FUNDAMENTAÇÃO TEÓRICA

Esta seção fornece uma breve explicação para alguns conceitos necessários para um melhor entendimento deste trabalho. Por exemplo, explicações sobre disponibilidade e confiabilidade, redes de Petri estocásticas, diagramas de bloco de confiabilidade, e análise de sensibilidade são mostradas ao longo da seção.

A. Disponibilidade e Confiabilidade

Um conceito importante é o de *dependability* do sistema que pode ser compreendido como a capacidade de oferecer uma determinada funcionalidade de forma justificadamente confiável [18]. Podendo ser usado para descrever um sistema, confiável durante determinada operação e período de tempo [19].

Os atributos de *dependability* são: disponibilidade, confiabilidade, segurança, confidencialidade, integridade e manutenibilidade [20]. São apresentados os conceitos dos atributos disponibilidade e confiabilidade, utilizados neste trabalho.

- Disponibilidade: corresponde a probabilidade do sistema está em um estado operacional quando este for requisitado [21].
- Confiabilidade: capacidade de fornecer serviços de forma correta e contínua, ou seja, a probabilidade de um defeito não acontecer partindo do tempo inicial ($T=0$) até um determinado período [21].

B. Redes de Petri Estocásticas

Redes de Petri Estocásticas surgiram em 1980 como um formalismo para a descrição de Sistemas Dinâmicos de Eventos Discretos (DEDS) cujo comportamento dinâmico poderia ser representado por meio de cadeias de Markov em tempo contínuo [22].

A Figura 1 representa um exemplo de uma rede de Petri estocástica composta por dois tipos de nós: um nó, representa os lugares, e o outro nó, representa as transições. Em uma SPN, os lugares são representados por círculos (NO0, NO1 e NO2) e as transições por retângulos (T0, T1 e T2). Um lugar se conecta a uma transição através de um arco direcionado, e uma transição pode ser ligada a um lugar através de um outro arco direcionado. Em outras palavras, em SPN, nunca haverá um lugar conectado a outro lugar, diretamente, ou ainda uma transição a outra transição [23]. Uma SPN pode apresentar dois tipos de transições, a imediata e estocástica. No exemplo da Figura 1, a transição imediata (T1) é disparada sempre que a condição de acionamento for satisfeita. Já a transição estocástica (T0 e T2) é acionada após um determinado período de tempo distribuído exponencialmente e associado a cada uma das transições estocásticas.

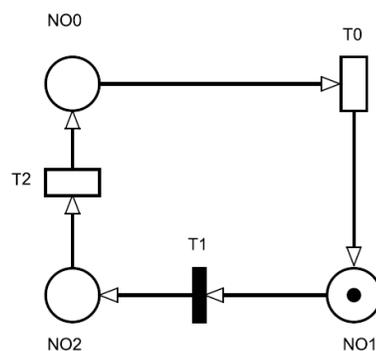


Fig. 1. Exemplo de Modelo SPN.

C. Diagramas de Bloco de Confiabilidade

O RBD fornece um método para avaliação de disponibilidade e/ou confiabilidade através do mapeamento em blocos que se configuram em série ou em paralelo. Cada bloco que compõe o modelo pode representar falhas em um componente individual ou em um subsistema [9].

A Figura 2(a) representa um modelo RBD, em série. Nesse caso, a falha de qualquer componente resulta em uma falha do sistema. Assumindo um sistema com n componentes independentes, a confiabilidade ou disponibilidade são obtidas por:

$$P_s = \prod_{i=1}^n P_i \quad (1)$$

Onde P_i é a confiabilidade $R_i(t)$, disponibilidade instantânea ($A_i(t)$) ou disponibilidade estacionária (A_i) do bloco bi .

Para uma disposição paralela (Figura 2(b)), o sistema funciona se pelo menos um componente funcionar. Assumindo um sistema com n componentes independentes, a confiabilidade, disponibilidade instantânea ou disponibilidade estacionária é obtida por:

$$P_s = 1 - \prod_{i=1}^n (1 - P_i) \quad (2)$$

Onde P_i é a confiabilidade $R_i(t)$, disponibilidade instantânea ($A_i(t)$) ou disponibilidade estacionária (A_i) do bloco bi .

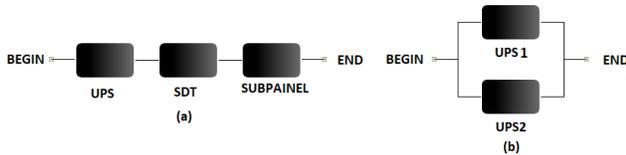


Fig. 2. Exemplo de Modelo RBD em série (a) e em paralelo (b)

D. Análise de Sensibilidade

A análise de sensibilidade (SA) é o estudo de como a variação na saída de um modelo (numérico ou não) pode ser afetada, dependendo da entrada do modelo [24]. O objetivo da SA é identificar insumos críticos (parâmetros e condições iniciais) de um modelo e quantificar como a entrada afeta o(s) resultado(s) do modelo [25]. Sendo assim, este método encontra os fatores que mais influenciam o sistema. Quando um determinado parâmetro é modificado ocasionando uma variação muito alta nos resultados, indica que o projeto ou aplicação é muito sensível a este parâmetro.

Existem alguns métodos para a análise de sensibilidade: variação um por um, diferencial paramétrico (SDP), diferença percentual, importância para a confiabilidade, importância para a disponibilidade, importância para confiabilidade e custo, importância para disponibilidade e custo, e planejamento de experimentos. Este trabalho faz uso de: (i) a análise da importância para confiabilidade e custo; e (ii) a importância para disponibilidade e custo. Ambas análises levam em consideração o custo de aquisição com a disponibilidade ou confiabilidade. A Equação 3 é adotada para computar ambos os índices.

$$Ic_i = I_i^B \times \left(1 - \frac{C_i}{C_{sys}}\right) \quad (3)$$

Onde, Ic_i é o índice de importância (para confiabilidade ou disponibilidade), I_i^B é o valor da importância para a

confiabilidade ou disponibilidade do sistema, C_i o é o custo de aquisição do equipamento i e C_{sys} é o custo de aquisição do sistema.

IV. MODELOS

Nesta seção são apresentados os modelos propostos para a replicação *warm standby* e *hot standby*. A Figura 3 apresenta o modelo básico adotado para representar o cálculo da disponibilidade de um equipamento. Esse modelo representa o comportamento do equipamento que pode estar em funcionamento ou falho. Para calcular sua disponibilidade, o tempo médio de falha (MTTF) e o tempo médio de reparo (MTTR) são os únicos parâmetros necessários, associados às transições de mesmo nome. Um token no lugar Equipamento_ON ou no Equipamento_OFF representa o funcionamento ou a falha do dispositivo, respectivamente.

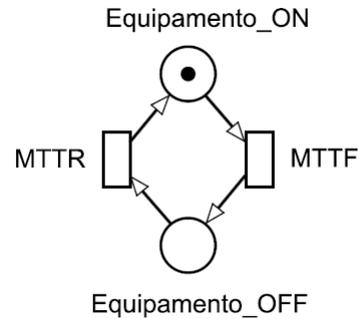


Fig. 3. Modelo Base em Redes de Petri Estocástica

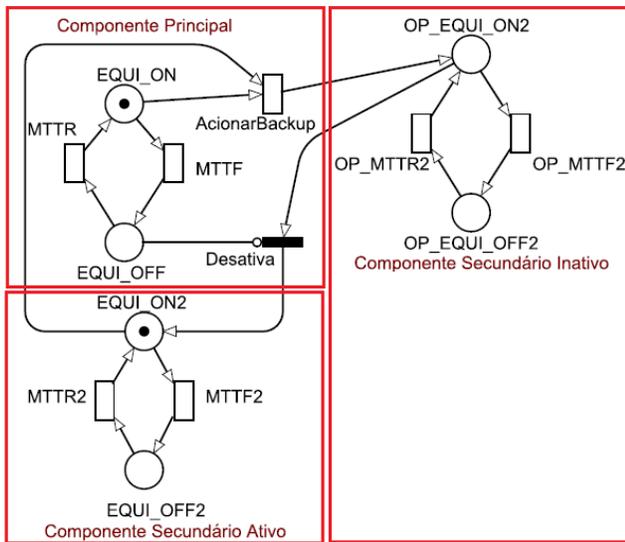
A. Modelo Warm Standby

Um sistema com uma redundância *warm standby* é constituído por dois componentes, onde tem-se um componente principal e um componente secundário. Este mecanismo de redundância possui o módulo reserva configurado, mas indisponível. O módulo secundário é ativado na presença de uma falha no ambiente principal e, por já se encontrar ligado, o tempo de ativação será menor quando comparado a abordagem *cold standby* [26].

A Figura 4 representa o modelo *warm standby*, nota-se que quando o componente principal falha, o componente secundário é ativado. Os lugares EQUI_ON e EQUI_OFF representam os estados operacional e não operacional do componente principal. Os lugares OP_EQUI_ON2 e OP_EQUI_OFF2 representam o componente secundário no estado operacional e não operacional. Os lugares EQUI_ON2 e EQUI_OFF2 representam a situação na qual o módulo secundário falha antes de ser ativado. Quando o módulo principal falha, a transição AcionarBackup é disparada para ativar o módulo secundário. Após a máquina principal ter sido reparada, a transição imediata Desativa é ativada e a máquina de backup é desligada.

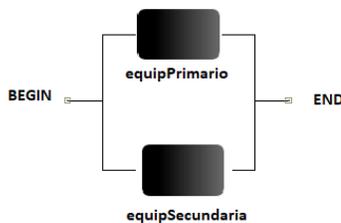
B. Modelo Hot Standby

O sistema com redundância *hot standby* é composto por dois equipamentos, o primário e o secundário. O equipamento

Fig. 4. Modelo *warm Standby*

secundário está no modo de espera funcionando em sincronia com o equipamento primário que está ativo [26]. Sendo assim os componentes do sistema secundário estão sempre ativos, mas não processam dados ou solicitações.

O modelo *hot standby* foi concebido utilizando diagrama de blocos de confiabilidade, pois não há a necessidade de representar a dependência entre os equipamentos. A Figura 5 apresenta o modelo da arquitetura A1 onde tem-se o equipamento redundante. Conforme pode ser observado na Figura 5, os blocos *equipPrimario* e *equipSecundaria* encontram-se em paralelo. Esses blocos representam os componentes primários e secundários.

Fig. 5. Modelo *Hot Standby*.

A replicação no modelo RBD significa que qualquer equipamento que for replicado assume uma modelagem semelhante à do equipamento principal, porém este novo equipamento pode ter seu MTTF e MTTR modificado ou igual ao equipamento principal.

V. ESTRATÉGIA DE MODELAGEM

A estratégia de modelagem utilizada neste artigo é uma modelagem híbrida e hierárquica. A modelagem é híbrida devido ao fato de serem adotados os formalismos RBD e SPN para realizar a modelagem e captura das métricas de disponibilidade e confiabilidade.

A Figura 6 representa a modelagem hierárquica através do modelo RBD. Os blocos *racki* (Figura 6) representam 15

equipamentos ligados em série. Os valores para o MTTF e MTTR do modelo representado na Figura 6, que representa todos os 15 racks em série, foram obtidos pela avaliação do modelo da Figura 6.



Fig. 6. Modelagem Hierárquica - 15 dispositivos em Série.

A ferramenta utilizada para a modelagem e realização dos experimentos foi o Mercury [27], uma ferramenta desenvolvida pelo grupo de pesquisa MODCS, que possibilita a avaliação de modelos de confiabilidade, desempenho e fluxo de energia. Oferece recursos úteis que não são facilmente encontrados em outras ferramentas, como: mais de 25 distribuições de probabilidade suportadas na simulação de SPN, análise de sensibilidade de modelos CTMC e RBD, cálculo de índices de importância de confiabilidade e correspondência de momento de dados empíricos [27].

Vale destacar que esse trabalho faz uso das SPNs e do RBD, utilizando as vantagens de cada estratégia de modelagem. Por um lado as SPNs possibilitam a representação de dependência entre os equipamentos (a falha de um equipamento aciona um outro), por outro lado ela sofre com a explosão do espaço de estado. Esse problema de explosão está relacionado ao número de estados que cresce e, praticamente, inviabiliza a análise do modelo em questão. Já os modelos em RBD representam diferentes cenários e podem ser solucionados via equações fechadas, sendo a solução rápida e eficiente. Porém, com o RBD não é viável a representação de dependência entre os componentes do sistema. Sendo assim, este artigo procura utilizar SPN quando existe dependência entre os equipamentos, por exemplo, nas redundâncias *cold standby*. Já para a redundância *hot standby*, optou-se por usar modelos desenvolvidos em RBD, por não ser necessário representar dependência entre os componentes. Dessa forma, usando essa estratégia de modelagem, pode-se evitar o problema da explosão do espaço de estados e se consegue modelar a dependência entre os equipamentos.

VI. ESTUDO DE CASO

O objetivo deste estudo de caso é mostrar a aplicabilidade da estratégia proposta em uma infraestrutura elétrica típica de *data centers*. A partir de uma arquitetura inicial, outras arquiteturas foram propostas baseadas na análise de sensibilidade feita. Essa análise identifica os equipamentos que devem ser replicados para aumentar, por exemplo, a disponibilidade do sistema. Após a identificação do equipamento mais sensível, este será replicado considerando duas alternativas de redundâncias (*warm standby* e *hot standby*). Sendo assim, o estudo caso compara qual dessas técnicas de redundância apresenta melhor resultado.

As arquiteturas A1 a A6 de *data centers* foram analisadas nesse estudo de caso. A arquitetura A2 foi proposta a partir da análise de sensibilidade feita na arquitetura A1. Similarmente, o processo foi repetido até se chegar a arquitetura A6. A seguir

são apresentados os componentes que compõem cada uma destas arquiteturas.

A Figura 7 ilustra a Arquitetura A1, esta não tem nenhuma redundância, sendo composta por UPS, SDT, SubPanel, Power strip, junction box e equipamento de TI (rack).

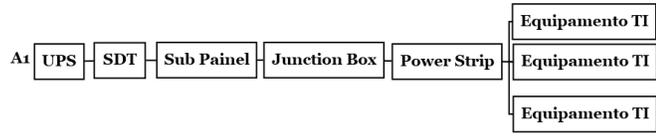


Fig. 7. Arquitetura A1

A Figura 8 mostra a Arquitetura A2 que é semelhante a Arquitetura A1 com a diferença na replicação do Power strip.

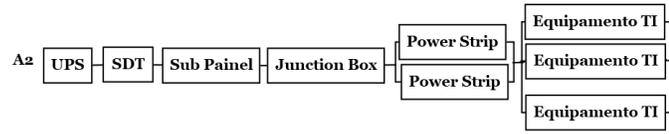


Fig. 8. Arquitetura A2

A Figura 9 ilustra a Arquitetura A3 com os mesmos componentes presentes na Arquitetura A1, com a diferença na replicação do SDT e Power strip, como também a adição de uma chave de transferência estática (STS).

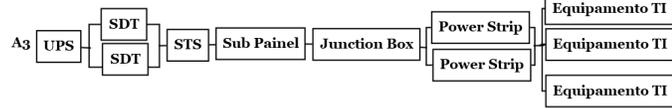


Fig. 9. Arquitetura A3

A Figura 10 apresenta a Arquitetura A4 onde temos os mesmos componentes presentes na Arquitetura A1, com a diferença que na replicação do SDT, Power strip e UPS.

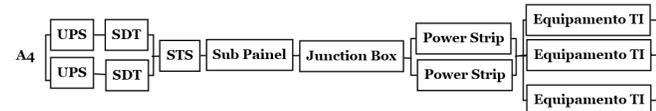


Fig. 10. Arquitetura A4

A Figura 11 apresenta a Arquitetura A5 onde temos os mesmos componentes presentes na Arquitetura A4, com a replicação do junction box.

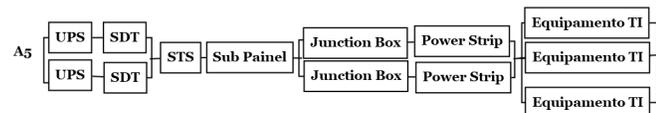


Fig. 11. Arquitetura A5

A Figura 12 ilustra a Arquitetura A6 que corresponde a Arquitetura A1 com todos os equipamentos replicados. Vale ressaltar que essa arquitetura não tem a necessidade do equipamento STS.

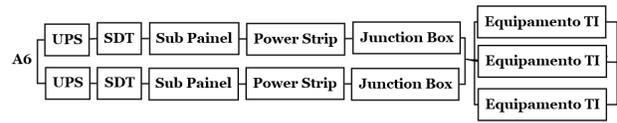


Fig. 12. Arquitetura A6

É importante ressaltar que a partir da arquitetura inicial, A1, foi realizada a análise de sensibilidade para se propor as demais arquiteturas que consideram redundância incremental dos dispositivos. Além disso, dois métodos distintos de redundância, *hot* e *warm standby*, foram escolhidos para realizar a replicação de cada dispositivo. Na redundância *hot standby* foi utilizado o modelo RBD, pois não há a necessidade de representar dependência entre os componentes. Já para a redundância *warm standby*, devido a dependência entre os componentes, foi utilizado o modelo SPN.

A infraestrutura elétrica de um *data center* é composta por fontes de alimentação sem interrupção (UPS), um transformador (SDT), um chaveador elétrico manual (STS), um painel elétrico, caixa de junção elétrica (junction box), régua de tomadas elétricas (power strip) e equipamento de TI. A Tabela I apresenta os MTTFs e MTTRs dos equipamentos utilizados neste trabalho [28].

TABELA I
RESUMO DOS PARÂMETROS DE ENTRADA.

Dispositivo	MTTF (h)	MTTR (h)		Custo de Aquisição	
		Equip. Primários (R\$)	Equip. Secundários (R\$)	Equip. Primários (R\$)	Equip. Secundários (R\$)
UPS	250000	8	21.553,29	15.087,30	
STS	24038462	6	2.282,28	1.597,60	
SDT	1412908	156,01	5.347,44	3.743,21	
Sub Painel	1520000	2,4	208,61	146,03	
Power Strip	11511175,62	3,8	1.817,58	1.272,31	
Junction Box	17200000	8	42,02	29,41	
Equipamento de TI	1481377,7474	4.000004	1.387,69	971,38	

A Tabela I apresenta ainda o custo de aquisição de cada equipamento utilizado nesta análise. Esses custos são utilizados tanto para o modelo *hot standby* como para o modelo *warm standby*. Porém, a máquina de backup utilizada apresenta um custo menor, tendo em vista que a utilização deste equipamento é menor quando comparada ao equipamento principal. Logo, considera-se para o equipamento de backup um custo de 70% em relação ao custo do equipamento original.

Tomando como base a arquitetura A1, outras foram propostas a partir da análise de sensibilidade (ver Tabela II). Levando em consideração a análise de sensibilidade para a disponibilidade, pode-se observar que o equipamento mais indicado para ser replicado da arquitetura A1 é o powerstrip (ver linha A1 da Tabela II, onde o maior valor se encontra em destaque). Sendo assim, a arquitetura A2 considera tal equipamento replicado. Esse mesmo procedimento foi adotado para se chegar nas demais arquiteturas. Vale ressaltar que tanto para a disponibilidade (Tabela II) quanto para confiabilidade (ver Tabela III) foi realizada a análise de sensibilidade em conjunto com o custo de aquisição de cada equipamento presente na arquitetura. No caso da confiabilidade, o modelo foi avaliado levando em consideração o período de 5 anos. Nas Tabelas II e III é possível identificar (em destaque) os equipamentos mais sensíveis encontrados a partir da análise de sensibilidade realizada em cada arquitetura.

TABELA II
EQUIPAMENTOS MAIS SENSÍVEIS PARA A
DISPONIBILIDADE NAS ARQUITETURAS DE A1 ATÉ A5

Arquitetura	Disponibilidade						
	PowerStrip	SDT	UPS	JB	SubPainel	Equip TI	STS
A1	1,000	0,999	0,9955	0,991	0,953	5,02E-03	-
A2	3,30E-09	1,000	0,996	0,992	0,954	5,02E-03	-
A3	3,31E-08	1,11E-12	1,000	0,997	0,972	5,81E-03	0,663
A4	3,32E-08	1,43E-12	1,43E-11	1,000	0,975	5,83E-03	0,666
A5	0,080	1,47E-11	1,46E-12	0,079	1,000	5,98E-03	0,684

TABELA III
EQUIPAMENTOS MAIS SENSÍVEIS PARA A CONFIABILIDADE
NAS ARQUITETURAS DE A1 ATÉ A5

Arquitetura	Confiabilidade						
	PowerStrip	SDT	UPS	JB	SubPainel	Equip TI	STS
A1	0,846	0,869	1,000	0,837	0,827	4,92E-11	-
A2	0,974	1,000	0,222	0,967	0,968	6,54E-11	0,643
A3	1,000	0,223	0,257	0,992	0,994	6,72E-11	0,660
A4	3,29E-06	0,225	0,259	0,999	1,000	6,76E-11	0,664
A5	2,01E-02	1,45E-12	1,45E-12	1,000	1,39E-12	5,14E-02	-

A Figura 13 apresenta o modelo RBD proposto para representar a disponibilidade obtida com a redundância *hot standby* na arquitetura A2. Neste modelo, o equipamento secundário encontra-se em modo de espera, contudo funcionando em paralelo ao equipamento principal, sem ser utilizado. Em caso de falha do equipamento principal, o equipamento secundário começa a ser utilizado.

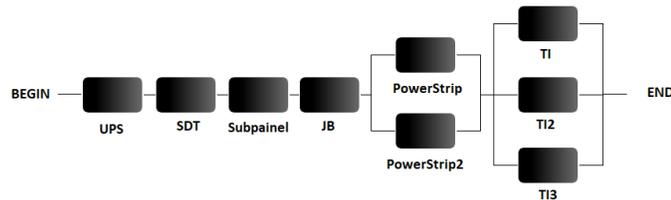


Fig. 13. Modelo *Hot Standby*

A Figura 14 apresenta o modelo SPN proposto para representar a disponibilidade obtida com a redundância *warm standby* na arquitetura A2. Neste modelo, o equipamento secundário está indisponível, sendo ativado em caso de falha do dispositivo principal (token no lugar POWERSTRIP_OFF). A disponibilidade dessa arquitetura é computada por:

$$A = (P\{(\#UPS_ON=1) \text{ AND } (\#SDT_ON=1) \text{ AND } (\#SUBPAINEL_ON=1) \text{ AND } (\#JB_ON=1) \text{ AND } ((\#POWERSTRIP_ON=1) \text{ OR } (\#OP_POWERSTRIP_ON2=1)) \text{ AND } ((\#RACK_ON=1) \text{ OR } (\#RACK_ON2=1) \text{ OR } (\#RACK_ON3=1))\})$$

A. Resultados - Disponibilidade

A Figura 15 apresenta a diferença em percentual do custo de aquisição das arquiteturas em relação a arquitetura A1. Vale ressaltar que o custo de aquisição é o mesmo para a redundância, *hot standby* e *warm standby*. Conforme pode ser observado nas Figura 15 e 16, o custo de aquisição e a disponibilidade tendem a aumentar com a adição dos equipamentos. Sendo assim, a aplicação da redundância nos equipamentos mais críticos é de grande valia para aumentar a disponibilidade do sistema.

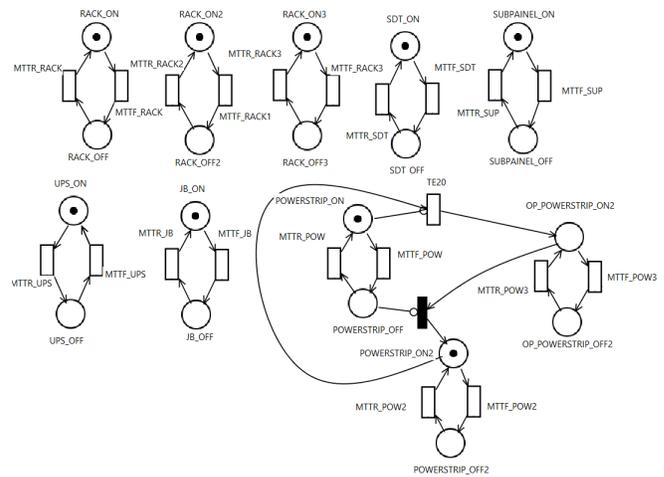


Fig. 14. Modelo *Warm Standby*

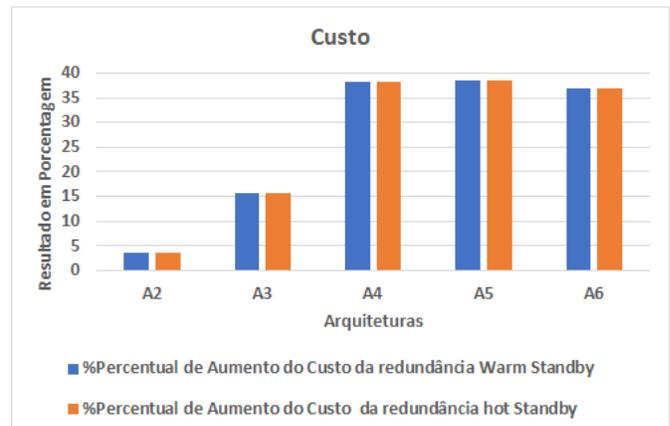


Fig. 15. Custo das Arquiteturas (A2, A3, A4 e 5) em Relação a Arquitetura A1.

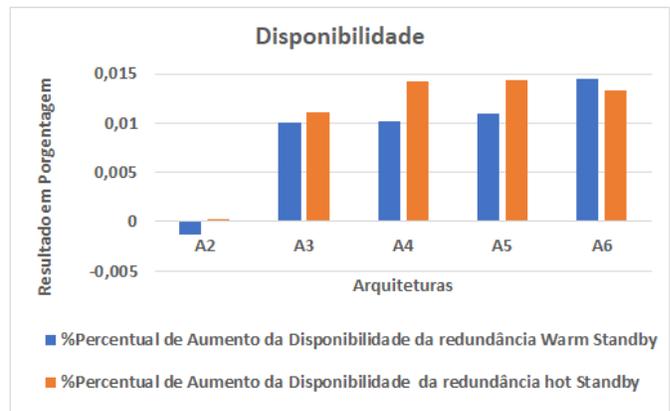


Fig. 16. Disponibilidade das Arquiteturas (A2, A3, A4 e A5) em Relação a Arquitetura A1.

Na Figura 16 pode-se observar que a disponibilidade das arquiteturas com a redundância *hot standby* foi superior a disponibilidade das arquiteturas com a redundância *warm standby*. Assim, pode-se concluir que a redundância *hot standby* pode ser adotada por apresentar melhores resultados de disponibilidade nas arquiteturas A1 até A5. Porém, na

arquitetura A6 com a redundância *warm standby* apresenta melhor resultado de disponibilidade, sendo, mas indicada para ser utilizada neste cenário. A disponibilidade da arquitetura A2 é um pouco menor que a disponibilidade da arquitetura A1 quando a redundância *warm standby* é adotada. Este comportamento é esperado visto que mesmo tendo replicado o equipamento mais crítico, existe um tempo de espera de 6 ms até que o dispositivo secundário seja ativado, visto que é utilizado um chaveamento para acionar o dispositivo redundante.

Conforme pode ser observado nos gráficos, a redundância *warm standby* na arquitetura A6 apresenta a melhor disponibilidade, porém também apresenta o custo mais elevado com um aumento percentual de 37% em relação a A1. Nas arquiteturas A4, A5 e A6 os valores da disponibilidade e custo estão próximos. Logo, mesmo fazendo uso da arquitetura A6, que apresenta o maior custo de aquisição, este custo está bem próximo ao custo das arquiteturas A4 e A5.

B. Resultados – Confiabilidade

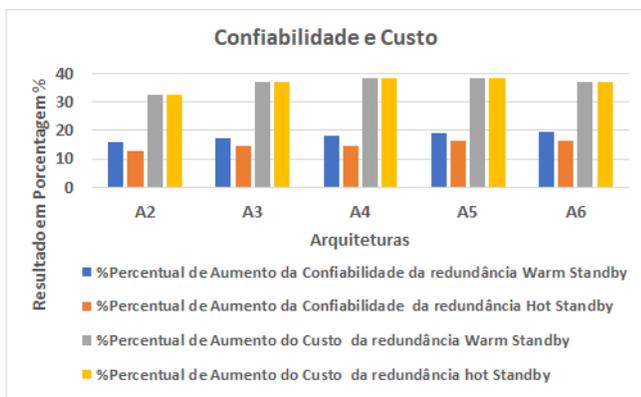


Fig. 17. Confiabilidade em percentual, das Arquiteturas (A2, A3, A4 e A5) em Relação a Arquitetura A1.

A Figura 17 apresenta os resultados obtidos para a confiabilidade das arquiteturas A1 até A6 quando são adotadas as redundâncias *hot standby* e *warm standby*, durante um período de 5 anos. A arquitetura A6 obteve o melhor resultado da confiabilidade para ambas as estratégias de redundância, apresentando um aumento de 19,32% para a redundância *warm standby* e um aumento percentual de 16,20% para a redundância *hot standby*. Porém, para a redundância *warm standby*, observa-se que os resultados foram bem melhores quando comparado a *hot standby*.

C. Considerações Finais

Com a estratégia de modelagem proposta foi possível analisar arquiteturas distintas de *data centers*, considerando diferentes técnicas de redundâncias, neste caso, através da replicação *hot* e *warm standby*. Constatou-se que ao ser comparada a disponibilidade obtida por cada tipo de redundância foi possível identificar, nas arquiteturas A1 a A5, que o uso da redundância *hot standby* conseguiu obter resultados que foram

superiores, quando comparados a redundância *warm standby*. Sendo assim, para essas arquiteturas o uso desta técnica foi a mais indicada.

No entanto, foi possível verificar que os resultados obtidos para a confiabilidade, no período de cinco anos, resultou na indicação da outra estratégia de redundância. Em outras palavras, os resultados obtidos mostraram que a técnica de redundância *warm standby* apresentou os melhores resultados para todas as arquiteturas analisadas. Sendo assim, analisando a confiabilidade das arquiteturas, a redundância que apresentou os melhores resultados foi a redundância *warm standby*.

Além do fato que faz uso de abordagens distintas, permitindo assim, uma modelagem híbrida e hierárquica, com auxílio de técnica de redes de Petri estocásticas e diagramas de bloco de confiabilidade. Além disso, com a análise de sensibilidade foi possível propor modelos de dependabilidade de acordo com as necessidades do ambiente de data center, possibilitando a criação de modelos incrementais. Fazendo uso também de duas técnicas de redundâncias distintas a *hot* e *warm standby*, onde dos trabalhos analisados poucos fazem esse tipo de comparação ainda mais para o cenário de *data center*.

VII. CONCLUSÃO

Este trabalho apresentou uma abordagem de modelagem híbrida e hierárquica que considera a utilização de redes de Petri e diagrama de bloco de confiabilidade para analisar a infraestrutura elétrica de *data centers*. A estratégia proposta por este trabalho faz uso de uma análise de sensibilidade com o objetivo de verificar qual equipamento é mais sensível as métricas de disponibilidade e custo, e confiabilidade e custo. Os equipamentos mais sensíveis foram replicados levando em consideração duas técnicas distintas (*hot standby* e *warm standby*), propondo assim, novas arquiteturas. Os experimentos realizados evidenciaram a viabilidade da abordagem proposta, fornecendo resultados importantes para os projetistas de *data centers* em auxiliar na escolha da melhor estratégia de redundância dos equipamentos. De acordo com os resultados obtidos, a utilização da redundância *warm standby* foi mais indicada ao se levar em consideração a confiabilidade do sistema. No entanto, quando se deseja levar em consideração a disponibilidade, a redundância indicada foi a *hot standby*.

Como trabalho futuro, estaremos ampliando a metodologia proposta para avaliar outras infraestruturas de *data centers*, por exemplo, TI e refrigeração. Outro possível direcionamento desta pesquisa é a avaliação de diferentes políticas de manutenção.

AGRADECIMENTOS

Os autores gostariam de agradecer à FACEPE e ao CNPq pelo suporte financeiro a esta pesquisa.

REFERÊNCIAS

- [1] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A berkeley view of cloud computing," *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, vol. 28, no. 13, p. 2009, 2009.

- [2] S. Chandel, T.-Y. Ni, and G. Yang, "Enterprise cloud: Its growth & security challenges in china," in *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2018, pp. 144–152.
- [3] E. d. C. Sousa, "Os benefícios do investimento na capacitação profissional da equipe de manutenção e operação de data center," *Datacenter: projeto, operação e serviços-Unisul Virtual*, 2017.
- [4] M. Arregoces and M. Portolani, *Data center fundamentals*. Cisco Press, 2003.
- [5] P. S. MARIN, "Data centers—engenharia: Infraestrutura física," 2016.
- [6] A. Saltelli, S. Tarantola, F. Campolongo, and M. Ratto, "Sensitivity analysis in practice: a guide to assessing scientific models," *Chichester, England*, 2004.
- [7] E. Bauer, R. Adams, and D. Eustace, *Beyond redundancy: how geographic redundancy can improve service availability and reliability of computer-based systems*. John Wiley & Sons, 2011.
- [8] A. N. da Silva, F. A. Lins, J. C. Júnior, N. S. Rosa, N. C. Quental, and P. R. Maciel, "Avaliação de desempenho da composição de web services usando redes de petri," in *Brazilian Symposium on Computer Networks. Curitiba, Paraná, Brazil*, 2006.
- [9] W. Torell and V. Avelar, "Tempo médio entre falhas: Explicação e padrões," *W. Kingston, Rhode Island: American Power Conversion*, 2004.
- [10] G. Callou, J. Ferreira, P. Maciel, D. Tutsch, and R. Souza, "An integrated modeling approach to evaluate and optimize data center sustainability, dependability and cost," *Energies*, vol. 7, no. 1, pp. 238–277, 2014.
- [11] J. Figueirêdo, P. Maciel, G. Callou, E. Tavares, E. Sousa, and B. Silva, "Estimating reliability importance and total cost of acquisition for data center power infrastructures," in *2011 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 2011, pp. 421–426.
- [12] É. Rocha, P. T. Endo, G. Leoni, J. Braga, and T. Lynn, "Analyzing the impact of power infrastructure failures on cloud application availability," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2017, pp. 1746–1751.
- [13] P. P. Nair, A. Sarkar, and S. Biswas, "Fault-tolerant real-time fair scheduling on multiprocessor systems with cold-standby," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [14] T. Zhu, T. Xia, Z. Wan, and C. Zhao, "A sensitivity analysis method for unbalanced distribution network based on linearized power flow model," in *2018 International Conference on Power System Technology (POWERCON)*. IEEE, 2018, pp. 1558–1563.
- [15] K. S. Trivedi, *Probability and statistics with reliability, queuing, and computer science applications*. Wiley Online Library, 1982, vol. 13.
- [16] P. J. Haas, *Stochastic petri nets: Modelling, stability, simulation*. Springer Science & Business Media, 2006.
- [17] M. Xie, Y.-S. Dai, and K.-L. Poh, *Computing system reliability: models and analysis*. Springer Science & Business Media, 2004.
- [18] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.
- [19] L. Petre, K. Sere, and E. Troubitsyna, *Dependability and Computer Engineering: Concepts for Software-intensive Systems*. Engineering Science Reference, 2011.
- [20] G. Callou, E. Sousa, P. Maciel, E. Tavares, C. Araujo, B. Silva, N. Rosa, M. Marwah, R. Sharma, A. Shah *et al.*, "Impact analysis of maintenance policies on data center power infrastructure," in *2010 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2010, pp. 526–533.
- [21] I. M. D. d. Silva, "Uma metodologia para modelagem e avaliação da dependabilidade de redes industriais sem fio," 2013.
- [22] G. Balbo, "Introduction to stochastic petri nets," in *School organized by the European Educational Forum*. Springer, 2000, pp. 84–155.
- [23] R. Briš, "Evaluation of the production availability of an offshore installation by stochastic petri nets modeling," in *The International Conference on Digital Technologies 2013*. IEEE, 2013, pp. 147–155.
- [24] A. Saltelli, K. Chan, and M. Scott, "Handbook of sensitivity analysis," 2000.
- [25] S. Marino, I. B. Hogue, C. J. Ray, and D. E. Kirschner, "A methodology for performing global uncertainty and sensitivity analysis in systems biology," *Journal of theoretical biology*, vol. 254, no. 1, pp. 178–196, 2008.
- [26] G. Levitin, L. Xing, and Y. Dai, "Cold vs. hot standby mission operation cost minimization for 1-out-of-n systems," *European Journal of Operational Research*, vol. 234, no. 1, pp. 155–162, 2014.
- [27] B. Silva, R. Matos, G. Callou, J. Figueiredo, D. Oliveira, J. Ferreira, J. Dantas, A. Junior, V. Alves, and P. Maciel, "Mercury: An integrated environment for performance and dependability evaluation of general systems," in *Proceedings of Industrial Track at 45th Dependable Systems and Networks Conference, DSN*, 2015.
- [28] V. Avelar, "Comparing availability of various rack power redundancy configurations," *APC White Paper*, vol. 48, pp. 1–22, 2003.



Felipe Fernandes is graduated in Bachelor of Information Systems at Federal Rural University of Pernambuco (UFRPE) and is a Msc candidate at Federal Rural University of Pernambuco (UFRPE). He has interest in optimization, maintenance, Performance evaluation of systems, Big data, data center.



Erica Sousa is graduated at Electronic Engineering from Pernambuco University (UPE/Brazil) and received her M. Sc and Ph.D. degree in the Federal University of Pernambuco (UFPE/Brazil). She has experience in computer science, and is involved in cloud computing, virtual learning environment, electronic funds transfer systems, stochastic models, performance model, dependability model, and performance analysis. Currently, she is assistant professor at Federal Rural University of Pernambuco.



Gustavo Callou is associate professor at the Federal Rural University of Pernambuco, Brazil. He has Ph.D. in Computer Science from the Federal University of Pernambuco, Brazil, with split-site doctoral program at Bergische Universität Wuppertal, Germany, in the area of Performance Evaluation. Key research interests include Petri nets, Reliability Analysis, Fault Tolerant Computing, Performance Engineering, Sustainability, Computer Networking, Cloud Computing and Data Centers. He also participated in several projects, such as: Reliability and Performance Evaluation of Storage Systems - DEPS (funded by EMC Corporation, USA), Reliability Assessment and Management of Sustainable Data Centers - DESDAC (funded by HP, Palo Alto, USA), Evaluation and Optimization of Performance, Reliability, Sustainability and Cost of Computational Systems. (Funded by FACEPE / CNPq in Brazil).