

UMA FERRAMENTA PARA ANÁLISE DE DEPENDABILIDADE DE PROCESSOS INDUSTRIAIS

DANIEL MACEDO*, IVANOVITCH SILVA*, LUIZ AFFONSO GUEDES*

**Laboratório de Informática Industrial*

Departamento de Engenharia de Computação e Automação, Instituto Metrópole Digital

Universidade Federal do Rio Grande do Norte

Campus Universitário Lagoa Nova CEP 59078-970

Natal, Rio Grande do Norte, Brasil

Emails: danielmacedo@dca.ufrn.br, ivan@imd.ufrn.br, affonso@dca.ufrn.br

Abstract— The demand for development of new tools to support designing, monitoring, maintaining and commissioning of industrial processes is permanent. The complexity of the industrial environment requires that these tools have flexible features in order to provide valuable data at the early planning and design phases. Furthermore, it is known that industrial processes have stringent requirements for dependability (reliability and availability), since failures can cause economic loss, environmental damage and danger to people. Thus, this work presents a framework which is able to estimate the reliability and availability of industrial processes modeled as a graph. The framework transforms the graph structure into a Fault Tree model in order to analyze the dependability of the process. A dependability study of an industrial wireless process is conducted to validate the proposal.

Keywords— Dependability, Industrial Processes, Fault Tree.

Resumo— A demanda por desenvolvimento de novas ferramentas para suporte ao projeto, monitoramento, manutenção e comissionamento de processos industriais é permanente. A complexidade do ambiente industrial exige que estas ferramentas sejam flexíveis para fornecer dados valiosos no planejamento inicial e na frase de projeto. Mais que isso, é conhecido que processos industriais têm requisitos rigorosos para dependabilidade (confiabilidade e disponibilidade), desde que falhas podem causar perda econômica, danos ambientais e por pessoas em risco. Assim, esse trabalho apresenta uma ferramenta que é capaz de estimar a confiabilidade e disponibilidade de processos industriais modelados como um grafo. A ferramenta transforma uma estrutura de grafo em um modelo de Árvore de Falhas para analisar a dependabilidade do processo. Um estudo da dependabilidade de uma rede industrial sem fio é conduzido para validar a proposta.

Palavras-chave— Dependabilidade, Processos Industriais, Árvore de Falhas.

1 Introdução

A pesquisa de ferramentas em ambientes industriais sempre irá existir, dado o crescente número de estudos, pesquisa e desenvolvimento na área (Krishnamurthy et al., 2005; Cinque et al., 2007; Xing et al., 2012). Nesse contexto, nós destacamos o desenvolvimento de ferramentas que monitoram o comportamento de processos industriais. Estimar a dependabilidade desses processos durante o começo do planejamento e na fase de projeto pode ajudar a antecipar importantes decisões, tais como o comportamento das falhas (confiabilidade do sistema), disponibilidade e criticidade dos dispositivos. Estes dados podem ser obtidos quantitativamente usando modelos matemáticos, por exemplo, Árvore de Falhas e Cadeias de Markov.

Um processo industrial é composto de dispositivos heterogêneos conectados por uma estrutura de rede. Falhas de dispositivos e conexões (*links*) podem causar uma falha no processo, que pode resultar em perdas financeiras, danos ambientais ou por trabalhadores em risco. O primeiro é geralmente afetado por falhas permanentes (funcionamento defeituoso de *hardware*) enquanto o último é mais comumente influenciado por falhas transitentes.

O principal objetivo desse trabalho é fornecer uma avaliação da dependabilidade de processos industriais onde ambos os dispositivos e as conexões da estrutura de processo estão sujeitos a falhas. A ferramenta transforma a estrutura de processo (mapeados por uma rede e modelado como um grafo) em um modelo de Árvore de Falhas, onde a avaliação de dependabilidade é conduzida.

O restante desse artigo é organizado da seguinte forma: Seção 2 descreve o estado da arte na área de confiabilidade e disponibilidade de redes. Na Seção 3 é apresentado o conceito de Árvore de Falhas. Na Seção 4, a ferramenta para avaliação da dependabilidade de processos industriais é proposta. Resultados são discutidos na Seção 5. Finalmente, na Seção 6 concluímos o artigo e apresentamos direções para estudos futuros.

2 Trabalhos Relacionados

A avaliação da dependabilidade de processos industriais pode ser simplificada se considerarmos este tipo de aplicação como uma rede (cabeadas ou sem fio). O processo industrial em si pode ser mapeado por uma estrutura de rede.

O problema de confiabilidade da rede é um problema clássico de confiabilidade (AboElFotouh

and Colbourn, 1989), que pode ser classificado como: *k-terminais*, *2-terminais* ou *todos-terminais*. Dada uma rede de N dispositivos e um conjunto de K dispositivos ($K \subset N$ e $|K| < |N|$). K é um conjunto composto por um dispositivo centralizador e $K-1$ dispositivos de campo. Definindo um dispositivo centralizador $s \in K$, o problema *k-terminais* é expressado como a probabilidade de que exista pelo menos um caminho de s para cada dispositivo de campo incluso em K . O problema *2-terminais* é o caso onde $K = 2$, ao passo que o problema de *todos-terminais* é o caso em que $|K| = |N|$.

Uma tentativa para criar uma metodologia para avaliar a dependabilidade de rede de sensores sem fio (RSSF) foi realizada em (Cinque et al., 2007). Os autores criaram um modelo de simulação, baseado no formalismo de Redes Ativas Estocásticas, para analisar falhas transientes. Para introduzir o conceito de arquitetura de modelos, os mesmos autores estenderam o trabalho anterior (Cinque et al., 2007) criando uma proposta dinâmica capaz de especializar o estudo descrito em (Di Martino et al., 2012).

Porém, para ambos os trabalhos anteriores, a condição de falha é apenas baseada em médias da rede (RSSF opera analisando se um dado número de dispositivos está funcionando) tampouco é possível definir condições de falhas usando dispositivos específicos. Mais que isso, métricas clássicas de dependabilidade não são suportadas, por exemplo, confiabilidade, disponibilidade e criticidade de dispositivos.

Recentemente, uma contribuição interessante para avaliação da dependabilidade de RSSF foi proposto em (Xing et al., 2012). A principal ideia é avaliar a influência de falhas em modo comum. O autor propõe um esquema progressivo baseado em diagramas de decisão binários para avaliação de uma topologia *ad-hoc*. Todavia, o modelo não suporta condições genéricas de falha na rede tampouco uma análise de importância dos dispositivos.

A partir da discussão acima se torna claro que os trabalhos já desenvolvidos na literatura têm fornecido apenas uma solução parcial para o problema visado, uma vez que a maioria deles é focado em situações muito específicas. Adicionalmente, esses trabalhos são muito restritivos no que diz respeito à definição das condições de falha da rede, métricas de confiabilidade, topologia e aspectos de reconfiguração. A ferramenta proposta neste trabalho utiliza-se de uma metodologia que não é uma abordagem nova, visto que o problema da confiabilidade em redes já foi avaliado na literatura (AboElFotouh and Colbourn, 1989), no entanto, a metodologia adotada visa eliminar a maioria das limitações dos trabalhos anteriores. Além disso, os trabalhos analisados geram seus próprios modelos de confiabilidade, o que dificulta a gene-

ralização dos resultados.

A ferramenta proposta resolve vários aspectos, uma vez que se adapta a diferentes tipos de cenários. As principais vantagens, quando comparada com as abordagens disponíveis na literatura, são as seguintes:

- Suporte para qualquer topologia de rede: mesh, estrela e linha;
- As condições de falha podem ser especificadas por um grupo de dispositivos ou um único dispositivo;
- Considera falhas nos enlaces e *hardware*;
- As taxas de falha e reparação podem ser baseadas em distribuições estatísticas;
- Diversos tipos de medidas de dependabilidade podem ser obtida a partir do mesmo modelo (confiabilidade, disponibilidade, tempo médio para falha, conjuntos mínimos de corte, criticidade, Fussell-de Vesely, Birnbaum);
- Fornece um módulo para monitorar o sistema em tempo real;
- Possibilidade de configurar dispositivos redundantes.

3 Árvore de Falhas

Árvore de Falhas é um modelo matemático amplamente usado na indústria (Limnios, 2007). Em resumo, Árvores de Falhas podem ser entendidas como um conjunto de eventos, os quais combinados através de portas lógicas convergem em um único nó, o topo da árvore ou evento topo.

Esse modelo pode ser usado para avaliar a confiabilidade e disponibilidade de uma rede. A principal vantagem da análise de Árvore de Falhas está relacionada com o procedimento intuitivo utilizado para descrever os acontecimentos que leva à falhas da rede. No entanto, para topologias complexas, a construção de uma Árvore de Falhas é uma tarefa demorada e demanda muito esforço. A solução usual é a adoção de uma abordagem que gera automaticamente a Árvore de Falhas (Majdara and Wakabayashi, 2009).

As portas lógicas de uma Árvore de Falhas mais comuns são as *and*, *or* e *k-out-n*. A representação e expressão de cada uma delas é apresentada na Figura 1, onde $F(t)$ é a probabilidade de um dispositivo ou porta lógica falhar, enquanto que $F_i(t)$ é a probabilidade do evento i falhar

O processo de construção de uma Árvore de Falhas é realizada de forma dedutiva e começa definindo o evento topo, que representa a condição de falha do sistema. De um ponto de vista probabilístico, a avaliação de uma Árvore de Falhas consiste em calcular a probabilidade do evento topo a partir das probabilidades dos eventos básicos.

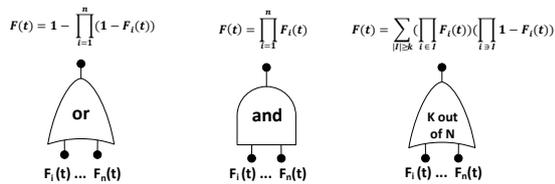


Figura 1: Expressões das portas lógicas *and*, *or* e *k-out-n*.

4 Proposta da ferramenta de avaliação

Nomeado de *BR-Industrial Process Expert*, o principal objetivo da ferramenta proposta neste trabalho é fornecer informações valiosas para o projetista do sistema, permitindo o desenvolvimento de aplicações industriais tolerantes a falhas e manutenção do sistema de forma mais eficiente.

4.1 Visão geral

A Figura 2 descreve uma visão geral da ferramenta proposta neste trabalho. Ela está organizada nos seguintes módulos: um editor da rede, um gerador de Árvore de Falhas, uma ferramenta de relatório e um módulo de supervisão.

A análise da confiabilidade começa no fornecimento de informações sobre a topologia da rede no primeiro módulo. Depois disso, a taxa de falha e de reparação dos dispositivos e a condição de falha da rede são definidos. O módulo gerador de Árvore de Falhas usa essas informações para criar uma Árvore de Falhas correspondente à rede. Por fim, as métricas de interesse são avaliadas na ferramenta de relatório. Passada a fase de projeto, o sistema real pode ser monitorado através do modo supervisor.



Figura 2: Visão geral da ferramenta de análise de dependabilidade.

4.2 Editor de Redes

O editor da rede define as abstrações da rede, uma das características mais importantes da ferramenta de avaliação da confiabilidade. A rede está organizada como um grafo $G(V, E)$ com n vértices (V) e k arestas (E). Os vértices representam dispositivos e as arestas do grafo representam as

ligações (*links*) entre os dispositivos. A interface gráfica do usuário (GUI) é mostrada na Figura 3, cuja tela principal é onde o usuário edita a topologia da rede.

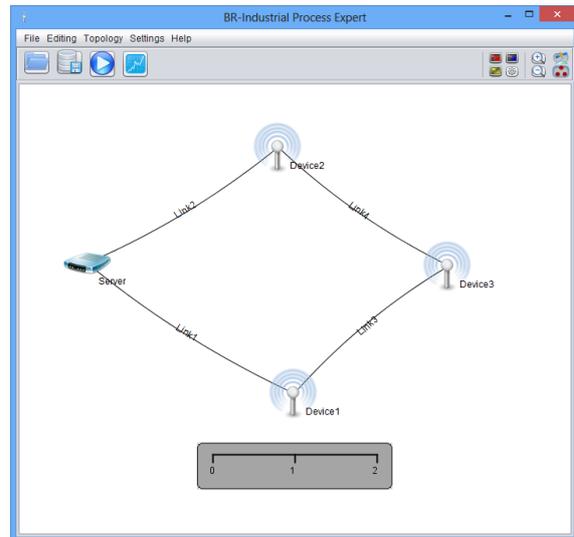


Figura 3: *Br-Industrial Process Expert's* Network Editor.

Nós consideramos falhas tanto em dispositivos quanto nos *links* do processo e ambos podem ser reparados após uma falha, se necessário. Depois de uma operação de reparo, o dispositivo ou *link* é considerado como novo. Nós assumimos que os processos de reparação de falhas são todos independentes e caracterizados por meio de uma função de distribuição cumulativa.

4.3 Gerador de Árvore de Falhas

Esta seção descreve os passos a serem seguidos para a construção de uma Árvore de Falhas a partir de um grafo. O primeiro passo é determinar as condições que possam levar à falha de um dispositivo e de sua redundância. A análise de dependabilidade de sistemas com redundância pode ser realizada através de uma Cadeia de Markov (Sahner et al., 1996), criando um sistema hierárquico, ou seja, cada evento da Árvore de Falha será representado por uma Cadeia de Markov.

Nesse caso, os nós da Cadeia de Markov representam os estados do sistema ou dispositivo (ativo ou desativado). A probabilidade do sistema passar de seu estado ativo (funcionando corretamente) para o desativado é dado por λ e o inverso é dado por μ . Para cada redundância acrescentada ao dispositivo, deve-se acrescentar um novo estado ao modelo proposto, representando a quantidade de dispositivos que devem falhar para o sistema falhar.

Portanto, a Cadeia de Markov na Figura 4 representa um dispositivo com uma única redundância. Quando o sistema está no estado 3, os dois componentes estão funcionando bem e cada

um deles tem probabilidade λ de falhar. Consequentemente o sistema tem probabilidade 2λ de mudar do estado 3 para o 2, em que apenas um dos componentes estão ativos. Por último, o estado 1 é quando nenhum dos componentes está ativo e, portanto, o sistema está desativado. De maneira análoga, o mesmo ocorre com as probabilidades de reparo μ . Na análise de confiabilidade não levamos em consideração a possibilidade de reparo do sistema e portanto $\mu = 0$, diferentemente da disponibilidade.

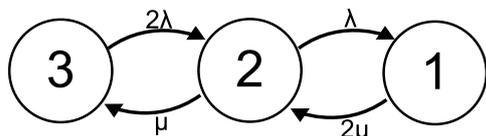


Figura 4: Análise de redundância através de Cadeia de Markov.

Três possibilidades de falhas são consideradas: (i) falha de *hardware*, (ii) falha no *link*, (iii) falha de um caminho entre o dispositivo e o centralizador (problema de conectividade). As condições (i) e (ii) não podem ser avaliadas em conjunto, porque falhas em *links* ocorrem com mais frequência do que as avarias de *hardware*. Por outro lado, a condição (iii) tem uma influência direta sobre ambas às condições (i) e (ii). Dessa forma, (iii) deve ser avaliado em ambos os casos, tanto para a condição (i) quanto para a condição (ii).

Todas as condições de falha do dispositivo são descritos na Figura 5. Em relação as avarias de *hardware*, um dispositivo i é representado pelo evento dev_i . Para falhas de *Link*, uma conexão j é representada pelo evento $link_j$. O evento cp_i (problema de conectividade) representa a condição de falha (iii). Este evento só é ativo quando todos os caminhos entre o dispositivo i e o centralizador falharem. Finalmente, um caminho dev_i-Path_m é considerado defeituoso, se pelo menos um dispositivo (*hardware*) ou um *link* ao longo do caminho falhou.

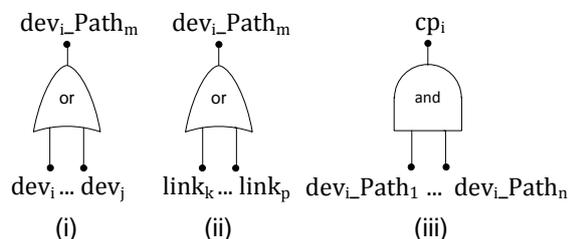


Figura 5: Condição de falha para o dispositivo i da rede considerando: (i) falha de *hardware*; (ii) falha de *link*; (iii) ausência de caminhos entre o dispositivo e o centralizador da rede.

O segundo passo na geração da Árvore de Falhas é definir quais as combinações de dispositivos

pode conduzir a uma falha de rede. A ferramenta proposta neste trabalho suporta qualquer combinação que pode ser expressa usando operadores booleanos (*and* e *or*). A fim de proporcionar uma compreensão clara, a Árvore de Falhas gerada a partir da topologia apresentada na Figura 3 é representada na Figura 6. Foi considerado apenas as falhas de *hardware* e condição de falha sendo $Device_1 + Device_2 + Device_3$.

Devido a condição de falha proposta, percebe-se que o evento topo é formado por três eventos (portas *and*), um para cada dispositivo. Note também que o $Device_1$ e o $Device_2$ têm apenas um caminho para o *gateway*¹, enquanto que o dispositivo $Device_3$ apresenta dois caminhos (duas portas *or*).

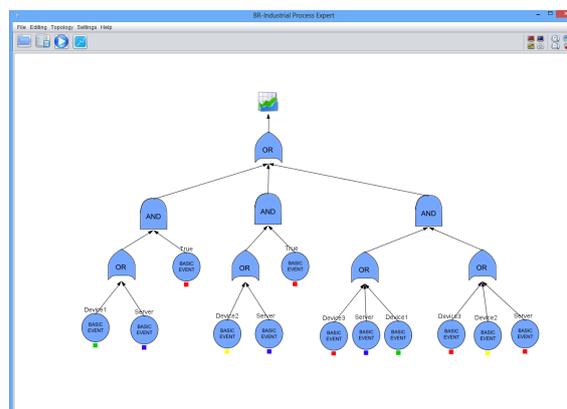


Figura 6: Árvore de Falhas baseada no exemplo da Figura 3 considerando falhas de *hardware*.

4.4 Ferramenta de relatório

A adoção de modelos matemáticos, como por exemplo, Cadeias de Markov, Redes Bayesianas e Árvore de Falhas é um procedimento útil para modelar a dinâmica da degradação de sistemas (Limnios, 2007). A eficácia e desempenho destas técnicas já são validadas na literatura, sendo uma base matemática genérica para diferentes aplicações com diferentes objetivos. Assim, é muito importante gerar dados quantitativos claros para os usuários finais, uma vez que esses modelos matemáticos talvez não sejam sua especialidade.

Tendo isso em mente, a análise quantitativa das métricas de avaliação é tratada pelo *Br-Industrial Process Expert* em um módulo separado. A ferramenta de relatório é responsável por solicitar aos módulos matemáticos que executem essas métricas. A comunicação entre a ferramenta de relatório e os módulos matemáticos é realizada através de *socket*. Nesse caso, os módulos matemáticos assumem o papel de servidor e a ferramenta de relatório assume a função de cliente.

¹O evento *true* é inserido nas portas *and* de uma entrada

A comunicação entre o servidor e o cliente é regida por um protocolo de comunicação. Uma linguagem foi definida para descrever os modelos matemáticos e assim a ferramenta de relatório pode solicitar sua execução aos módulos matemáticos. Após a execução do modelo analítico, os módulos matemáticos retornam o resultado para a ferramenta de relatório. Através dessa linguagem descritiva e o uso do *socket*, garante-se que outros *softwares*, assim como o *Br-Industrial Process Expert*, poderão usufruir dos módulos matemáticos.

Na Figura 7 é ilustrado um exemplo simples de um descritor de um modelo de Árvore de Falha. Nesse código é descrito dois eventos (chamados de *a* e *b*), cada um com sua distribuição estatística baseada em uma Cadeia de Markov (*modeloExemplo*). Esses eventos são conectados a uma porta lógica *and* (denominada de *portaAnd*) que converge no topo da árvore. Por sua vez a Cadeia de Markov possui dois estados, o primeiro (*st1*) representa a condição de normalidade do evento e o segundo (*st2*) a de falha. É também descrito uma transição (nomeada de *t1*) de *st1* para *st2*, com probabilidade 0.75 de ocorrer.

```
STARTTREE
  event a markov modeloExemplo
  event b markov modeloExemplo
  and portaAnd a b
  top portaAnd
ENDTREE

STARTMODEL modeloExemplo
  STARTMARKOV
    state st1 probInitial 1.0
    state st2 probInitial 0.0
    tran t1 st2 0.75
  ENDMARKOV
ENDMODEL
```

Figura 7: Descritor de um evento na Árvore de Falha usando Cadeia de Markov.

A arquitetura da interação entre *Br-Industrial Process Expert* e os modelos matemáticos é descrita na Figura 8. Os modelos matemáticos calculam o evento topo da Árvore de Falhas enquanto as métricas de avaliação são resolvidas usando o algoritmo MOCUS (amplamente adotado para os formalismos de Árvore de Falhas) (Limnios, 2007). As seguintes medidas podem ser calculadas: confiabilidade, disponibilidade, MTTF e a importância de um componente na árvore (métrica Birnbaum).

A ferramenta de relatório também é responsável em capturar o resultado do processamento dos modelos matemáticos e exibi-los em forma de gráfico, tornando o resultado facilmente compreensível para o usuário final.

4.5 Sistema Supervisório

Os sistemas supervisórios permitem que informações a partir de uma unidade física ou processo de produção possam ser monitorados e controla-

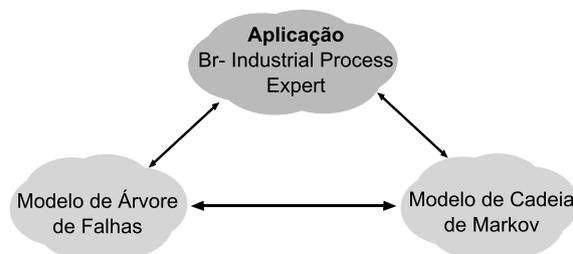


Figura 8: Editor de rede do *Br-Industrial Process Expert*.

dos. Esta informação é recolhida utilizando equipamentos de aquisição de dados para serem exibidas ao usuário final. O monitoramento do comportamento do sistema permite fazer decisões relacionadas com o processo para melhoria de seu desempenho ou prevenção de falhas.

Além de suas ferramentas de confiabilidade, o *Br-Industrial Process Expert* é capaz de supervisionar informações sobre o processo por meio de dados extraídos do sistema de supervisão. As formas de obter essas informações depende do tipo de sistema de supervisão. No entanto, a maioria deles capturam as informações usando o protocolo XML-RPC (procedimento remoto de chamadas baseado em XML e HTTP). Assim, é possível obter informação sobre a procura e a dependabilidade de processo, o estado de dispositivos e aspectos da comunicação.

5 Resultado

Nesta Seção, vamos apresentar alguns resultados obtidos pelo uso do quadro proposto para avaliar o processo industrial descrito na Figura 3. Neste cenário, assume-se que a condição de falha do sistema é definida como o seguinte: $Device_1 + Device_2 + Device_3$. Em outras palavras, o sistema falha se pelo menos um dispositivo falhar. Assume-se também que a aplicação requer uma confiabilidade maior do que 50% durante as primeiras 275 horas de operação e que o processo de reparação e falha ocorre a uma taxa constante (isto é, a distribuição exponencial). As taxas de falha e reparo são as mesmas para todos os dispositivos, $1e-3$ e $0,1$ respectivamente.

Foi realizada uma análise de sensibilidade (confiabilidade e disponibilidade), uma vez que estamos interessados em medir as tendências relativas ao invés de valores absolutos. Nesse caso, estamos avaliando o aumento da confiabilidade do sistema, considerando melhorias no $Device_3$. Foram definidos quatro cenários (apenas para o $Device_3$): (I) $\lambda = 1e-3$, (II) λ 1,5 vezes mais confiável, (III) λ duas vezes mais confiável, (IV) um dispositivo de redundância. Os resultados são descritos na Figura 9 e Tabela 1.

Os resultados da confiabilidade (Figura 9)

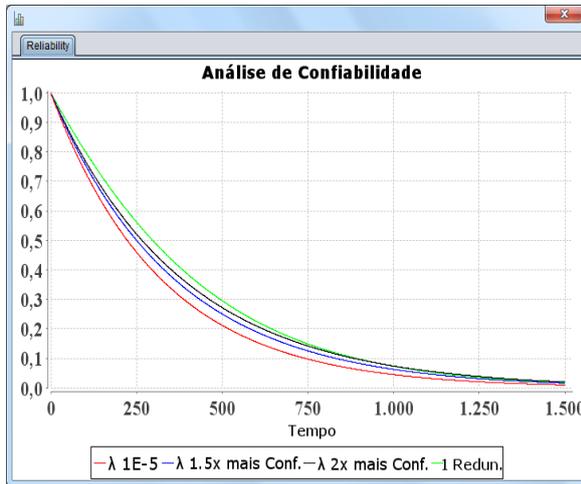


Figura 9: Análise de sensibilidade considerando a confiabilidade do sistema.

Tabela 1: Análise de sensibilidade considerando a disponibilidade do sistema.

Cenário	Interrupções(h/a)	Disp. Relativa
$\lambda = 1e-3$	266.12	-
$\lambda = 1.5x$ mais Conf.	237.94	10.58 %
$\lambda = 2x$ mais Conf.	223.86	15.87 %
1 redundância	182.02	31.60 %

mostraram que apenas o cenário onde a redundância foi adotada atende aos requisitos da aplicação. Esta análise de sensibilidade pode ser estendida para qualquer processo industrial (concebido como uma rede/gráfico). Além disso, nós também realizamos uma avaliação da disponibilidade (Tabela 1) considerando-se como métrica a interrupção do sistema (medido em horas por ano). Nota-se que, se for configurada uma redundância no *Device₃*, a interrupção do sistema teria diminuído 31,60% (valor em relação a referência usada no cenário I). Os resultados da disponibilidade mostraram que adotar uma redundância no *Device₃* é pelo menos duas vezes melhor do que utilizar um dispositivo duas vezes mais confiável (cenário III).

6 Conclusão

O desenvolvimento de ferramentas genéricas para a análise de confiabilidade e disponibilidade de um processo industrial é uma demanda iminente. A ferramenta desenvolvida neste trabalho apoia a análise quantitativa destas métricas, proporcionando valiosas informações para o projetista que lhe permite desenvolver sistemas robustos e tolerantes a falhas. A proposta assume uma aplicação de processo industrial concebido como uma rede/gráfico, onde ambos os dispositivos e *links* de comunicação podem falhar. O método de avaliação pode ser utilizado durante a fase inicial do projeto de qualquer aplicação de processo indus-

trial.

Em pesquisas futuras, pretendemos apoiar Redes Bayesianas e modelos de Árvore de Falhas dinâmicas. Além disso, pretendemos também considerar a confiabilidade de sistemas em tempo real, estendendo o módulo supervisor.

Agradecimentos

Os autores agradecem ao CNPq e à CAPES, pelo suporte financeiro e à UFRN pela infraestrutura de suporte ao desenvolvimento deste trabalho.

Referências

- AboElFotouh, H. and Colbourn, C. (1989). Computing 2-terminal reliability for radio-broadcast networks, *Reliability, IEEE Transactions on* **38**(5): 538–555.
- Cinque, M., Cotroneo, D., Di Martinio, C. and Russo, S. (2007). Modeling and assessing the dependability of wireless sensor networks, *Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems, SRDS '07*, IEEE Computer Society, Washington, DC, USA, pp. 33–44.
- Di Martino, C., Cinque, M. and Cotroneo, D. (2012). Automated generation of performance and dependability models for the assessment of wireless sensor networks, *IEEE Trans. Comput.* **61**(6): 870–884.
- Krishnamurthy, L., Adler, R., Buonadonna, P., Chhabra, J., Flanigan, M., Kushalnagar, N., Nachman, L. and Yarvis, M. (2005). Design and deployment of industrial sensor networks: Experiences from a semiconductor plant and the North Sea, *SenSys '05: Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, ACM, New York, pp. 64–75.
- Limnios, N. (2007). *Fault Trees*, 2 edn, ISTE Ltd.
- Majdara, A. and Wakabayashi, T. (2009). Component-based modeling of systems for automated fault tree generation, *Reliability Engineering and System Safety* **94**(6): 1076–1086.
- Sahner, R., Puliafito, A. and Trivedi, K. S. (1996). *Performance and reliability analysis of computer systems: an example-based approach using the SHARPE software package*, Kluwer, Boston, MA.
- Xing, L., Liu, H. and Shrestha, A. (2012). Infrastructure communication reliability of wireless sensor networks considering common-cause failures, *International Journal of Performability Engineering* **8**(2): 141–150.