Revista de Ingeniería Energética, 2018, vol 39, n. 1, Enero/Abril, p. 56-61
Centro de Investgación y Pruebas Electroenergéticas, Facultad de Ingeniería Electríca,
Universidad Tecnológica de La Habana, José Antonio Echeverría, Cujae
ISSN 1815-5901 RNPS- 1958

APLICACIONES INDUSTRIALES

Avaliação de árvores de falhas mediante uma planilha EXCEL

Evaluación de árboles de fallos mediante una planilla EXCEL

Fault tree evaluation using an EXCEL worksheet

José de Jesús Rivero Oliva[1] **Antonio Torres Valle**[2]
Jesús Salomón Llanes[2] **Manuel Perdomo Ojeda**[2]

[1]Centro de Tecnología Universidad Federal do Rio Janeiro,Brasil.
[2]Instituto Superior de Tecnologías y Ciencias Aplicadas,Universidad de La Habana,Cuba.
Email:rivero@nuclear.ufrj.br

Licencia de uso y distribución Creative Commons Reconocimiento-No Comercial 4.0 Internacional.

Recibido: septiembre 2017 Aprobado: noviembre 2017

RESUMEN/*ABSTRACT*
O presente trabalho foi dedicado à avaliação de árvores de falhas mediante uma planilha EXCEL. A determinação dos Cortes Mínimos (CM) foi realizada formando todas as combinações possíveis dos eventos básicos que integram a árvore. O método impede que o cálculo colapse por explosão combinatória. A memória disponível nunca constitui uma limitação. Foi aplicada a fatoração de eventos não repetidos, um método recursivo para a formação das combinações de eventos e um ordenamento dos componentes que da prioridade aos mais repetidos e próximos do portão topo. A planilha EXCEL determina os CM mais importantes, a probabilidade de falha do sistema e as medidas de importância dos componentes. Também são possíveis análises de indisponibilidade instantânea. São apresentados os resultados para duas árvores de falhas representativas que foram resolvidas em tempos razoáveis, mostrando um desempenho adequado para aplicações industriais de moderada complexidade.
Palabras clave: Árvores de falhas; Planilha EXCEL; Corte Mínimo

El presente trabajo fue dedicado a la evaluación de árboles de fallos mediante una planilla EXCEL. La determinación de los Cortes Mínimos (CM) fue realizada formando todas las combinaciones posibles de los sucesos básicos que integran el árbol. El método impide que el cálculo colapse por explosión combinatoria. La memoria disponible nunca constituye una limitación. Fue aplicada la factorización de sucesos no repetidos, un método recursivo para la formación de las combinaciones y un ordenamiento de los componentes que prioriza los más repetidos y próximos a la puerta tope. La planilla EXCEL determina los CM más importantes, la probabilidad de fallo del sistema y las medidas de importancia de los componentes. También son posibles análisis de indisponibilidad instantánea. Se presentan los resultados para dos árboles de fallos representativos que fueron resueltos en tiempos razonables, mostrando un desempeño adecuado para uso en aplicaciones industriales de moderada complejidad.
Palabras clave: *árboles de fallo, planilla Excel, Corte Mínimo*

The present paper was dedicated to the evaluation of fault trees through an EXCEL worksheet. The determination of the Minimal Cut Sets (MCSs) was accomplished performing all possible combinations of the basic events that take part of the tree. The method prevents the calculation from collapsing due to a combinatorial explosion. The available memory is never a limitation. It was applied the factorization of non-repeated events, a recursive method for the generation of the events combinations and an ordering scheme giving priority to the components which are more repeated and appear closer to the top gate. The EXCEL worksheet determines the most important MCSs, the system failure probability, and the components importance measures. Instantaneous unavailability analysis is also possible. The results for two representative fault trees are presented. They were resolved in a reasonable time, showing an adequate performance for industrial applications of moderate complexity.
Key words: *fault trees, Excel sheet, minimum cut*

INTRODUÇÃO

As analises de confiabilidade e risco mediante árvores de falhas têm sido aplicadas de forma ampla em diversas áreas que incluem aeronáutica, engenharia nuclear, engenharia de fatores humanos e gerenciamento de segurança [1]. Nos processos industriais onde os perigos são elevados se precisa de sistemas de segurança com alta confiabilidade para reduzir os riscos; sistemas onde são utilizados componentes redundantes e as falhas ao nível do sistema se devem a combinações de falhas de equipamentos e/ou erros humanos.
A análise mediante árvores de falhas tem a vantagem de constituir uma técnica de análise de sistemas, onde os eventos de falha ou possíveis erros humanos não são considerados de forma separada, senão constituindo cenários, formados por combinações de eventos. Esta abordagem resulta muito mais apropriada para sistemas de alta confiabilidade, mas resulta necessário um software de cálculo para realizar as avaliações, qualitativa e quantitativa, com capacidade para analisar as árvores complexas e interdependentes que surgem nos casos de interesse prático. A avaliação de grandes árvores de falhas continua sendo um desafio [2].

MATERIAIS E MÉTODOS

Existem diversos métodos de solução de árvores de falhas. A metodologia clássica, de ampla utilização na indústria nuclear, consta de dois níveis; qualitativo e quantitativo. Ela está baseada na avaliação dos Cortes Mínimos (CM), determinados na etapa qualitativa [3]. O método clássico consiste basicamente em um processo sistemático de substituição dos portões lógicos por suas entradas, que pode ser de cima para baixo (algoritmo top-down) ou de baixo para cima (algoritmo bottom-up). Desta forma são gradualmente geradas as combinações de eventos que conduzem à falha do sistema até chegar às combinações de eventos básicos que determinam à ocorrência do evento topo não desejado. Aqui aparecem dois grandes problemas:

1) Uma quantidade imensa de combinações de eventos, que podem ser geradas inclusive por árvores de falhas relativamente pequenas, devido à ocorrência de um fenômeno denominado explosão combinatória. O número total de combinações chega a resultar ingovernável, tanto por falta de capacidade de armazenamento da informação quanto pelo longo tempo de execução dos cálculos.

2) Não todas as combinações geradas são CM, e para determinar aquelas onde se combina o número mínimo imprescindível de eventos que determinam a falha do sistema resulta necessário realizar um processo de redução booleana mediante a comparação de eventos, o qual demanda longos tempos de execução e grandes capacidades de armazenamento de informação.

Para contornar as limitações do método clássico, foi proposto outro tipo de algoritmo mais eficiente que realiza a avaliação de árvores de falhas mediante a codificação da árvore como um Diagrama de Decisão Binário (DDB) [4-7]. Neste caso o próprio método de codificação garante que todas as combinações avaliadas sejam mínimas, pelo qual não resulta necessária a redução booleana. Não obstante, a metodologia DDB também é afetada pela explosão combinatória, sendo que em alguns casos práticos, em que as árvores são muito complexas, os correspondentes BDD resultariam excessivamente grandes e não podem ser construídos [5]. Isto se deve ao incremento exponencial do número de nodos com a complexidade da árvore de falhas [6]. Assim, a principal limitação para a análise de árvores de falhas complexas é a insuficiente memória de trabalho. Quando uma árvore de falhas resulta complexa demais para ser analisada na memória de trabalho disponível, a prática habitual é o uso de técnicas de truncado para determinar apenas os CM mais significativos [6]. Para contornar estas limitações, no presente trabalho a determinação dos CM é realizada sem seguir a lógica da árvore de falhas, senão formando todas as combinações possíveis dos eventos que integram a árvore, identificando e avaliando apenas aquelas que são CM. Este processo implica gerar e testar uma imensa quantidade de combinações de eventos, mas tem a vantagem de não precisar de redução booleana nem do armazenamento dos CM gerados. Cada CM é gerado, avaliado e descartado. Para a tomada de decisões apenas é preciso reter um número reduzido de CM, aqueles de maior probabilidade e, consequentemente, de maior contribuição à probabilidade de falha total. Por outro lado, o próprio método de formação das combinações garante que a contribuição de um único CM não seja considerada varias vezes. A princípio, o método permite formar e avaliar todos os CM da árvore de falhas, a única restrição seria o tempo de execução necessário, pois a memória disponível não constituiria nunca uma limitação.

Para o desenvolvimento do algoritmo foram aplicadas as técnicas seguintes:
1) Fatoração de eventos não repetidos entrando a portões O [8].
2) Utilização de um procedimento recursivo, desenvolvido para a formação das combinações de eventos, o qual conserva a progressão lógica das falhas para os eventos considerados com anterioridade, sem necessidade de partir sempre do estado inicial onde todos os componentes estão disponíveis.
3) Estabelecimento de uma ordem de seleção dos componentes para a formação das combinações, que da prioridade aos eventos atendendo à camada da árvore onde se encontram e seu número de repetições [9; 10]. Isto permite realizar de forma mais eficiente o processo de formação das combinações de eventos para chegar antes aos CM.

Aplicando as técnicas anteriores foram desenvolvidos os algoritmos (Macros) para a determinação dos CM de uma árvore de falhas, como parte de uma planilha EXCEL com capacidade para a avaliação de árvores de falhas de mediana complexidade. O método avalia todos os CM que contribuem significativamente à probabilidade do evento topo e, adicionalmente, retém os CM mais importantes.

Eles são precisamente os de interesse prático para sustentar uma tomada de decisões capaz de aumentar a confiabilidade do sistema e reduzir o risco da instalação de maneira efetiva e sem custo excessivo.

A planilha permite que os profissionais da indústria possam realizar as análises de confiabilidade e risco em um ambiente amigável e de fácil compreensão. Caso contrário, eles precisariam de um software de cálculo comercial, mais específico e complexo.

As facilidades principais que oferece o sistema proposto são as seguintes:
a) Dados gerais com especificações de truncado por ordem e/ou probabilidade (figura 1).

Dados gerais	
Formato dos CM	Números
Avaliação dos CM como	eventos raros
Portão Topo	1
Número máximo de CM	5000
Ordem máxima dos CM	15
Probabilidade de Corte	1,00E-07

Fig. 1. Especificação dos dados gerais na planilha EXCEL.

b) Introdução de dados de confiabilidade dos componentes, com cálculo automático das probabilidades de falha de cada evento (figura 2).
c) Introdução dos dados da lógica da árvore de falhas com possibilidades de comprovação da consistência da árvore (figura 3).
d) Cálculo do valor total de probabilidade de falha do sistema e das medidas de importância Redução de Risco (RRW) (figura 4) e Incremento de Risco (RAW).
e) Determinação dos CM mais importantes (figura 5), ordenados por probabilidade (em um formato de análise de Pareto).
f) Determinação da indisponibilidade média do sistema para um ciclo de trabalho mediante a integração da indisponibilidade instantânea (figura 6).

No	Código	Tipo	Taxa de falha [1/h]	Prob. / Freq. de falha [1/a]	Intervalo entre testes [h]	Tempo de teste [h]	Indispon. do teste	Tempo de reparo [h]	Tempo Espera / Operação / Inicial [h]	EF	Indispon. / Prob. de falha
1	CM-RR246S10/O	Espera	4,80E-07		240					3,0	**5,76E-05**
2	CM-RR246D01-S	Espera	2,58E-07		240					4,0	**3,10E-05**
3	CM-RR246S22-F	Espera	9,60E-07		240					5,0	**1,15E-04**
4	CM-RR246S05-O	Espera	4,80E-07		240					6,0	**5,76E-05**
5	CM-RR246D01-R	Operação	2,58E-06						24	3,0	**6,19E-05**
6	CM-RR246S17-O	Espera	4,80E-07		240					4,0	**5,76E-05**
7	CM-RR246S18-E	Espera	4,80E-07		240					5,0	**5,76E-05**
8	CM-RR246S10-E	Espera	4,80E-07		240					6,0	**5,76E-05**
9	CM-RR246S04-F	Espera	9,60E-07		240					3,0	**1,15E-04**
10	CM-RR246S11-F	Espera	9,60E-07		240					4,0	**1,15E-04**
11	H3-RR60D01	Espera		1,00E-03						5,0	**1,00E-03**

Fig. 2. Especificação dos dados de Confiabilidade de componentes na planilha EXCEL.

Verificação | Reset | Renumerar | Reset | Matar (q=1)

No	Código	Tipo	E1	E2	E3	E4	E5	E6	E7
1	C1	1	-2	-3					
2	C2	1	-221	-226	-231	-236	-241	-246	-247
3	C3	2	-4	-5					
4	C4	3	-6	-7	-8	-9			
5	C5	4	-10	-11	-12	-13			
6	C6	1	-14	-22					
7	C7	1	-15	-23					
8	C8	1	-16	-24					
9	C9	1	-17	-25					
10	C10	1	-18	-22					
11	C11	1	-19	-23					
12	C12	1	-20	-24					
13	C13	1	-21	-25					
14	C14	3	-26	-27	-128				
15	C15	3	-29	-30	-132				

Fig.3. Especificação dos dados da lógica da árvore de falhas na planilha EXCEL.

RESULTADOS

A planilha EXCEL foi testada com várias árvores de falha de complexidade média, conseguindo um desempenho adequado em aplicações industriais de moderada complexidade. A seguir são apresentados os resultados para duas árvores de falhas representativas.

- Árvore de falhas European1

Esta é a árvore de mediana complexidade, composta de 84 portões e 61 eventos básicos muito interdependentes. Na tabela 1, são mostrados os resultados de várias rodadas. Usando o truncado por probabilidade foram determinados os CM mais importantes (até 5000) em um tempo de cálculo que para a rodada 1 foi de pouco mais de um minuto. Estes são os CM que determinam a confiabilidade do sistema e sobre os quais se centraria a tomada de decisões para aumentar a confiabilidade.

Nas rodadas 2 e 3 o valor da probabilidade de corte é reduzido e os tempos de execução começam a aumentar significativamente, mas os novos CM adicionados são de baixa probabilidade e só aumentam levemente a probabilidade de falha total. Os CM mais importantes permanecem praticamente os mesmos.

Tabela 1. Resultados da avaliação da árvore de falhas European1.

No.	Probabilidade de Corte	Número de CM	Probabilidade de falha total	Probabilidade de falha dos CM mais importantes (% de contribuição)	Tempo de Execução (Min:Seg)
1	1,0 E-10	1613	1,42E-6	1,42E-6 (84,52%)	01:20
2	1,0 E-11	8277	1,66E-6	1,60E-6 (95,24%)	04:31
3	1,0 E-12	14054	1,68E-6	1,60E-6 (95,24%)	13:33

A figura 4, mostra a análise da medida de importância Redução de Risco (RRW) na forma de um Diagrama de Pareto. Conclui-se que uma tomada de decisões efetiva sobre os 6 componentes mais importantes identificados pelo estudo, permitiria um aumento da confiabilidade e, consequentemente, uma redução de risco de 50%.

- Benchmark (sistema de segurança de uma usina nuclear)

Trata-se de uma árvore com 370 portões lógicos e 675 eventos básicos, mas que gera uma imensa quantidade de CM, superior a 10^{12}, com contribuições bastante uniformes, que reduzem a efetividade do truncado por probabilidade. Neste caso a planilha Excel permitiu avaliar grandes quantidades de CM e determinar os CM mais importantes para a tomada de decisões (figura 5). Os tempos de execução não resultaram excessivos. Os resultados são mostrados na tabela 2. Adicionalmente, a figura 6, mostra uma análise de indisponibilidade

instantânea, que permite considerar o impacto da estratégia de testes periódicos dos componentes. Esta avaliação determina um valor mais realista da indisponibilidade média do sistema (1,03E-2), mostrando a necessidade de um escalonamento dos testes de componentes redundantes.

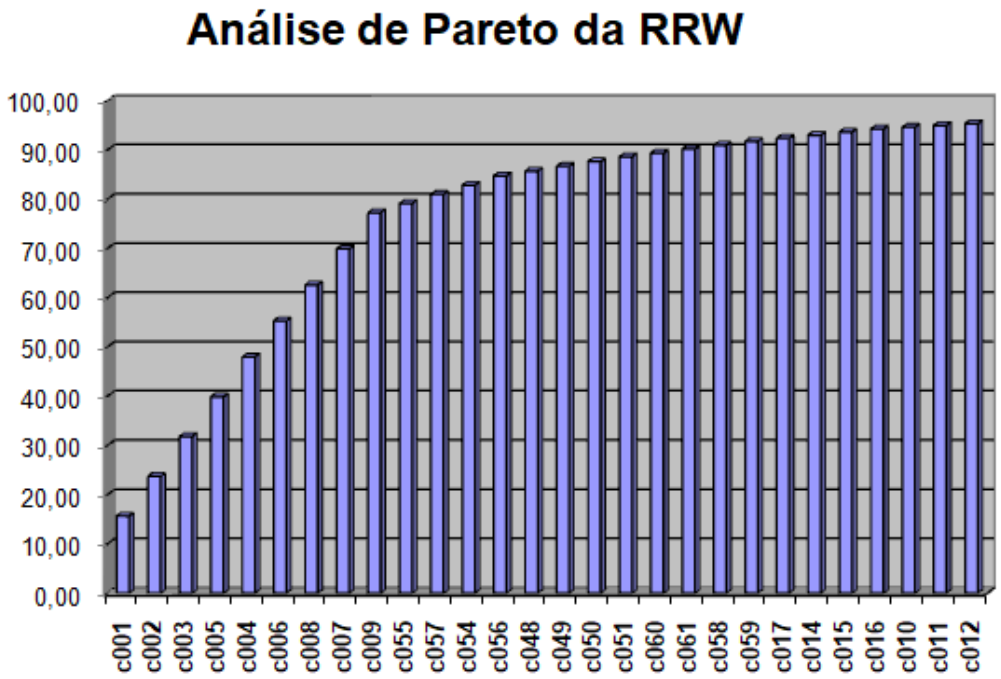

Fig. 4. Análise de Pareto baseado na medida de importância Redução de Risco (RRW).

0:00:31		100%				Calcular	
No.	Prob.	Pr. Acum.	%	% Acum.	E1	E2	E3
1	1,00E-03	1,00E-03	16,57	16,57	H3-RR40S21-O1		
2	7,60E-04	1,76E-03	12,60	29,17	LF-1BV13Q-C	NOMNT-TF20	
3	8,44E-05	1,84E-03	1,40	30,57	NOMNT-TF60	LF-RL40S03-F	LF-RR20S04-F32
4	8,44E-05	1,93E-03	1,40	31,97	NOMNT-TF60	LF-RL40S03-F	LF-RR20S04-F1
5	8,44E-05	2,01E-03	1,40	33,37	NOMNT-TF60	LF-RL40S03-F	LF-RR20S11-F1
6	8,29E-05	2,10E-03	1,37	34,74	NOMNT-TF60	LF-RL40S03-F	LF-TF44S31-O
7	4,32E-05	2,14E-03	0,72	35,46	NOMNT-TF60	LF-RR20S04-F1	LF-RR20S11-F1
8	4,32E-05	2,18E-03	0,72	36,17	NOMNT-TF60	LF-RR20S11-F1	LF-RR20S22-F1
9	4,32E-05	2,23E-03	0,72	36,89	NOMNT-TF60	LF-RR20S22-F1	LF-RR20S04-F32
10	4,32E-05	2,27E-03	0,72	37,60	NOMNT-TF60	LF-RR20S04-F1	LF-RR20S22-F1
11	4,32E-05	2,31E-03	0,72	38,32	NOMNT-TF60	LF-RR20S11-F1	LF-RR20S04-F32
12	4,24E-05	2,35E-03	0,70	39,02	NOMNT-TF60	LF-TF44S31-O	LF-RR20S22-F1
13	4,24E-05	2,40E-03	0,70	39,72	NOMNT-TF60	LF-TF44S31-O	LF-RR20S04-F1
14	4,24E-05	2,44E-03	0,70	40,43	NOMNT-TF60	LF-TF44S31-O	LF-RR20S04-F32

Fig.5. Determinação dos CM mais importantes para um sistema de segurança de uma usina nuclear.

Tabela 2 . Resultados da avaliação da árvore de falhas de um sistema de segurança de uma usina nuclear.

No.	Probabilidade de Corte	Número de CM	Probabilidade de falha total	Probabilidade de falha dos CM mais importantes (% de contribuição)	Tempo de Execução (Min:Seg)
1	1,0 E-7	125450	6,03E-3	5,58E-3 (91,33%)	00:31
2	1,0 E-8	161022	6,10E-3	5,73E-3 (93,78%)	02:07

CONCLUSÕES

Foi desenvolvida uma planilha EXCEL para a avaliação de árvores de falhas. Ela foi testada com várias árvores de falha de complexidade média, conseguindo um desempenho adequado em aplicações industriais de moderada complexidade. Foram apresentados os resultados para duas árvores de falhas representativas.

A planilha determina os CM mais importantes, que são os de interesse prático para sustentar uma tomada de decisões capaz de aumentar a confiabilidade dos sistemas e reduzir os riscos das instalações de maneira efetiva e sem custo excessivo. Ela permite que os profissionais da indústria possam realizar as análises de confiabilidade e risco mediante árvores de falhas em um ambiente amigável e de fácil compreensão.

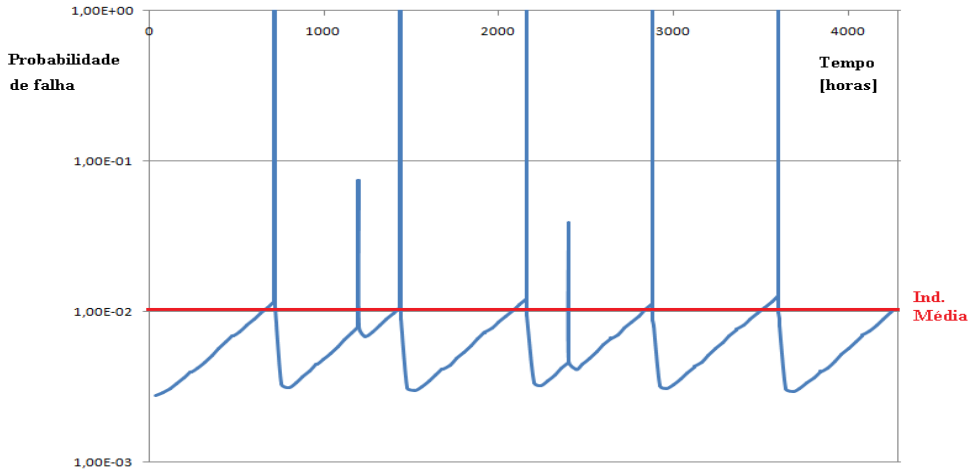

Fig. 6. Análise de indisponibilidade instantânea para a árvore de falha de um sistema de segurança de uma usina nuclear.

REFERÊNCIAS

[1] Hyun, K. et al. “Risk analysis using fault-tree analysis (FTA) and analytic hierarchy process (AHP) applicable to shield TBM tunnels”. *Tunnelling and Underground Space Technology*. 2015, Vol. 49, p. 121-129. ISSN: 0886-7798.
[2] Li, Z.F., Ren , Y., Liu , L.L., Wang , Z.L. “Parallel algorithm for finding modules of large-scale coherent fault trees”. *Microelectronics Reliability*. 2015, Vol. 55, p. 1400-1403. ISSN: 0026-2714.
[3] Kabir, S. “An overview of fault tree analysis and its application in model based dependability analysis”. *Expert Systems With Applications*. 2017, Vol. 77, p. 114-135. ISSN: 0957-4174
[4] Rauzy, A., “New algorithms for fault trees analysis”. *Reliability Engineering and System Safety*. 1993, Vol. 40, p. 203-211. ISSN: 0951-8320.
[5] Wang, J. et al. “Fault-tree-based instantaneous risk computing core in nuclear power plant risk monitor”. *Annals of Nuclear Energy*. 2016, Vol. 95, p. 35-41. ISSN: 0306-4549.
[6] Matuzas, V., Contini, S. “Dynamic labeling of BDD and ZBDD for efficient non-coherent fault tree analysis”. *Reliability Engineering and System Safety*. 2015, Vol. 144, p. 183-192. ISSN: 0951-8320.
[7] Wei, G., Quinfang, Z., Guofeng, T. “Development of an advanced fault tree quantification engine based on BDD/ZBDD algorithm”. Em 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, Korea. 2016. Consultado em 29/07/2017. Disponível em http://www.iapsam.org/PSAM13/program/Abstract/Oral/A-454.pdf.
[8] Chen, S. et al. “Efficient reduction and modularization for large fault trees stored by pages”. *Annals of Nuclear Energy*.2016, Vol. 90, p. 22-25. ISSN: 0306-4549.
[9] Mo, Y. Variable ordering to improve BDD analysis of phased-mission systems with multimode failures. *IEEE Transactions on Reliability*. 2009, Vol. 58, No 1, p. 53-57. ISSN: 0018-9529
[10] Mo, Y. et al. “Efficient Ordering Heuristics in Binary Decision Diagram–based Fault Tree Analysis”. *Quality and Reliability Engineering International*. 2013, Vol. 29, p. 307-315. ISSN: 1099-1638.