Calculation of MTTF values with Markov Models for Safety Instrumented Systems

BÖRCSÖK J., UGLJESA E., MACHMUR D.
University of Kassel
Department of Computer Architecture and System Programming
Wilhelmshöher Allee 73
Germany

Abstract: - This paper deals with the calculation of MTTF values with the help of Markov models. It shows what Markov models are and how they can be utilised to achieve valid and important information for safety instrumented systems. In few examples the different calculations steps are presented, detailed and examined.

Key-words: stochastic model, Markov model, safety related system, MTTF

1 Introduction

Probability calculation is applied to predict future events or development with the help of stochastic models. Additional, it is possible that a stochastic process behaves in periodic manner. Simple description of such relationships was done by the Russian mathematician Andrei Andrejewitsch Markov (1856-1922).With so called Markov chains, it is possible to describe and examine stochastic processes over a longer period without a lot of difficulties, which makes them very interesting to observe future events. Andrei Markov was born in Rjasan, Russia. He studied under Professor Pafnuti Tschebyschow (often in Literature stated as Tschebyscheff or Tschebyschev) in St. Petersburg and became member of the academy of science in 1886. Markov is known for this developed theories of stochastic processes. In 1913, he calculated the characters sequences in Russian literature to proof the necessity of independency of the law of large numbers. The calculations can also be used to state the quality of shapeliness of the orthography of character chains. From this approach were general stochastic tools developed, the so called stochastic Markow process, which can be used to predict future events or developments on base of current knowledge. Today's application using hidden Markov models for voice recognition software. Markov chains and Markov inequalities are named after Andrei Markov.

2 Basic Theory of stochastic Processes

Since Markov chains are stochastic processes, fundamental concepts and terms have to be defined and described first. A stochastic process describes a sequence of stochastic experiments, which can be expressed by a function $X(t)$ wit $t \in T$. T is the amount of all possible points in time of the system and is stated as parameter space. It T possesses only integer elements is the system time discrete and if T contains real elements the system is called continuous in time. Besides the amount of time points, a states space exists as well, which is often described as M or Z. The state space is the number of states a system can occupy. These states have to be independent, since the system can only be in one state. If a fixed number of states exists, then the space is discrete otherwise is it continuous. In the next few examples different architectures of Markov models will be detailed.

2.1 Simple examples of Markov models

A Markov models primarily knows two system states. Either the systems is operating, that means the system is fully functioning without errors, or the system is out of order, which means the system is in state which has a dangerous failures. States are presented as circle and a transition is shown as a transition line as presented in Fig 1.

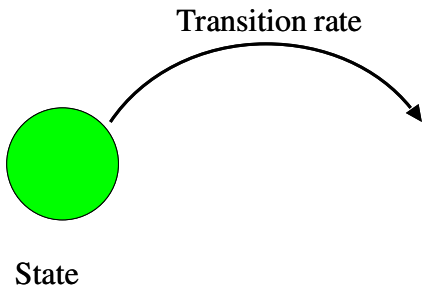

Fig. 1: Representation of a Markov model

Changes a state to another, then this will be presented with two circles and a transition line or transition arch. It has to be assured that the direction of the arrow points towards the new state. Generally, a Markov model can have two different systems. The first system possesses a

no repairable component the second system has a repairable element. Non repairable systems, cannot be repaired if a dangerous failure occurred, except the faulty component gets exchanged. Figure 2 shows such a system.

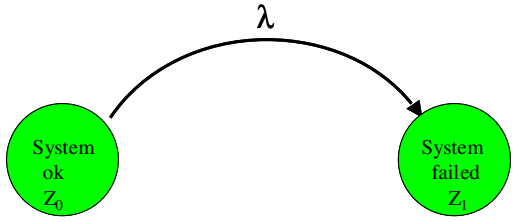

Fig. 2: Non repairable system with Markov model

The system ins operating in state Z_0. After a certain time the system changes from state Z_0 according to a transition rate or failure rate λ into state Z_1: the system has failed. The state Z_1 represents the condition, when the system is our of order. To change the condition, the system's component has to exchanged, since the system cannot be repaired.

Repairable systems, are systems which can be brought into fully operation when after a dangerous failure occurred the system is getting repaired. Figure 3 shows such a architecture.

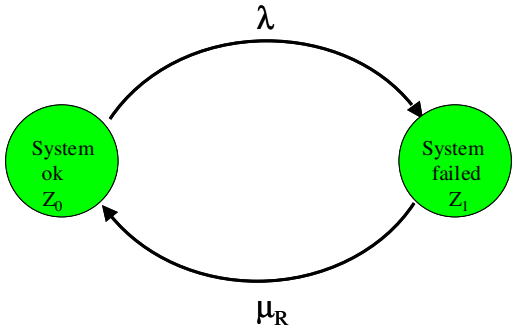

Fig. 3: repairable system as Markov model

After a system changes its state from Z_0 (fully operational) to Z_1(failed), the system can be brought after a certain time, here repair time R, into the fully operational state Z_0. In the next section the transitions will be mathematically described.

3 Mathematical description of state transitions

The transition probability from current states to other states can mathematically be described. Migrates the state Z_j within a time interval dt into the state Z_k, then transition probability exists for the two states. This can be described as:

$$p(Z_j \rightarrow Z_k) = p_{jk} = \lambda_{jk} \cdot dt \qquad (1)$$

where as λ_{jk} is the transition rate and it has to be valid that $\lambda_{jk} \geq 0$. When for example $\lambda_{jk} = 0$ then this means that the a transition for state Z_0 to state Z_1 is not possible.

The question might be risen how a transition from state Z_0 to the same state Z_0 within the time interval dt can be expressed. This is illustrated in equation 2:

$$p(Z_j \rightarrow Z_k) = p_{jj} = 1 - \sum_{k=0}^{n} \lambda_{jk} \cdot dt \qquad (2)$$

$$\text{with } (j = 0,1,2,...,n; k = 0,1,2,...,n;\ j \neq k)$$

The second term in equation 2 can be simplified as:

$$\sum_{k=0}^{n} \lambda_{jk} \cdot dt = \lambda_{jj} \cdot dt \qquad (3)$$

Inserting equation 3 into equation 2 results in:

$$p(Z_j \rightarrow Z_k) = p_{jj} = 1 - \lambda_{jj} \cdot dt \qquad (4)$$

Applying equation 4 for state Z_0,with a transition to the same state, results in:

$$p_{jj} = p_{00} = 1 - \lambda_{00} \cdot dt \qquad (5)$$

To present all states of a Markov model a transition matrix is used. The general form of this matrix is shown in equation 6:

$$P = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0n} \\ p_{10} & p_{11} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{n0} & p_{n1} & \cdots & p_{nn} \end{bmatrix} \qquad (6)$$

Using the transition rates as in equations 4 and 5, equation 6 becomes:

$$P = \begin{bmatrix} 1-\lambda_{00} \cdot dt & \lambda_{01} \cdot dt & \cdots & \lambda_{0n} \cdot dt \\ \lambda_{10} \cdot dt & 1-\lambda_{11} \cdot dt & \cdots & \lambda_{1n} \cdot dt \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{n0} \cdot dt & \lambda_{n1} \cdot dt & \cdots & 1-\lambda_{nn} \cdot dt \end{bmatrix} \qquad (7)$$

With the transition matrix P all states transitions of an arbitrary Markov model architecture can be described. If no direct connection between two states exists then this will be represented the matrix with a zero. To ensure that a transition matrix of an arbitrary Markov model is correct, all parameters can be summed up. Is the result of the summation equal to one, then the matrix is correct. It has to be mentioned that the P-Matrix as shown in equation 7 represents the initial state of the system at $T=1$. If a transition matrix at time $T=3$ should be

calculated then the initial P-matrix has to taken by the power of three as shown in equation 8:

$$P(T=3)=P(T=1)\cdot P(T=1)\cdot P(T=1)=[P(T=1)]^3 \qquad (8)$$

The next section shows how the MTTF (Mean Time To Failure) of Markov models can be calculated:

4 General mathematical description of MTTF

MTTF stands for Mean Time To failure and gives the mean time between to failures of a system. To calculate the MTTF value for a system described with a Markov model, the transmission matrix for Markov models is necessary. The following steps are necessary to determine the MTTF for a system.

- First step: Determine the Q-matrix:

The reliability matrix also known as Q-matrix can be derived from the P-matrix. To determine the Q-matrix from the P-matrix some criteria has to be fulfilled and observed. Firstly, the system has to be in an operational mode and absorbing states do not exist. Secondly, the following states are excluded, which are safe states and dangerous undetected states. An absorbing state possesses either a transition to a safe state or to a failure free state and has not other transition. Therewith the Q-matrix can be determined.

- Second step: Determine the M-matrix:

After the Q-matrix is established, the M-matrix has to be derived. Therefore the Q-matrix has to subtracted from the unity matrix, as shown in equation 9:

$$M = I - Q \qquad (9)$$

- Third step: Determine the N-matrix:

The N-matrix is established with the help of the M-matrix. The N-matrix is the inverse of the M-matrix as shown below:

$$N = [M]^{-1} \qquad (10)$$

- Fourth step: Determine the MTTF value

To calculate the MTTF value from a system described as a Markov model the sum of all elements from the first row of the N-matrix has to be calculated. With these for steps the general MTTF calculation for Markov models is finished.

4.1 Examples for a P-matrix

The P-matrix should be derived from the Markov model shown in Figure 4.

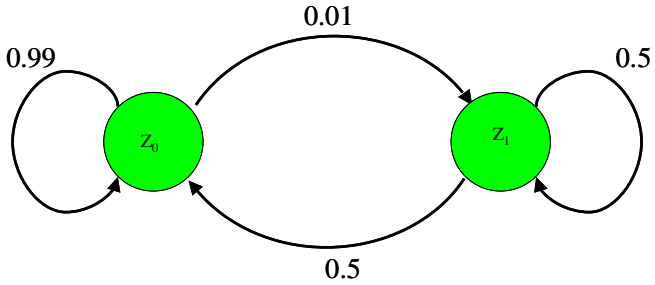

Fig. 4: Simple Markov model

Since the Markov model has only two states, the P-matrix has a dimension of 2x2. The general P-matrix of this architecture is shown in equation 11:

$$P = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} \qquad (11)$$

The values from Figure 4 can be inserted in equation 11 and results in:

$$P = \begin{bmatrix} 0.99 & 0.01 \\ 0.5 & 0.5 \end{bmatrix} \qquad (12)$$

The sum of each row of the P-matrix has to be always one, which is true for the presented example and therefore the P-matrix is correct.

4.2 Example for a MTTF calculation

The MTTF value for the Markov model illustrated in Figure 5 should be calculated. The system has four states Z_0, Z_1, Z_2 and Z_3. It is assumed that system is operation in states Z_0, Z_1. Since four states exists the P-matrix has a dimension of 4x4.

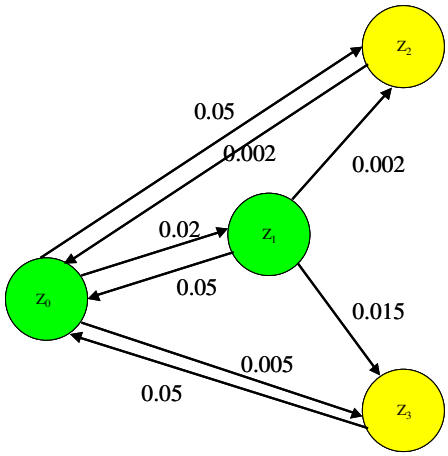

Fig. 5: Example of a Markov model

Using Equation 7 the P-matrix results in:

$$P = \begin{bmatrix} 0.973 & 0.02 & 0.002 & 0.005 \\ 0.05 & 0.933 & 0.002 & 0.015 \\ 0.05 & 0.0 & 0.95 & 0.0 \\ 0.05 & 0.0 & 0.0 & 0.95 \end{bmatrix} \quad (13)$$

The next step is to determine the Q-matrix out of the P-matrix. The condition for the Q-matrix are, that it has to be operating states and do not have any absorbing states. Since this is true for the states Z_0, Z_1, the Q-matrix is:

$$Q = \begin{bmatrix} 0.973 & 0.02 \\ 0.05 & 0.933 \end{bmatrix} \quad (14)$$

The next step is to calculate the M-matrix using Equation 9:

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0.973 & 0.02 \\ 0.05 & 0.933 \end{bmatrix} = \begin{bmatrix} 0.027 & -0.02 \\ -0.05 & 0.067 \end{bmatrix} \quad (15)$$

The next step is to calculate the N-matrix from equation 10:

$$N = \begin{bmatrix} 0.027 & -0.02 \\ -0.05 & 0.067 \end{bmatrix}^{-1} = \begin{bmatrix} 82.81829 & 24.72188 \\ 61.8047 & 33.37454 \end{bmatrix} \quad (16)$$

Finally, the MTTF value can be calculated by summing up the first row of the N-matrix:

$$MTTF = 82.81829 + 24.72188 = 107.5h \quad (17)$$

The example system has a mean life cycle of 107.5h hours.

5 1oo1-System as Markov Model

The Markov model of a 1oo1 architecture is presented in the figure below. This model possesses no redundant components and is already in a critical state, when one single component fails due to a dangerous undetected failure.

This Markov model has four states. Every system has a initial state Z_0. This state is the failure free state (system ok) and the system is operating correctly. From this initial state (system ok), three other states can be reached.

- State Z_1

The state "system s" constitutes a safe state. Safe states mean that the failure or fault is safe detected. This failures does not harm the system, since it is a safe one, one can eliminate (repair) it safely and this state can be left with a transition rate μ_R.

- State Z_2

This state "system DD" has a dangerous detected failure. With the transition rate μ_0 and μ_R the system can reach the failure free state.

- State Z_3

The failure free state changes into the dangerous undetected state "system DU". This state is critical for the system. Since the system failure due to a undetected failure, the system can reach only the state failure free after the life cycle duration LT, which means the system has to be completely exchanged.

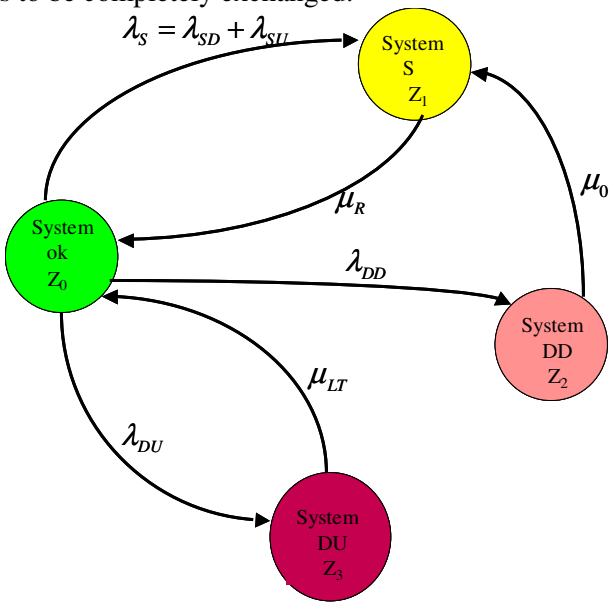

Fig. 6: 1oo1 System as Markov model

5.1 MTTF calculations for a 1oo1 system

Again, the calculations starts with the determination of the P-matrix:

$$P = \begin{bmatrix} 1-(\lambda_S+\lambda_D)dt & \lambda_S dt & \lambda_{DD} dt & \lambda_{DU} dt \\ \mu_R dt & 1-\mu_R dt & 0 & 0 \\ 0 & \mu_0 dt & 1-\mu_0 dt & 0 \\ \mu_{LT} dt & 0 & 0 & 1-\mu_{LT} dt \end{bmatrix} \quad (18)$$

Since only one failure free state exists, the Q-matrix becomes:

$$Q = 1-(\lambda_S - \lambda_D) \quad (19)$$

The M-matrix is the unity matrix subtracted from the Q-matrix:

$$M = I - Q = 1 - [1-(\lambda_S - \lambda_D)] = (\lambda_S + \lambda_D) \quad (20)$$

The N-matrix is the inverse of the M-matrix and is stated as:

$$N = [M]^{-1} = \frac{1}{(\lambda_S + \lambda_D)} \quad (21)$$

Since equation 21 is a matrix with dimension one, the N-matrix is equal to the MTTF value.

$$MTTF_{1oo1} = N = \frac{1}{(\lambda_S + \lambda_D)} \quad (22)$$

6 1oo2 System as Markov model

The 1oo2 system has two independent channels. The safety function is still functioning if one channels is able to operate. If two channels fail then the system is not functioning and therefore out of order. The next example is going to illustrate this. In state Z_0 both systems are in operation (System ok). Next, the different states are going to be described:

- State Z_1

As in the previous example, this is the state 'system safe'. This state can be reached from the failure free state with a transition of $2\lambda_S$. The value 2 results from the fact that the system has two independent channels. λ_S stands for the safe failures of the system. These failures do not present any risk for the system. λ_s can be divided into λ_{SD} and λ_{SU}. The first are safe detected failures and the second are safe undetected failures.

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad (23)$$

With a transition rate μ_R of (repair) can the system return to the failure free state Z_0.

$$\mu_R = \frac{1}{\tau_R} \quad (24)$$

- State Z_2

The system is in a critical situation, when it reaches this state. One system is operating the other one is in the state of a dangerous detected failure λ_{DD}. The state Z0 can be reached with the transition rates of μ_R and μ_0 via the state Z_1.

$$\mu_0 = \frac{1}{\tau_{test}} \quad (25)$$

- State Z_3

One system is functioning correctly, the second is in state of dangerous undetected failure λ_{DU}. This means that the system is in dangerous situation, but the system cannot be repaired, since it is not known that the system is in this particular state. Therefore, one has to wait, until the life cycle or life time (LT) is expired and the component is getting exchanged or the repaired. The transition rate to the initial state is μ_{LT}.

$$\mu_{LT} = \frac{1}{\tau_{LT}} \left[\frac{1}{s}\right] \quad (25)$$

Additionally, the possibility exists that a transition is carried out to state Z_0 via the states Z_5 and Z_1 with the transition rates μ_0 and μ_R, respectively.

- State Z_4 , Z_5, Z_6

The remaining states are where both systems have dangerous detected failures (Z_4), or one system has a dangerous detected failure, while the other has a undetected failure (Z_5) and last state (Z_6) is where both systems have dangerous undetected failures.

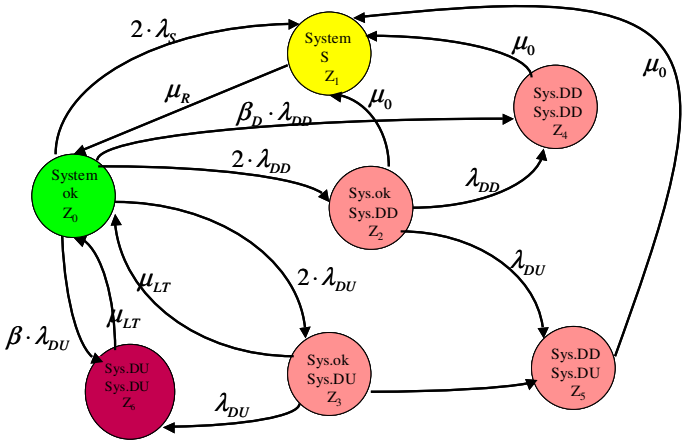

Fig. 7: 1oo2 System as Markov model

The P-matrix can de determined, whereby the following abbreviations are used:

$$A_1 = 2 \cdot \lambda_S + \beta_D \cdot \lambda_{DD} + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU} + \beta\lambda_{DU} \quad (26)$$

$$A_2 = \mu_0 + \lambda_{DD} + \lambda_{DU} \quad (27)$$

$$A_3 = \mu_{LT} + \lambda_{DD} + \lambda_{DU} \quad (28)$$

The P-matrix with the abbreviations are stated in equation 29:

$$P=\begin{bmatrix} 1-A_1dt & 2\lambda_S dt & 2\lambda_{DD}dt & 2\lambda_{DU}dt \\ \mu_R dt & 1-\mu_R dt & 0 & 0 \\ 0 & \mu_0 dt & 1-A_2dt & 0 \\ \mu_{LT}dt & 0 & 0 & 1-A_3dt... \\ 0 & \mu_0 dt & 0 & 0 \\ 0 & \mu_0 dt & 0 & 0 \\ \mu_{LT}dt & 0 & 0 & 0 \end{bmatrix} \quad (29)$$

$$\begin{bmatrix} \beta_D\lambda_{DD}dt & 0 & \beta\lambda_{DU}dt \\ 0 & 0 & 0 \\ \lambda_{DD}dt & \lambda_{DU}dt & 0 \\ 0 & \lambda_{DD}dt & \lambda_{DU}dt \\ 1-\mu_0 dt & 0 & 0 \\ 0 & 1-\mu_0 dt & 0 \\ 0 & 0 & 1-\mu_{LT}dt \end{bmatrix}$$

The necessary Q-matrix is taken from the equation 29 and results in equation 30:

$$Q=\begin{bmatrix} 1-A_1dt & 2\lambda_{DD}dt & 2\lambda_{DU}dt \\ 0 & 1-A_2dt & 0 \\ \mu_{LT}dt & 0 & 1-A_3dt \end{bmatrix} \quad (30)$$

Equation 30 can be simplified since for this 1oo2 system described as a Markov model, $\tau_{LT} \rightarrow \infty$ and therefore : $\mu \approx 0$ and equation 30 becomes:

$$Q=\begin{bmatrix} 1-A_1dt & 2\lambda_{DD}dt & 2\lambda_{DU}dt \\ 0 & 1-A_2dt & 0 \\ 0 & 0 & 1-A_3dt \end{bmatrix} \quad (31)$$

The next step is to calculate the M-matrix:

$$M\cdot dt=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}-\begin{bmatrix} 1-A_1dt & 2\lambda_{DD}dt & 2\lambda_{DU}dt \\ 0 & 1-A_2dt & 0 \\ 0 & 0 & 1-A_3dt \end{bmatrix} \quad (32)$$

and results in:

$$M=\begin{bmatrix} A_1 & -2\lambda_{DD} & -2\lambda_{DU} \\ 0 & A_2 & 0 \\ 0 & 0 & A_3 \end{bmatrix} \quad (33)$$

To determine the MTTF value the N-matrix has to be computed:

$$N=[M]^{-1}=\begin{bmatrix} A_1 & -2\lambda_{DD} & -2\lambda_{DU} \\ 0 & A_2 & 0 \\ 0 & 0 & A_3 \end{bmatrix}^{-1} \quad (33)$$

And the final result is:

$$N=\begin{bmatrix} \frac{1}{A_1} & \frac{2\lambda_{DD}}{A_1A_2} & \frac{2\lambda_{DU}}{A_1A_3} \\ 0 & \frac{1}{A_2} & 0 \\ 0 & 0 & \frac{1}{A_3} \end{bmatrix} \quad (34)$$

The MTTF value can now be calculated, by taken the first row of the N-matrix:

$$MTTF_{1oo2}=\frac{1}{A_1}+\frac{2\lambda_{DD}}{A_1A_2}+\frac{2\lambda_{DU}}{A_1A_3} \quad (35)$$

Equation 35 presents the mean life cycle (life time) of a 1oo2 architecture derived from Markov models.

7 Conclusion

The paper presented a systematic approach from the set up of Markov models to the final step of calculating the MTTF value, which is an important parameter for in the research area of safety instrumented systems. Two different architecture were examined a 1oo1 and a 1oo2 architecture. This systematic approach can applied to different safety related architectures and systems.

References:

[1] Börcsök, J.. Elektronic Safety Systems. *Heidelberg: Hüthig publishing company* 2004

[2] Börcsök J., Ugljesa E.. Advanced 2oo4 hardware architectures for safety related systems, *Journal WSEAS Transactions on Computer Research*, Vol. 6, Issue 1, pp. 14-20, ISSN: 1991-8755, 2007

[3] Goble, W. M. 1995. Safety of programmable electronic systems – *Critical Issues, Diagnostic and Common Cause Strength Proceedings of the IchemE Symposium*, Rugby, U. K: Institution of Chemical Engineers

[4] Shooman, M.L.. Probabilistic reliability. *McGraw-Hill.* 1986

[5] Smith, D.J.. Reliability Maintainability and Risk. *Newnes*. 2001

[6] Storey N.. Safety critical computer systems, *Addison Wesley*. 1996