IT303 – SOFTWARE ENGINEERING

ASSIGNMENT 1

Name: **Sachin Prasanna**
Roll No.: **211IT058**

Problem Statements:
i) Implementation of Fault Tee Analysis (FTA), RBD, of Safety critical system using Sharpe tool. Evaluate the qualitative and quantitative analysis.

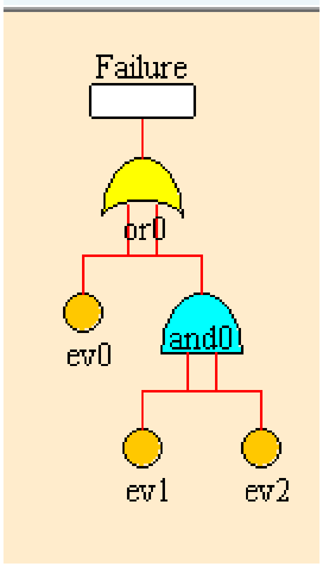
ii) Implement Markov chain and Petri nets for evaluation of dependability attributes with respect to all metrics present in the Sharpe tool.

Compare these 4 models with respect to Reliability, Unreliability, MTTF and Variance. Conclude your findings

Answers:

Safety Critical System 1: **Server System**

(i) Fault Tree Analysis:



Explanation:

Top event: **Server Downtime**

Other events:

- **Ev0:** Hardware Failure
- **Ev1:** No Spare Parts
- **Ev2:** Power Supply Failure

Observations:

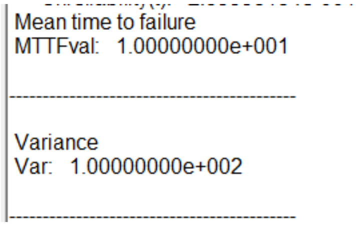
(i) Qualitative Analysis:

I have analyzed a scenario where the server goes down for downtime. This could be possible majorly due to 2 reasons, that is, Hardware Failure or Loss of Power.

And, the loss of power is caused when there no spare parts available and the power supplier has failed to provide power.

In this situation, certain probability of failures is attached to each event, and the probability of failure of the entire safety critical system is calculated using Fault Tree Analysis.

(ii) Quantitative Analysis:



```
Mean time to failure
MTTFval:   1.00000000e+001

--------------------------------------------

Variance
Var:   1.00000000e+002

--------------------------------------------
```

Figure 1: Analysis of parameters

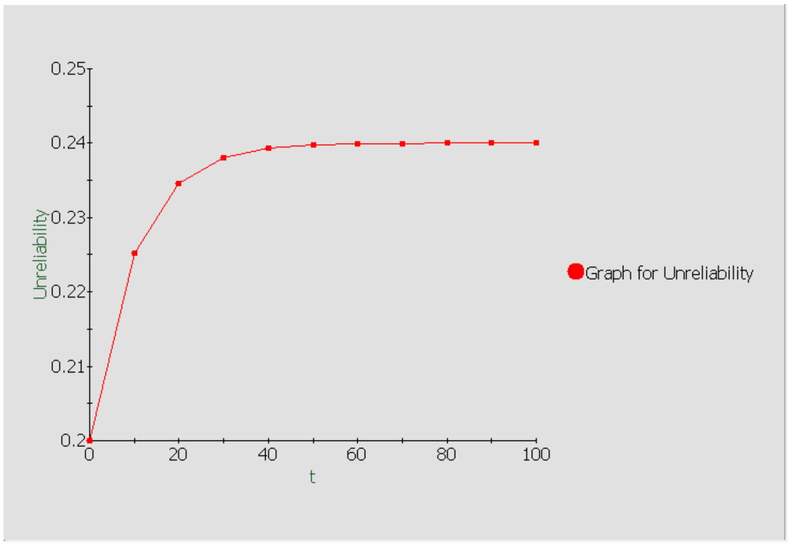


Figure 2: Unreliability of the system with time

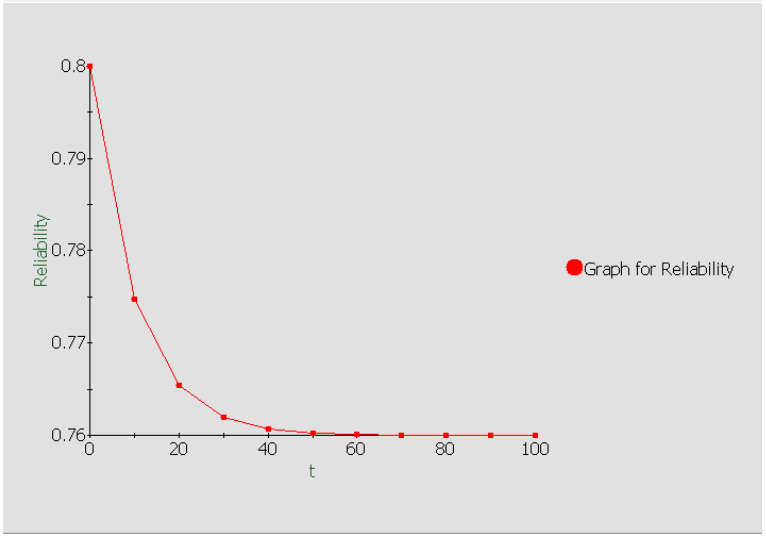
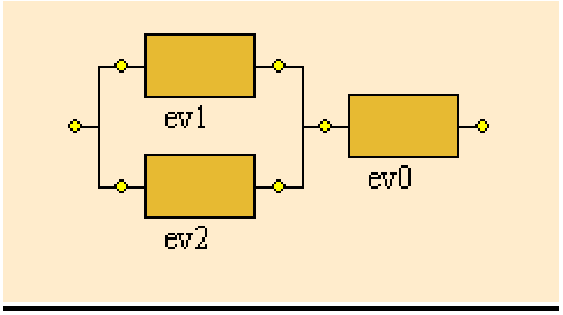


Figure 3: Reliability of the system with time

Results:

The Fault Tree Analysis (FTA) conducted on the scenario of server downtime reveals important insights into the factors contributing to the potential failure of the system. The analysis considers two primary causes for the top event "Server Downtime": Hardware Failure and Loss of Power. By quantifying the probabilities of failure associated with each event, the analysis provides a means to assess the overall probability of the top event "Server Downtime" occurring.

(ii) Reliability Block Diagram:



The above RBD is the conversion of the FTA according to the rules of converting an FTA to RBD.

Explanation:

Top event: **Server Downtime**

Other events:

- **Ev0:** Hardware Failure
- **Ev1:** No Spare Parts
- **Ev2:** Power Supply Failure

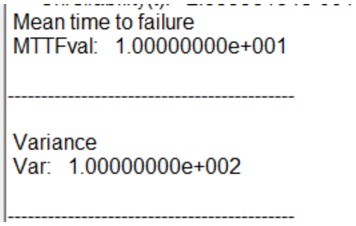
Observations:

(i) Qualitative Analysis:

I have analyzed a scenario where the server goes down for downtime using Reliability Block Diagrams. This could be possible majorly due to 2 reasons, that is, Hardware Failure or Loss of Power. And, the loss of power is caused when there no spare parts available and the power supplier has failed to provide power.

In this situation, certain probability of failures is attached to each event, and the reliability of the system is calculated by analysis of the reliability block diagram.

(ii) Quantitative Analysis:



```
Mean time to failure
MTTFval:   1.00000000e+001

------------------------------------------

Variance
Var:   1.00000000e+002

------------------------------------------
```

Figure 4: : Analysis of parameters

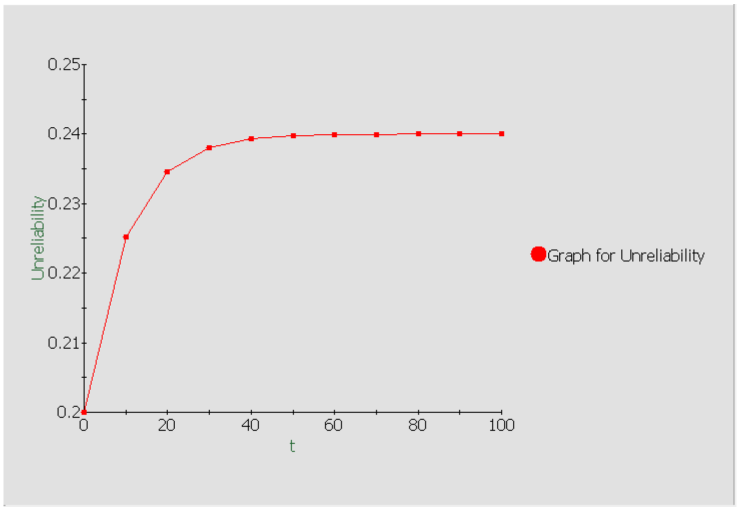


Figure 5: Unreliability of the system with time

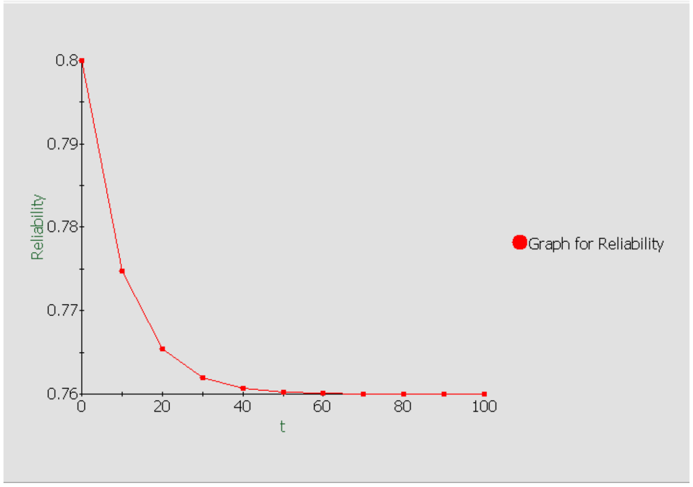
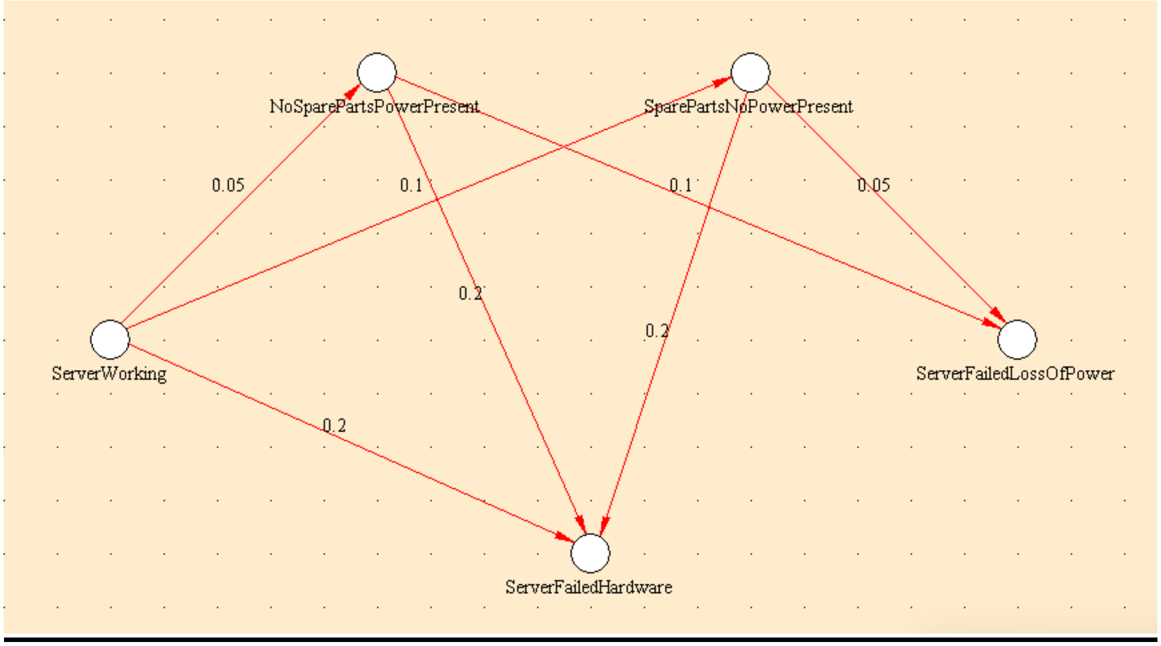


Figure 6: Reliability of the system with time

Results:

The Reliability Block Diagram (RBD) constructed on the scenario of server downtime reveals important insights into the factors contributing to the potential failure of the system. The analysis considers two primary causes for the top event "Server Downtime": Hardware Failure and Loss of Power. Using simple probabilistic logic and analysis, the reliability of the system and the probability of failure of the system is determined.

(iii) Markov Chain:



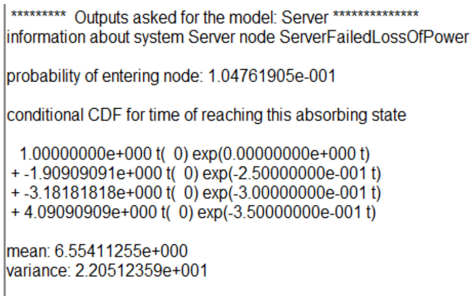
Explanation:

In the Markov Chain model of the safety critical system, there can be 5 possibilities (nodes). Namely:

- Server is Working
- Server has failed due to hardware issues
- Server has failed due to loss of power, which is a combination of two events.
- Spare parts not available, but power supply available
- Power supply not available, but spare parts available

The same Fault Tree has been modelled as a Markov chain, keeping in mind the probabilities associated with each event.

Observations/Analysis:



```
 *********  Outputs asked for the model: Server **************
information about system Server node ServerFailedLossOfPower

probability of entering node: 1.04761905e-001

conditional CDF for time of reaching this absorbing state

   1.00000000e+000 t(  0) exp(0.00000000e+000 t)
 + -1.90909091e+000 t(  0) exp(-2.50000000e-001 t)
 + -3.18181818e+000 t(  0) exp(-3.00000000e-001 t)
 + 4.09090909e+000 t(  0) exp(-3.50000000e-001 t)

mean: 6.55411255e+000
variance: 2.20512359e+001
```

Figure 7: Analysis of parameters

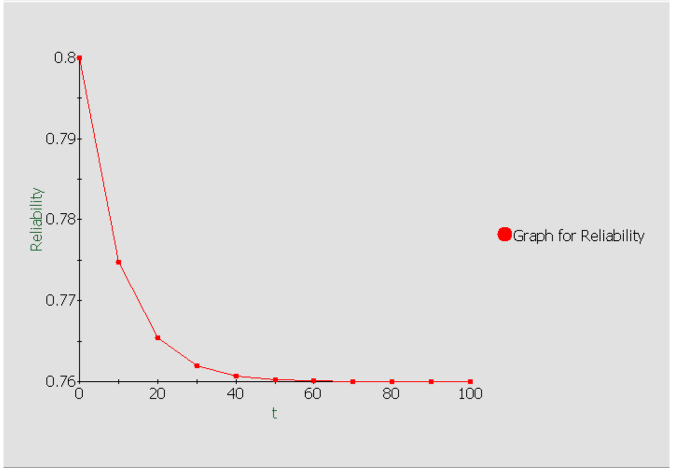


Figure 8: Reliability of System with time

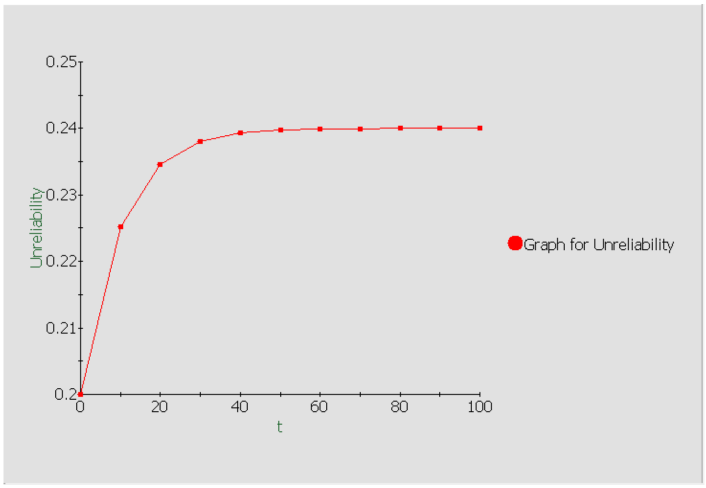
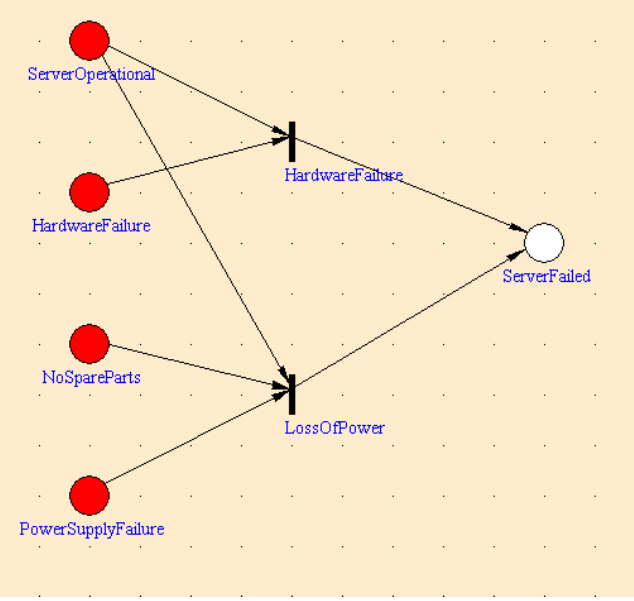


Figure 9: Unreliability of System with time

(iv) Petri Net:



Explanation:

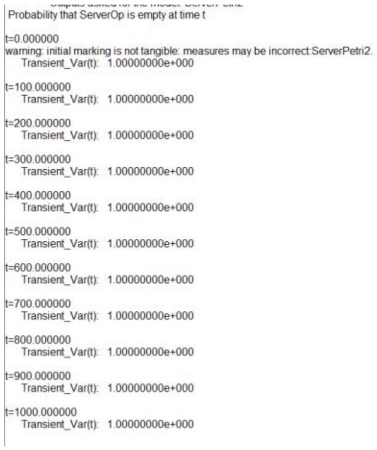
In the Petri Net model, there are 5 places and 2 transitions. The transitions fire if all its inputs have at least one token. Hence, we can say that the server can fail by the following 2 reasons:

i) **Hardware Failure (Transition):** Requires the server to be operational (1 token) and the hardware to fail.
ii) **Loss of Power:** Requires the server to be operational (1 token), spare parts to not be available (1 token) and the power supply to fail (1 token).

If any of the transition fire, then we will have an output token in the Server Failed place, which represents a failure of the server.

Observations/Analysis:

i) Assuming there is a token with all the inputs, then the system will definitely fail, as depicted by the analysis. These graphs show that the probability that the token at server operational is empty is 1, which means there is no token present at server operational, which means the server is never operational, if the above conditions occur.



```
 Probability that ServerOp is empty at time t

t=0.000000
warning: initial marking is not tangible: measures may be incorrect:ServerPetri2.
    Transient_Var(t):   1.00000000e+000

t=100.000000
    Transient_Var(t):   1.00000000e+000

t=200.000000
    Transient_Var(t):   1.00000000e+000

t=300.000000
    Transient_Var(t):   1.00000000e+000

t=400.000000
    Transient_Var(t):   1.00000000e+000

t=500.000000
    Transient_Var(t):   1.00000000e+000

t=600.000000
    Transient_Var(t):   1.00000000e+000

t=700.000000
    Transient_Var(t):   1.00000000e+000

t=800.000000
    Transient_Var(t):   1.00000000e+000

t=900.000000
    Transient_Var(t):   1.00000000e+000

t=1000.000000
    Transient_Var(t):   1.00000000e+000
```

Figure 10: Probability that the token at Server operational is empty

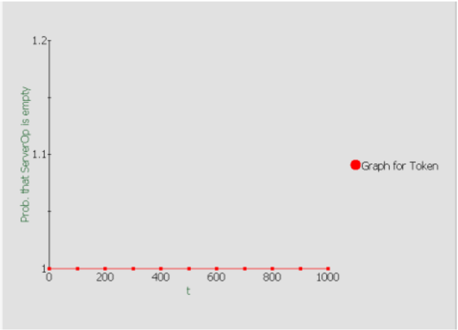
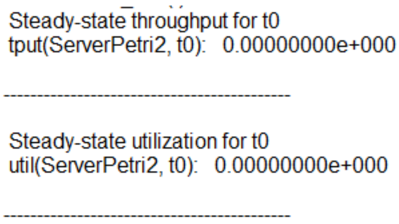


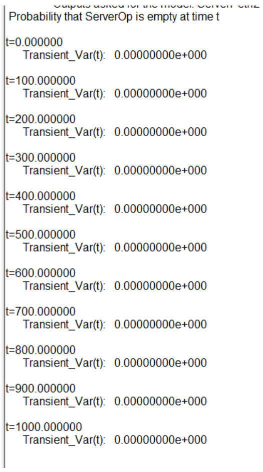
Figure 11: Graph for probability that the token at Server Operational is empty



```
Steady-state throughput for t0
tput(ServerPetri2, t0):   0.00000000e+000

--------------------------------------------

Steady-state utilization for t0
util(ServerPetri2, t0):   0.00000000e+000

--------------------------------------------
```

Figure 12: Other parameters analyzed, such as throughput and utilization for transition t0

ii) Assuming there is a token with server is operational node, but the hardware failure node and No spare parts nodes do not have a token, then the system can never fail, which is verified by the following analysis and graph. These graphs show that the probability that the token at server operational is empty is 0, which means a token is always present at server operational, which means the server is always operational, if the above-mentioned failures do not occur.



```
          Outputs asked for the model: Server-ctrl2
 Probability that ServerOp is empty at time t

t=0.000000
     Transient_Var(t):   0.00000000e+000

t=100.000000
     Transient_Var(t):   0.00000000e+000

t=200.000000
     Transient_Var(t):   0.00000000e+000

t=300.000000
     Transient_Var(t):   0.00000000e+000

t=400.000000
     Transient_Var(t):   0.00000000e+000

t=500.000000
     Transient_Var(t):   0.00000000e+000

t=600.000000
     Transient_Var(t):   0.00000000e+000

t=700.000000
     Transient_Var(t):   0.00000000e+000

t=800.000000
     Transient_Var(t):   0.00000000e+000

t=900.000000
     Transient_Var(t):   0.00000000e+000

t=1000.000000
     Transient_Var(t):   0.00000000e+000
```

Figure 13: Probability that the token at Server operational is empty

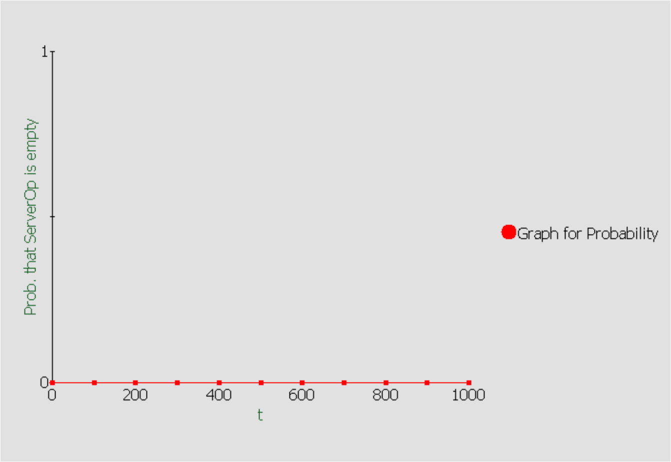
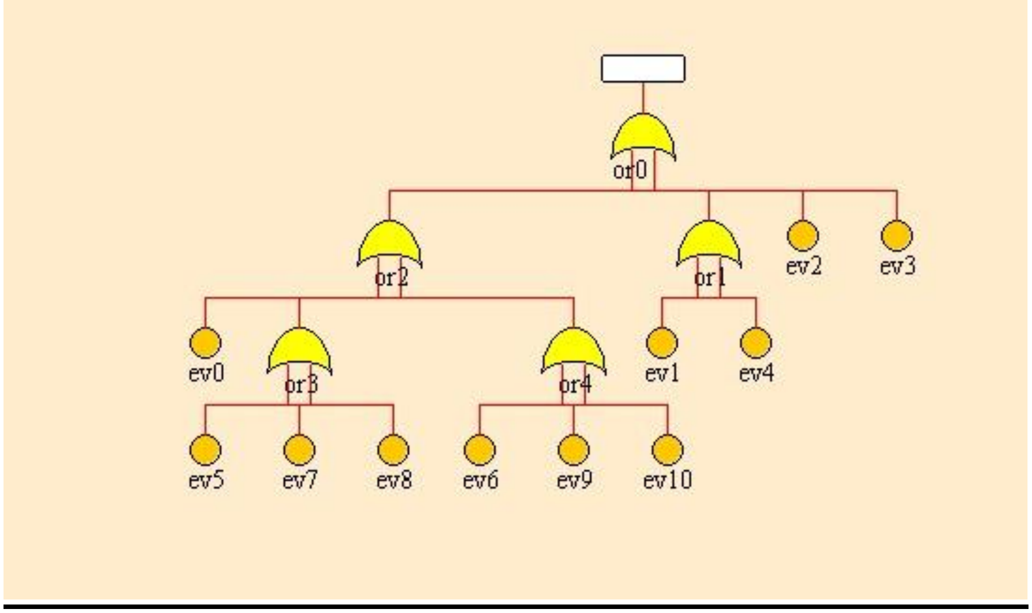


Figure 14: Graph for probability that the token at Server Operational is empty

Safety Critical System 2: **Traction Power Supply System (TPSS) in railway electrification**

(i) Fault Tree Diagram:



Explanation:

Top event: **Traction Power Supply System failure**
Attribute analyzed: **Failure Rate**

Basic events, with their failure rate in millions per hour

- **Ev0:** 15Kv Power Cable Failure
- **Ev5:** OCS Isolator Switch fail
- **Ev7:** Cantilever failure
- **Ev8:** Contact suspension Fail
- **Ev6:** Track failure
- **Ev9:** OVPD failure

- **Ev10:** Stray current cable failure
- **Ev1:** Tran arrester failure
- **Ev4:** CB fail
- **Ev2:** AIS fail
- **Ev3:** SCADA failure

Observations:

(i) Qualitative Analysis:

I have analyzed a scenario where the traction power supply system of a railway fails. It can be due to several factors, namely the ones taken into consideration as basic events. A combination of these events through OR gates give the final failure rate of the top event.

(ii) Quantitative Analysis:

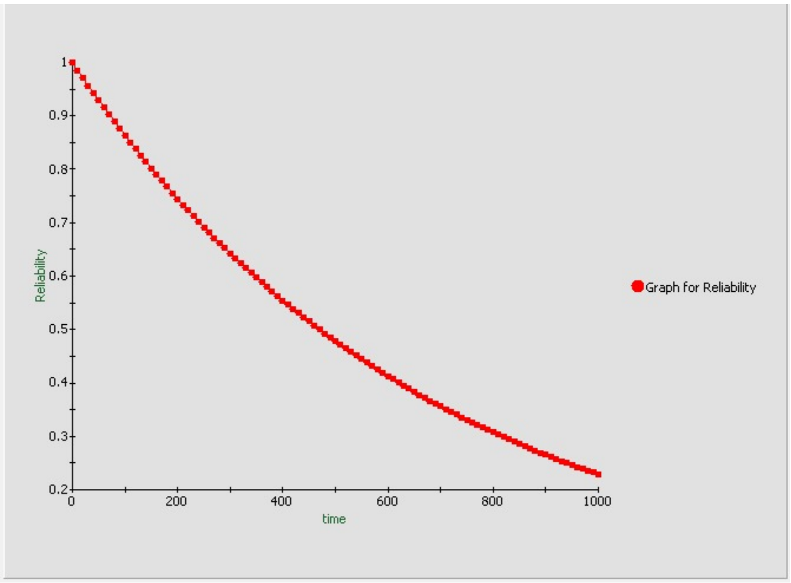


Figure 15: Reliability Graph with time

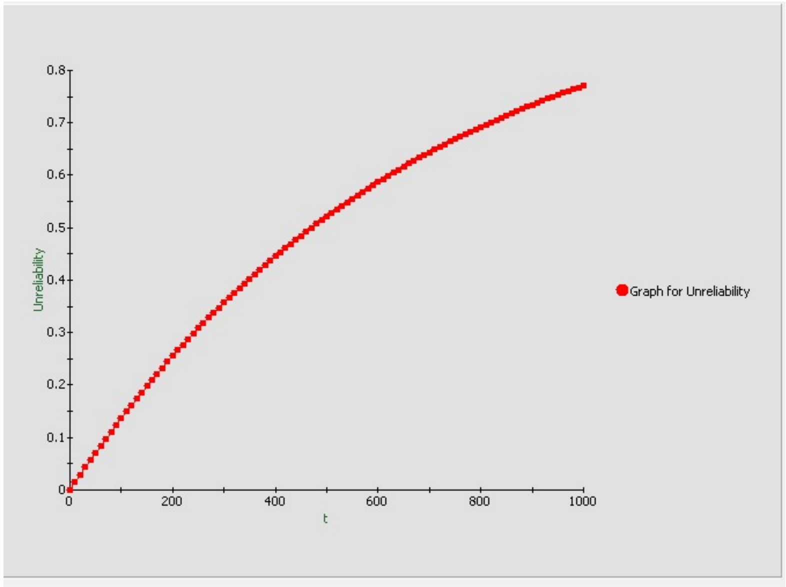
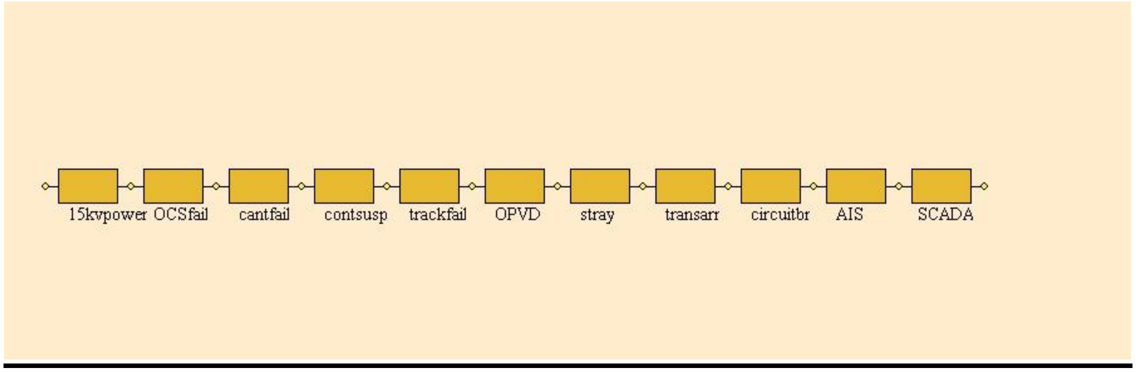


Figure 16: Unreliability graph with time

Results:

By conducting Fault Tree Analysis, we get a quantitative measure of the failure of the top event. As evident by the analysis done, the system gets more and more unreliable with time, as some basic event is likely to fail, which reduces reliability of the top event.

(ii) Reliability Block Diagram:



The above RBD is the conversion of the FTA according to the rules of converting an FTA to RBD. Each basic event has been abbreviated to their names in the block diagram.

Observations:

(i) Qualitative Analysis:

I have analyzed a scenario where the traction power supply system of a railway fails. It can be due to several factors, namely the ones taken into consideration as basic events. Upon considering these, a reliability block diagram is drawn corresponding to the Fault tree diagram before, and analyzed.

(ii) Quantitative Analysis:

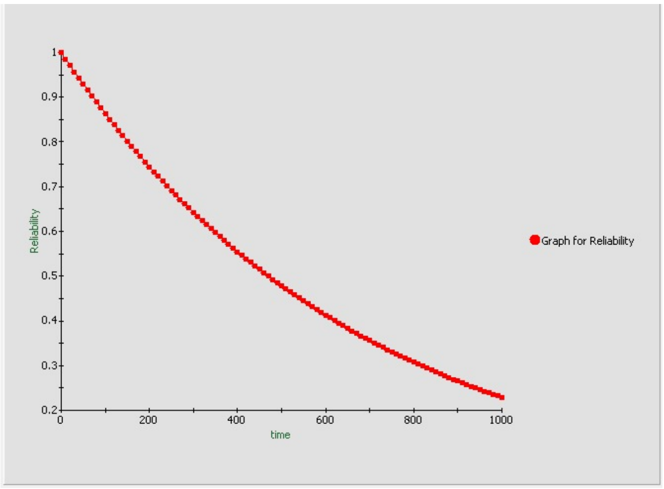


Figure 17: Reliability Graph with time

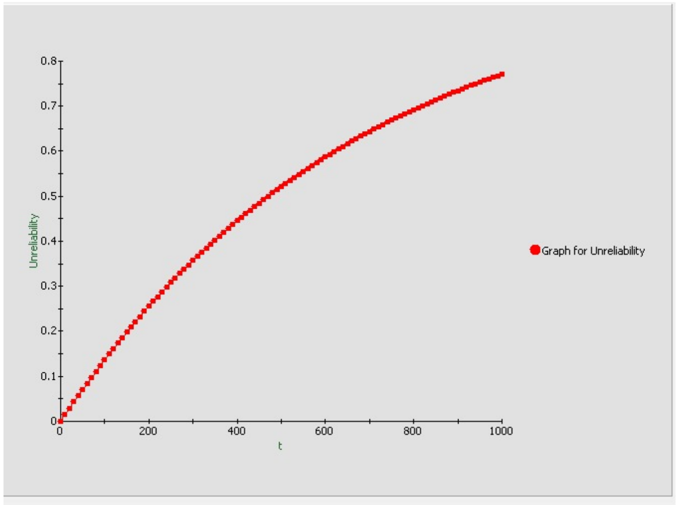
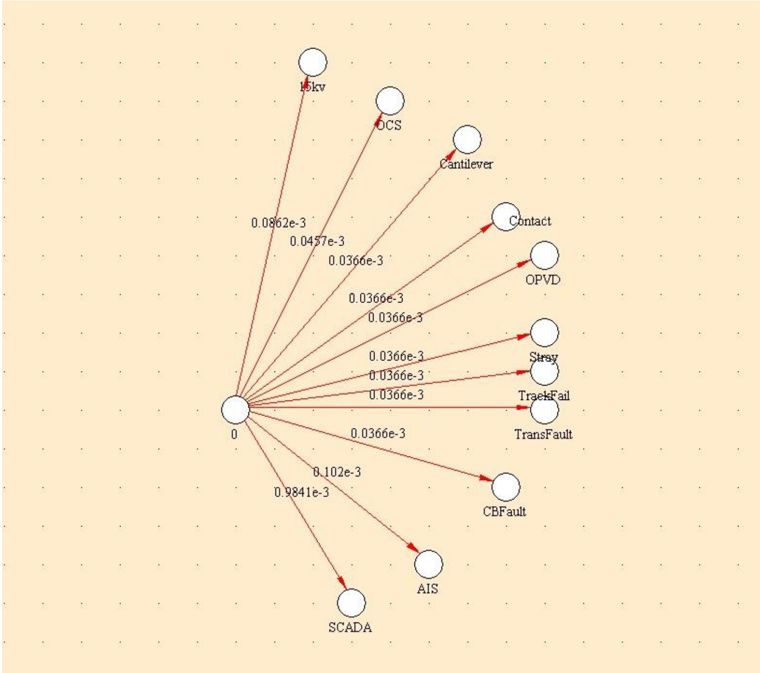


Figure 18: Unreliability Graph with time

Results:

By constructing the reliability block diagram of the corresponding Fault tree, we get a quantitative measure of the failure of the top event. As evident by the analysis done, the system gets more and more unreliable with time, as some basic event is likely to fail, which reduces reliability of the top event, which further supports our fault tree analysis as well.

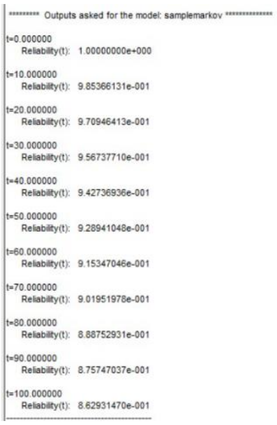
(iii) Markov Chain:



Explanation:

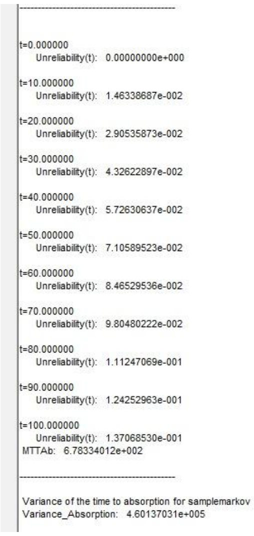
The same Fault Tree has been modelled as a Markov chain, keeping in mind the probabilities associated with each event. In the Markov Chain model of the safety critical system, there can be 12 possibilities (nodes) as depicted in the picture above.

Observations/Analysis:



```
********* Outputs asked for the model: samplemarkov **************

t=0.000000
    Reliability(t):   1.00000000e+000

t=10.000000
    Reliability(t):   9.85366131e-001

t=20.000000
    Reliability(t):   9.70946413e-001

t=30.000000
    Reliability(t):   9.56737710e-001

t=40.000000
    Reliability(t):   9.42736936e-001

t=50.000000
    Reliability(t):   9.28941048e-001

t=60.000000
    Reliability(t):   9.15347046e-001

t=70.000000
    Reliability(t):   9.01951978e-001

t=80.000000
    Reliability(t):   8.88752931e-001

t=90.000000
    Reliability(t):   8.75747037e-001

t=100.000000
    Reliability(t):   8.62931470e-001
------------------------------------------
```

Figure 19: Analysis of Reliability



```
-------------------------------------------


t=0.000000
    Unreliability(t):   0.00000000e+000

t=10.000000
    Unreliability(t):   1.46338687e-002

t=20.000000
    Unreliability(t):   2.90535873e-002

t=30.000000
    Unreliability(t):   4.32622897e-002

t=40.000000
    Unreliability(t):   5.72630637e-002

t=50.000000
    Unreliability(t):   7.10589523e-002

t=60.000000
    Unreliability(t):   8.46529536e-002

t=70.000000
    Unreliability(t):   9.80480222e-002

t=80.000000
    Unreliability(t):   1.11247069e-001

t=90.000000
    Unreliability(t):   1.24252963e-001

t=100.000000
    Unreliability(t):   1.37068530e-001
 MTTAb:   6.78334012e+002

-------------------------------------------

 Variance of the time to absorption for samplemarkov
 Variance_Absorption:   4.60137031e+005
```

Figure 20: Analysis of unreliability and other parameters

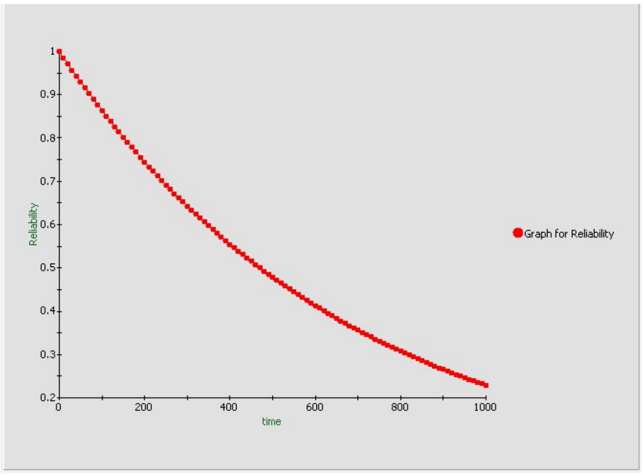


Figure 21: Reliability with time

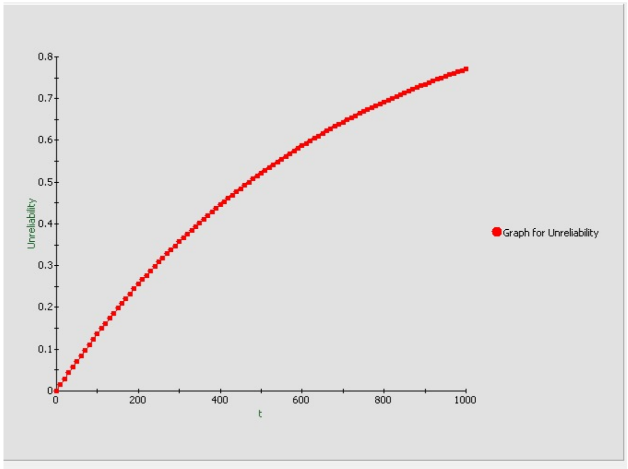
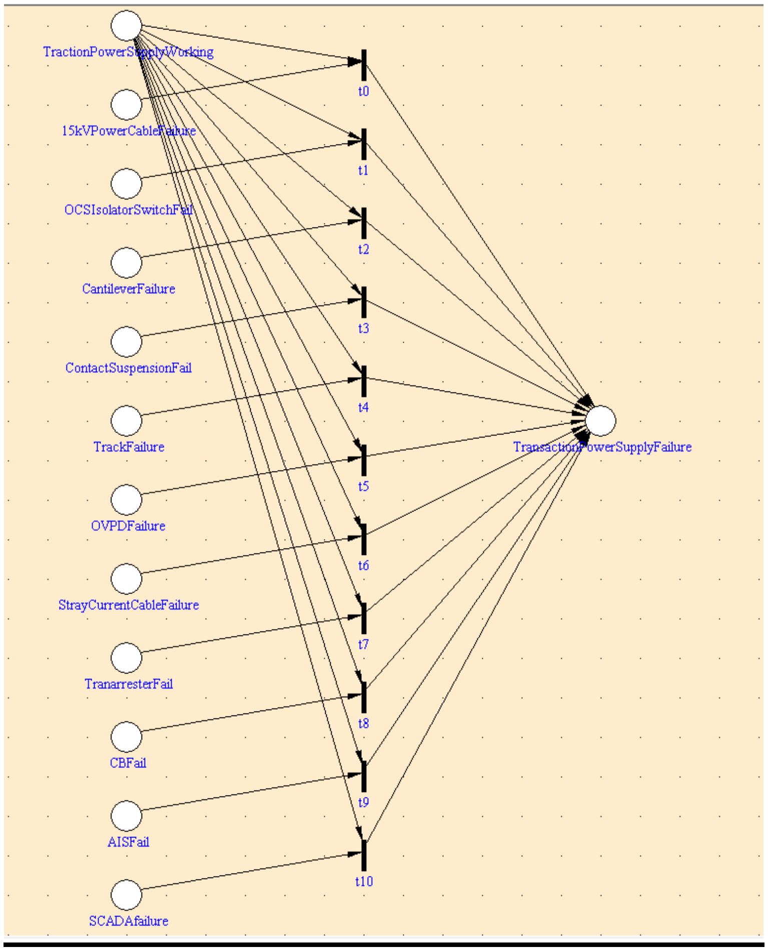


Figure 22: Unreliability with time

(iv) Petri Net:



Explanation:

In the Petri Net model, there are 12 places and 11 transitions. The transitions fire if all its inputs have at least one token. Hence, we can say that the traction power supply can fail by the following reasons:

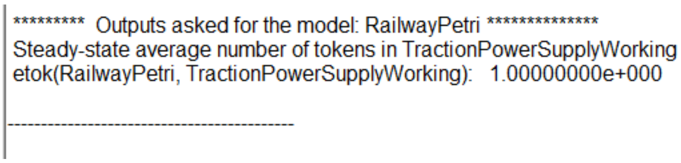
i) **15Kv Power Cable Failure:** Requires the traction power system to be operational (1 token) and the 15kv Power Cable to fail (1 token).
ii) **OCS Isolator Switch Fail:** Requires the traction power system to be operational (1 token) and the OCS Isolator switch to fail (1 token).

iii) **Cantilever Failure:** Requires the traction power system to be operational (1 token) and the Cantilever to fail (1 token).
iv) **Contact Suspension Fail:** Requires the traction power system to be operational (1 token) and the contact suspension to fail (1 token).
v) **Track Failure:** Requires the traction power system to be operational (1 token) and the track to fail (1 token).
vi) **OVPD Failure:** Requires the traction power system to be operational (1 token) and the OVPD to fail (1 token).
vii) **Stray Current Cable Failure:** Requires the traction power system to be operational (1 token) and the stray current cable to fail (1 token).
viii) **Tran arrester Failure:** Requires the traction power system to be operational (1 token) and the Tran arrester to fail (1 token).
ix) **CB Fail:** Requires the traction power system to be operational (1 token) and the CB to fail (1 token).
x) **AIS Fail:** Requires the traction power system to be operational (1 token) and the AIS to fail (1 token).
xi) **SCADA Failure:** Requires the traction power system to be operational (1 token) and the SCADA to fail (1 token).

If any of the transition fire, then we will have an output token in the traction power supply place, which means the traction power supply has failed.

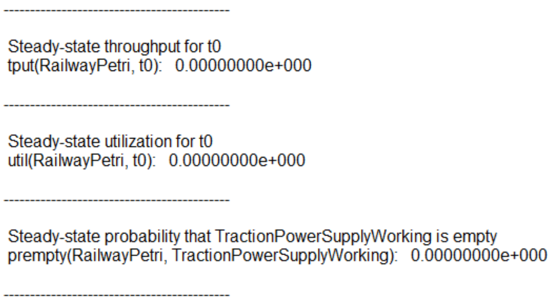
Observations/Analysis:

i) Consider a scenario, where the traction system is working (has 1 token) but no other failures have occurred. So in this case, the traction system has to continue working, as confirmed by the analysis and graphs shown below:



```
*********  Outputs asked for the model: RailwayPetri **************
Steady-state average number of tokens in TractionPowerSupplyWorking
etok(RailwayPetri, TractionPowerSupplyWorking):   1.00000000e+000

--------------------------------------------
```

Figure 23: Tokens present in the traction power supply working node



```
---------------------------------------------

Steady-state throughput for t0
tput(RailwayPetri, t0):   0.00000000e+000

---------------------------------------------

Steady-state utilization for t0
util(RailwayPetri, t0):   0.00000000e+000

---------------------------------------------

Steady-state probability that TractionPowerSupplyWorking is empty
prempty(RailwayPetri, TractionPowerSupplyWorking):   0.00000000e+000

---------------------------------------------
```

Figure 24: Transition t0 analysis and probability that traction power supply is empty analysis

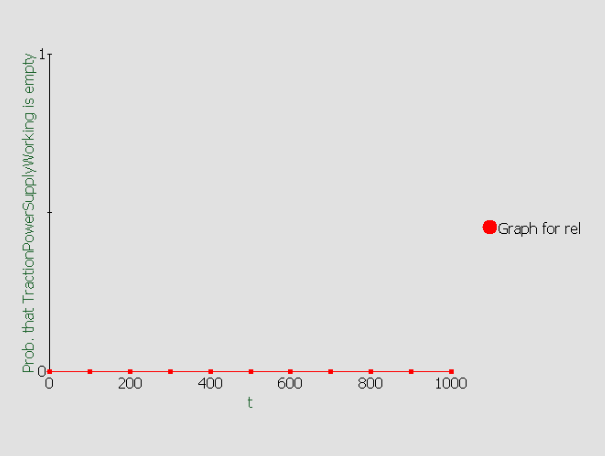
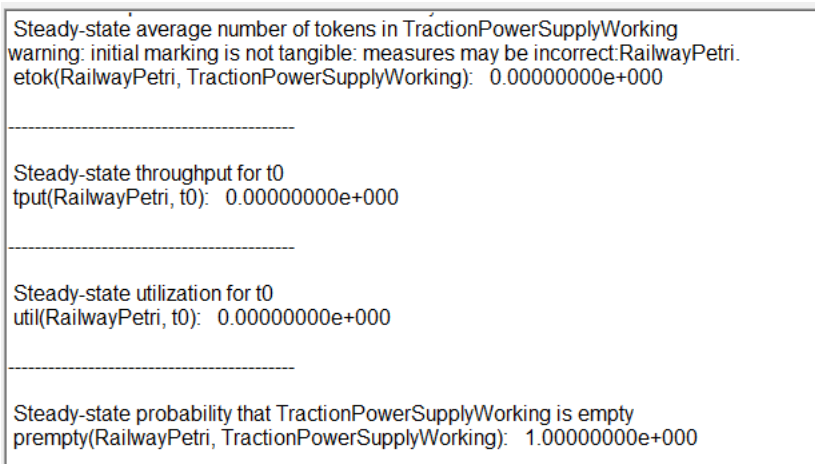


Figure 25: Graph for Probability that the transaction power supply working is empty

ii) Consider a scenario, where the traction system is working (has 1 token) and the cantilever has failed(has 1 token). In this case, the system will fail which is proved by the analysis done below:



```
Steady-state average number of tokens in TractionPowerSupplyWorking
warning: initial marking is not tangible: measures may be incorrect:RailwayPetri.
 etok(RailwayPetri, TractionPowerSupplyWorking):   0.00000000e+000

---------------------------------------------

Steady-state throughput for t0
tput(RailwayPetri, t0):   0.00000000e+000

---------------------------------------------

Steady-state utilization for t0
util(RailwayPetri, t0):   0.00000000e+000

---------------------------------------------

Steady-state probability that TractionPowerSupplyWorking is empty
prempty(RailwayPetri, TractionPowerSupplyWorking):   1.00000000e+000
```

Figure 26: Analysis of attributes

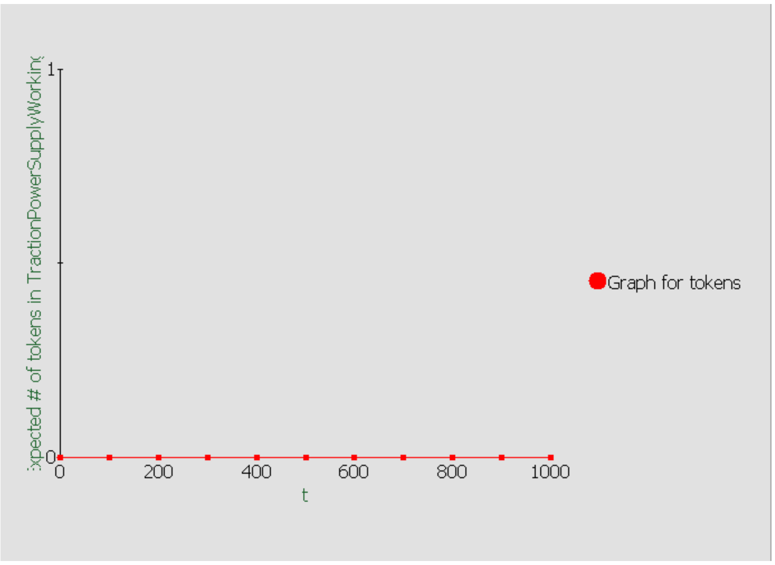


Figure 27: Graph of expected number in Traction Power Supply Working node

Conclusions:

After analyzing 2 safety critical systems with the 4 measures, namely – Fault Tree Analysis, Reliability block diagram, Markov chains and petri nets, the following points are of note:

i) FTA is primarily used to analyze system reliability. It identifies the ways in which different events or component failures can lead to system failure.

ii) RBD is used to model and analyze system reliability by connecting components in series, parallel, or other configurations.

iii) Markov Chains are also used for reliability analysis, especially for systems with discrete states. They model transitions between states and can incorporate reliability data.

iv) Markov Chains can calculate parameters like MTTF, variance of a system property based on state transitions and failure rates.

v) Petri nets can also model system behavior, but they are not inherently focused on reliability analysis. They focus on different situations where a place has a token or not, which basically is a matter of a yes or no. If the places which need to have a token for the system to fail have a token, then the system will fail, or else not.

References:

- Reliability Analysis of Addis Ababa Light Rail Transit Traction Power Supply System - http://213.55.95.56/bitstream/handle/123456789/21026/Destaw%20Addisu.pdf?sequence=1&isAllowed=y
- ITIL Fault Tree Analysis FTA - https://www.itsmsolutions.com/newsletters/DITYvol1iss5.htm
- Sharpe Tool - https://sharpe.pratt.duke.edu/node/10
- Das, Madhusmita and R. Mohan, Biju and Guddeti, Ram Mohana Reddy, Qualitative and Quantitative Risk Assessment of Drone Crash System Using Fault Tree Analysis. Available at SSRN: https://ssrn.com/abstract=4513147
- MTBF calculator, accessed Mar'23 https://aldservice.com/Reliability-Software/free-mtbf-calculator.html
- MTBF Calculator User Guide, accessed Mar'23https://aldservice.com/Free-MTBF-Calculator-User-Guide.html

****