Markov Modelling Primer – Calculating System PFDs for the design of Safety Instrumented Systems.

By Peter Morgan

For the control specialist involved in the specification or design of Safety Instrumented Systems (SIS), the Markov model provides an approach that is effective in providing critical statistics for Safety Integrity Level (SIL) determination as well as providing an important illustrative record of the system design basis. Unfortunately more mystery is associated with the method than is merited and the application of the approach is often avoided by all but safety system specialists. Moreover some of the most notable texts on the subject describe the successive matrix manipulations necessary to arrive at time dependent failure probabilities, when the control system specialist typically requires probabilities of failure on demand (PFDs) of repairable systems which can be calculated using relatively simple steady state equations.

This brief paper is intended to shed light on the Markov modeling approach with specific reference to 2oo3 voting logic which is typically used for process variable measurement in critical systems.

Markov Model for Single Repairable Device

Figure 1 shows the Markov model for a single repairable device.

The values P(n) and P(n+1) are the fractional times spent in each state so that "1" means that the system is continuously in that state and "0" means that the system is never in that state. The average rate at which the system transitions from one state (Pn) to the other is given by the product P(n) λ_n , where λ_n is the average failure rate for the subject component. Similarly if the system is returned to state P(n) from state P(n+1) at an average rate of μ_n (by repair or replacement), the rate at which the system returns to the unfailed state is given by the product P(n+1) μ_n.

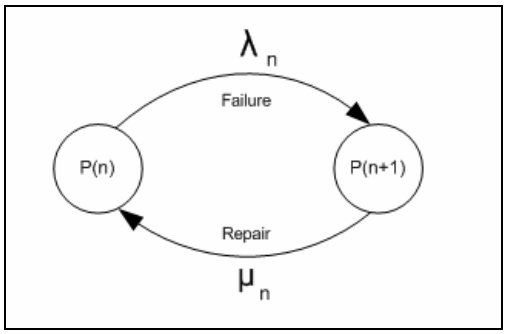

Figure 1. Markov Model for Single Repairable Device

The system depicted in fig 1 will reach a steady state when the repair rate is equal to the failure rate. In this condition P(n) and P(n+1) are the final fractional times spent in each

state. Note that the fractional time spent in each state and the fractional probability of being in a particular state at any time are one and the same.

The state equations in this case are:

$$\lambda P0 - \mu P1 = 0$$
$$P0 + P1 = 1$$

This simultaneous equation is easily solved by substitution to give:

$$P1 = \lambda / (\mu + \lambda)$$

When repair rates are much greater than failure rates:

$$P1 = \lambda / \mu$$

note that this is the same as MTTR/MTBF where MTTR is the mean time to repair and MTBF is the mean time between failures for the system component (e.g. transmitter).

Markov Model for 2oo3 Transmitter Logic

Calculating the fractional probability of the system being in a degraded or failed state while always possible by "hand" becomes arduous and prone to error as the system becomes more complex. This is where the Markov model and matrix inversion come into their own.

For 2003 transmitter logic, it is assumed that a trip is to be initiated when at least two transmitters indicate the trip state. One transmitter can fail without inhibiting a trip, however two failures (to the dangerous state) will cause the system to fail dangerously. The logic solver monitors individual signals to verify that the transmitters are not frozen, and compares each transmitter with the median value to alert the operator of a possible transmitter failure when there is a deviation. The system is periodically tested (annually) to expose undetected failures.

In the Markov model shown in figure 2, four states are identified:

0	system is OK (all transmitters normal)
1	One transmitter is failed and failure is detected
2	One transmitter is failed but the failure is not detected
3	System is in the fail state and the condition is detected
4	System is in the fail state and the condition is not detected

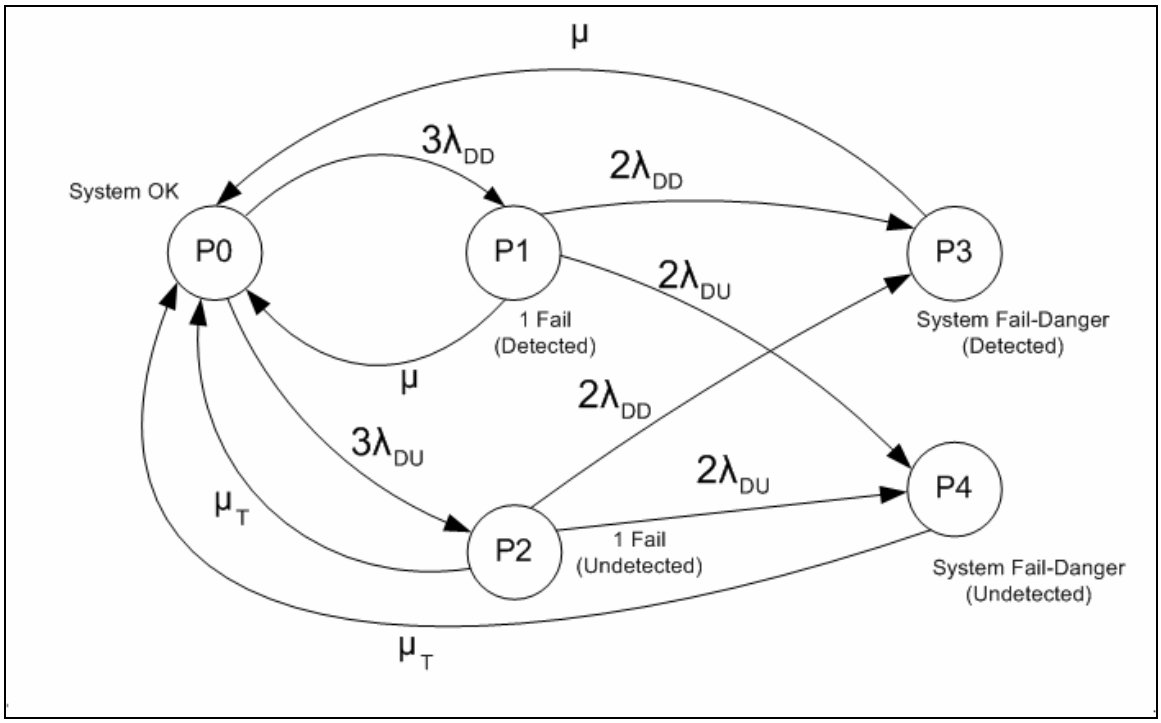

Figure 2. Markov Model for 2003 Transmitter Logic

Defining the failure and repair rates:

λ_{DD}	Individual device (transmitter) failure rate for detected failures (per year)
λ_{DU}	Individual device (transmitter) failure rate for undetected failures (per year)
μ	Repair rate for detected failures (per year)
μ_T	Repair rate for undetected failures (per year)

Steady State Equation:

$$-(3\lambda_{DD+}3\lambda_{DU})\,P0 + \mu\,P1 + \mu_T\,P2 + \mu\,P3 + \mu_T\,P4 = 0 \quad (1)$$

$$3\lambda_{DD}\,P0 - (2\lambda_{DD+}2\lambda_{DU} + \mu)P1 = 0 \quad (2)$$

$$3\lambda_{DU}\,P0 - (2\lambda_{DD+}2\lambda_{DU} + \mu_T)P2 = 0 \quad (3)$$

$$2\lambda_{DD}\,P1 + 2\lambda_{DD}\,P2 - \mu\,P3 = 0 \quad (4)$$

$$2\lambda_{DU}\,P1 + 2\lambda_{DU}\,P2 - \mu_T\,P4 = 0 \quad (5)$$

$$P0+P1+P2+P3+P4 = 1 \quad (6)$$

Adding like terms on the left side of equation (6) to the left side of equation (1) and adding 1 to the right side of equation (1) incorporates the properties of equation (6) and reduces the number of equations to 5 to allow a solution for the fractional state probabilities using matrix inversion of the resultant "Square" matrix.

$$[1-(3\lambda_{DD+}3\lambda_{DU})]\ P0 + [1+\mu]\ P1 + [1+\mu_T]\ P2 + [1+\mu]\ P3 + [1+\mu_T]\ P4 = 1$$

$$3\lambda_{DD}\ P0 - (2\lambda_{DD+}2\lambda_{DU} + \mu)P1 = 0$$

$$3\lambda_{DU}\ P0 - (2\lambda_{DD+}2\lambda_{DU} + \mu_T)P2 = 0$$

$$2\lambda_{DD}\ P1 + 2\lambda_{DD}\ P2 - \mu\ P3 = 0$$

$$2\lambda_{DU}\ P1 + 2\lambda_{DU}\ P2 - \mu_T\ P4 = 0$$

λ_{DD}	=	0.1	failures per year (10 years between detected failures)
λ_{DU}	=	0.01	failures per year (100 years between undetected failures)
μ	=	2190	(number of hours in a year/ repair time (4 hours))
μ_T	=	2	(2/manual test interval in years)

Note that although an undetected failure could occur at any time between manual system tests, on average they can be assumed to occur half way through the test interval. On this basis the system components can be assumed to be failed for half the test period in which case the rate at which devices are returned to their functional state is 2/manual test interval (in years).

The final state equations can now be written in the form of a matrix so that the state probabilities P0 to P4 - in particular P3 and P4 - can be obtained by matrix inversion.

$$\begin{bmatrix} 0.67 & 2191 & 3 & 2191 & 3 \\ 0.3 & -2190.22 & 0 & 0 & 0 \\ 0.03 & 0 & -2.22 & 0 & 0 \\ 0 & 0.2 & 0.2 & -2190 & 0 \\ 0 & 0.02 & 0.02 & 0 & -2 \end{bmatrix} \text{ X } \begin{bmatrix} P0 \\ P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \text{ Equals } \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

The "Inverse" of a matrix is another matrix which when multiplied by the original matrix, gives a matrix with values of 1 for all diagonal elements and 0 for off-diagonal elements. It follows that when both sides of the state matrix equation are multiplied by the inverse, the following matrix equation is obtained:

$$\begin{bmatrix} P0 \\ P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \text{ Equals } \begin{bmatrix} P \text{ inverse} \end{bmatrix} \text{ X } \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Noting that the right hand matrix product gives a column matrix of values equal to those in the first column of the Inverse of the P matrix, the values in the first column of the inverse matrix are the required fractional state probabilities.

This does mean that only the first column of the inverse matrix needs to be calculated, however since the P matrix inversion can be easily obtained using MINVERSE function in a spread sheet, the redundant values in the matrix are obtained without effort.

It is worth noting that although the inverse matrix can be obtained by hand calculation, this process can be arduous for all but the simplest of systems. The use of the matrix inversion function available in spreadsheets is not only quick and easy but avoids the errors so easily introduced in a lengthy hand calculation.

Using the Xcel array function "MINVERSE", the inverse of the example Pmatrix is:

Inverse				
0.986399	0.986854	1.435207	0.98685	1.479599
0.000135	-0.000321	0.000197	0.000135	0.000203
0.01333	0.013336	-0.431056	0.013336	0.019995
1.23E-06	1.19E-06	-3.93E-05	-0.000455	1.84E-06
0.000135	0.00013	-0.004309	0.000135	-0.499798

Where the state fractional probabilities P0 to P4 are provided in the first column.

Noting that the state P3 is the probability of the system failing on demand (PFD) due to detected failures and P4 is the PFD for undetected failures, and the net PFD is the sum of both, it is clear that PFD for the system is heavily dependent on the proof test interval to limit the exposure due to undetected failure.

2oo3 With no undetected failures from State P1 to P4 (an approximation)

The state equations in matrix form for this case are:

$$\begin{bmatrix} 0.67 & 2191 & 3 & 2191 & 3 \\ 0.3 & -2190.2 & 0 & 0 & 0 \\ 0.03 & 0 & -2.22 & 0 & 0 \\ 0 & 0.2 & 0.2 & -2190 & 0 \\ 0 & 0 & 0.02 & 0 & -2 \end{bmatrix} \text{ X } \begin{bmatrix} P0 \\ P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \text{ Equals } \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

and the inverse of the Pmatrix is:

Inverse

0.986401	0.986851	1.435209	0.986851	1.479601
0.000135	-0.000321	0.000197	0.000135	0.000203
0.01333	0.013336	-0.431056	0.013336	0.019995
1.23E-06	1.19E-06	-3.93E-05	-0.000455	1.84E-06
0.000133	0.000133	-0.004311	0.000133	-0.4998

In comparing the PFDs for this case and the previous case, it will be noted that there is little difference between the PFD due to undetected failures. This is because the failure duration in state P1 (the repair time) is much smaller than that in state P2 (half the test interval) and therefore the number of transitions between state P1 and state P4 are much lower than the number of transitions between state P2 and state P4. For this reason, the Markov model sometimes omits transitions between state P1 and state P4. Since the inclusion of this failure path does not materially add to the complexity of the calculations it is suggested that the approximation is unnecessary and that transitions between state P1 and state P4 be included for completeness.

Calculating System PDF directly from the Markov model

The general form of the P matrix for 2oo3 logic and any system with up to five states is:

$$\begin{bmatrix} 1-\sum R_{0\text{-ALL}} & 1+R_{1\text{-}0} & 1+R_{2\text{-}0} & 1+R_{3\text{-}0} & 1+R_{4\text{-}0} \\ R_{0\text{-}1} & -\sum R_{1\text{-ALL}} & R_{2\text{-}1} & R_{3\text{-}1} & R_{4\text{-}1} \\ R_{0\text{-}2} & R_{1\text{-}2} & -\sum R_{2\text{-ALL}} & R_{3\text{-}2} & R_{4\text{-}2} \\ R_{0\text{-}3} & R_{1\text{-}3} & R_{2\text{-}3} & -\sum R_{3\text{-ALL}} & R_{4\text{-}3} \\ R_{0\text{-}4} & R_{1\text{-}4} & R_{2\text{-}4} & R_{3\text{-}4} & -\sum R_{4\text{-ALL}} \end{bmatrix}$$

$\sum R_{j\text{-ALL}}$ these diagonal elements are the sum of all transition rates from state j to all other states that are "connected". This includes failures from state j to other degraded states and repairs that take the system to a less degraded state.

$R_{i\text{-}j}$ is the transition rate from state i to state j. If the Markov model shows no transition between state i and state j, the entry is zero.

Example: for Markov model in figure 2 $\sum R_{0\text{-ALL}} = 3\lambda_{DD+}3\lambda_{DU,}$ $R_{1\text{-}0} = \mu$, $R_{2\text{-}0} = \mu_{T,}$ $R_{3\text{-}0} = \mu$, $R_{4\text{-}0} = \mu_T$

Note that the matrix can be extended to cover any number of states by adding elements and maintaining the convention for the first row, for diagonal elements and off-diagonal elements.

For any system, after substituting failure and repair rates, the matrix can be inverted (using a spread sheet MINVERSE function) and the PDFs directly obtained from the first column of the inverse matrix. The reader is invited to try this approach for various failure and repair rates, and to extend the matrix to include "Fail Save" states, noting that the approach does not change.

About the Author

Peter Morgan, P.Eng., is Principal Consultant of Control System Design Services Inc.
His e-mail is morgan@controlinsight.com