Reliability Analysis of Electronic Systems using Markov Models

István Matijevics

Polytechnical Engineering College, Subotica, Serbia and Montenegro,
matistvan@yahoo.com

Zoltán Jeges

Polytechnical Engineering College, Subotica, Serbia and Montenegro,
zjeges@vts.su.ac.yu

Abstract: Programmable Electronic Systems are tools for safety protection applications in industrial processes. These electronic solutions have special circuits and architectures. Markov Models can expressively represent the operation of a programmable electronic system as various system components fail and/or are repaired. This paper describes one method and shows examples of the reliability analysis of control system. In model are multiple failure rates as a function of failure state, common cause failures, on-line diagnostic capability of a programmable electronic system, multiple failure modes, and different repair rates as a function of failure state.

Keywords: Reliability analysis; Programmable electronic controls; Markov models

1 Introduction [2]

In process industry nowadays there are a great number of PES (Programmable Electronic Systems) system applications. These systems are very important for the management of risk. These systems consist of sensors, computers (microcontrollers) and actuators. The unwanted failure events damage the environment and cause loss of production and investments in equipment.

New international standards (IEC61508 [3] and ISA-S84.01 [4,5]) are required especially for high safety applications and quantification of the achieved safety.

The following main objectives are necessary in the teaching on reliability in PES (Programmable Electronic Systems) [1]:

- Reliability specifications-oriented design,

- Re-design after analyzing field data,
- Reliability analysis of an existing design,
- Failure analysis of components, circuits or systems,
- Maintainability analysis of an existing design and

Understand and apply reliability standard.

2 Most Used Analysis Techniques [2]

Some reliability analysis techniques are graphically represented in Fig. 1. These techniques are grouped into:

- quantitative – the interval between the resulting numbers and the ratio of the resulting numbers has a meaning - and
- qualitative – the resulting numbers are only used for distinction or rank ordering.

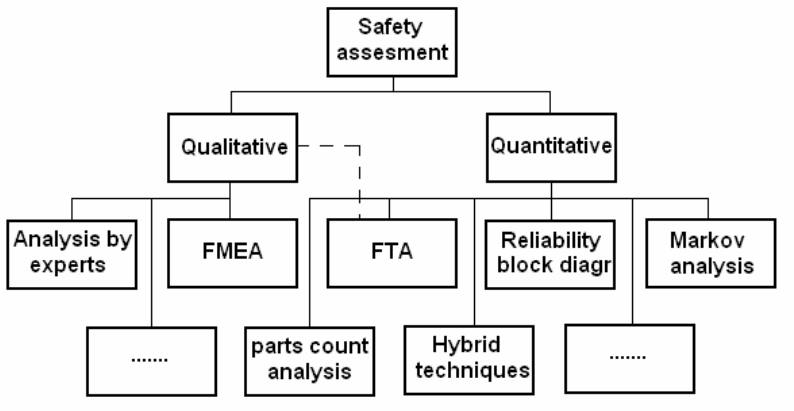

Figure 1

Most used analysis techniques

- Analysis by experts: based on previous experience in similar applications.
- FMEA (failure mode and effect analysis and derivatives): bottom-up analysis of a system, by examining all component failures and determining the effects of these failures on the entire system.
- Parts count analysis or component count analysis: is an analysis technique to calculate the failure rate of a system when the failure rates of its components are known.

- RBD (reliability block diagrams): a model of the behavior of a system by showing graphically the condition for a successful operation.
- Hybrid techniques: combinations of reliability block diagrams and Markov analysis results for redundant configurations.
- FTA (fault tree analysis): top-down method, how basic events may lead to a certain top-event.
- Markov analysis: the safety of a system is analyzed by representing the system by beans of the different states and transitions between these states.

3 Programmable Electronic Systems Architectures (PES) [5]

Traditional automatic protection systems used in industrial processes mechanical relays. A PES offers advantages for these safety protection applications including fast response times, digital communications capability and extensive on-line diagnostics to detect electronic component failures.

The on-line self-diagnostic capability of the system is a critical variable. Good diagnostics improve both safety and availability. Two types of diagnostics are used in a PES:

- reference diagdostics and
- comparison diagnostics.

3.1 Failure Modes and Effects Analysis

An **FMEA** (Failure Mode Effect Analysis) is a bottom up technique that used qualitatively, quantitatively or as a combination of both and is very effective in identifying critical component failures in a **PES**. An **FMEDA** (Failure Mode Effect and Diagnostic Analysis) is an **FMEA** variation. It combines standard **FMEA** techniques with extensions to identify online diagnostic techniques. It is a technique recommended to generate failure rates for each important category:

- safe detected,
- safe undetected,
- dangerous detected and
- dangerous undetected

in the safety models.

Fig. 2 shows an input circuit from **PES**, Fig. 3 shows **FMEDA** done on the input circuit.

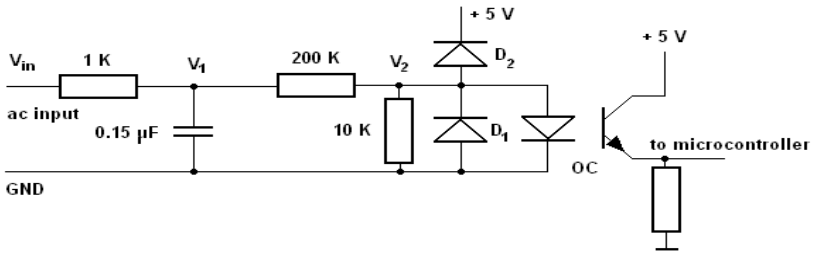

Figure 2
PES input circuits

FMEDA				***Failures/billion hours***					***Safe***	***dange rous***
compo nent	Mode	Effect	criticality	FIT	Safe	Dang.	Det.		0	0
R1	short	Loose filter	Safe	0.13	0.125	0	0		0.50	0
	open	Logic 0	Safe	0.50	0.50	0	1		0	0
C1	short	Logic 0	Safe	2	2	0	0		0	0
	open	Loose filter	Safe	0.50	0.50	0	0		0	0
R2	short	Overvoltage	Dang.	0.13	0	0.13	0		0.50	0
	open	Logic 0	Safe	0.50	0.50	0	1		0	0
R3	short	Logic 0	Safe	0.13	0.125	0	0		0	0
	open	overvoltage	Dang.	0.50	0	0.50	0		0	0
D1	short	Logic 0	Safe	2	2	0	0		0	0
	open	Blow out circuit	Dang.	5	0	5	0		0	0
D2	short	Logic 1	Dang.	2	0	2	0		0	0
	open	Blow out circuit	Dang.	5	0	5	0		0	0
OC	Led dim	No light	Safe	28	28	0	0		0	0
	Tran. short	Logic 1	Dange.	19	0	19	0		0	0
	Tran. open	Logic 0	Safe	5	5	0	0		0	0
R4	short	Logic 0	Safe	0.13	0.125	0	0		0	0

FMEDA				*Failures/billion hours*					*Safe*	*dangerous*
	open	Logic 1	Dang.	0.50	0	0.50	0		1	0
				71	38.88	32			0.0257	
				Total	Safe	Dang.				
				Failure rates						

Figure 3
FMEDA for **PES** input circuit

4 Markov Models for Reliability Analysis of PES [3]

Markov model (failure state diagram) is good tool in reliability analysis of **PES**, because the method is flexible and gives a realistic model. The method can include the following:

- common cause failures,
- multiple failures,
- different repair times and
- variable failure rates.

Markov model is a state diagram model with circles and arrows. The circles represent the component states (working or failed), the arrows stand for the direction of transitions between the states (failure or repair), so the arrows are directed arcs. The failure or repair rates are presented by the arrows with numeric values. A simple Markov model (one repairable component) is presented on Fig. 4.

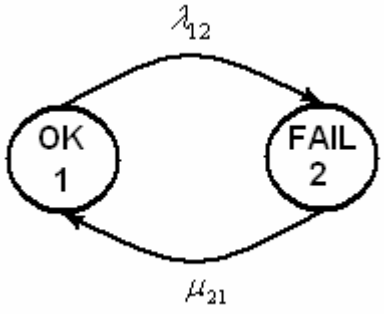

Figure 4
Markov model of repairable component

The component is in state 1, if it is successful, or in state 2, if it failed. The model can move from state 1 to state 2 at a rate of λ_{12} (the failure rate), or from state 2 to state 1 at μ_{21} (the repair rate).

5 Common Cause Failures [4]

Common cause failures are simultaneous outages of many components, caused by a single traumatic event (Fig. 5).

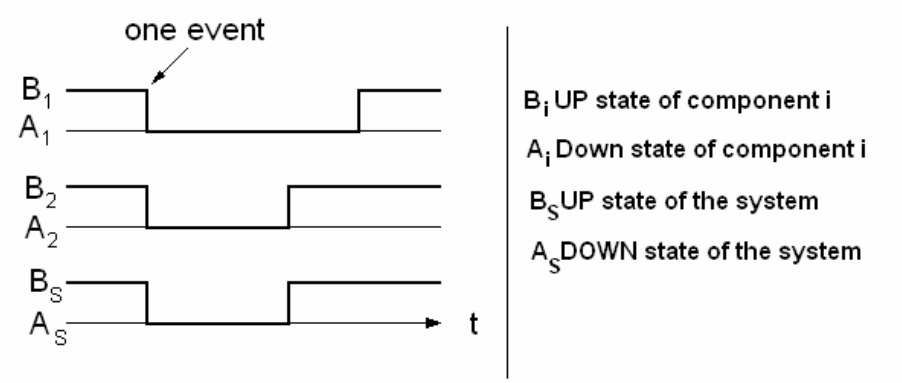

Figure 5
State-time diagram including common cause failures

The stochastic model for common cause failures will be derived from the state space of two stochastically independent components (Fig. 4). λ_1 and λ_2 are the outage rates of components 1 and 2, while μ_1 and μ_2 denote their repair rates. λ and μ are generally known as transition rates.

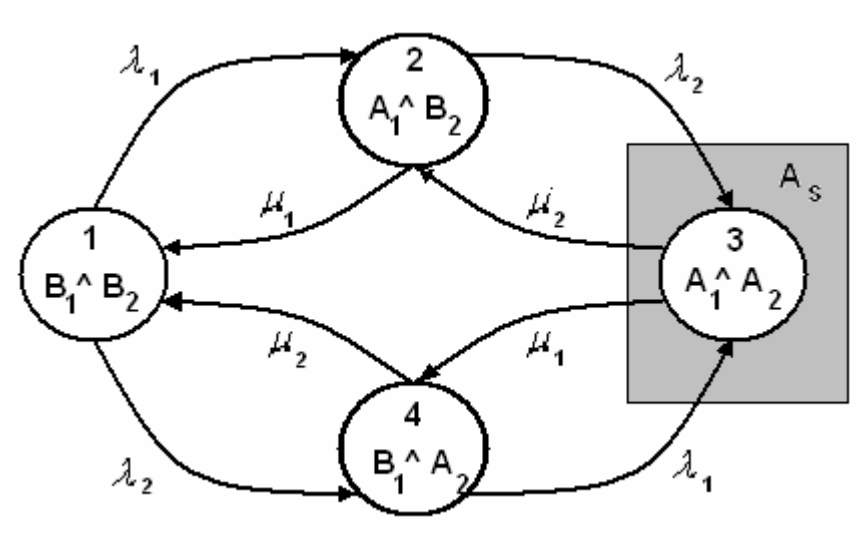

Figure 6
State-space of a system with two stochastically independent components

In the state space in Fig. 7, containing the possibility of the occurrence of common mode failures of two components, there is a direct transition from state 1 to 4, determined by the common cause outage rate. This rate is determined by the mean time $T(B_c)$ between two successive common cause outages:

$$\lambda_c = \frac{1}{T(B_c)} \tag{1}$$

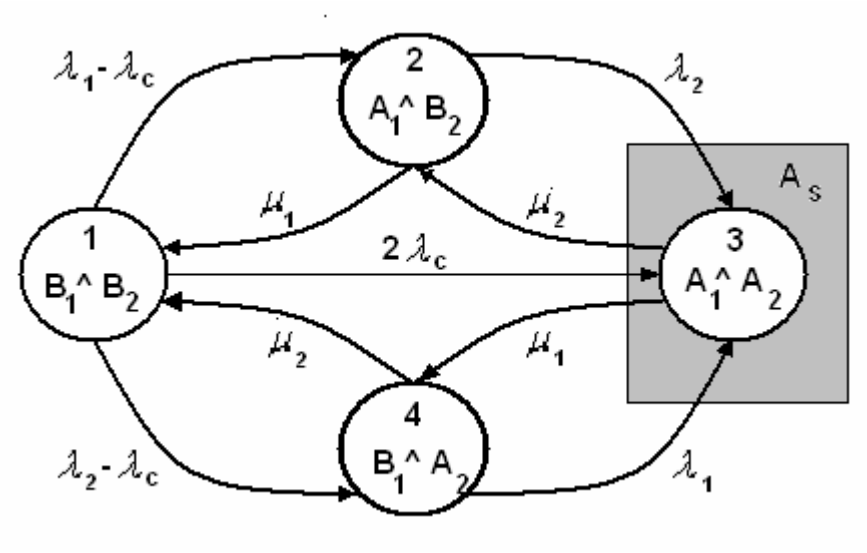

Figure 7
State-space of the system with two components including common cause outages

The rate λ_c (which will be further assumed as being equal for both components) is dependent on the system, in contrast to the component-specific rates λ_1 and λ_2, so it is system-specific.

According to Fig. 7, to determine the transition rates from state 1 to state 2 and 3, respectively, the outage rates λ_1 and λ_2 must be reduced by λ_c. The reason for this is that the outage rates λ_1 and λ_2 represent all the outages of the separately studied components. However, inside the system, some of them are single outages, while the rest are common cause outages. So, the sum of the transition rates for transitions starting from state 1 is equal to $\lambda_1 + \lambda_2$, just as in case of independent outages.

6 Limited Repair Capacities

The number of repair teams is not unlimited. Only one repair team will be considered here, therefore in double outages the repair of the component which failed second must be delayed until the completion of repair of the component which failed first (Fig. 8).

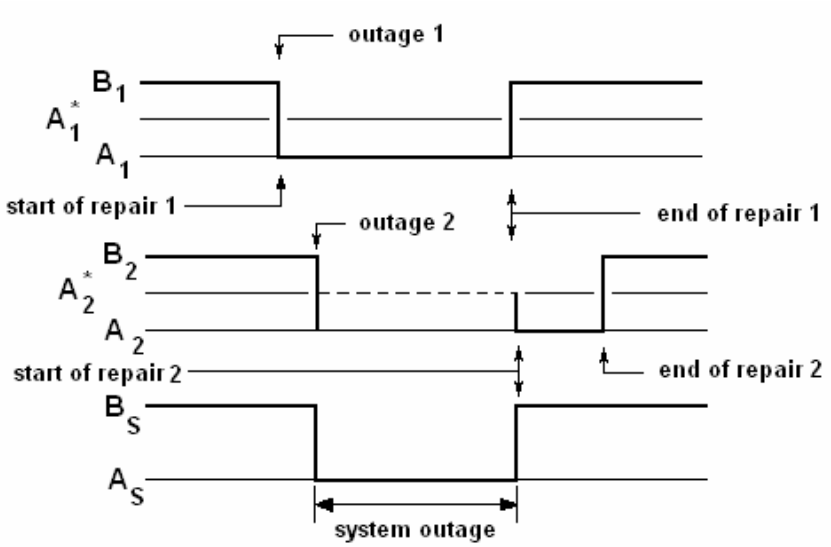

Figure 8
State-time diagram including repair postponability

The possibility for repair postponability results in an additional outage state $A*$ in the state pace of the component in Fig. 9. Starting from the operating state B, according to whether another component has failed first or not, there are two possible transitions, to states A and $A*$ respectively. Figure 10 shows the state space of a system consisting of two components when employing only one repair team.

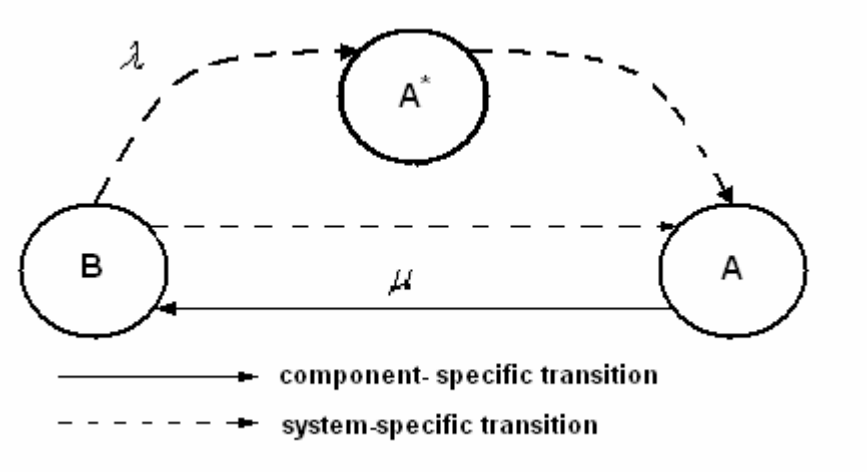

Figure 9
State-space of a single component including repair postponability

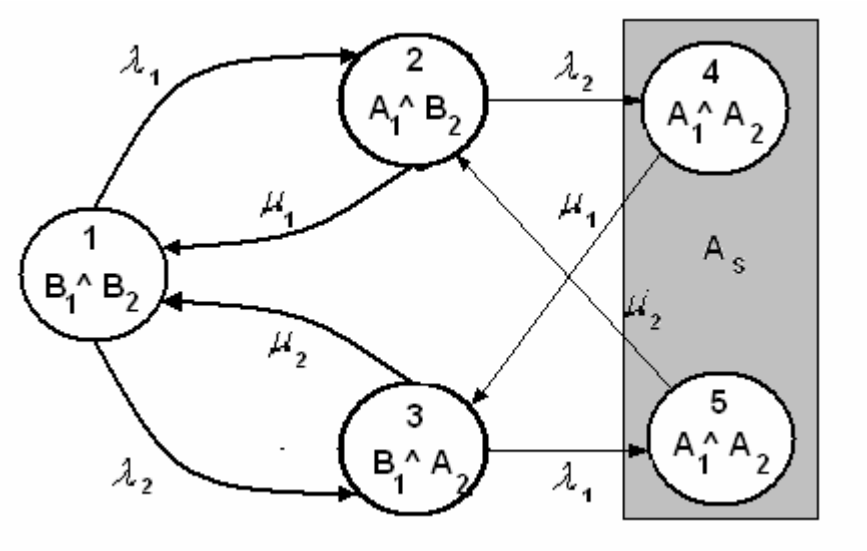

Figure 10
State-space for a system with only one repair team

7 PES Example with 4 Logic Parts [3]

There is a **PES** example in [3] in control electronics. The architecture of the system is given in Fig. 11, the Markov model for the system in Fig. 12 and Fig. 13.

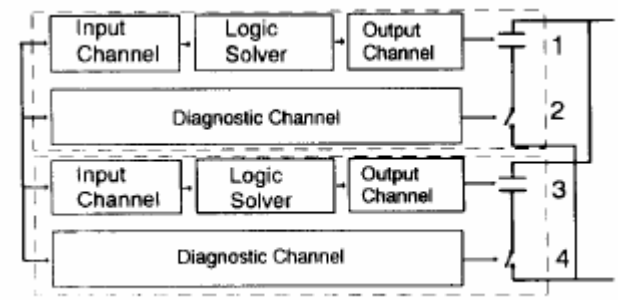

Figure 11
Two channel logic architectures

There are detected and undetected failures:

- λ^{SD}: safe, detected failures;
- λ^{SU}: safe, undetected failures;
- λ^{DD}: dangerous, detected failures;
- λ^{DU}: dangerous, undetected failures.

To properly account for common cause failures, each failure rate should be partitioned into normal and common cause. This result in eight failure rates for each physical set of channels in PES:

- λ^{SDN}: safe, detected normal stress failures;
- λ^{SUN}: safe, undetected normal stress failures;
- λ^{SDC}: safe, detected common cause failures;
- λ^{SUC}: safe, undetected common cause failures;
- λ^{DDN}: dangerous, detected normal stress failures;
- λ^{DUN}: dangerous, undetected normal stress failures;
- λ^{DDC}: dangerous, detected common cause failures;
- λ^{DUC}: dangerous, undetected common cause failures.

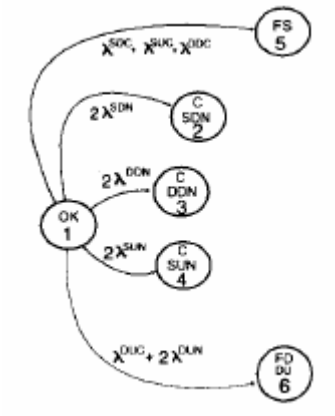

Figure 12

Markov model of **PES** (calculate-calculate mode)

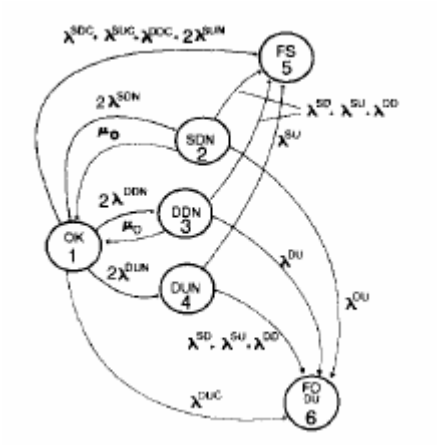

Figure 13
Markov model of **PES** (calculate-verify mode)

References

[1] Jorge Marcos, Luis Molinelli, Santiago Fernandez-Gomez, "Software-Aided Reliability Education", ASEE/IEEE Frontiers in Education Conference, TIC-18, October 10-13, 2001 Reno

[2] J. L. Roovroye, E. G. van den Bliek, "Comparing safety analysis techniques", Reliability Engineering and System Safety", 75 (2002) 289-294

[3] Julia V. Bukowski, Wiliam M. Goble, "Using Markov models for safety analysis of programmable electronic systems", Elsevier, Isa Transactions 34, 1995 pp. 193-198

[4] István Matijevics, Lajos Józsa, "An Expert-system-assisted Reliability Analysis of Electric Power Networks, Engng Applic. Artif. Intell. Vol. 8, No. 4, pp. 449-460, 1995

[5] William M. Goble, Julia V. Bukowski, A. C. Brombacher, "How diagnostic coverage improves safety in programmable electronic systems", Elsevier, Isa Transactions 36, pp. 345-350, 1998