Journal of Universal Computer Science, vol. 5, no. 10 (1999), 644-667
submitted: 15/4/99, accepted: 27/10/99, appeared: 28/10/99 © *Springer Pub. Co.*

Efficient Approximate Reliability Evaluation using the Markovian Minimal Cut Approach

Hans-Dieter Kochs
(Gerhard Mercator University Duisburg, Germany,
kochs@mti.uni-duisburg.de)

Holger Hilmer
(Gerhard Mercator University Duisburg, Germany,
hilmer@mti.uni-duisburg.de)

Thomas Nisbach
(Gerhard Mercator University Duisburg, Germany,
nisbach@mti.uni-duisburg.de)

Abstract: The Reliability analysis of information and automation systems has to cope with complex system structures and a large number of different components. Adapted to these requirements, the Markovian minimal cut approach has been developed. The Markovian minimal cut approach combines the advantages of two well-known approaches, the minimal cut and the Markovian path approach. The minimal cut approach allows the efficient evaluation of large scale systems. The Markovian path approach is able to model and evaluate real operation and outage behavior under realistic conditions. It includes outage and disconnection partitions, maintenance strategies (inspection, maintenance, repair), and operation and control strategies, which may lead to complicated stochastic dependencies. The Markovian minimal cut approach reduces the modelling and evaluation effort of real systems significantly because only a small number of Markovian states have to be modelled. In some applications the use of this approach first makes it possible to model and calculate the reliability of the system. The error of the approximations, induced by the Markovian path models have been proven to be less than 0.1% in practical systems. The approximations give the advantage of a result in an analytical context vs. pure computer-based numerical- or simulation-methods.

Key Words: Reliability of information and automation systems, System reliability, Markovian processes, Minimal cuts, Markovian minimal cuts.

1 Introduction

This contribution presents an efficient and easy to handle method for reliability calculation of complex systems while taking into account operational conditions. Information, computer, automation and control systems are complex systems. Systems having the following properties will be called *complex systems*:

- meshed system structures which occur when a component state lies in more than one path of a logical network (in a reliability block diagram), e.g. k-out-of-n, bridge and cross-structures;

- multi-stage components, e.g. operation, partial operation, outage and maintenance states (inspection, replacement, repair), as well as outage and shutdown partitions;
- stochastic dependencies between component states, e.g. common mode failure, maintenance strategies, automatic switch-off of partial systems due to the outage of components.

Additionally, real systems possess a large number of different components - in many cases more than thousand components, i.e. they are very large *and* complex systems.

Today following approaches for modelling and calculating system reliability are well known: Elementary probability theory [Singh (77)], minimal cut sets [Billinton (92)], Petri nets [Schneeweiss (99b)], Markovian processes [Billinton (92)], graph theory [Shooman (92)], fault tree analysis [Schneeweiss (99)] and reliability block diagrams [Kochs (84)]. These methods have some gaps: State space based methods (Markovian processes, Petri nets) are only suitable to model and calculate small systems because the number of system states increases exponentially with additional components. Therefore the number of system states 'explodes' and cannot be handled when modelling large systems. Otherwise stochastic component dependencies can easily be modelled by using state space based methods. Network methods (minimal cut sets, graph theory, fault trees, reliability block diagrams) are suitable to model and calculate large systems but the methods assume stochastic independencies between the components. Additionally only two-state component models are taken into account.

Thus for the reliability evaluation of large *and* complex systems the idea was adopted to combine already available approaches and make use of the advantages without getting the disadvantages. For this purpose the *Minimal cut approach* (for large scale systems) and the *Markovian path approach* (for stochastic dependencies between components) were enhanced to simple, user-friendly approaches and combined to the *Markovian minimal cut approach (MMCA).* In this paper a sample MMCA reliability analysis is illustrated on a typical, distributed industrial control system. Although the sample system is not very large and complex, it shows the practicability and advantages of this approach. Additionally, in order to demonstrate the accuracy of the approximations given by the Markovian path approach - used by MMCA - an error analysis is done in chapter 5, comparing a Markovian Path Approach (MPA) and an exact Markovian reliability calculation.

2 System analysis: Automation and control system

Figure 1 shows a typical automation and control system used in systems with high dependability constraints such as manufacturing engineering, power and process control systems. Systems of this type consist of a man machine interface (MMI) connected to a control computer (CC) which acquires data from the industrial process via a high-level industrial communication system (LAN). The process is connected to the communication system via process interfaces (PI). The process interfaces acquire data from sensors and drive the actuators, typical via a fieldbus system. The process data is stored in the process database which is located on a hard disk (HD) connected to the control computer. By this technique the operator can gain any input/output value of the process from the database and build up virtual instrumentation and control systems.

The system consists of a redundant control board (CB), a redundant local area network (LAN) and process interface components (PI). The coupling with the CC and the PI to the LAN takes place by means of LAN controllers (C) and transceivers (T).

During normal operation one of the control computers is the master computer. The other is a slave computer which is continually actualized by the master computer. Should the master computer suffer an outage then the slave computer immediately takes over without information losses or information duplication. For system operation at least one control computer must be in operation.

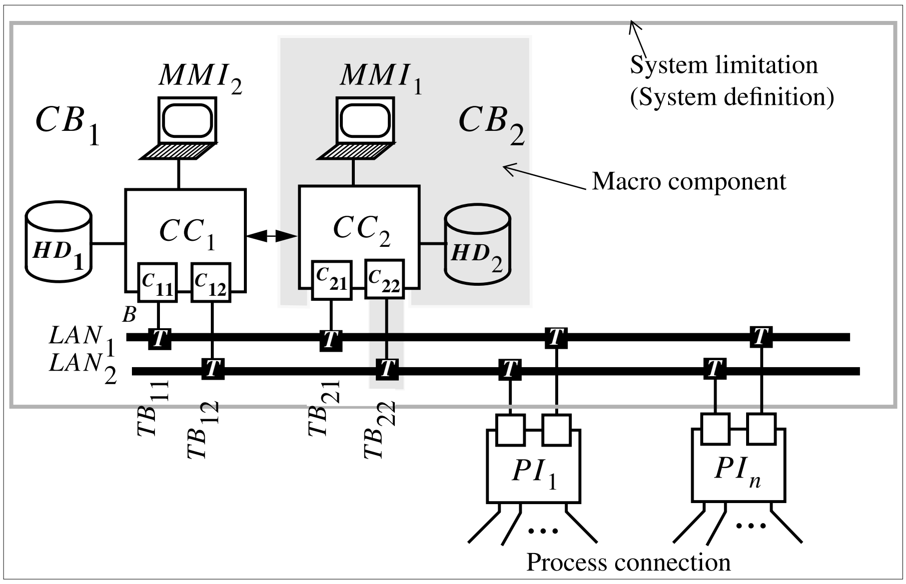

Figure 1: Central Automation and Control System

2.1 System states

Reliability statements (indices) are always related to *functions*, not to the system itself. The functions to be evaluated are defined by the system states: *system up state (system operation)* and *system down state (system outage)*.

Definition of the system up state U_S :

Monitoring, control and visualization of the process. For this at least the following components are necessary: a control computer (CC), the related hard disc (HD), the related visualization and control system (MMI) and a LAN connection.

Definition of the system down state D_S :

The system down state is the complement to system up state ($D_S = \overline{U}_S$).

For the reliability calculation of a system the definition of a number of system up and system down states are necessary. The aim of the system reliability analysis is to determine the complete set of reliability indices for U_S and D_S.

2.2 Fault Model

The system is operating in an organizational and technical framework. The environment of such a framework can have a powerful effect on reliability. All relevant properties influencing the reliability of the components and system (and their models) are therefore to be defined in the reliability analysis phase. The assumptions and constraints influencing component and system reliability are:

1) The components fail stochastically, indicated by the *outage rate* λ. In the case of transceivers and controllers the following outage properties influence the reliability:

   - Faults in the *transceiver* and *controller* can block the bus. A bus deadlock is practically the same as a bus outage. This is expressed by the probabilities b_T of a bus deadlock due to transceiver outage and b_C of a bus blockade due to controller outage:
     - amount of bus outage rate due to transceiver outage: $b_T \cdot \lambda_T$
     - amount of bus outage rate due to controller outage: $b_C \cdot \lambda_C$.

   The bus outage rates can be allocated to the LAN-bus outage rates:

   $$\lambda'_{LAN} = \lambda_{LAN} + n_{T/LAN} \cdot b_T \cdot \lambda_T + n_{C/LAN} \cdot b_C \cdot \lambda_C$$

   with $n_{T/LAN}$ the number of transceivers and $n_{C/LAN}$ the number of controllers per LAN.

- Faults in a *controller* can lead to outage or shut-down of the linked computer (also called computer deadlock). This is expressed by the probability r_C of a computer deadlock due to controller failure:

  - Amount of computer outage rate due to controller outage: $r_C \cdot \lambda_C$.
    This amount can be allocated to the outage rate of the computer:

$$\lambda'_{CC} = \lambda_{CC} + n_{C/CC} \cdot r_C \cdot \lambda_C$$

  with $n_{C/CC}$ being the number of controllers per control computer.

2) Components with the same effects on the system outage can be drawn together to macro components [Fig. 1]. Components are drawn together to macro components by adding together their outage rates. Macro components are treated like components.

3) After an outage the components are repaired by the repair rate. The total repair μ consists of:

   - Information and arrival of the service personnel, expressed by the arrival rate α,
   - Preparation, i.e. failure localization, failure diagnosis, acquisition of spare components, expressed by the preparation rate υ and
   - Replacement of the faulty component, expressed by the replacement rate τ.

4) When a controller is exchanged the linked computer has to be switched off, i.e this effect is the same as a computer outage.

5) Under the event of simultaneous outage of a number of components the component which failed first is repaired first before starting with the repair of the other components (practically given by the limited repair capacity). The failed components in a minimal cut are hereby repaired with first priority. After repair of the component which failed initially, only the preparation and exchange (not arrival of service personnel) are considered for the following faulty components.

6) If the system outage has occurred, all failed components of a minimal cut are repaired successively before system operation commences, i.e. the minimal cut is completely remedied.

These assumptions and constraints influence the component and system models, which partially entail stochastic dependencies between the component states, resulting in dependencies between the minimal cuts.

3 Component modelling

3.1 Component Reliability Parameter Estimation

For the component and system models transition rates are needed which are assumed to be constant. Constant transition rates can be calculated as reciprocal of the mean durations:

$$
\begin{aligned}
&T(U_i) : \text{mean operation time } (MTTF) \rightarrow \text{outage rate } \lambda_i = \frac{1}{T(U_i)} \\
&T(D_i) : \text{mean total repair time } (MTTR) \rightarrow \text{total repair rate } \mu_i = \frac{1}{T(D_i)}
\end{aligned}
\tag{1}
$$

According to assumption 3 the mean repair rate is split up into:

$$
\begin{aligned}
&T(D_{i,\alpha}) : \text{mean arrival time} \rightarrow \text{arrival rate } \alpha_i = \frac{1}{T(D_{i,\alpha})} \\
&T(D_{i,\upsilon}) : \text{mean preparation time} \rightarrow \text{preparation rate } \upsilon_i = \frac{1}{T(D_{i,\upsilon})} \\
&T(D_{i,\tau}) : \text{mean replacement time} \rightarrow \text{replacement rate } \tau_i = \frac{1}{T(D_{i,\tau})}
\end{aligned}
\tag{2}
$$

The component models can now be set up with the described assumptions, requirements and these indices. In principle, the values of the indices can be determined, but their acquisition and determination can cause difficulties. The uncertainty of the indices are not considered here. The *MTTF* values are determined by the producers of electronic modules and computers, e.g. according to MIL-HDBK-217F [DoD (91)], the *MTTR* values are determined according to the repair and maintenance strategies of the user.

3.2 General component model

Figure 2 shows the general model of a component. According to assumption 3 the component down-state consists of a sequence of outage states. The differentiation of the outage state is necessary in the case of simultaneous outages of two or more components (according to assumption 5) although the effects of the states are identical. The state $D_{i,y}$ is necessary to be able to reflect the assumption 6 in the system model. The probability distribution resulting from the addition of the three exponential distributions theoretically is not exponential but approximated by an exponential distribution. The mean value is not affected by this approximation.

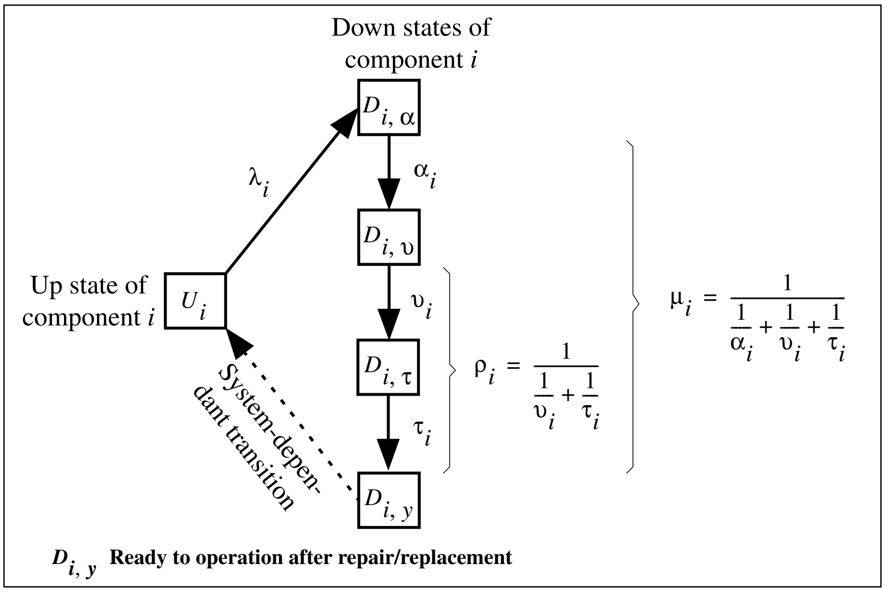

Figure 2: General Model of Components (excluding controllers)

According to assumption 1 the following *extended outage rates* are set for the outage rate λ_i in figure 2:

- control computer (*CC*): $\lambda'_{CC} = \lambda_{CC} + n_{C/CC} \cdot r_C \cdot \lambda_C$ (3)
- local area network (*LAN*): $\lambda'_{LAN} = \lambda_{LAN} + n_{T/LAN} \cdot b_T \cdot \lambda_T + n_{C/LAN} \cdot b_C \cdot \lambda_C$
- transceiver (*T*): $\lambda'_T = (1 - b_T) \cdot \lambda_T$

For simplification of the system model the following macro components CB and TB are formed according to assumption 2:

- control board (*CB*): $\lambda'_{CB} = \lambda'_{CC} + \lambda_{MMI} + \lambda_{HD}$
- transceiver bus connection (*TB*): $\lambda'_{TB} = \lambda'_T + \lambda_B$

(4)

3.3 Component model for a controller

An exception to the general component model is the controller [Fig. 3] whose outage leads to computer outage (switched off) according to assumption 4.

The parts of the controller outage leading to a blockade of the adjoined computer (immediate outage/shutdown of CC) and to bus blockade (immediate outage/deadlock of LAN, left side of figure 3) are modelled according to figure 2. The right side of figure

3 considers that part of the controller outage for which the computer shutdown can be arranged. This part is called single outage of the controller with postponable computer shut down $D_{C,\,\dots} \rightarrow S_{CC}$. Computer shutdown is postponed if this prevents a system outage (see system model in the following chapter).

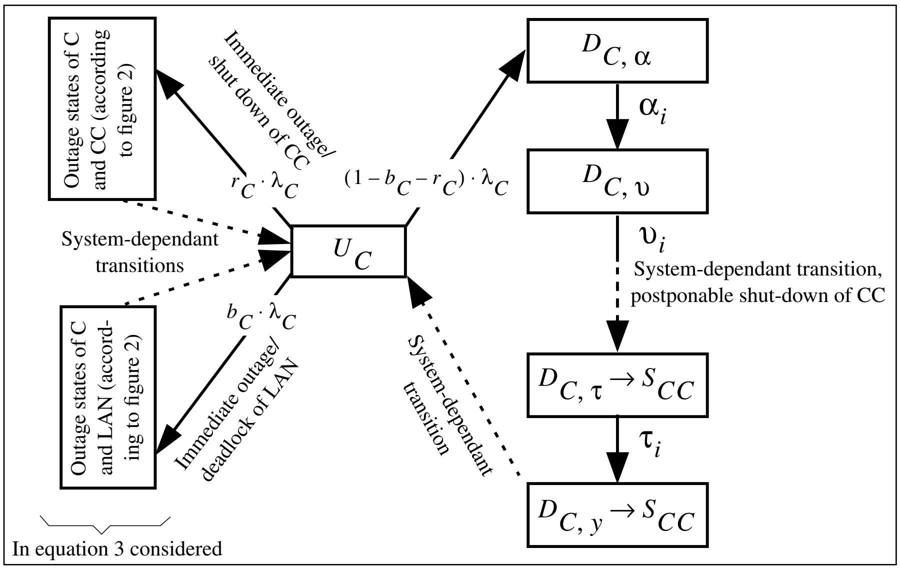

Figure 3: Component Model of a Controller with Influence/Dependencies to other Components

4 System modelling and calculation

The Markovian minimal cut approach comprises the following main steps [Fig. 7]: Determination of relevant minimal cut sets and modelling of the minimal cuts by Markovian path approach. After this the results are put together to calculate the system reliability indices.

4.1 Minimal cuts

Minimal cuts are determined directly from the functional structure in figure 1. All minimal cuts are listed in table 1. Altogether 78 single minimal cuts of the 2., 3. and 4. order occur containing the *complete logical operation and outage structure*. The next task is to determine the probabilities *P(M)* and the mean frequencies *F(M)* of each minimal cut needed for the calculation of the system indices.

Minimal cut types	Number
$M_1 = D_{CB} \wedge D_{CB}$	1
$M_2 = D_{LAN} \wedge D_{LAN}$	1
$M_3 = D_{CB} \wedge [D_C \rightarrow S_{CB}]$	4
Minimal cuts of higher order	
$M_4 = D_{CB} \wedge D_C \wedge D_C$	2
$M_5 = D_{CB} \wedge D_{TB} \wedge D_C$	4
$M_6 = D_{CB} \wedge D_{LAN} \wedge D_C$	4
$M_7 = D_{CB} \wedge D_{TB} \wedge D_{TB}$	2
$M_8 = D_{CB} \wedge D_{LAN} \wedge D_{TB}$	4
$M_9 = [D_C \rightarrow S_{CB}] \wedge D_C \wedge D_C$	4
$M_{10} = [D_C \rightarrow S_{CB}] \wedge D_{TB} \wedge D_C$	8
$M_{11} = [D_C \rightarrow S_{CB}] \wedge D_{LAN} \wedge D_C$	8
$M_{12} = [D_C \rightarrow S_{CB}] \wedge D_{TB} \wedge D_{TB}$	4
$M_{13} = [D_C \rightarrow S_{CB}] \wedge D_{LAN} \wedge D_{TB}$	8
$M_{14} = D_{LAN} \wedge D_C \wedge D_C$	2
$M_{15} = D_{LAN} \wedge D_{TB} \wedge D_C$	4
$M_{16} = D_{LAN} \wedge D_{TB} \wedge D_{TB}$	2
$M_{17} = D_C \wedge D_C \wedge D_C \wedge D_C$	1
$M_{18} = D_{TB} \wedge D_C \wedge D_C \wedge D_C$	4
$M_{19} = D_{TB} \wedge D_{TB} \wedge D_C \wedge D_C$	6
$M_{20} = D_{TB} \wedge D_{TB} \wedge D_{TB} \wedge D_C$	4
$M_{21} = D_{TB} \wedge D_{TB} \wedge D_{TB} \wedge D_{TB}$	1

Table 1: Minimal Cuts

4.2 The Markovian path approach

The **analytical** evaluation of Markovian processes can be very sophisticated, if not impossible. There are programs which can calculate Markovian processes numerically; however due to their transparency, practicability (user friendliness) and their flexibility analytical solutions are to be preferred. Analytical results also allow further processing (e.g. importance analyses, uncertainty indices, fuzzy indices).

Another problem we have to face is the fact - as this little example demonstrates - that large scale and complex (as a rule real) systems cannot be modelled completely, so that computing programs are of no aid here. They are not applicable for such systems. The *Markovian path approach* offers the possibility to determine (and model) only the few paths responsible for system reliability (without having to model the totality of all the states in a system). The probable paths can be calculated in a simple manner (in a decoupled mode) independently of each other.

4.2.1 Basics of the Markovian path approach

The principle of the approach is presented in the partial view of the Markovian process in figure 4. In each technical system there is one (or more) operational state, e.g. Z_1 which should be disrupted at least as possible, and there are outage states which rarely occur. For $\lambda \ll \mu$ the following relation is valid

$$P(Z_1) \gg \sum_{\forall i \neq 1} P(Z_i) \qquad \text{i.e.} \qquad P(Z_1) \approx 1 \tag{5}$$

Z_1 is the initial state from which all *probable transitions* to the (to be calculated) target state Z_k are determined. All probable transitions chained together constitute the *probable path.* The probable path is the direct path into the target state without diversions or loops. If more than one target state occurs there exists naturally more than one probable path. In a target state or a state along a probable path other probable paths can open up. The probable path is marked in figure 4 by bold arrows. Thus paths are decoupled from the initial states into the target states. The goal is the evaluation of the reliability indices of the target state Z_k. Starting at the initial state Z_1 the indices *probability, mean frequency* and *mean time* of each state along the probable path are evaluated until the target state is reached. For the evaluation of the indices of one state only the previous adjacent states (due to Markovian process) under consideration of the transitions from and to the target state have to be taken into account.

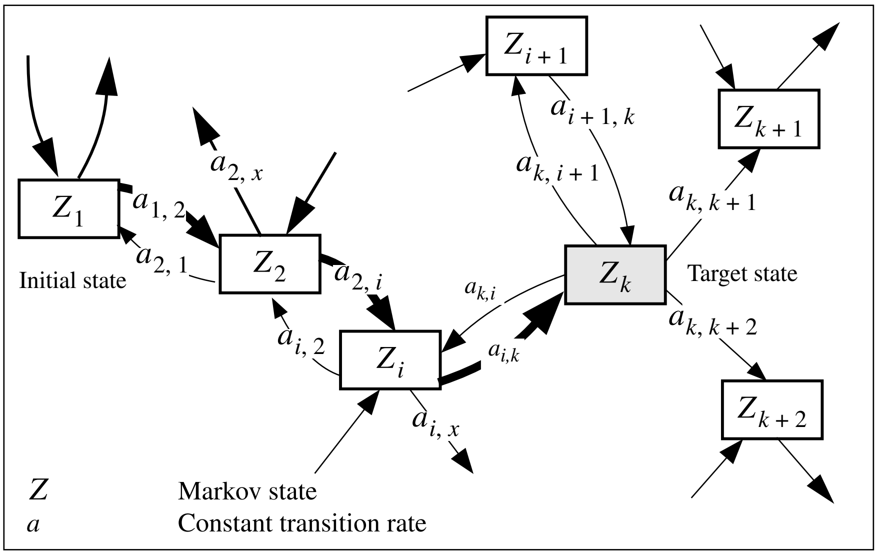

Figure 4: Part of a Markov Process with Probable (Direct) Transitions from the Initial State to the Target State Z_k

The mathematical foundation is derived from the well-known steady-state Markovian equation (6) where $\bar{P}$ is the steady-state vector and $\bar{A}$ is the transition matrix:

$$\bar{\mathbf{0}}^{\mathrm{T}} = \bar{\boldsymbol{P}}^{\mathrm{T}} \cdot \bar{\boldsymbol{A}} = \begin{bmatrix} P(Z_1) \\ \vdots \\ P(Z_n) \end{bmatrix}^{\mathrm{T}} \cdot \begin{bmatrix} -a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & -a_{n,n} \end{bmatrix} \tag{6}$$

The diagonal elements of a Markovian transition matrix are given by

$$a_{k,k} = \sum_{i \neq k} a_{k,i} \tag{7}$$

Equation (6) can be expressed for a single state Z_k as:

$$0 = \sum_{i \neq k} P(Z_i) \cdot a_{i,k} - P(Z_k) \sum_{i \neq k} a_{k,i} \tag{8}$$

Equation (8) can be interpreted in the following way: The inflow to Z_k (left term) and the outlet (right term) are equal for the steady-state (equilibrium). With equation (7) the probability of Z_k can be calculated from (8) as:

$$P(Z_k) = \frac{1}{a_{k,k}} \sum_{i \neq k} P(Z_i) \cdot a_{i,k} \tag{9}$$

The mean duration of Z_k is the reciprocal value of the diagonal transition rate

$$T(Z_k) = \frac{1}{a_{k,k}} \tag{10}$$

With (9) and (10) the mean frequency of Z_k is calculated as quotient

$$F(Z_k) = \frac{P(Z_k)}{T(Z_k)} = \sum_{i \neq k} P(Z_i) \cdot a_{i,k} \tag{11}$$

One can therefore pass through from the initial state Z_1 - which probability is known due to approximation (5) - to the target state(s) Z_k by evaluating the set of these indices along the probable path(s) (**pp**). For practical applications the triple set of reliability indices can be combined in the general form:

$$
\begin{aligned}
F(Z_k) &= \sum_{pp(i \to k)} P(Z_i) \cdot a_{i,k} \\
T(Z_k) &= \frac{1}{a_{k,k}} \\
P(Z_k) = F(Z_k)T(Z_k) &= \sum_{pp(i \to k)} P(Z_i) \cdot a_{i,k} \cdot \frac{1}{a_{k,k}}
\end{aligned}
\tag{12}
$$

The notation $pp(i \to k)$ means that only the transitions along the probable path have to be considered. By considering all states of the model and not only those along the probability path, the Markovian process state-probabilities can be calculated exactly. There is, however, one difficulty for this exact calculation. The probability $P(Z_1)$ at the start of the evaluation is unknown. Through the approximation $P(Z_1) \approx 1$ made at the beginning (5) the probable path can be calculated as an approximation. The following formation rule can be developed from the triple set of indices (12).

Formation rule for the determination of the reliability indices of the target state $Z = Z_{\text{target}}$ along the probable path

- The mean frequency $F(Z_{\text{target}})$ is calculated as the product of the transition rates along the probable path divided by the sum of the transition rates leading away from the states (except for Z_{target}).

- The probability is calculated as $P(Z_{\text{target}}) = F(Z_{\text{target}})T(Z_{\text{target}})$ whereby the mean duration $T(Z_{\text{target}})$ is the reciprocal value of the sum of the transition rates leading away from the state Z_{target}.

The indices for the state Z_k in figure 4 are determined according to this rule.

$$
\begin{aligned}
&Z_1 \to Z_2 \to Z_i \to Z_k \\
&F(Z_k) \approx \frac{a_{1,2}}{a_{2,1} + a_{2,i} + a_{2,x}} \cdot \frac{a_{2,i}}{a_{i,2} + a_{i,k} + a_{i,x}} \cdot a_{i,k} \\
&T(Z_k) = \frac{1}{a_{k,i} + a_{k,i+1} + a_{k,k+1} + a_{k,k+2}} \\
&P(Z_k) = F(Z_k)T(Z_k)
\end{aligned}
\tag{13}
$$

Generally these approximations are sufficiently accurate for real applications ($\lambda \ll \mu$). With equations (12) one can design a numerical algorithm to evaluate the indices iteratively.

4.3 Minimal cut indices

The minimal cuts of the sample system [Fig. 1] are modelled and calculated using the Markovian minimal cut approach. The figures 5 and 6 show sample Markovian minimal cuts. All minimal cuts can be modelled in an analog way.

Markovian minimal cut model for minimal cut type $D_i \wedge D_j$ [Fig. 5]

The Markovian minimal cut model is designed by a combination of two component models from figure 2. It contains all probable paths into the minimal cut type $D_i \wedge D_j$ which are needed for the calculation of the minimal cuts M_1 and M_2 [Tab. 1]. There are two paths into this minimal cut type whereby it is just necessary to develop one path as the other one is symmetrical. Due to outage of component i Z_1 is passed over to Z_2 and according to assumption 3 component i is repaired with μ_i. If component j in Z_2 fails then a transition to the state Z_3 occurs which represents a state in the minimal cut being searched for. The repair of component j according to assumption 5 is first started when component i has been repaired. The arrival time (depending on the application also the preparation time) has not to be considered as the service personnel is already at the location. One therefore assumes that component j can be repaired with ρ_j. ρ_j represents the combination of υ_j and τ_j according to figure 2. Only when both components are ready for operation the system starts in operation mode according to assumption 6, i.e. the minimal cut is deleted. Following the formation rules for the determination of indices (12) the probable path approach for the states Z_3 and Z_4 provides the following probabilities (whereby in the denominator due to $\lambda \ll \mu$ the outage rate λ can be neglected)

$$\text{Probable Path: } Z_1 \rightarrow Z_2 \rightarrow Z_3 \rightarrow Z_4$$

$$\underbrace{\underbrace{\frac{\lambda_i}{\mu_i + \lambda_j} \cdot \frac{\lambda_j}{\mu_i}}_{P(Z_3)} \cdot \frac{\mu_i}{\rho_j}}_{P(Z_4)} \tag{14}$$

The indices of the minimal cuts are the result of the application of the Markovian minimal cut approach

$$P(D_i \wedge D_j) = P([Z_3 \vee Z_4]_{Path1 + Path2}) \approx \frac{\lambda_i\lambda_j}{\mu_i}\left(\frac{1}{\mu_i} + \frac{1}{\rho_j}\right) + \frac{\lambda_i\lambda_j}{\mu_j}\left(\frac{1}{\mu_j} + \frac{1}{\rho_i}\right)$$
$$F(D_i \wedge D_j) = F([Z_3]_{Path1 + Path2}) \approx \frac{\lambda_i\lambda_j}{\mu_i} + \frac{\lambda_i\lambda_j}{\mu_j} \quad (15)$$

When calculating the mean frequency the transitions of $Z_3 \rightarrow Z_4$ within the Markovian states are not to be considered.

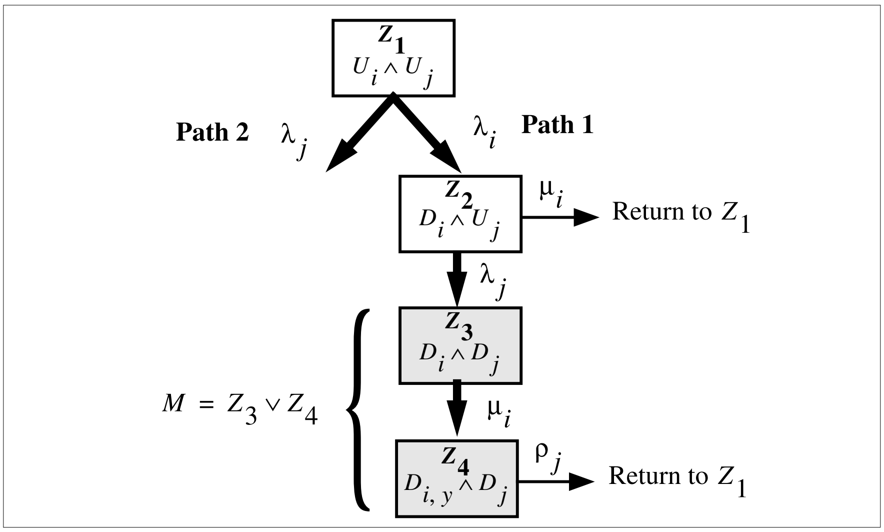

Figure 5: Modelling of the Minimal Cut Type: $M = D_i \wedge D_j$

Markovian minimal cut model for minimal cut type $D_i \wedge [D_C \rightarrow S_{CB}]$ [Fig. 6]

For the Markovian minimal cut model the component models for component i and C in figure 2 and figure 3 are combined. Starting from Z_1 there is only one probable path into the minimal cut. A shutdown of the computer, i.e. transition from Z_3 to Z_4 only occurs when component i has not failed or, in other words, fails component i in Z_3 then computer shutdown is delayed which means that the transition to Z_4 does not occur and thus a minimal cut does not occur. However, if Z_4 is realized then component i can fail and cause a minimal cut. The indices of the minimal cut are (λ_i neglected in the denominator)

$$P(D_i \wedge [D_C \rightarrow S_{CB}]) = P(Z_5 \vee Z_6) \approx \frac{(1 - b_C - r_C)\lambda_C\lambda_i}{\tau_C}\left(\frac{1}{\tau_C} + \frac{1}{\rho_i}\right)$$
$$F(D_i \wedge [D_C \rightarrow S_{CB}]) = F(Z_5) \approx \frac{(1 - b_C - r_C)\lambda_C\lambda_i}{\tau_C} \quad (16)$$

The examples demonstrate how simple the modelling and calculation of the minimal-cuts is using the above presented approach, and how difficult - if not impossible - a complete modelling of the Markovian process would be.

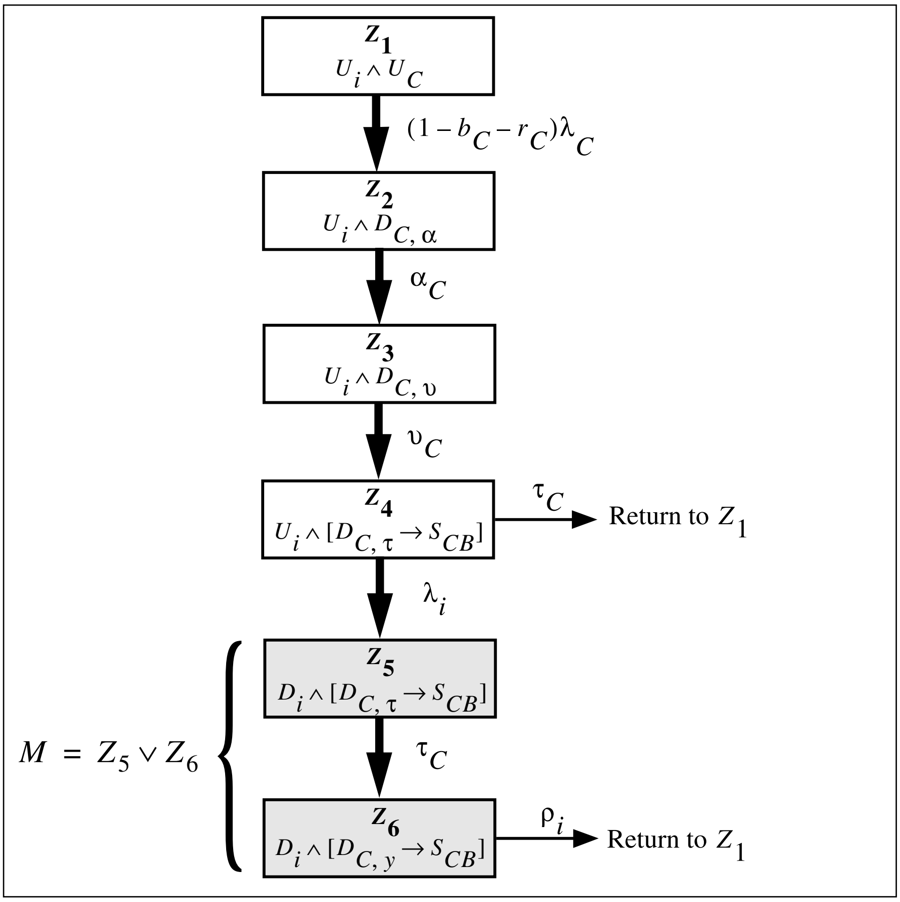

Figure 6: Modelling of Minimal Cut Type: $M = D_i \wedge [D_C \rightarrow S_{CB}]$

4.4 System indices

To calculate the probability $P(D_S)$ and the frequency $F(D_S)$ of system-outage D_S, the disjunction of all minimal cuts has to be calculated:

$$P(D_S) = P(\bigvee_{\forall i} M_i) = \sum_{\forall i} P(M_i) - \sum_{\substack{\forall i,j \\ i<j}} P(M_i \wedge M_j) + \ldots$$
$$F(D_S) = F(\bigvee_{\forall i} M_i) = \sum_{\forall i} F(M_i) - \sum_{\substack{\forall i,j \\ i<j}} F(M_i \wedge M_j) + \ldots \qquad (17)$$

Equation (17) cannot be solved easily because of the large amount of minimal cut combinations. With the exact calculated probabilities of all minimal cuts an upper limit can be written as (a lower limit too, but not considered here):

$$P(D_S) \le \sum_{\forall i} P(M_i) \quad ; \quad F(D_S) \le \sum_{\forall i} F(M_i) \tag{18}$$

Notice: Although equations (17) and (18) are well-known for system-reliability evaluation with stochastic-independent components, these equations are exactly valid too in the case of stochastic-dependent components. However in that case, the equations (even(18)) normally are incalculable, because the minimal cuts are dependent on each other which will lead to very complex expressions.

By calculating the minimal cut sets independently from each other (in other words: neglecting stochastically dependencies *between* the minimal cuts of realistic systems - not between the components *inside* minimal cuts M_i!), one can give an approximation for the system outage-probability as written in (19).

$$P(D_S) \approx \sum_{\forall i} P(M_i) \quad ; \quad F(D_S) \approx \sum_{\forall i} F(M_i) \tag{19}$$

In practical systems the number of minimal cuts can increase enormously, e.g. 100.000. If so, only the minimal cuts of lowest order are considered. This can be done because the influence of higher-order minimal cuts are very small under the condition of $\lambda \ll \mu$ (found in real systems). Therefore we get easier to calculate approximations for the system indices as:

$$P(D_S) \approx \sum_{\substack{\forall i \in \\ M \text{ of lowest order}}} P(M_i) \quad ; \quad F(D_S) \approx \sum_{\substack{\forall i \in \\ M \text{ of lowest order}}} F(M_i) \tag{20}$$

The system indices are simply determined as the sum of the lowest order minimal cut indices. The reliability of the sample system in figure 1 is therefore only determined by the 2. order minimal cuts [Tab. 1]. The relevant minimal cuts and the system indices for the sample system are presented in table 2.

The indices for the whole system and the communication system (grey shaded sector) are calculated separately. In particular minimal cuts affecting communication components are counted to the communication system. This also includes minimal cuts containing additional computer components. This means that the reliability of the communication system is affected by non-communication components also.

Table 2 shows the results of the reliability evaluation by using the Markovian Minimal Cut Approach (MMCA) (upper part) and the Minimal Cut Approach (MCA) (lower part). The base outage indices of the components are typical values, available from computer manufacturers. Repair rates are typical values depending on the operators of the automation control system. In the MMCA the described stochastic dependencies and computer shutdowns due to controller outage are considered. In the MCA these effects are neglected, thus the probabilities of the minimal cuts are calculated by simple multiplication of the component outage probabilities, e.g.

$$P(D_{CB}) = \lambda_{CB}/(\lambda_{CB} + \mu_{CB}) \approx \lambda_{CB}/\mu_{CB} \Rightarrow P(D_{CB} \wedge D_{CB}) = P(D_{CB})^2 = \lambda^2_{CB}/\mu^2_{CB}$$

The frequencies are calculated in an equivalent manner. The MMCA yields a probability of $P(D_S) = 2,4 \cdot 10^{-6}$ for the total system down state and $P(D_{Com}) = 2,5 \cdot 10^{-8}$ for the communication system down state, whereas the MCA only yields $P(D_S) = 1 \cdot 10^{-6}$ for the total system down state and $P(D_{Com}) = 1 \cdot 10^{-10}$ for the communication system down state. The MCA overstates the reliability by factors of 2,4 respectively 250. Conclusion: The neglect of real world conditions like stochastic component dependencies or shut down areas gives too optimistic (wrong) results in reliability calculation. The MMCA is capable to consider real world conditions with minimal effort in reliability modelling.

Reliability calculation by MMCA

M_i		$P(M_i)$		$F(M_i)/h^{-1}$	
$D_{CB} \wedge D_{CB}$	1	$2\frac{\lambda'^2_{CB}}{\mu_{CB}}\left(\frac{1}{\mu_{CB}} + \frac{1}{\rho_{CB}}\right)$	$2,4 \cdot 10^{-6}$	$2\frac{\lambda'^2_{CB}}{\mu_{CB}}$	$2,0 \cdot 10^{-7}$
$D_{LAN} \wedge D_{LAN}$	1	$2\frac{\lambda'^2_{LAN}}{\mu_{LAN}}\left(\frac{1}{\mu_{LAN}} + \frac{1}{\rho_{LAN}}\right)$	$2,4 \cdot 10^{-8}$	$2\frac{\lambda'^2_{LAN}}{\mu_{LAN}}$	$2,0 \cdot 10^{-9}$
$D_{CB} \wedge [D_C \rightarrow S_{CB}]$	4	$\frac{(1 - b_C - r_C)\lambda_C\lambda'_{CB}}{\tau_C}\left(\frac{1}{\tau_C} + \frac{1}{\rho_{CB}}\right)$	$1,1 \cdot 10^{-9}$	$\frac{(1 - b_C - r_C)\lambda_C\lambda'_{CB}}{\tau_C}$	$4,5 \cdot 10^{-10}$
Total system		$P(D_S)$:	$2,4 \cdot 10^{-6}$	$F(D_S)/h^{-1}$:	$2,0 \cdot 10^{-7}$
Communication system only		$P(D_{Com})$:	$2,5 \cdot 10^{-8}$		$2,5 \cdot 10^{-9}$

Reliability calculation by MCA

M_i		$P(M_i)$		$F(M_i)/h^{-1}$	
$D_{CB} \wedge D_{CB}$	1	$\frac{\lambda^2_{CB}}{\mu^2_{CB}}$	$1,0 \cdot 10^{-6}$	$\frac{\lambda^2_{CB}}{\mu_{CB}}$	$1,0 \cdot 10^{-7}$
$D_{LAN} \wedge D_{LAN}$	1	$\frac{\lambda^2_{LAN}}{\mu^2_{LAN}}$	$1,0 \cdot 10^{-10}$	$\frac{\lambda^2_{LAN}}{\mu_{LAN}}$	$1,0 \cdot 10^{-11}$
Total system		$P(D_S)$:	$1,0 \cdot 10^{-6}$	$F(D_S)/h^{-1}$:	$1,0 \cdot 10^{-7}$
Communication system only		$P(D_{Com})$:	$1,0 \cdot 10^{-10}$		$1,0 \cdot 10^{-11}$

Base indices: $\lambda'_{CB} = 10^{-4}h^{-1}$ $\lambda_C = 10^{-5}h^{-1}$ $\lambda_{LAN} = 10^{-6}h^{-1}$ $\lambda'_{LAN} = 10^{-5}h^{-1}$
$r_C = 0,05$ $b_C = 0,05$ $\mu = 0,1h^{-1}$ $\tau = 2h^{-1}$ $\rho = 0,5h^{-1}$

Table 2: System Calculation and Comparison of MCA and MMCA Results

4.5 Summary of Markovian minimal cut approach

An overview of the steps of the Markovian minimal cut approach is given in figure 7:

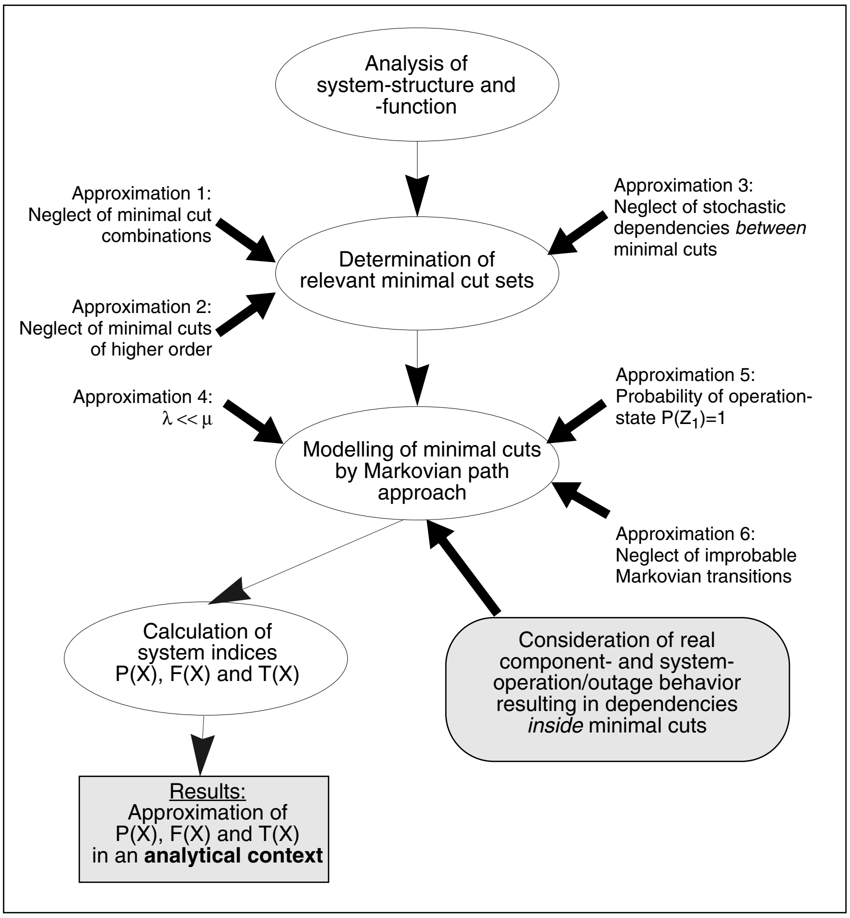

Figure 7: Overview on Markovian Minimal Cut Approach with Approximation Steps

The advantages of this method are:

- Realistic modelling of multi-stage components (e.g. components with several up- and down-states due to real operation and maintenance conditions)
- Realistic modelling of component dependencies (e.g. common-mode failures, maintenance strategies, partial shut down areas, limited repair capacities)
- Significant model reduction, that means reduction of states and transitions in the Markovian model using Markovian path approach

- Results are in an analytical context and can be used in further analytical methods (e.g. importance analysis, uncertainty-analysis)

5 Error analysis of the Markovian path approach

The error ΔP_i between the results of the Markovian path approach and the exact Markovian approach shall be calculated exemplarily. The procedure is based on a typical 2. order minimal cut with dependencies due to common mode failures and limited repair capacity (first failed component is repaired first) [Fig. 8]. Systems pertaining to such minimal cuts are often found within complex systems. In this example the factors $p_{c_{j,i}}$ and $p_{c_{j,i}}$ can be varied between $0\ldots1$ (no dependency....strong dependency).

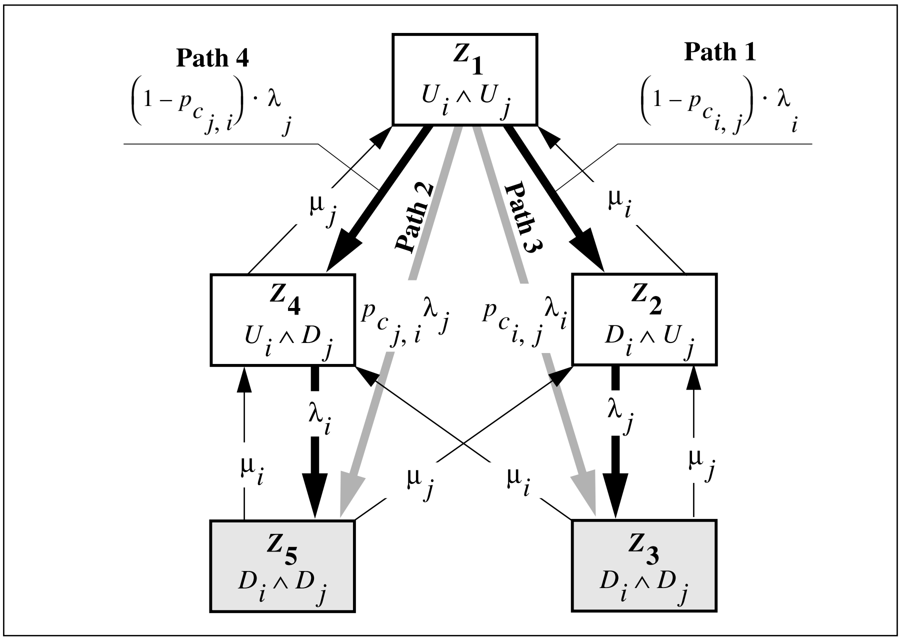

Figure 8: Modelling of the Minimal Cut Type 2. Order: $D_i \wedge D_j$ (Markov Minimal Cut Model 2. Order)

Abbreviation: $P_i := P(Z_i)$. Diagonal elements: $a_{1,1} = \lambda_i + \lambda_j$, $a_{2,2} = \mu_i + \lambda_j$, $a_{3,3} = \mu_i + \mu_j$, $a_{4,4} = \lambda_i + \mu_j$, $a_{5,5} = \mu_i + \mu_j$. Assumption: $\lambda \ll \mu$.

The Markovian equations of the Markov model in figure 8 can be written with the secondary condition $\sum_{\forall i} P_i = 1$ (first column) as

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}^T = \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{bmatrix}^T \cdot \begin{bmatrix} 1 & \frac{\left(1 - p_{c_{i,j}}\right)\lambda_i}{a_{2,2}} & \frac{p_{c_{i,j}}\lambda_i}{a_{3,3}} & \frac{\left(1 - p_{c_{j,i}}\right)\lambda_j}{a_{4,4}} & \frac{p_{c_{j,i}}\lambda_j}{a_{5,5}} \\ 1 & -1 & \frac{\lambda_j}{a_{3,3}} & 0 & 0 \\ 1 & \frac{\mu_j}{a_{2,2}} & -1 & \frac{\mu_i}{a_{4,4}} & 0 \\ 1 & 0 & 0 & -1 & \frac{\lambda_i}{a_{5,5}} \\ 1 & \frac{\mu_j}{a_{2,2}} & 0 & \frac{\mu_i}{a_{4,4}} & -1 \end{bmatrix} \tag{21}$$

All elements of the transition matrix are less or equal 1, which is advantageous for the computation. Splitting the transmission matrix in submatrices the Markovian equations (21) can be written in the general form

$$\begin{bmatrix} 1 \\ \mathbf{0} \end{bmatrix}^T = \begin{bmatrix} P_1 \\ \bar{\boldsymbol{P}} \end{bmatrix}^T \cdot \begin{bmatrix} 1 & \bar{\boldsymbol{A}}_{\mathbf{1}} \\ \mathbf{1} & \bar{\boldsymbol{A}} \end{bmatrix} \tag{22}$$

The solution of this matrix equation yield

$$1 = P_1 + \bar{\boldsymbol{P}}^{\boldsymbol{T}}\mathbf{1} = P_1 + \sum_{i>1} P_i \tag{23}$$

$$\mathbf{0}^T = P_1 \bar{\boldsymbol{A}}_{\mathbf{1}} + \bar{\boldsymbol{P}}^{\boldsymbol{T}} \bar{\boldsymbol{A}} \tag{24}$$

P_1 from (23) is inserted in (24)

$$\mathbf{0}^T = \left(1 - \sum_{i>1} P_i\right) \bar{\boldsymbol{A}}_{\mathbf{1}} + \bar{\boldsymbol{P}}^{\boldsymbol{T}} \bar{\boldsymbol{A}} \tag{25}$$

The submatrices have the features: $\left\|\bar{\boldsymbol{A}}_{\mathbf{1}}\right\| \ll 1$, $\sum_{i>1} P_i \ll 1$ or $\left\|\bar{\boldsymbol{P}}^{\boldsymbol{T}}\right\| \ll 1$ and $\left\|\bar{\boldsymbol{A}}\right\| \geq 1$

(in other words: This error calculation is only valid with these features). Therefore the expression $\left(\sum_{i>1} P_i\right)\bar{\boldsymbol{A}}_{\boldsymbol{1}}$ in (25) is negligible

$$\boldsymbol{0}^T \approx \bar{\boldsymbol{A}}_{\boldsymbol{1}} + \bar{\boldsymbol{P}}^{\boldsymbol{T}}\bar{\boldsymbol{A}} \tag{26}$$

The equations (12) of the Markovian path approach applied to the example in figure 8 yield following result

$$\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}^T = \begin{bmatrix}P_1\\P_2\\P_3\\P_4\\P_5\end{bmatrix}^T \cdot \begin{bmatrix} 1 & \dfrac{\left(1-p_{c_{i,j}}\right)\lambda_i}{a_{2,2}} & \dfrac{p_{c_{i,j}}\lambda_i}{a_{3,3}} & \dfrac{\left(1-p_{c_{j,i}}\right)\lambda_j}{a_{4,4}} & \dfrac{p_{c_{j,i}}\lambda_j}{a_{5,5}} \\ 0 & -1 & \dfrac{\lambda_j}{a_{3,3}} & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & \dfrac{\lambda_i}{a_{5,5}} \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix} \tag{27}$$

Introducing the same submatrices as in the exact calculation the general form of the equations of the Markovian path approach is

$$\begin{bmatrix}1\\\boldsymbol{0}\end{bmatrix}^T = \begin{bmatrix}P_1\\\tilde{\boldsymbol{P}}\end{bmatrix}^T \cdot \begin{bmatrix}1 & \tilde{\boldsymbol{A}}_{\boldsymbol{1}}\\ \boldsymbol{0} & \tilde{\boldsymbol{A}}\end{bmatrix} \tag{28}$$

The submatrix $\tilde{\boldsymbol{A}}$ in (28) is much more simple than $\bar{\boldsymbol{A}}$ in (22) because all elements below the diagonal and according to the application additional elements above the diagonal are zero. From (28) the following relations are derived

$$P_1 = 1 \tag{29}$$

$$\boldsymbol{0}^T = \tilde{\boldsymbol{A}}_{\boldsymbol{1}} + \tilde{\boldsymbol{P}}^{\boldsymbol{T}}\tilde{\boldsymbol{A}} \tag{30}$$

It is given that $\tilde{\boldsymbol{A}}_{\boldsymbol{1}} = \bar{\boldsymbol{A}}_{\boldsymbol{1}}$, meaning that all transitions away from Z_1 are to be considered. Setting the relations $\tilde{\boldsymbol{P}} = \bar{\boldsymbol{P}} - \Delta\bar{\boldsymbol{P}}$ and $\tilde{\boldsymbol{A}} = \bar{\boldsymbol{A}} - \Delta\bar{\boldsymbol{A}}$ in (30) and using (26) the following elementary relationship can be derived

$$\Delta\bar{\boldsymbol{P}}^T \approx -\bar{\boldsymbol{P}}^{\boldsymbol{T}}\Delta\bar{\boldsymbol{A}}\,\tilde{\boldsymbol{A}}^{-1} \tag{31}$$

The matrix $\Delta\bar{\boldsymbol{A}}$ expresses the difference of the elements from (21) and (27). For relative small models the inverse matrix $\tilde{\boldsymbol{A}}^{-1}$ is simple to determine. For the example in figure 8 the results are

$$\Delta\bar{\boldsymbol{A}} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \frac{\mu_j}{a_{2,2}} & 0 & \frac{\mu_i}{a_{4,4}} & 0 \\ 0 & 0 & 0 & 0 \\ \frac{\mu_j}{a_{2,2}} & 0 & \frac{\mu_i}{a_{4,4}} & 0 \end{bmatrix} \qquad \tilde{\boldsymbol{A}}^{-1} = \begin{bmatrix} -1 & -\frac{\lambda_j}{a_{3,3}} & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & -\frac{\lambda_i}{a_{5,5}} \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{32}$$

According to (31) the approximate relative calculation error is evaluated to

$$\frac{\Delta(P_3 + P_5)}{P_3 + P_5} \approx \frac{\lambda_j \mu_j}{a_{2,2} a_{3,3}} + \frac{\lambda_i \mu_i}{a_{3,3} a_{5,5}} \tag{33}$$

Assuming the indices $\lambda = \lambda_i = \lambda_j = 10^{-4} h^{-1}$ and $\mu = \mu_i = \mu_j = 10^{-1} h^{-1}$ the relative error is calculated to

$$\frac{\Delta(P_3 + P_5)}{P_3 + P_5} \approx 10^{-3} \tag{34}$$

Expressions like (33) sometimes comprise in addition to P_i other probabilities on the right side, thus it seems difficult to determine the relative error $\Delta P_i / P_i$. In such cases one can iteratively replace these probabilities with (8).

Result: The minimal cut given in figure 8 is a typical minimal cut which can be found in systems with common mode failures and limited maintenance capacities. Other component dependencies can be modelled accordingly. Therefore we can derive that in many practical systems the error which is caused by the approximate Markovian path approach is negligible.

6 Summary

In this contribution the Markovian minimal cut approach is applied to a typical automation structure whose reliability could previously not be calculated in great detail with current reliability approaches. A systematic procedure considering system operation and outage in the 'real world' and its modelling technique are exemplified. Both component and system outage modelling as well as the calculation process allow the calculation of large *and* complex system structures. The approach can be applied in general to many technical systems.

7 Appendix

Acronyms

B	bus connection line
C	controller
CB	macro component: control board (serial connection of CC, MMI and HD)
CC	control computer
HD	hard disk
MCA	minimal cut approach
MMCA	Markovian minimal cut approach
MMI	man machine interface
MPA	Markovian path approach
PI	process interface
T	transceiver
TB	macro component: transceiver bus connection (serial connection of T and B)

Notation

b_C	probability of bus outage/blockade due to controller failure
b_T	probability of bus outage/blockade due to transceiver failure
D_i	down state (outage state) of component *i*
D_S	down state (outage state) of the system
$D_i \rightarrow S_j$	down state (outage) of component *i* and (postponable) shut down of component *j*
$F(X)$	mean frequency of *X*
M	minimal cut
$n_{C/LAN}$	number of controllers connected to one LAN
$n_{C/CC}$	number of controllers connected to one control computer
$n_{T/LAN}$	number of transceivers connected to one LAN
$P(X)$	probability of *X*
$p_{c_{i,j}}$	common mode probability: component *j* fails common with component *i*
r_C	probability of computer outage/blockade due to controller failure
$T(X)$	mean duration of *X*
U_i	up state (operation state) of component *i*
U_S	up state (operation state) of the system
X	random state (stochastic variable)
$X_j \mid X_k$	conditional state: X_j depends on X_k
Z	Markov state
$a_{i,j}$	constant transition rate from state *i* to state *j*
α_i	arrival rate for service of component *i*
λ_i	outage (failure) rate of component *i*
λ'_i	compound outage (failure) rate of component *i*
μ_i	repair rate of component *i*

ρ_i compound rate of component *i*
τ_i exchange rate of component *i*
υ_i preparation rate of component *i*

References

[Allan (94)] R.N. Allan, R. Billinton, A.M. Breipohl, C.H. Grigy: *Bibliography on the Application of Probability Methods in Power System Reliability Evaluation.* IEEE-Transactions on Power Systems, Vol. 9, No 1, February 1994.

[Billinton (92)] R. Billinton, R. Allan: *Reliability Evaluation of Engineering Systems - Concepts and Techniques.* Plenum Press, New York and London, 1992.

[DoD (91)] MIL-HDBK-217F: *Reliability Prediction of Electronic Equipment.* US Department of Defense, Washington DC, 1991.

[Edwin (79)] K.W. Edwin, H.-D. Kochs: *Reliability determination of non-Markovian power systems, Part I: An analytical procedure.* IEEE A 79502-6, PES Summer Meeting, Vancouver, July 1979.

[Endrenyi (79)] J. Endrenyi: *Reliability Modeling in Electric Power Systems*. John Wiley & Sons, Toronto, 1979.

[Kochs (84)] H.-D. Kochs: *Zuverlässigkeit elektrotechnischer Anlagen - Einführung in die Methodik, die Verfahren und ihre Anwendung. (Reliability Evaluation of electrical systems - Introduction to Methods, Approaches and Applications).* Springer Berlin, New York, 1984.

[Kochs (95)] H.-D. Kochs, W. Dieterle, E. Dittmar: *Reliability Evaluation of Highly Reliable Computer Control Systems for Energy Generation, Transmission and Distribution.* European Transactions on Electrical Power Engineering (ETEP), 1995.

[Misra (93)] K. B. Misra: *New Trends in System Reliability Evaluation.* ELSEVIER Amsterdam, 1993.

[Schneeweiss (89)] W. Schneeweiss: *Boolean Functions with Engineering Applications and Computer Programs.* Springer Berlin, New York, 1989.

[Schneeweiss (99)] W. Schneeweiss: *The Fault Tree Method.* LiLoLe-Verlag GmbH, Hagen, 1999.

[Schneeweiss (99b)] W. Schneeweiss: *Petri Nets for Reliability Modeling.* LiLoLe-Verlag GmbH, Hagen, 1999.

[Shooman (92)] A. M. Shooman: *Exact Graph-Reduction Algorithms for Network Reliability Analysis.* Ph.D Thesis, Polytechnic University, Brooklyn, New York, June 1992.

[Singh (77)] C. Singh, R. Billinton: *System Reliability Modelling and Evaluation.* Hutchinson, London, 1977.