On some variants of a switch model from the literature

J. Schuster and M. Siegle
University of the Federal Armed Forces Munich,
{*johann.schuster,markus.siegle*}*@unibw.de*

Abstract This paper considers a classical switch model of Kececioglu and some of its specialisations. By means of an example of a small reliable system we consider the impact of the switch model on the reliability function of the entire reliable system. We relate the different specialisations of Kececioglu's switch model to each other by fitting the reliability functions of the example system. Further, we show how the specialisations of the switch models influence the failure modes observed and how one can relate the models to data collected during the CIGRE studies.

1 Introduction

In this paper we consider an error model given in the literature (Kececioglu, 1991) of a single pole, double throw switch, c.f. the switching subsystem in Fig. 2b. We compare three specialisations of this error model by means of a small reliable system containing one such switch. We will consider the question of (1) relating the on-demand failures of the different models and (2) relating modelled switch failure modes to the measured failure modes of the reliable system. The paper is organised as follows: In Sec. 2 we introduce Kececioglu's switch model and some specialisations. The switch models are compared by means of a small reliable system that is introduced and analysed in Sec. 3. The different specialisations of the switch model are related in Sec. 3.1, and in Sec. 3.2 we relate one specialisation to failure mode distributions given e.g. by CIGRE enquiries (Colombo, Dialynas, Heising, Janssen & Lanz, 1994). Sec. 4 concludes the paper.

2 Switch models

In the sequel, we will use the following terms: An *on-demand failure* (ODF for short) is a failure that occurs triggered by some event (i.e. attempt to open a switch). It is associated with an on-demand-failure probability p. A *stochastic failure* is a failure that occurs without external influence, driven by a random variable. The random variable describes the time to failure. We distinguish two types of failures: A failure is said to be *visible* if it can be immediately detected by the environment. On the other side a failure is *hidden* if it cannot be detected immediately by the environment. It can only be detected after a certain event (e.g. switching attempt) has taken place. Note that a hidden failure does not immediately result in a system error.

2.1 Kececioglu's switch model

In this paper, we treat a special variant of the switch model given in (Kececioglu, 1991) where all stochastic failures are driven by exponentially distributed random variables. We call such

```
(1) SW(state[2]):=
(2)     [state=OK] -> (*changecommand, 1*); ( (*swODsuccess,(1-p)*); SW(OK)
(3)                                         + (*swODfailed,p*); SW(FAILED_VISIBLE) )
(4)     [state!=OK]-> (*changecommand, 1*); (*swODfailed,1*); SW(FAILED_VISIBLE)
(5)     [state!=FAILED_VISIBLE] -> (fail_SWv,lv); (*swfailed,1*);SW(FAILED_VISIBLE)
(6)     [state=OK] -> (fail_SWh,lh); SW(FAILED_HIDDEN)
```

(a) Kececioglu's general model

```
(5')    [state=OK] -> (fail_SWv,lv); (*swfailed,1*);SW(FAILED_VISIBLE)
```

(b) changes for S_{III}

Figure 1: CASPA code of switch models

stochastic failures also Markovian failures. They are specified by their *rate*. The switch model uses two exponentially distributed failures, a visible and a hidden one. Further, it also has an on-demand failure probability p, which is the probability for an unsuccessful switching attempt. The switch has three states, namely `OK`, `FAILED_HIDDEN` and `FAILED_VISIBLE`. It can fail hidden as long as it is in the OK state and it can fail visible both from the OK and from the `FAILED_HIDDEN` state. If the switch has failed before (hidden failure), a switching attempt will fail with probability one and if it has not failed before, a switching attempt will succeed with probability $1 - p$, otherwise it will fail. We will use annotation K in the sequel to indicate Kececioglu's model.

The CASPA (Bachmann, Riedl, Schuster & Siegle, 2009) model of the switch is given in Fig. 1a. Line (2) is the case where a change command is received and the switch has not failed so far. Therefore the switching attempt can be completed successfully (with a probability of $(1 - p)$) or it can fail with probability p (defined by line (3)). On the other hand, if a switch command is received but the switch has failed before (either visible or hidden), the switching attempt cannot be completed and a hidden failure becomes visible. This is described in line (4). Line (5) describes the fact that if the switch has not failed visible so far, it still can do so (with rate `lv` which will be denoted by λ_v in the sequel). Finally, in line (6) we specify that a hidden error always can occur as long as the switch is working (with rate `lh` which will be denoted by λ_h in the sequel).

2.2 Specialisations

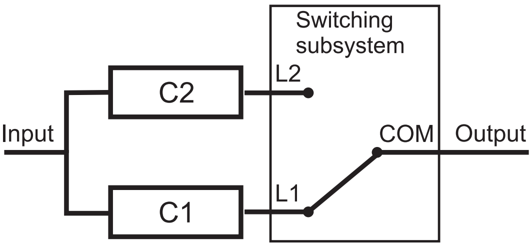
An overview of the different specialisations of Kececioglu's model is shown in Fig. 2a. Specialisation S_I is the model proposed in (Bouissou & Bon, 2003). In specialisation S_{II} all on-demand failures are exclusively induced by preceding hidden errors of the switch. Specialisation S_{III} uses the idea that no multiple errors can occur. This is realised by changing line (5) in Fig. 1a to line (5') given in Fig. 1b. An error can therefore only occur as long as the switch is in state `OK` (i.e. only one error can occur).

3 Analysing a small reliable system by the state space method

To show the difference between S_I, S_{II} and S_{III}, we present a small reliable system as shown in Fig. 2b. It consists of components C1 and C2 that provide a certain service where C1 is initially active and C2 is a hot spare. If C1 fails, the switch has to change its position to make C2 the active component. To keep it simple, we do not consider repairs, so the system will surely fail if we have an infinite amount of time. In this section, we present the state spaces

	K	S_I	S_{II}	S_{III}
Visible error	λ_v	λ_v	λ_v	λ_v
Hidden error	λ_h	0	λ_h	λ_h
ODF probability	p	p	0	0
Multiple stoch. switch failures	yes	no	yes	no

(a) Comparison



(b) Small reliable system

Figure 2: Comparison and small reliable system

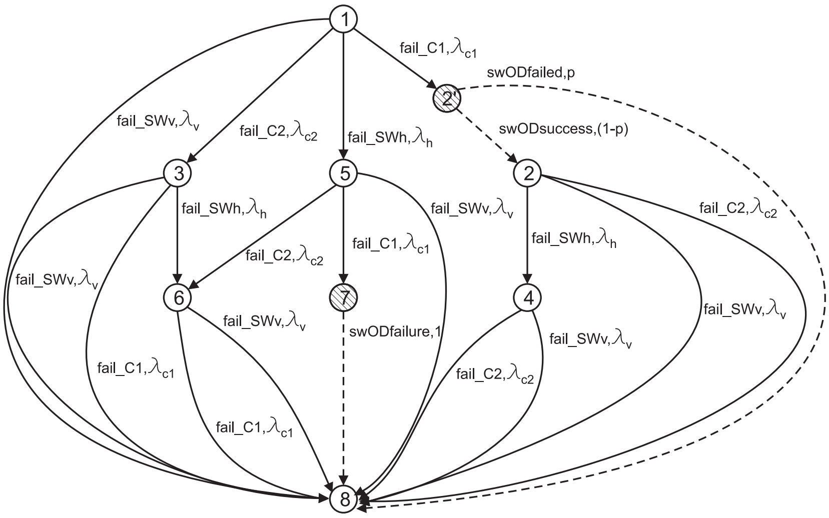


Figure 3: State space of the small reliable system (using Kececioglu's general switch model)

of the corresponding CASPA models using the different switch models as they were generated by the CASPA tool (after elimination of some transitions used only for synchronisations such as `changecommand`, `swfailed`, etc.). For the analytical solution we produced parameterised transition matrices out of the transition systems given by the CASPA tool and analysed them with the tool MAPLE.

The transition system for the general Kececioglu model (in the exponential case) is given in Fig. 3. The dashed (solid) edges are timeless (timed) transitions. The shaded states are *vanishing states* that can be eliminated before the model analysis takes place. For the calculation of the induced on-demand failure probabilities it is useful to know the probability $p_7(t)$ observed in state 7. Therefore we removed the `swODfailure` transition leading from state 7 to state 8. The probability that the system has failed up to time t, i.e. the *unreliability*, is then given as $U_K(t) := p_7(t) + p_8(t)$. We eliminated vanishing state 2' in order to end up at a purely Markovian model. Generator matrix Q_K is given in Eq. 1 (states are enumerated according to Fig. 3, the d_i denote the corresponding negative row sums). The upper left block belongs to the transient states, the upper right block describes the rates into the absorbing states and the lower two blocks are zero, as they belong to the absorbing states. It can be shown, that Q_K is not nilpotent. Despite this fact, MAPLE was able to calculate the exact solution for the exponential $e^{Q_K \cdot t}$. From $e^{Q_K \cdot t}$ the probability of being in one of the error states at a certain time can be calculated as $p_i(t) = e_1^\intercal \cdot e^{Q_K \cdot t} \cdot e_i$ (e_i denotes the i-th unit

Model	$R_{\texttt{Model}}(t)$	$P(ODF_{\texttt{Model}})$
K	$e^{-(\lambda_v+\lambda_{c1})\cdot t} + \frac{(1-p)\cdot\lambda_{c1}}{\lambda_{c1}+\lambda_h} \cdot (e^{-(\lambda_v+\lambda_{c2})\cdot t} - e^{-(\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h)\cdot t})$	$\frac{\lambda_h+p\cdot(\lambda_v+\lambda_{c1}+\lambda_{c2})}{\lambda_v+\lambda_h+\lambda_{c1}+\lambda_{c2}}$
S_I	$e^{-(\lambda_v+\lambda_{c1})\cdot t} + (1-p)\cdot(e^{-(\lambda_v+\lambda_{c2})\cdot t} - e^{-(\lambda_{c1}+\lambda_{c2}+\lambda_v)\cdot t})$	p
S_{II}	$e^{-(\lambda_v+\lambda_{c1})\cdot t} + \frac{\lambda_{c1}}{\lambda_{c1}+\lambda_h} \cdot (e^{-(\lambda_v+\lambda_{c2})\cdot t} - e^{-(\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h)\cdot t})$	$\frac{\lambda_h}{\lambda_v+\lambda_h+\lambda_{c1}+\lambda_{c2}}$
S_{III}	$c_1(\lambda_v,\lambda_h,\lambda_{c1})\cdot e^{-\lambda_{c1}\cdot t} + c_2(\lambda_v,\lambda_h,\lambda_{c1})\cdot e^{-\lambda_{c2}\cdot t}+$ $c_3(\lambda_v,\lambda_h,\lambda_{c1})\cdot e^{-(\lambda_v+\lambda_h+\lambda_{c2})\cdot t} + c_4(\lambda_v,\lambda_h,\lambda_{c1})\cdot e^{-(\lambda_v+\lambda_h+\lambda_{c1})\cdot t}+$ $c_5(\lambda_v,\lambda_h,\lambda_{c1})\cdot e^{-(\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h)\cdot t}$	$\frac{\lambda_h}{\lambda_h+\lambda_{c1}+\lambda_{c2}}$

Figure 4: Reliability functions and on-demand failure probabilities

column vector) from which the unreliability $U_K(t)$ and the reliability $R_K(t) := 1 - U_K(t)$ follow.

$$Q_K := \left(\begin{array}{cccccc|cc} d_1 & (1-p)\cdot\lambda_{c1} & \lambda_{c2} & 0 & \lambda_h & 0 & 0 & \lambda_v + p\cdot\lambda_{c1} \\ 0 & d_2 & 0 & \lambda_h & 0 & 0 & 0 & \lambda_v+\lambda_{c2} \\ 0 & 0 & d_3 & 0 & 0 & \lambda_h & 0 & \lambda_v+\lambda_{c1} \\ 0 & 0 & 0 & d_4 & 0 & 0 & 0 & \lambda_v+\lambda_{c2} \\ 0 & 0 & 0 & 0 & d_5 & \lambda_{c2} & \lambda_{c1} & \lambda_v \\ 0 & 0 & 0 & 0 & 0 & d_6 & 0 & \lambda_v+\lambda_{c1} \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \qquad (1)$$

All specialisations can be obtained from the transition system given in Fig. 3 with the following changes: For S_I $\lambda_h = 0$, for S_{II} $p = 0$, and for S_{III} `fail_SWv` transitions emanating from states 4, 5 and 6 are omitted. The different reliability functions $R_{\texttt{Model}}(t)$ are given in Fig. 4, the $P(ODF_{\texttt{Model}})$-column is calculated in the next section. All results are obtained in the same way as before. Note that the reliability function of S_{III} (with rational functions c_i) has a different structure than the other specialisations.

3.1 Relating on-demand failure probabilities and hidden error rates

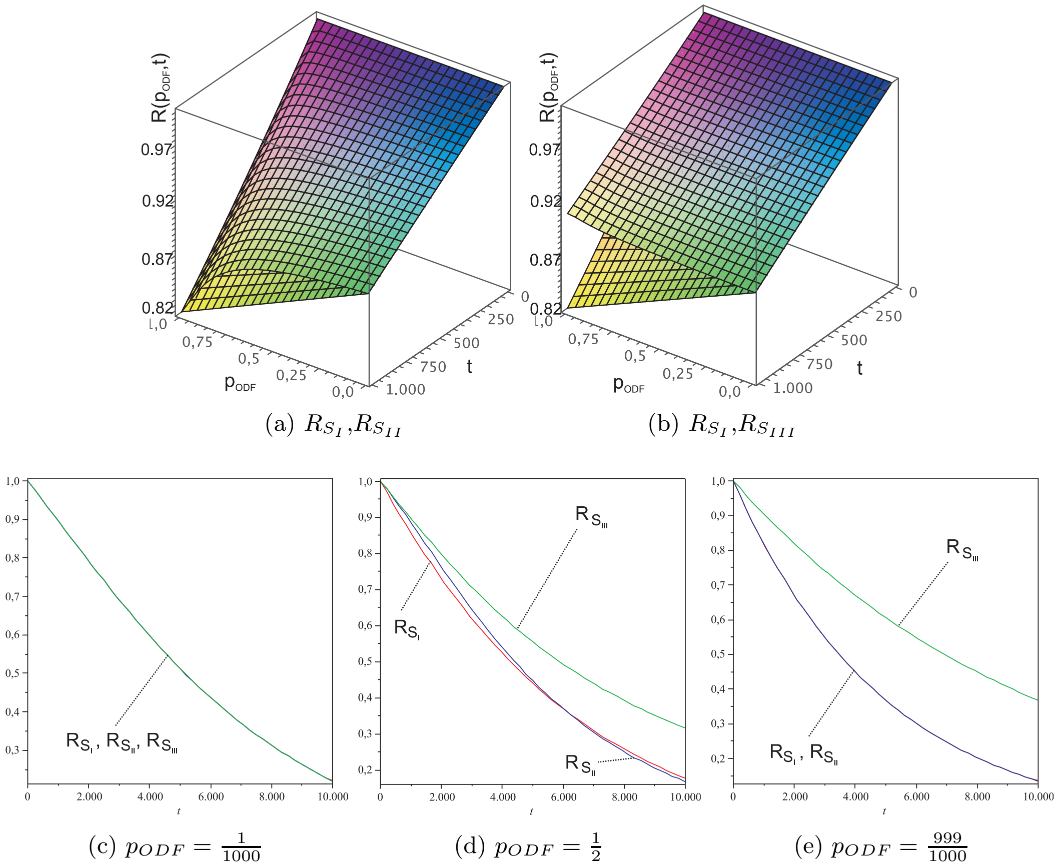
In this section, on-demand failure probabilities are related to the ratio of error rates. More specifically, we want to calculate approximations $S_I \Leftrightarrow S_{II}$ and $S_I \Leftrightarrow S_{III}$ for our reliable system example. The on-demand failure probability $P(ODF_K)$ of the general Kececioglu model can be calculated as follows. A failure during switching occurs if one of the following paths in Fig. 3 is taken: `Init->fail_SWh->fail_C1` or `Init->fail_C1->swODfailed` so the corresponding probability is

$$p_{fail,K} := \frac{\lambda_h}{\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h} \cdot \frac{\lambda_{c1}}{\lambda_{c1}+\lambda_{c2}+\lambda_v} + \frac{p\cdot\lambda_{c1}}{\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h}.$$

The switch can be operated successfully in the path `Init->fail_C1->swODsuccess` (i.e. no hidden error occurred before) with a probability

$$p_{succ,K} := \frac{(1-p)\cdot\lambda_{c1}}{\lambda_{c1}+\lambda_{c2}+\lambda_v+\lambda_h}.$$

From this the ODF can be calculated as $P(ODF_K) = P(\texttt{failure}|\texttt{switch operated}) = \frac{P(\texttt{failure}\cap\texttt{switch operated})}{P(\texttt{switch operated})} = \frac{p_{fail,K}}{p_{fail,K}+p_{succ,K}}$. In the same way the ODF probabilities of the other switch models can be calculated, thus leading to the right column in Fig. 4.



(a) R_{S_I},$R_{S_{II}}$

(b) R_{S_I},$R_{S_{III}}$

(c) $p_{ODF} = \frac{1}{1000}$

(d) $p_{ODF} = \frac{1}{2}$

(e) $p_{ODF} = \frac{999}{1000}$

Figure 5: Parametric plots of the fitted reliability curves

The other way around, given an ODF probability p_{ODF} we now try to adjust the hidden failure rates of S_{II} and S_{III} such that the expected time to a visible error does not change (i.e. $\lambda_v = const$) and $P(ODF_{\texttt{Model}}) = p_{ODF}$. We discuss briefly the accuracy of the approximations by means of some quantitative results. For this purpose we fix the parameters $\lambda_i = 10^{-4}\,{}^{1}\!/\mathrm{h}$ for $i \in \{c1, c2, v\}$ and leave p_{ODF} and t as parameters. S_I will be taken as a reference by setting $p := p_{ODF}$. S_{II} (S_{III}) is fitted by setting $\lambda_h := \frac{p_{ODF}\cdot(\lambda_{c1}+\lambda_{c2}+\lambda_v)}{(1-p_{ODF})}$ ($\lambda_h := \frac{p_{ODF}\cdot(\lambda_{c1}+\lambda_{c2})}{(1-p_{ODF})}$). Resulting reliability functions R_{S_I} and $R_{S_{II}}$ ($R_{S_{III}}$) are plotted over t and p_{ODF} in Fig. 5a (Fig. 5b). In both cases, the lower surface belongs to R_{S_I} (linear in p_{ODF}, c.f. Fig. 4). On a larger time horizon we have plotted the resulting reliability curves for three different on-demand failure probabilities in Fig. 5c-5e. For the practically relevant case $p_{ODF} \approx 0$, the three specialisations can be well-approximated by each other. It is notable that for $p_{ODF} = \frac{1}{2}$ R_{S_I} and $R_{S_{II}}$ intersect at $t \approx 6000$h, i.e. $R_{S_{II}}$ is not always an upper bound for R_{S_I}.

3.2 Relation of failure mode distributions

Specialisation S_{III} has a nice analogy to the CIGRE studies, (where failure mode distributions are calculated): If we put a certain failure mode distribution in the switch (in this paper we restrict ourselves to two modes, namely visible and hidden) and we assume that every failure is finally detected, then the observed failure mode distribution in a reliable system environment is the same as the distribution in the switch. This is shown by the following observation: In the state space of the example system using switch model S_{III} there are *decision points*, namely in states $I = \{1, 3, 2\}$ there are both hidden and visible errors possible. By the law of total probability, one can deduce that the probability of running into a visible switch error is $P(visible) = \sum_{i \in I} p_i \cdot \frac{\lambda_v}{\lambda_v + \lambda_h + c_i}$ where I is the set of decision points, p_i is the probability of getting into the decision point $i \in I$ and c_i is the cumulated transition rate out of state i that does not lead into a switch error. The conditional probability of observing a visible switch error under the condition that a switch error occurred (given that finally we detect *every* hidden error) is $P(visible|error) = \ldots = \frac{\lambda_v}{\lambda_h + \lambda_v}$. Note that this is *not* the case for K, S_I and S_{II} (assuming the free variables to be non-zero).

4 Conclusion

Kececioglu's switch model and some specialisations have been studied in this paper. Calculations forth and back have been performed to transform on-demand-failure probabilities to hidden failure rate approximations and vice versa. As was empirically shown by a small example, the same reliability distribution functions can in general never be achieved using different switch models. Nevertheless for the practically relevant case $p_{ODF} \approx 0$ the resulting reliability functions fit quite well. As recommended in (Colombo et al., 1994) it would be interesting to use even more sophisticated error models related to the CIGRE data (e.g. different modes for "does not close/open on command" as there are different probabilities for these modes). We will study more complex models to show how different error models change the reliability function of a reliable system.

Acknowledgement

Special thanks to Alexander Gouberman for sharing his mathematical background and sustained proof-reading the manuscript. Thanks to Thomas Krieger for the fruitful discussions. The authors would like to thank Deutsche Forschungsgemeinschaft for supporting this work under grant SI 710/5-1. This work is partially supported by DFG/NWO bilateral research programme ROCKS.

References

Bachmann, J., Riedl, M., Schuster, J. & Siegle, M. (2009). An Efficient Symbolic Elimination Algorithm for the Stochastic Process Algebra tool CASPA. In *Sofsem 2009* (p. 485-496). Springer, LNCS 5404.

Bouissou, M. & Bon, J.-L. (2003). A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering and System Safety*, *82*, 149-163.

Colombo, E., Dialynas, E., Heising, C., Janssen, A. & Lanz, W. (1994). Summary Of CIGRE 13.06 Working Group World Wide Reliability Data And Maintenance Cost Data On High Voltage Circuit Breakers Above 63 kV. In *Conf. record of the industry applications society annual meeting* (p. 2226-2234). IEEE.

Kececioglu, D. (1991). *Reliability Engineering Handbook Volume 2.* Prentice Hall. (available also through google books (last checked Dec. 2010))