Modeling of Complex Redundancy in Technical Systems with Bayesian Networks

Thorben Kaul[1], Tobias Meyer[2] and Walter Sextro[3]

[1,2,3] *University of Paderborn, Faculty of Mechanical Engineering, Mechatronics and Dynamics, 33098 Paderborn, Germany*
thorben.kaul@uni-paderborn.de
tobias.meyer@uni-paderborn.de
walter.sextro@uni-paderborn.de

Abstract

Redundancy is a common approach to improve system reliability, availability and safety in technical systems. It is achieved by adding functionally equivalent elements that enable the system to remain operational even though one or more of those elements fail. This paper begins with an overview on the various terminologies and methods for redundancy concepts that can be modeled sufficiently using established reliability analysis methods. However, these approaches yield very complex system models, which limits their applicability. In current research, Bayesian Networks (BNs), especially Dynamic Bayesian Networks (DBNs) have been successfully used for reliability analysis because of their benefits in modeling complex systems and in representing multi-state variables. However, these approaches lack appropriate methods to model all commonly used redundancy concepts. To overcome this limitation, three different modeling approaches based on BNs and DBNs are described in this paper. Addressing those approaches, the benefits and limitations of BNs and DBNs for modeling reliability of redundant technical systems are discussed and evaluated.

1. Redundancy in Dependable Technical Systems

There are various definitions for system dependability that differ in focus on certain systems, terminology and scope. When it comes to dependability of technical systems, the most common norms, such as IEC 60050-191 ”Dependability and Quality of Service” (International Electrotechnical Commission, 1990) in the U.S., VDI 4001-2 ”Reliability Terminology” (Verein Deutscher Ingenieure, 2006) and VDI 4003 ”Reliability Management” (Verein Deutscher Ingenieure, 2007) in Germany, do not take a strong influence of software on dependability into account, as compared to mechatronic systems. This growing contribution of software creates a need to consider this in the definition of the dependability of technical systems. Avižienis *et al.* gave a definition for the basic concepts of secure computing (Avižienis et al., 2004), that was adapted for self-optimizing systems, which are based on mechatronic systems (Gausemeier et al., 2014). Self- optimizing systems emphasize the necessity for dependability concepts including software because of their inherent intelligence. In (Avižienis et al., 2004), dependability for computer-based systems is comprised of the following attributes: reliability, availability, safety, integrity and maintainability (see Fig. 1). Based on these attributes, additional definitions are made to address the threats to dependability (faults, errors and failures) and means to achieve the attributes (fault prevention, fault tolerance, fault removal, fault forecasting). In this paper, only attributes with focus on reliability, availability and safety are considered. The two remaining, integrity and maintainability, cannot directly be influenced by adding redundancy to a technical systems and are therefore neglected. Although the definition for dependability given by (Avižienis et al., 2004) comprises software and aspects of technical systems as well, the given concepts for software redundancy are not considered in this paper, because analysis methods and techniques to investigate dependability of software differ from methods applied to technical systems such as mechanical, hydraulic and electronic.

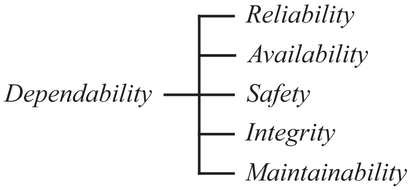


Figure 1. Dependability attributes (Avižienis et al., 2004)

The availability of a technical system is comprised of maintainability, available resources for repair and reliability. Although safety relies on reliability, a reliable system is not necessarily a safe system, since safety takes the severity of the event into account as well. Even very rare failures of systems with high reliability might lead to catastrophic events, e.g. train derailments, plane crashes or nuclear power plant meltdowns.

When individual elements are built as reliable as technology permits, but system reliability is still not sufficiently high, an improvement of safety and reliability can only be reached by adding redundancy to the system. Redundancy is the existence of more than one element required to successfully perform a certain function, but it does not imply a simple duplication of those elements. Since common mode and systematic failures have to be avoided, all redundant elements should be designed and manufactured independently ((Sagan, 2004), (Birolini, 2007)). Redundancy aims to provide perpetual functionality of a system even if elements fail. With focus on the bare functionality, mechatronic systems offer the possibility to cover hardware failures by virtual elements using *analytical redundancy*, e.g. an observer that covers a failure of a sensor by estimating the measures (Isermann, 2002). Since all current mechatronic systems inherently feature some sort of digital processing power, redundancy can be achieved without adding hardware elements to the system. While omitted hardware elements could lower cost, the savings should not be outweighed by additional cost for design and implementation of software-based analytic redundancy. Besides increasing cost, redundancy also increases system complexity compared to a system without redundant elements. The increasing complexity is likely to make the system more prone to errors and failures. In addition, (Sagan, 2004) names three threats to reliability and safety of systems with redundancy: *common mode failures* as already discussed above, *social shirking* (individual or groups of users reduce attention to reliability and safety due to the assumption that someone else will take care of problems) and *overcompensation* (a safer system eventually encourages individual or a group of users to increase operation of the system in dangerous ways).

In order to cope with increasing complexity and to avoid common mode failures in systems with redundancy, advanced modeling techniques are required. Thus, Bayesian Networks (BNs) and especially Dynamic Bayesian Networks (DBNs) have been successfully used for reliability analysis of state of the art technical systems in current research (Weber & Jouffe, 2003), (Weber et al., 2012), (Kaul et al., 2015). These approaches need to cover redundancy concepts as well, but either lack appropiate methods to cover commonly used concepts or making the model increasingly complex, i.e. (Boudali & Dugan, 2005), (Marquez et al., 2010), (Mahadevan et al., 2001). However, the objective of this paper is to discuss the use of established modeling methods for systems with redundancy, i.e. Reliability Block Diagrams (RBDs), Dynamic Fault Trees (DFTs) and Markov Chains (MCs), in contrast to Bayesian approaches based on a comprehensive definition of redundancy concepts.

The remainder of the paper is organized as follows: Sec. 2 introduces the different concepts of redundancy. Sec. 3 gives an overview on established analysis methods for the reliability of systems with redundancy. In Sec. 4 Bayesian Networks (BNs) and Dynamic Bayesian Networks (DBNs) are introduced as reliability models that is used in Sec. 5 to develop three different approaches to model systems with redundancy. In Sec. 6 these approaches are evaluated regarding their benefits to reliability analysis. The paper ends with a short conclusion in Sec. 7.

2. CONCEPTS OF REDUNDANCY

The concepts of redundancy in technical systems investigated within this work are limited to the basic structures: *k-out-of-n* in *hot*, *warm* and *cold* redundancies in *nonrepairable* systems. Among the general concepts of redundancy appear even more complex representatives, such as bridge structures and majority redundancy in systems endowed with voting-techniques. The intention of this work is to give an overview on different approaches based on BN compared to established methods where only fundamental structures are taken into account.

Each of the subsequently introduced concepts can be realized with a k-out-of-n structure: such systems consist of n functionally identical elements, of which k elements are necessary to perform the required function. Accordingly, $n-k$ elements are redundant and remain in as spare to cover failures.

In *hot* redundancy, the redundant, or *standby*, elements fully contribute to operation and are subjected to the same operating conditions and loads as the operating elements. The elements are either treated as statistically independent, which implies that the load on each element is identical but the complete load is not necessarily equally shared by all active elements, or dependent, where the load is shared among active elements (*load sharing*). If elements are assumed to be statistically dependent, the load on individual active elements increases with each failure. Thus, the load and in turn degradation of active elements increases over operating time for each failure.

In *warm* redundancy, the failure rate of standby elements is assumed to be nonzero, but lower than that of active elements. If the system with warm redundancy is designed for load sharing, standby elements are subjected to lower load than active elements until one of the active element fails. In systems without load sharing, the standby elements are unloaded, but degrade because of operating and environmental conditions or aging. If load sharing is present, the assumption for statistically dependent elements arises, whereas unloaded or aged elements can be interpreted as independent.

Cold redundancy can be seen as idealized warm redundancy, because only active elements are subjected to load and all standby elements are not affected by any load or degradation. Hence, the failure rate of standby elements is assumed to be zero since only active elements are likely to fail and load sharing is not possible.

The difference between warm and cold redundancy is not always clearly drawn when it comes to real world applications. E.g. the spare tire in a car can be modeled as cold redundancy since this assumption holds for sufficiently low failure rates of unloaded or slightly loaded elements. For a more exact approach, where degradation or aging of unloaded standby elements should be taken into account, warm redundancy is likely to be chosen.

3. ANALYSIS METHODS

This section gives an overview on established methods for modeling fundamental concepts of redundancy as mentioned in Sec. 2 and focuses on the limitations that arise for each method. Reliability investigations for those methods are based on *Boolean* (RBDs) and *state space* (MCs, DFTs, BNs, DBNs) functions. The investigation of system reliability in the state space is split up into two different approaches: *event-based* (MCs see Sec. 3.2) and *time-slice-based* (DBNs).

3.1. Established Methods: RBD

RBDs are the most common method to model and analyse reliability of systems with redundancy, since those systems are modeled with a simple parallel structure (see Fig. 2 left). However, comprehensive modeling of basic concepts of redundancy (Sec. 2) is not possible, since RBDs cannot handle temporal dependencies between elements, i.e. in warm redundancy, and are limited to binary states (*operational*, *failed*) of elements. If *hot* redundancy is investigated using RBDs, statistically identical but independent elements $1...n$ are assumed, which have reliability R over operating time t with $R_1(t) = \ldots = R_n(t)$. For common distribution functions, i.e. Exponential, Weibull, Gaussian, analytical solutions for reliability of systems with a hot redundancy can be determined based on the binomial distribution (Birolini, 2007):

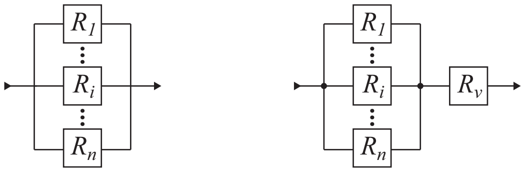


Figure 2. RBD for parallel structures in hot redundancy (left), RBD with voter R_v for hot or cold redundancy

$$R_{sys}(t) = \sum_{i=k}^{n} \binom{n}{i} R^i(t)(1 - R(t))^{n-i}, R_{sys}(0) = 1. \quad (1)$$

When investigating *cold* redundancy, there are different additional elements taken into account, e.g. ideal/real voter R_v (Fig. 2 right) and measurement elements, in order to decide which redundant element is set to operation (Birolini, 2007). Those approaches are limited to constant failure rates, because an analytical solution is easily obtained. Considering the restrictions stated above, RBDs are limited in practical application, but offer an intuitive introduction to the concept of redundancy.

3.2. Established Methods: MC

Markovian approaches investigate reliability and availability of a system as a discrete or continuous time stochastic process in its finite state space. Markov models are supposed to be *memoryless*, a future state only depends on the present state and not on any preceding states in the past (Markov property).

MCs describe a sequence of directed graphs, where dependencies between states of the system for different time steps are modeled using stochastic transitions, i.e. conditional probabilities. To allow for analysis of time continuous MCs, the state probabilities $P_i(t)$ are obtained from a system of differential equations, which is given by consecutive state changes between two adjacent time points t and $t + \delta t$ for $\delta t \to 0$.

MCs are a comprehensive approach to model the basic concepts of redundancy (Sec. 2), but face an exponentially increasing number of states for additionally investigated elements (*state explosion*). (Birolini, 2007) proposes an approach for modeling systems with redundancy as shown in Fig. 3 to limit the number of states for increasing n in k-out-of-n redundancy. This model is also used in Sec. 5.1. In Fig. 3, it is assumed that in state $Z_i, i = 0, ..., n - k$ elements have failed and thus all elements have failed in state Z_{n-k+1}. The state probability $P_{n-k+1}(t)$ is interpreted as reliability of the system with redundancy. The failure rates for operating elements λ and for redundant elements λ_r are assumed to be constant and identical for all elements. The following redundancies can be handled with this MC:

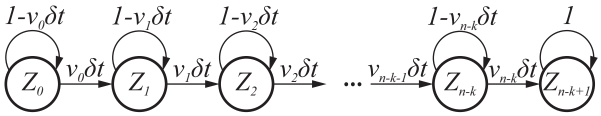


Figure 3. MC for hot,warm and cold k-out-of-n redundancy for arbitrary t (Birolini, 2007)

1. Hot redundancy without load sharing: $\nu_i = (n - i)\lambda$,
2. Hot redundancy with load sharing: $\nu_i = (n - i)\lambda(i)$ and $\lambda(i)$ increases with each preceding state (failure),
3. Warm redundancy with load sharing: $\nu_i = k\lambda + (n - k - i)\lambda_r$ and $\lambda_r < \lambda$,
4. Cold redundancy: $\nu_i = k\lambda$ and $\lambda_r \equiv 0$.

For warm redundancy, this MC approach can handle lightly loaded or aged redundant elements as introduced in Sec 2.

Although MCs have proven to be a comprehensive approach for modeling systems with redundancy, they are restricted to a continuous and memoryless distribution (exponential distribution) of state transitions. This limits their practical application, since failures of many mechanical elements follow Weibull distribution.

3.3. Established Methods: DFT

A fault tree (FT) is a graphical representation of a set of events and their combination that cause or contribute to the occurrence of an undesired top event, in general a failure at system level. In contrast to RBDs, FTs use negative notation: as the top event is defined as failure of the system, *true* is used for the occurrence of failure and *false* for operating. To allow for modeling reliability based on the combination and contribution of events to a system failure, FTs contain static gates (*and*, *or*), that can only handle Boolean combinations of events and can thus not handle temporal dependencies (Birolini, 2007).

To overcome this limitation, FTs are combined with a Markovian approach using dynamic gates to allow for modeling states and time dependencies. The most popular dynamic gates (see Fig. 4) are: priority AND (PAND), warm spare (WSP) and probabilistic dependency (PDEP). A PAND gate fails, if all input events $E_{1...n}$ have occurred in a preassigned order (in graphical notation from left to right). The output event O of a WSP gate occurs, if the number of spare elements $S_{1...n}$ is less than the minimum required P. In PDEP gates, a trigger event T causes the conditional occurrence of other input events $C_{1...n}$ in order to define a failure of the gate. Those dynamic gates require continuous time Markov process to allow for quantitative analysis of DFTs. The Markov process is solved to obtain state probabilities, which will be used as occurrence probability for the output event of the gate O. DFTs were comprehensively investigated for modeling reliability of systems with redundancy (Montani et al., 2006), (Dugan et al., 1992), (Ren & Dugan, 1998) and have proved to sufficiently model the concepts of redundancy as introduced in Sec. 2.

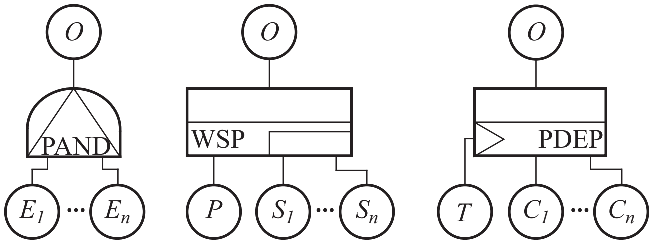


Figure 4. Dynamic gates in DFTs

Although DFTs have been successfully applied to reliability investigation of complex systems, the use of a Markovian approach limits their practical application for the reasons stated in Sec. 3.2 for MCs.

4. BAYESIAN MODELS

Directed acyclic graph (DAG) models, also known as Bayesian or belief networks, are used for causal modeling and interpretation of static data or systems. To do so for dynamical systems or temporal data, dynamic DAG models (DBNs) can be used. In this section BNs and DBNs are introduced and their application to model system reliability is shown briefly.

4.1. Bayesian Networks

BNs are DAG models with nodes representing a set of stochastic variables $\mu = \{X_1, X_2, ..., X_n\}$ that are endowed with distributions. A directed graph model is fully defined for a given DAG and Conditional Probability Distributions (CPDs) for every node. Each stochastic variable of $\{X_1, X_2, ..., X_n\}$ represents a set of a finite number of possible states. A variable can only have one of its states at a time. Variables can be endowed with individual probability distributions, e.g. Weibull or Exponential. BNs set up for μ specify a unique joint probability distribution $P(\mu)$ given by the product of all CPDs:

$$P(\mu) = \prod_{i=0}^{n} P(X_i \mid Pa(X_i)) \tag{2}$$

where X_i represents node i and $Pa(X_i)$ is the set of its parents. If the variables $\{X_1, X_2, ..., X_n\}$ are discrete, they can be represented by a Conditional Probability Table (CPT), which lists the probability that the child node C takes on each of its different states for each combination of states of its parent nodes $P(C|Pa(C))$ (Nielsen & Jensen, 2009). The probability table of a root node K (nodes without parents) is reduced to an unconditional probability table $P(K)$ that includes only *a priori* probabilities.

BNs can be seen as causal networks to be used for reasoning about relevance and causal analysis for propagation of beliefs throughout the network. Therefore they can be used to model the causal dependencies in functionality in a technical system, e.g. is a failure of element A relevant for functionality of element B?

4.2. Reliability Modeling: BN

In a reliability model for technical systems, the set of variables μ represent a set of elements of the technical system. In a first approach it is assumed for all elements to have binary states: true tr representing an element in *operable state* and false fa representing an element *failure*.

The probability tables $P(A)$ for an element A and conditional table $P(B|A)$ for an element B in a Bayesian Network as system reliability model as shown in Fig. 5, represent element reliability $R_A(t)$ and $R_B(t)$ as well as causal failure propagation represented by binary table entries. It is still assumed that both elements have binary states and B conditionally fails when a failure of A occurs. Thus, B eventually fails on its own account with $1 - R_B(t)$ when A is in operable state. Considering Eq. (2), the joint probability distribution of the Bayesian Network $P(A, B)$ can be interpreted as system reliability $R_S(t)$. The Bayesian Network as set up above represents system and element reliability $R_C(t)$ and $R_S(t)$ only at a particular operating time t. System reliability $R_S(t)$ has to be evaluated over system lifetime to obtain a discrete graph.

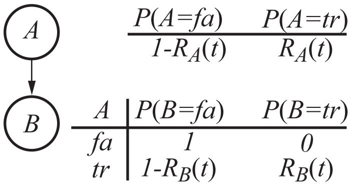


Figure 5. BN with CPTs used as system reliability model

4.3. Dynamic Bayesian Networks

A DBN is a BN extended by a temporal dimension to model discrete-time stochastic processes for dynamic systems. If a system evolves over time, a DAG is used to model the system for each discrete *time slice*. These slices are connected through temporal probabilistic links to constitute a full model.

According to Murphy's two-slice temporal Bayes Net (2TBN) respresentation of DBNs (Murphy, 2002), the value of a variable can be calculated from the immediate prior and the internal regressor.

A set of stochastic variables $\xi_t = \{Z_1, Z_2, ..., Z_m\}$ is increased for every additional time slice t and, based on 2, $P(\xi_t \mid \xi_{t-1})$ is given as follows:

$$P(\xi_t \mid \xi_{t-1}) = \prod_{j=1}^{m} P(Z_t^j \mid Pa(Z_t^j)), \tag{3}$$

where the notation is similar as introduced in Sec. 4.1; Z_j^t is the jth node at time t and $Pa(Z_j^t)$ are the parents of Z_j^t. The parents of the investigated node $Pa(Z_j^t)$ can either be in the same time slice t or in the previous time slice $t-1$. Thus, assuming a first-order Markov process, time slice t is conditionally independent of its predecessor (Murphy, 2002).

Given T observations of ξ_t, a DBN with T time slices is obtained. The resulting joint probability distribution for the *unrolled* DBN (see 3) is given by:

$$P(\xi_{1:T}) = \prod_{t=1}^{T} \prod_{j=1}^{m} P(Z_t^j \mid Pa(Z_t^j)). \tag{4}$$

In addition to the modeling of causal and probabilistic dependencies of technical systems in BNs and calculation of system reliability, DBNs offer the possibility to model temporal dependencies between elements and can thus be seen as a more extensive modeling approach for the reliability of technical systems.

4.4. Reliabilitiy Modeling: DBN

The assumptions made in Sec. 4.2, regarding the reliability modeling of technical systems with BNs, still hold for DBNs. The set of variables introduced in Sec. 4.3, ξ_t, represents a collection of elements of the system at two time slices t and proceeding time slice $t + \Delta t$.

Hence, DBNs can be used to model temporal dependencies among elements and to estimate the dynamic behavior of system or element reliability (Weber & Jouffe, 2003). Considering the system as shown in Fig. 5, it is assumed that element A evolves over time due to degradation. A DBN is set up accordingly in Fig. 6.

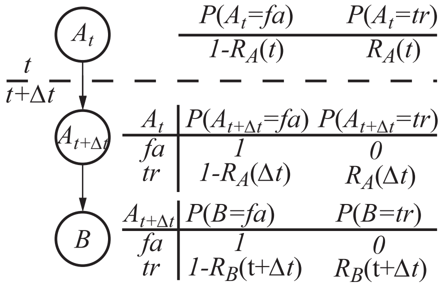


Figure 6. A DBN with CPTs in 2TBN representation used as system reliability model for exponentially distributed R_A and R_B

The CPT of element A_t gives the *a priori* reliability $R_A(t)$ and probability of failure $1 - R_A(t)$. In the proceeding time slice $t + \Delta t$, the CPT for element $A_{t+\Delta t}$ is given for the conditional dependency on A_t: $A_{t+\Delta t}$ fails, only if A_t has already failed in the previous time slice with

$$Pr(A_{t+\Delta t} \mid A_t) = \frac{Pr(A_{t+\Delta t} \cap A_t)}{Pr(A_t)} = \frac{Pr(A_{t+\Delta t})}{Pr(A_t)}. \tag{5}$$

If exponential distribution is assumed for elements A and B, then $Pr(A_{t+\Delta t} \mid A_t)$ simplifies with $Pr(A_{t+\Delta t}) = R_A(t + \Delta t)$ to

$$\frac{R_A(t+\Delta t)}{R_A(t)} = \frac{e^{(-\lambda(t+\Delta t))}}{e^{(-\lambda t)}} = e^{(-\lambda(\Delta t))} = R_A(\Delta t). \tag{6}$$

Element B is basically not infected by the temporal dependency of element A, since Markov process is assumed and is thus accordingly defined as in Sec. 4.2.

5. MODELING APPROACHES

The methods introduced in Sec. 3 have limitations in modeling even the basic concepts of redundancy. Thus in this section, three different approaches, all based on standard and dynamic Bayesian models, are proposed and discussed considering limitations, efforts and requirements that arise from the chosen models.

5.1. Markovian Approach

The intention of the Markovian approach[1] is, to take advantage of the comprehensive modeling of reliability using BNs on the one hand, and, on the other hand, make use of established methods for modeling systems with redundancy, i.e. Markovian models.

The proposed method uses BNs for modeling the reliability of arbitrary technical systems and MCs to cover redundant subsystems. The BN is evaluated for discrete time (see Sec. 4.2), while the MC is evaluated for continuous time. To allow for modeling of a redundant subsystems, a MC is set up that comprises only elements that contribute (active or standby) to that redundancy. Afterward all contributing elements are identified and redundancy concept is chosen, the MC is evaluated and the obtained subsystem reliability is given to the CPT of the corresponding node in the BN.

Considering a MC as shown in Fig. 5, let A be the representative of a system with redundancy and its children, B, an arbitrary nonredundant element with given $R_B(t)$ that functionally rely on A. Then, $R_A(t)$ is the reliability of the redundant subsystem that is determined by solving the MC for the state probability of the last node (Z_{n-k+1}). The analysis of the BN as model of overall system reliability can be done using standard algorithms without further inquiries.

The DAG is unaffected by this Markovian approach, because the BN keeps the compact structure of a system without redundancy, while the MC covers only the redundant subsystem with a minor number of states than the overall system. As shown in Sec. 3.2, the basic concepts of redundancy can be modeled using the proposed MC, anyhow it is restricted to the inherent limitation of MCs.

In Fig. 7 the reliability $R(t)$ for exponentially distributed failures of an 1-out-of-3 redundancy is shown for a set of basic concepts.

Reliability $R(t)$ is computed for $t = 0...500h$, overall concepts for $\lambda = 1/50$, in hot redundancy with load sharing for $\lambda(i) = (i + 1/n)\lambda$ and in warm redundancy for $\lambda_r = 0.2\lambda$. The results are obtained by using the Bayes Net Toolbox for Matlab by Murphy (Murphy et al., 2001). In real-world application, the influence of dynamic load situations on the lifetime and failure rate λ of an element is rather complex and might be nonlinear, i.e. Arrhenius Model. So, the calculation of $\lambda(i)$ is only a rough estimate to illustrate the modeling approach. However, considering the graph of the hot redundancy with load sharing, the system is at first almost as reliable as the system with hot redundancy without load sharing. When the first element fails, load is increased on the remaining elements and reliability is accordingly lowered because $\lambda(i)$ is assumed to increase by $1/3$ for each element failure i.

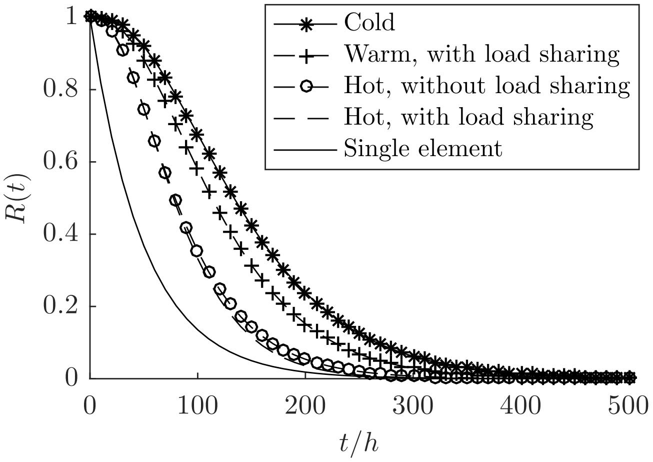


Figure 7. Reliability $R(t)$ modeled with Markovian approach

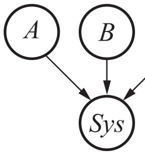
5.2. BN Approach

The modeling of systems with redundancy using BNs follows the general approach for modeling reliability of systems as introduced in Sec. 4.2. Since BNs cannot handle temporal dependencies in a straight forward approach using only component reliabilities, different approaches has been proposed to overcome this limitation. To enable BNs to appropriately model systems with temporal or event-based dependencies, different approaches have been proposed either based on discretization of operating time (Boudali & Dugan, 2005), (Marquez et al., 2010) or focusing on correlation between system components (Mahadevan et al., 2001). However, those approaches require additional computation efforts to obtain conditional probabilities and are therefore neglected. In fact, only *hot* k-out-of-n redundancies can be modeled straight forward using BNs as exemplarily shown for an 1-out-of-3 redundancy in Fig. 8.

In hot redundancy without load sharing all elements contribute by the same amount and fail independently from each other because load on remaining elements is the same in occurrence of element failures.

System reliability $R(t)$ is investigated for the same parameters λ and t as used in Sec. 5.1. Perpetually, element reliabilities are assumed to be exponentially distributed $R_{A,B,C}(t) = e^{-\lambda t}$. The results are shown in Fig. 10 and identical to the

[1] This approach was developed by L. Bathelt in his bachelor thesis at the University of Paderborn in 2015 and was supervised by W. Sextro.



$P(A,B,C{=}fa)$	$P(A,B,C{=}tr)$
$1\text{-}R_{A,B,C}(t)$	$R_{A,B,C}(t)$

A B C	$P(Sys{=}fa)$	$P(Sys{=}tr)$
fa fa fa	1	0
fa fa tr	0	1
⋮ ⋮ ⋮	⋮	⋮
tr tr tr	0	1

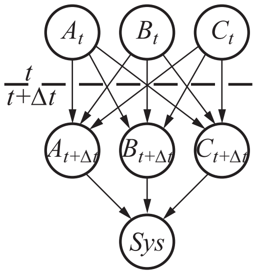
Figure 8. BN for a hot 1-out-of-3 redundancy without load sharing

results obtained from the Markovian approach. However, the use of standard BN for modeling systems with redundancy restricts the possible scope of redundancy concepts to hot spares without load sharing.

5.3. DBN Approach

DBN are used in a wide field of providing an appropriate analysis method for DFTs such as in (Montani et al., 2006), (Marquez et al., 2010). Montani describes a transformation algorithm to convert DFTs into DBNs with focus on handling dynamic gates inherent to a DFT in order to provide an exhausting analysis method. To do so, Montani describes an approach for modeling commonly used redundancy concepts that is applied to the introduced concepts in Sec. 2.

The DBN as shown in Fig. 9 shows the basic outline for hot, warm and cold 1-out-of-3 redundancy respectively with load sharing and the introduced modeling approach using DBN in Sec. 4.4. To model *hot* redundancy with load sharing, the failure rate of each element depends on the number of element failures i and is defined as $\lambda(i) = ((i+1)/n)\lambda$ for exponentially distributed reliability $R_A = R_B = R_C = e^{-\lambda(i)t}$ for $i = 0$ in time slice t. It thus follows that each element (failure) effects all other elements, which is considered in the DAG. Considering Eq. 6, reliabilities in time slice $t + \Delta t$ with $\Delta t = 10h$ for one element failure ($i = 1$) are assumed to be $R_{A|C} = R_{A|B} = R_{B|A} = R_{B|C} = R_{C|A} = R_{C|B} = e^{-\lambda(i)(\Delta t)}$. If two element failures have occured ($i = 2$), reliabibility is $R_{B|AC} = R_{C|AB} = e^{-\lambda(i)(\Delta t)}$. The results for a system with hot redundancy with load sharing obtained from the DBN differ slightly from the results computed with the MC approach. In fact, the maximum absolute error between both approaches is $\max(|\ R_{MC} - R_{DBN}\ |) = 2.8\%$.



$A_tB_tC_t$	$P(A_{t+\Delta t}{=}fa)$	$P(A_{t+\Delta t}{=}tr)$
fafafa	1	0
⋮ ⋮ ⋮	⋮	⋮
tr tr tr	$1\text{-}R_A(\Delta t)$	$R_A(\Delta t)$
tr tr fa	$1\text{-}R_{A\vert C}(\Delta t)$	$R_{A\vert C}(\Delta t)$
tr fa tr	$1\text{-}R_{A\vert B}(\Delta t)$	$R_{A\vert B}(\Delta t)$
tr fafa	$1\text{-}R_{A\vert BC}(\Delta t)$	$R_{A\vert BC}(\Delta t)$

$B_tA_tC_t$	$P(B_{t+\Delta t}{=}fa)$	$P(B_{t+\Delta t}{=}tr)$
fafafa	1	0
⋮ ⋮ ⋮	⋮	⋮
tr tr tr	$1\text{-}R_B(\Delta t)$	$R_B(\Delta t)$
tr tr fa	$1\text{-}R_{B\vert C}(\Delta t)$	$R_{B\vert C}(\Delta t)$
tr fa tr	$1\text{-}R_{B\vert A}(\Delta t)$	$R_{B\vert A}(\Delta t)$
tr fafa	$1\text{-}R_{B\vert AC}(\Delta t)$	$R_{B\vert AC}(\Delta t)$

Figure 9. DBN for an 1-out-of-3 redundancy with load sharing. CPT for $C_{t+\Delta t}$ is accordingly defined to $B_{t+\Delta t}$.

To allow for modeling of systems with *warm* redundancy and load sharing, the same DAG and CPT structure is used as shown in Fig. 9. The failure rate of active elements is assumed to be λ and the failure rate for standby elements is $\lambda_r = \alpha\lambda$, which is invariant to element failures. α is called dormancy or degradation factor to indicate lesser degradation of standby elements (Montani et al., 2006). In time slice t, element reliabilities are given by $R_B = R_C = e^{-\lambda_r t}$ for standby elements and $R_A = e^{-\lambda t}$ for active element. Perpetually, the reliabilities in time slice $t + \Delta t$ are defined for one standby element failure as $R_{B|C} = R_{C|B} = e^{-\lambda_r(\Delta t)}$ and for failures of the active and one redundant element $R_{B|AC} = R_{C|AB} = e^{-\lambda(\Delta t)}$.

If warm redundancy is modeled as stated above, it becomes obvious that the arcs $B_t \rightarrow A_{t+\Delta t}$ and $C_t \rightarrow A_{t+\Delta t}$ have no influence on $A_{t+\Delta t}$ and could therefore be neglected. However, due to model consistency, these arcs are kept visible.

The results for reliability of warm redundancy also shown in Fig. 10. Although warm redundancy behaves as expected - it is more reliable than systems with hot spares - its reliability significantly differs from the results obtained using the MC approach. The maximum absolute error between both approaches is $\max(|\ R_{MC} - R_{DBN}\ |) = 3.8\%$.

The DBN outlined in Fig. 9 can also be used to model systems with *cold* redundancy. In cold redundancy, the redundant elements are inactive with idealized reliability. Considering Fig. 9, elements B and C are assumed inactive with $R_B = R_C = 1$ until active element A fails with $R_A = e^{-\lambda t}$ in time slice t. Inherent to this modeling approach of cold, and of warm, redundancy is an activation order for redundant elements B and C. After a failure of A, B is supposed to be activated first, while C is only actived if A and B already failed. Thus, reliabilities after failure of active A or, A and B given by $R_{B|A} = R_{C|AB} = e^{-\lambda(\Delta t)}$. If A did not fail in time slice t, reliability of A in time slice $t + \Delta t$ is given by $R_A = e^{-\lambda(\Delta t)}$; reliabilities of redundant elements B and C are still idealized.

As already stated for warm redundancy, arcs $B_t \rightarrow A_{t+\Delta t}$ and $C_t \rightarrow A_{t+\Delta t}$ can be neglected.

The results obtained from this approach for cold redundancy gives the same results as the MC approch. Since the activation of redundant elements is event-triggered by the failure of active elements, the time step Δt between the time slices has to be chosen appropriately in this DBN approach in order to obtain sustainable results.

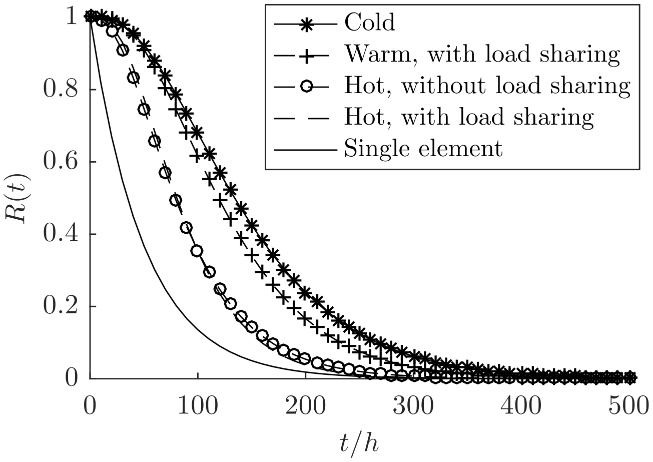


Figure 10. Reliability $R(t)$ modeled with Bayesian approaches

6. DISCUSSION

RBDs are, besides FTs, the most common modeling and analysis method used for systems with redundancy, because of their intuitive representation in parallel structure. However, RBDs and FTs have some major restrictions concerning dynamic or temporal dependencies among elements, which contribute to redundancy, i.e. sequenced failure order, because of the Boolean description of reliability. Hence, RBDs and FTs are not considered for use in Bayesian approaches in this work.

Markovian models offer various approaches to model system reliability in discrete/continuous state space for discrete/ continuous time and are common method to investigate reliability of complex systems. In Sec. 5.1, the state space of the reliability of a redundant subsystem is discretized and evaluated for continuous time using a MC. The obtained reliability of the system with redundancy is afterwards given to a BN, which is used as model of system reliability. The drawbacks that arise from this approach are inherent to Markovian models, such as their limitation to exponentially distributed state transitions. State explosion is not a problem, if Bironilini's approach for modeling redundant subsystems is used, but is still present for complex systems.

Since this work employs BNs or DBNs as models of system reliability, two approaches are introduced and their capability of investigating redundancies is discussed. The introduced approach for BNs has its major limitation in handling dynamic or temporal dependencies such as RBDs and FTs. Anyway, BNs can directly be used for exact modeling of hot spares without load sharing. To overcome this limitation, the DBN approach was developed to cope with redundancies featuring load sharing. The results, obtained from DBNs, were compared to the results of the MC approach. The computed maximum absolute error is significant because BNs and DBNs as well cannot appropriately handle event-based changes in state probabilities, which is necessary to tackle redundancy concepts with load sharing. In order to obtain sustainable results, the time step Δt has to be chosen rather small, making this expensive concerning execution time.

Boudali introduced an *event-based* BN (Boudali & Dugan, 2005) that splits the operating time in discrete intervals and analytically computing the reliability of an element for each interval. The conditional probabilities of the proceeding element are computed as the inherent reliability of the element with reference to the parent element failure in a certain interval of the operating time. The accuracy and execution time depend on the number of intervals and is thus eventually an expensive approach. Another issue might arise from the increasing size of the CPTs due to increasing number of intervals, which makes the handling and filling of the CPTs an exhausting task. However, the proposed method to analytically compute conditional reliabilities in systems with k-out-of-n redundancy might become intractable for sufficiently large n.

Based on (Boudali & Dugan, 2005), Marquez extended the idea of event-based BNs by some kind of dynamic discretization of operating time using *hybrid* BNs in order to improve execution time (Marquez et al., 2010). Hybrid BNs use continuous and discrete variables and cannot perform exact probability updating on nongaussian distributed variables.

In this paper, only exponentially distributed variables, i.e. element reliabilties, are used for simplification purposes. Since DBNs require a stationary process, the structure and conditional probabilies are thus time-invariant, the use of exponentially distributed variables is straight forward and easy to implement (see Eq. 6). Arbitrary distributed variables require more comprehensive approaches to estimate the state probabilities (Nielsen & Jensen, 2009), making the described approaches increasingly complex. However, an extension for arbitrary distributions is necessary to cope with real-world applications, i.e degradation processes that are sufficiently described by Weilbull distributions (Birolini, 2007).

7. CONCLUSION

To allow for modeling of complex redundancy and its basic concepts, established and advanced methods were briefly introduced and three modeling approaches based on Bayesian models were described. These approaches were discussed and compared to the results of established Markov Chains. The major limitations of Bayesian models were outlined in this work and, in order to overcome these limitations, Dynamic Bayesian Networks can be used as an expert system tool to investigate reliability of complex systems.

ACKNOWLEDGEMENT

The authors would like to thank Kevin Murphy for providing access to Bayes Net Toolbox for Matlab (BNT).

REFERENCES

Avižienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, *1*(1), 11–33.

Birolini, A. (2007). *Reliability engineering* (Vol. 5). Springer.

Boudali, H., & Dugan, J. B. (2005). A discrete-time bayesian network reliability modeling and analysis framework. *Reliability Engineering & System Safety*, *87*(3), 337–349.

Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability*, *41*(3), 363–377.

Gausemeier, J., Rammig, F. J., Schäfer, W., & Sextro, W. (2014). *Dependability of self-optimizing mechatronic systems*. Springer.

International Electrotechnical Commission. (1990). *Iec 60050 (191) international electrotechnical vocabulary, chapter 191: Dependability and quality of service.*

Isermann, R. (2002). Fehlertolerante komponenten für drive-by-wire-systeme. *ATZ - Automobiltechnische Zeitschrift*, *104*(4), 382–391.

Kaul, T., Meyer, T., & Sextro, W. (2015). Integrated model for dynamics and reliability of intelligent mechatronic systems. In Podofillini et al (Ed.), *European safety and reliability conference (esrel2015).* Taylor and Francis.

Mahadevan, S., Zhang, R., & Smith, N. (2001). Bayesian networks for system reliability reassessment. *Structural Safety*, *23*(3), 231–251.

Marquez, D., Neil, M., & Fenton, N. (2010). Improved reliability modeling using bayesian networks and dynamic discretization. *Reliability Engineering & System Safety*, *95*(4), 412–425.

Montani, S., Portinale, L., Bobbio, A., Varesio, M., & Codetta-Raiteri, D. (2006). A tool for automatically translating dynamic fault trees into dynamic bayesian networks. In *Reliability and maintainability symposium, 2006. rams'06. annual* (pp. 434–441).

Murphy, K. P. (2002). *Dynamic bayesian networks: representation, inference and learning* (Unpublished doctoral dissertation). University of California, Berkeley.

Murphy, K. P., et al. (2001). The bayes net toolbox for matlab. *Computing science and statistics*, *33*(2), 1024–1034.

Nielsen, T. D., & Jensen, F. V. (2009). *Bayesian networks and decision graphs*. Springer.

Ren, Y., & Dugan, J. B. (1998). Design of reliable systems using static and dynamic fault trees. *IEEE Transactions on Reliability*, *47*(3), 234–244.

Sagan, S. D. (2004). The problem of redundancy problem: Why more nuclear security forces may produce less nuclear security. *Risk Analysis*, *24*(4), 935–946.

Verein Deutscher Ingenieure. (2006). *Vdi-richtlinie 4001 - blatt 2: Termonologie der zuverlässigkeit.* Beuth.

Verein Deutscher Ingenieure. (2007). *Vdi-richtlinie 4003: Zuverlässigkeitsmanagement.* Beuth.

Weber, P., & Jouffe, L. (2003). Reliability modelling with dynamic bayesian networks. In *In 5th ifac symposium on fault detection, supervision and safety of technical processes (safeprocess'03), washington, dc, usa.*

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2012). Overview on bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*, *25*(4), 671–682.

BIOGRAPHIES

Thorben Kaul studied mechanical engineering and mechatronics at the University of Paderborn. Since 2014 he is with the research group Mechatronics and Dynamics at the University of Paderborn. His research focusses on the integrated modeling of dependability and system behaviour.

Tobias Meyer studied mechanical engineering and mechatronics at the University of Paderborn. Since 2011 he is with the research group Mechatronics and Dynamics at the University of Paderborn. His research focusses on the use of self-optimizing techniques to adapt system behaviour in order to increase dependability.

Walter Sextro studied mechanical engineering at the Leibniz University of Hanover and at the Imperial College in London. After his studies he was development engineer at Baker Hughes Inteq in Celle, Germany and Houston, Texas. Back as research assistant at the University of Hanover he was awarded the academic degree Dr.-Ing. in 1997. Afterward he habilitated in the domain of mechanics under the topic Dynamical contact problems with friction: Models, Methods, Experiments and Applications. From 2004-2009 he was professor for mechanical engineering at the Technical University of Graz, Austria. Since March 2009 he is professor for mechanical engineering and head of the research group Mechatronics and Dynamics at the University of Paderborn.