# A Formally Verified Algebraic Approach for Dynamic Reliability Block Diagrams

Yassmeen Elderhalli(✉), Osman Hasan, and Sofiène Tahar

Electrical and Computer Engineering, Concordia University, Montréal, Canada
{y_elderh,o_hasan,tahar}@ece.concordia.ca

**Abstract.** Dynamic reliability block diagrams (DRBDs) are introduced to overcome the modeling limitations of traditional reliability block diagrams, such as the inability to capture redundant components. However, so far there is no algebraic framework that allows conducting the analysis of a given DRBD based on its structure function. In this paper, we propose a new algebra to formally express the structure function and the reliability of a DRBD with spare constructs based on basic system blocks and newly introduced DRBD operators. We present several simplification properties that allow reducing the structure of a given DRBD. We formalize the proposed algebra in higher-order logic to ensure its soundness, and formally verify its corresponding properties using the HOL4 theorem prover. This includes formally verifying generic reliability expressions of the spare costruct, series, parallel and deeper structures in an extensible manner that allows verifying the reliability of complex systems. Finally, we demonstrate the applicability of this algebra by formally analyzing the reliability of two real-world systems in HOL4.

**Keywords:** Dynamic reliability block diagrams · Algebra · Theorem proving · HOL4

## 1 Introduction

Reliability of a system is the probability that it will continue to provide its desirable service in a given period of time. Fault trees (FTs) [14] and reliability block diagrams (RBDs) [8] are the most commonly used reliability modeling techniques. FTs graphically model the sources of failure of a system using FT gates. An RBD, on the other hand, is a graphical representation of the reliability of a system. The components of a system are modeled as blocks and are connected using connectors (lines) to create a path or multiple paths from the RBD input to its output. These paths represent the required working blocks (system components) for the system to have a successful operation. The modeled system fails when components fail in such a manner that leads to the disconnection of all the paths between the input and the output. RBDs can be connected in a *series*, *parallel*, *series-parallel* or *parallel-series* fashion to create the appropriate modeling structure depending on the behavior and the components redundancy


Y. Ait-Ameur and S. Qin (Eds.): ICFEM 2019, LNCS 11852, pp. 253–269, 2019.
https://doi.org/10.1007/978-3-030-32409-4_16

of the modeled system, which provides flexible and extensible modeling configurations to represent complex systems. However, both the traditional RBDs and FTs are unable to model the dynamic behavior of system components, where the change of state of one component can affect the state of other components.

Dynamic fault trees (DFTs) [14] are proposed as an extension to traditional FTs by introducing DFT gates, such as spare gates, to overcome the abovementioned limitation. However, the only behavior that is captured by DFTs is the dynamic failure effect of one system component in the failure or activation of other components. To overcome the modeling limitations of DFTs, RBDs are extended to *dynamic reliability block diagrams* (DRBDs) to model the dynamic dependency among system components by introducing new DRBD blocks [4], which enable capturing the effect of sharing a load and spare constructs that model the reliability of spare parts in a DRBD.

Formal methods have been used in the analysis of RBDs and DRBDs. In [16], the formal semantics of DRBD constructs in Object-Z formalism [15] have been proposed. However, analyzing and verifying the behavior of DRBDs based on this formalism are not feasible due to the non-availability of tool support. Thus, the DRBDs have been proposed to be converted into a Colored Petri Net (CPN) to be analyzed using Petri nets tools [15]. An algorithm to automatically convert a DRBD into a CPN has been also proposed in [13]. However, due to the usage of CPNs, only a few state-based properties of the modeled system can be analyzed. In [1], Ahmed *et al.* used the HOL4 theorem prover [9] to formalize several configurations of static RBDs. However, this formalization can only analyze the combinatorial behavior of systems and cannot be extended to formalize and reason about the dynamic aspects, and hence DRBDs. One of the main reasons for this deficiency is the lists based formalization of independence between multiple failure events. In this paper, we propose a completely new and different formalization from [1] that supersedes these deficiencies. In particular, we propose a more generic formalization of dynamic failure dependencies [7], based on a set-theoretic definition of independence [12] and Lebesgue integral. Thus, our proposed formalization can model and analyze both dynamic and static RBDs.

In system engineering, it is important to be able to analyze DRBDs qualitatively to identify the sources of system vulnerability, and quantitatively to evaluate the system reliability. However, to the best of our knowledge, there is no algebraic approach that mathematically models a given DRBD and enables expressing its function based on basic components just like the DFT algebra [10]. Using such algebra in the reliability analysis will result in simpler and fewer proof steps than the DFT-based algebraic analysis [10], since the probabilistic principle of inclusion and exclusion will not be invoked. In this paper, we propose, for the first time, a new algebraic approach for DRBD analysis that allows having a DRBD expression to be used for both qualitative and quantitative analyses. We introduce new operators to mathematically model the dynamic behavior in DRBD structures and constructs. In particular, we use these operators to model a DRBD spare construct besides traditional series, parallel, series-parallel and parallel-series structures. Moreover, we provide simplification theorems that allow reducing the structure of a given DRBD. This DRBD structure can be then analyzed to obtain a generic expression of the system reliability.

The reliability expressions obtained using this approach are generic and independent of the distribution and density functions that represent the system components. Although basic operators, such as OR and AND, were introduced in [4], they are only useful to model parallel and series constructs of dependent components. In addition, these constructs [4] are quite complex, which makes the modeling of large systems quite difficult. Therefore, we use the constructs proposed in [16] as they are much simpler. Leveraging upon the expressive nature of HOL, we formally verify the soundness of the proposed DRBD algebra using HOL theorem proving. We choose the HOL4 theorem prover for our work to benefit from our existing formalization of DFT algebra. Our ultimate goal is to develop a formally verified algebra that follows the traditional reliability expressions of the series and parallel structures in an easily extensible manner and at the same time can capture the dynamic behavior of real-world systems. Our formalization totally differs from and overcomes the formalization of static RBDs presented in [1] in the sense that it can formally express the structure function of a DRBD using the introduced DRBD operators. In addition, it can formally model and analyze DRBD spare constructs. Furthermore, we model the static RBD structures, i.e., series, parallel and deeper structures in a way similar to the mathematical models available in the literature, which makes it easily understood and followed by reliability engineers that are not familiar with HOL theorem proving. Finally, we illustrate the usefulness of the proposed developments in conducting the formal analysis of two real-world systems: the terminal reliability of a shuffle-exchange network and the reliability of a drive-by-wire system.

## 2 DRBD Algebra

In this section, we present, for the first time, an algebra for DRBD analysis that allows modeling the structure function of DRBDs with spare constructs. Moreover, we present some simplification properties that enable reducing the structure function when possible. Throughout this work, we assume that system components or blocks are represented by random variables that in turn represent their time-to-failures. In addition, we assume that system components are non-repairable, i.e., we are interested in expressing the reliability of the system considering that the failed components will not be repaired. It is worth mentioning that our proposed algebra follows the general lines for the DFT algebra [10].

The reliability of a single component, which time-to-failure function is represented by random variable $X$, is mathematically defined as [8]:

$$R_X(t) = Pr\{s \mid X(s) > t\} = 1 - Pr\{s \mid X(s) \leq t\} = 1 - F_X(t) \quad (1)$$

where $F_X(t)$ is the cumulative distribution function (CDF) of $X$. We call $\{s \mid X(s) > t\}$ as a DRBD event as it represents the set that we are interested in finding the probability of until time $t$:

$$event\ (X,\ t)\ =\ \{s \mid X(s)\ >\ t\} \quad (2)$$

### 2.1 Identity Elements, Operators and Simplification Properties

Similar to the identity elements of ordinary Boolean algebra and DFT algebra [10], we introduce two identity elements, i.e., ALWAYS and NEVER, that represent two states of any system block. The *ALWAYS* element represents a system component that stops working from time 0 ($ALWAYS = 0$). While the *NEVER* element represents a component that continues to work until $+\infty$, i.e., its failure time is $+\infty$ ($NEVER = +\infty$). These identity elements play an important role in the reduction process of the structure functions of DRBDs. We introduce operators to model the relationship between the various blocks in a DRBD. These operators can be divided into two categories: (1) The AND and OR operators that are not concerned with the dependencies among system components. (2) Temporal operators, i.e., *After*, *Simultaneous* and *Inclusive After*, that can capture the dependencies between system components. DRBDs are concerned with modeling the several paths of success of a given system. Thus, if we are concerned in the success behavior of a DRBD until time $t$, it means that we are interested in how the system would not fail until time $t$. As a result, we can use the time-to-failure random variables in modeling the time-to-failure of a given DRBD, i.e., its structure function. It is assumed that for any two system components that possess continuous failure distribution functions, the possibility that these components fail at the same time can be neglected.

In [4], AND and OR operators were introduced to model the parallel and series constructs between dependent components only without providing any mathematical model to these operators. We propose to use the AND ($\cdot$) and OR ($+$) operators to model series and parallel blocks in a DRBD, respectively, without any restriction. We provide a mathematical model for each operator based on the time of failure of its inputs, as listed in Table 1, to be used in the proposed algebra. The AND operator models the series connection between two or more system blocks. For example, the 2-block series DRBD in Table 1 continues to work only if components $X$ and $Y$ are working. We model the AND operator as the minimum time of its input arguments. Similarly, the OR operator models the connection between parallel components in a DRBD, i.e., all the components in a parallel structure should fail for this DRBD to fail. We model the OR operator as the maximum time of failure of its input arguments that represent basic system blocks or sub-DRBDs. This approach facilitates using these operators to model even the complex structures. If $X$ and $Y$ are independent, then the reliability of the 2-block systems can be expressed as given in Table 1. To reach these expressions, we need to express the DRBD events as the intersection and union for the AND and OR operators, respectively.

**Table 1.** Mathematical and reliability expressions of AND and OR operators

| Operator | Math. Model | Reliability | 2-block Structure |
|---|---|---|---|
| AND | $X{\cdot}Y{=}min\ (X{,}Y)$ | $R_{(X\cdot Y)}(t) = R_X(t) \times R_Y(t)$ | Series  |
| OR | $X{+}Y{=}max\ (X{,}Y)$ | $R_{(X+Y)}(t) = 1-((1-R_X(t))\times(1-R_Y(t)))$ | Parallel  |

**Table 2.** Mathematical expressions of temporal operators

| After ($\rhd$) | Simultaneous ($\Delta$) | Inclusive after ($\trianglerighteq$) |
|---|---|---|
| $X \rhd Y = \begin{cases} X, & X > Y \\ +\infty, & X \leq Y \end{cases}$ | $X \Delta Y = \begin{cases} X, & X = Y \\ +\infty, & X \neq Y \end{cases}$ | $X \trianglerighteq Y = \begin{cases} X, & X \geq Y \\ +\infty, & X < Y \end{cases}$ |

$$event\ ((X \cdot Y),\ t)\ =\ event\ (X,\ t)\ \cap\ event\ (Y,\ t) \tag{3}$$

$$event\ ((X + Y),\ t)\ =\ event\ (X,\ t)\ \cup\ event\ (Y,\ t) \tag{4}$$

In order to model the dynamic behavior of systems in DRBDs, we introduce new temporal operators: *after* ($\rhd$), *simultaneous* ($\Delta$), and *inclusive after* ($\trianglerighteq$), as listed in Table 2. The *after* operator represents a situation where it is required to model a component that continues to work after the failure of another. The time of failure of the after operator equals the time of failure of the last component, which is required to fail. However, if the required sequence does not occur, then the output can never fail, i.e., the time of failure equals $+\infty$. The behavior of the simultaneous operator is similar to the one introduced in the DFT algebra [10]. The output of this operator fails if both its inputs fail at the same time, otherwise it can never fail. Finally, the inclusive after operator encompasses the behavior of both the after and simultaneous operators, i.e, it models a situation where it is required that one component continues to work after another one or fail at the same time, otherwise it can never fail. When dealing with basic components, the inclusive after will behave in a similar way as the after operator. Therefore, their probabilities can be expressed for independent random variables as:

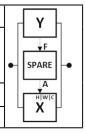
$$R_{(X \rhd Y)}(t) = 1 - \int_0^t f_X(x) \times F_Y(x)\ dx \tag{5}$$

where $f_X$ is the probability density function (PDF) of $X$ and $F_Y$ is the CDF of $Y$. We introduce several simplification properties to reduce the structure function of a DRBD. These simplification properties range from simple ones, such as the associativity and idempotence of the operators, to more complex theorems. The idea of these properties is to reduce the algebraic expressions based on the time of failure. For example, $X \cdot ALWAYS = ALWAYS$ means that if a component in a series structure is not working, i.e., always fails, then the series structure is not working. The full list of simplification theorems is available at [6].

### 2.2 DRBD Constructs and Structures

The spare construct, shown in Table 3 [16], is introduced in DRBDs to model situations where a spare part is activated and replaces the main part, after its failure, by introducing a spare controller to activate the spare [16]. Depending on the failure behavior of the spare part, we can have three variants, i.e., hot, warm and cold ($H|W|C$) spares. For the hot spare (HSP) construct, the spare possesses the same failure behavior in both its active and dormant states.

**Table 3.** Mathematical and reliability expressions of spare constructs

| Math. Model | Reliability | |
|---|---|---|
| $Q_{WSP}=(X_a \rhd Y)\cdot(Y \rhd X_d)$ | $R_{WSP}(t)=1-\int_0^t \int_y^t f_{(X_a \mid Y=y)}(x)\ f_Y(y)dxdy - \int_0^t f_Y(y)F_{X_d}(y)dy$ |  |
| $Q_{CSP}=X_a \rhd Y$ | $R_{cold\ spare}(t)=1-\int_0^t \int_y^t f_{(X_a \mid Y=y)}(x)\ f_Y(y)\ dx\ dy$ | |
| $Q_{HSP}=X+Y$ | $R_{HSP}(t)=1-((1-R_X(t))\times(1-R_Y(t)))$ | |



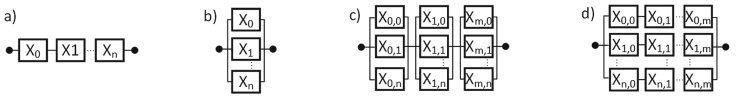



**Fig. 1.** DRBD Structures: (a) Series, (b) Parallel, (c) Series-Parallel (d) Parallel-Series

The cold spare (CSP) cannot fail in its dormant state and is only activated after the failure of the main part. The failure behavior of the warm spare (WSP) in the dormant state is attenuated by a dormancy factor from the active state. In order to distinguish between the dormant and active states of the spare, just like the DFT algebra [10], we use two different symbols to model the spare part of the DRBD spare construct, one for the dormant state and the other for the active one. For the WSP construct, in Table 3, the spare $X$ is represented by $X_a$ and $X_d$ for the active and dormant states, respectively. After the failure ($F$) of the main part $Y$, $X$ will be activated ($A$) by the spare controller. We model the structure function of the WSP construct ($Q_{WSP}$) using the DRBD operators based on the description of its behavior as given in Table 3. Thus, we need two conditions to be satisfied in order for the spare to work. Firstly, the active state of the spare will continue to work after the failure of the main part ($X_a \rhd Y$). Secondly, the main part will continue to work after the failure of the spare in its dormant state ($Y \rhd X_d$). However, since the spare part can only fail in one of its states ($X_a, X_d$) but not both as it is non-repairable, only one of the terms of the $Q_{WSP}$ affects the behavior and the other can never fail, i.e., it fails at $+\infty$.

Since the DRBD spare construct and the DFT spare gate exhibit complementary behavior, i.e., the DRBDs consider the success and the DFTs consider the failure, we can use the probability of failure of the warm spare DFT gate [10] to find the reliability of the WSP DRBD construct. It is assumed that the dormant spare and the main part are independent since the failure of one does not affect the failure of the other. However, the failure of the active spare is affected by the time of failure of the main part, since it will be activated after the failure of the main part. Thus, we express the reliability of the WSP as given in Table 3, where $f_{(X_a|Y=y)}$ is the conditional density function of $X_a$ given that $Y$ failed at time $y$. $Q_{WSP}$ and $R_{WSP}$ represent the general behavior of the spare, i.e., the warm spare. The hot and cold spares represent its special cases and can be expressed as given in Table 3. For $Q_{HSP}$, the spare part $X$ has the same behavior in both states and thus there is no need to distinguish both states. The reliability of CSP and HSP (using the OR operator) can be expressed as given in Table 3.

**Table 4.** Mathematical and reliability expressions of DRBD structures

| Structure | Math. Model | Reliability expression |
|---|---|---|
| Series | $\bigcap_{i=1}^{n}(event\ (X_i,\ t))$ | $\prod_{i=1}^{n} R_{X_i}(t)$ |
| Parallel | $\bigcup_{i=1}^{n}(event\ (X_i,\ t))$ | $1-\prod_{1=1}^{n}(1-R_{X_i}(t))$ |
| Series-Parallel | $\bigcap_{i=1}^{m}\bigcup_{j=1}^{n}(event\ (X_{(i,j)},\ t))$ | $\prod_{i=1}^{m}(1-\prod_{j=1}^{n}(1-R_{X_{(i,j)}}(t)))$ |
| Parallel-Series | $\bigcup_{i=1}^{n}\bigcap_{j=1}^{m}(event\ (X_{(i,j)},\ t))$ | $1-(\prod_{i=1}^{n}(1-\prod_{j=1}^{m}(R_{X_{(i,j)}}(t))))$ |

The series structure (Fig. 1(a)) represents a collection of blocks that are connected in series. The system continues to work until the failure of one of these blocks. We define a series structure that represents the intersection of all events of the blocks in this structure as in Table 4, where $X_i$ represents the $i^{th}$ block in the series structure and $n$ is the number of blocks. Interestingly, any block in our proposed algebra can represent a basic system component or a complex structure, such as a spare construct. Moreover, since we are dealing with the events, we can use the ordinary reliability expressions for the series structure assuming the independence of the individual blocks. The parallel structure (Fig. 1(b)) represents a system that continues to work until the failure of the last block in the structure. The behavior of the parallel structure can be expressed using the OR operator. We represent the parallel structure as the union of the individual events of the blocks. The series-parallel structure (Fig. 1(c)) represents a series structure, where the blocks of the series structure are parallel structures. The structure function of this structure can be expressed using AND of ORs operators. Table 4 lists the model for this structure with its reliability expression, where $n$ is the number of blocks in the parallel structure and $m$ is the number of parallel structures that are connected in series. The parallel-series structure (Fig. 1(d)) represents a group of series structures that are connected in parallel. Its structure function can be expressed using OR of ANDs operators.

## 3 Formalization of DRBDs in HOL

In this section, we present our formalization for the newly proposed DRBD algebra including DRBD events, operators, constructs, simplification theorems and reliability expressions. First, we review some HOL probability theory preliminaries required for understanding the rest of the paper.

### 3.1 HOL Probability Theory

The probability space is defined in HOL as a measure space, where the measure (probability) of the entire space is 1. It is defined as a triplet $(\Omega, \mathcal{A}, \mathcal{P}r)$, where $\Omega$ is the space, $\mathcal{A}$ are the probability events and $\mathcal{P}r$ is the probability [11]. Two functions are defined in HOL; `p_space p` and `events p`, that return the space

($\Omega$) of the above triplet and the events ($\mathcal{A}$), respectively. A random variable is a measurable function that maps the probability space $p$ to another space [11].

The cumulative distribution function (CDF) is defined as [7]:

**Definition 1.** $\vdash \forall$`p X t. CDF p X t = distribution p X {y | y ≤ (t:real)}`

where `p` is a probability space, `X` is a real-valued random variable, `t` is a variable of type real that represents time and `distribution` is defined as the probability that a random variable belongs to a certain set; {`y|y≤(t:real)`} in this case.

Independence of random variables is an important property that ensures that the probability of the intersection of the events of these random variables equals the product of the probability of the individual events. We use `indep_vars p M X ii` [12] to ensure that a group $X$ is composed of random variables indexed by the elements in set $ii$ and that the events represented by the preimage of these random variables are independent using `indep_sets`. `indep_var` is defined, based on `indep_vars`, to capture the behavior of independence for two random variables [12]. More details about these definitions can be found in [6].

Finally, the Lebesgue integral is defined in HOL4 based on positive simple functions and then extended for positive functions and functions with positive and negative values [11]. Throughout this work, we use the Lebesgue integral for positive functions, i.e., `pos_fn_integral`, since we are integrating distribution and density functions, which are always positive. The integration is over the real line and thus we use the Lebesgue-Borel measure (`lborel`) [12] for this purpose. For the ease of understanding, we use the regular mathematical expressions.

### 3.2 DRBD Event

In our formalization, we define the inputs, or the random variables representing the time-to-failure of system components, as lambda abstracted functions with a return datatype of extended-real (`extreal`), which represents real numbers and $\pm\infty$. We define the DRBD event of Eq. (2) as:

**Definition 2.** $\vdash \forall$`p X t. DRBD_event p X t = { s | Normal t < X s} ∩ p_space p`

where `Normal` typecasts the real value of `t` from real to `extreal`. This type conversion is required since we need real-valued random variables. However, we need to deal with `extreal` datatype to model the `NEVER` element. Thus, we define the time-to-failure functions to return `extreal` and typecast the values from `extreal` to real using the function `real` and vice versa using `Normal`.

We define the reliability as the probability of the DRBD event (Eq. (1)):

**Definition 3.** $\vdash \forall$`p X t. Rel p X t = prob p (DRBD_event p X t)`

We verify the reliability-CDF relationship (Eq. (1)) as:

**Theorem 1.** $\vdash \forall$`p X t. rv_gt0_ninfinity [X] ∧`
`random_variable (real o X) p borel ⇒ (Rel p X t = 1- CDF p (real o X) t)`

where `real` typecasts the values of the random variable from `extreal` to real as the CDF is defined for real-valued random variables, `random_variable (real o X) p borel` ensures that `(real o X)` is a random variable over the real line represented by the `borel` space [12], and `rv_gt0_ninfinity` ensures that the random variable is greater than or equal to 0 and not equal to $+\infty$, which means that the time of failure of any component cannot be negative or $+\infty$. Theorem 1 is verified based on the fact that the `DRBD_event` and the set of the CDF are the complement of each other. Therefore, the probability of one of them equals one minus the other. For the rest of the paper, we will denote `CDF p (real o X) t` by $F_X(t)$ to facilitate the understanding of the theorems.

### 3.3 Identity Elements, Operators and Simplification Theorems

Our formalization of the identity elements and DRBD operators is listed in Table 5, where `extreal` is the extended-real datatype in HOL4, `PosInf` represents $+\infty$, and `min` and `max` return the minimum and maximum values of their arguments, respectively. This formalization follows the proposed definitions in Tables 1 and 2. However, we define the operators as lambda abstracted functions to be able to conduct the probabilistic analysis later. We verify several simplification theorems based on the properties of `extreal` numbers in HOL. The full list of these theorems and the proof script are available at [6] and [5], respectively.

In order to verify the reliability of the DRBD constructs, such as the spare, we need first to verify the reliability of the DRBD operators that are used to express the structure function of these constructs. For the AND and OR operators, we verify their reliability expressions as in Theorems 2 and 3, respectively.

**Theorem 2.** $\vdash$ `∀p X t. rv_gt0_ninfinity [X;Y] ∧`
`indep_var p lborel (real o X) lborel (real o Y) ⇒`
`(Rel p (X·Y) t = Rel p X t * Rel p Y t)`

**Theorem 3.** $\vdash$ `∀p X t. rv_gt0_ninfinity [X;Y] ∧`
`indep_var p lborel (real o X) lborel (real o Y) ⇒`
`(Rel p (X + Y) t = 1 - (1 - Rel p X t) * (1 - Rel p Y t))`

We verify Theorem 2 by first rewriting using Definition 3. Then, we prove that `DRBD_event` of the AND operator equals the intersection of the individual events, as in Eq. (3). Utilizing the independence of the real-valued random variables `(real o X)` and `(real o Y)`, the probability of intersection of their events equals the product of the probability of the individual events. Since `X` and `Y` are greater than 0 and are not equal to $+\infty$, based on the function `rv_gt0_ninfinity`, the events in the probability space that correspond to $X$ and $Y$ are equal to the ones that correspond to `real o X` and `real o Y`. As a result, the `DRBD_events` of `X` and `Y` are independent. Hence, the probability of their intersection equals the product of the probability of the individual events, i.e., their reliability. Theorem 3 is verified in a similar way. However, we prove that the `DRBD_event` of the OR operator equals the union of the individual events, as in Eq. (4).

**Table 5.** Definitions of identity elements and DRBD operators

| Element/Operator | Mathematical expression | Formalization |
|---|---|---|
| `Always element` | $ALWAYS = 0$ | ⊢ `R_ALWAYS = (λs. (0:extreal))` |
| `Never element` | $NEVER = +\infty$ | ⊢ `R_NEVER = (λs. PosInf)` |
| `AND` | $X \cdot Y = min(X,Y)$ | ⊢ `∀X Y. R_AND X Y =(λs. min (X s) (Y s))` |
| `OR` | $X + Y = max(X,Y)$ | ⊢ `∀X Y. R_OR X Y = (λs. max (X s) (Y s))` |
| `After` | $X \triangleright Y = \begin{cases} X, & X > Y \\ +\infty, & X \leq Y \end{cases}$ | ⊢ `∀X Y. R_AFTER X Y = (λs. if Y s < X s then X s else PosInf)` |
| `Simultaneous` | $X \Delta Y = \begin{cases} X, & X = Y \\ +\infty, & X \neq Y \end{cases}$ | ⊢ `∀X Y. R_SIMULT X Y = (λs. if X s = Y s then X s else PosInf)` |
| `Inclusive After` | $X \trianglerighteq Y = \begin{cases} X, & X \geq Y \\ +\infty, & X < Y \end{cases}$ | ⊢ `∀ X Y. R_INCLUSIVE_AFTER X Y = (λs. if Y s ≤ X s then X s else PosInf)` |

We verify that this union of events equals to the complement of the intersection of the complements of the individual events. Then, Theorem 3 can be proven using the independence of random variables.

We extend the definition of the AND and OR operators to n-ary operators, `nR_AND` and `nR_OR`, that can be used to represent the relationship between an arbitrary number of elements. We formally define `nR_AND` and `nR_OR` as:

**Definition 4.**
⊢ `∀X s. nR_AND X s = ITSET (λe acc. R_AND (X e) acc) s R_NEVER`

**Definition 5.**
⊢ `∀X s. nR_OR X s = ITSET (λe acc. R_OR (X e) acc) s R_ALWAYS`

where `ITSET` is the HOL function to iterate over sets. These definitions apply the `R_AND` and `R_OR` over the elements of `X` indexed by the numbers in `s`. `R_NEVER` and `R_ALWAYS` are the identity elements of the `R_AND` and `R_OR` operators, respectively. The reliability of these operators is similar to the reliability of the series and parallel structures, respectively, as will be described in the following section.

Finally, we verify the reliability expression of the after operator as:

**Theorem 4.** ⊢ `∀X Y p` $f_x$ `t. rv_gt0_ninfinity [X; Y] ∧ 0 ≤ t ∧ indep_var p lborel (real o X) lborel (real o Y) ∧ distributed p lborel (real o X)` $f_x$ `∧ (∀x. 0 ≤` $f_x$ `x) ∧ cont_CDF p (real o Y) ∧ measurable_CDF p (real o Y) ⇒ (Rel p (X ▷ Y) t = 1-` $\int_0^t f_X(x) \times F_Y(x)\, dx$)

where `distributed p lborel (real o X)` $f_x$ ensures that random variable `real o X` has a PDF $f_x$, `cont_CDF` and `measurable_CDF` ensure that $F_y$ is continuous and measurable [7]. The proof of this theorem is based on $Pr(Y < X < t) = \int_0^t f_X(x) \times F_Y(x)\, dx$, which is verified in [7] using the properties of the Lebesgue integral and independence of random variables. As the DRBD and DFT events complement one another, the above expression allows us to verify the reliability expression of the *after* operator, since it represents a situation where the system continues to work until two components fail in sequence.

### 3.4 DRBD Constructs and Their Reliability Expressions

We present the formalization of the warm spare (WSP) construct. The expressions of the rest of the spares; hot and cold, can be found in [6].

**Definition 6.** $\vdash$ `∀Y Xa Xd. R_WSP Y Xa Xd = (Xa ▷ Y) · (Y ▷ Xd)`

Since the DRBD and DFT events complement one another, we use our formalization of the probability of failure of the warm spare gate [7] to verify the reliability of the WSP construct:

**Theorem 5.** $\vdash$ `∀p Y Xa Xd t fY fXaY fXa|Y. 0 ≤ t ∧`
`(∀s. ALL_DISTINCT [Xa s; Xd s; Y s]) ∧ DISJOINT_WSP Y Xa Xd t ∧`
`rv_gt0_ninfinity [Xa; Xd; Y] ∧ den_gt0_ninfinityfXaY fY fXa|Y ∧`
`∀y. cond_density lborel lborel p (real o Xa)(real o Y) y fXaY fY fXa|Y) ∧`
`indep_var p lborel (real o Xd) lborel (real o Y) ∧`
`cont_CDF p (real o Xd) ∧ measurable_CDF p (real o Xd) ⇒`
$\big($`Rel p (R_WSP Y Xa Xd) t)=1-(`$\int_0^t f_Y(y) * (\int_y^t$ `f(Xa|Y=y) (x) dx)dy+`$\int_0^t$ `fY(y)FXd(y)dy`$\big)$

where `ALL_DISTINCT` ensures that the main and spare parts cannot fail at the same time, `DISJOINT_WSP Y Xa Xd t` ensures that until time `t`, the spare can only fail in one of its states and `den_gt0_ninfinity` ascertains the proper values of the density functions; joint ($0 \leq f_{XY}$), marginal ($0 < f_Y$) and conditional ($0 \leq f_{X_a|Y}$) [7]. Theorem 5 is verified by first defining a conditional density function `fXa|Y` for random variables (`real o Xa`) and (`real o Y`) using `cond_density`. This is required as the failure of the spare part is affected by the time of failure of the main part. Therefore, it is required to define this conditional density function then prove the expression based on the probability of failure of the DFT spare gate, which is verified based on the properties of the Lebesgue integral.

The formal definitions of the series and parallel structures are listed in Table 6. We define the series structure as a function that accepts a group of sets, `Y`, that are indexed by the numbers in set `s` and returns the intersection of these sets. The parallel structure is defined in a similar way but it returns the union of the sets rather than the intersection. The group of sets, `Y`, in both structures represents a family of events, i.e, `Y` will be instantiated later with DRBD events. We verify the reliability expressions of the series and parallel structures, given in Table 4, as shown in Table 6, where `s≠{} ∧ FINITE s` ensures that the set of indices, `s`, is nonempty and finite. The reliability of the series structure is verified based on the independence of the input events using `indep_sets`, which ensures that for the probability space `p`, the given group of sets (`(λi. {rv_ti_event p X t i})`) indexed by the numbers in set `s` are independent. The family of sets (`(λi. {rv_to_event p X t i})`) represents the DRBD events of the group of time-to-failure functions, `X`, where `rv_to_event` is defined as:

**Definition 7.** $\vdash$ `∀p X t. rv_to_event p X t = (λi. DRBD_event p (X i) t)`

This function enables us to create the group of `DRBD_event` of time-to-failure functions of system blocks (`X`). Based on the independence of these sets and the definition of the series structure (intersection of sets), we verify that the

probability of the series structure equals to the product of the reliability of the individual blocks (`Rel p (X i) t`), where `i`$\in$`s`. The product function ($\prod$) in HOL4 returns a real value and the probability returns `extreal`, therefore, it is required to typecast the product function to `extreal` using `Normal`. Similarly, the product function finds the product of real-valued functions, thus, it is required to typecast the reliability function (`Rel`) to real using the `real` function. Similarly, we replace the parallel structure (the union of events) with the complement of the intersection of the complements of the events. Then, we verify that the probability of this complement equals one minus the probability of the intersection of the complements. This requires the condition that all DRBD events created using `rv_to_event` belong to the events of the probability space `p`.

We verify that the series and parallel structures are equal to the DRBD events of the `nR_AND` and `nR_OR`, respectively.

**Table 6.** Formal definitions and reliability of the series and parallel structures

| | Series Structure | Parallel Structure |
|---|---|---|
| Definition | $\vdash \forall$Y s. DRBD_series Y s = $\bigcap_{i \in s}$ (Y i) | $\vdash \forall$Y s. DRBD_parallel Y s = $\bigcup_{i \in s}$ (Y i) |
| Reliability | $\vdash \forall$p X t s. s $\neq \{\} \wedge$ FINITE s $\wedge$ indep_sets p ($\lambda$i. {rv_to_event p X t i}) s $\Rightarrow$ (prob p (DRBD_series (rv_to_event p X t) s) = Normal ($\prod_{i \in s}$ (real (Rel p (X i) t)))) | $\vdash \forall$p X t s. s $\neq \{\} \wedge$ FINITE s $\wedge$ indep_sets p ($\lambda$i. {rv_to_event p X t i}) s $\wedge$ ($\forall$i. i $\in$ s $\Rightarrow$ rv_to_event p X t i $\in$ events p) $\Rightarrow$ (prob p (DRBD_parallel (rv_to_event p X t) s) = 1 - Normal ($\prod_{i \in s}$ (real (1 - Rel p (X i) t)))) |

**Theorem 6.** $\vdash \forall$p X t s. FINITE s $\wedge$ s $\neq \{\} \Rightarrow$
(DRBD_event p (nR_AND X s) t = DRBD_series (rv_to_event p X t) s)

**Theorem 7.** $\vdash \forall$p X t s. FINITE s $\wedge$ 0 $\leq$ t $\Rightarrow$
(DRBD_event p (nR_OR X s) t = DRBD_parallel (rv_to_event p X t) s)

We verify Theorems 6 and 7 by inducting on set `s` using `SET_INDUCT_TAC` that creates two subgoals to be solved; one for the empty set and another one for inserting an element to a finite set. Then, we use the fact that the DRBD events of the AND and OR operators equal the intersection and the union of the individual events, respectively. For Theorem 7, an additional condition is required, 0 $\leq$ t, to be able to manipulate the sets and reach the final form of the theorem.

These structures can be easily extended to model and verify more complex structures, such as two-level structures, i.e., series-parallel and parallel-series structures, as shown in Table 7. The main idea in building these two-level structures is to partition the family of blocks into distinct groups, where we use a set, `J`, to index these partitions, i.e., it has the number of groups in the first top level. For each group in this top level, we have another set, {s j| j $\in$ J}, that has the indices of the blocks in the second level, i.e. the subgroups. For example, for the parallel-series structure of Fig. 1(d), if $n = m = 1$, then the outer parallel

structure has two series structures, where each series structure has two blocks. Thus, `J = {0;1}`. For each `j` ∈ `J`, we have a certain set `s j` that has the indices of the blocks in the inner series structure. Thus, `s = (λj. if j = 0 then {0;1} else {2;3})`. This also applies to the series-parallel structure. Therefore, the structure of the DRBD can be determined based on the given sets of indices.

We verify the theorems in Table 7 by extending the proofs of the series and parallel structures. However, it is required to deal with the intersection of unions in case of the series-parallel structure and the union of intersections in case of parallel-series structure. Therefore, we need to extend the independence of sets properties to include the independence of union and intersection of partitions of the events. We verify the independence of union of partitions as:

**Theorem 8.** ⊢ ∀p s J Y. `indep_sets p (λi. {Yi}) ⋃`$_{j\in J}$ `(s j) ∧ J ≠ {} ∧ (∀i. i ∈ J ⇒ countable (s i)) ∧ FINITE J ∧ disjoint_family_on s J ⇒ indep_sets p (λj. {⋃`$_{i\in s\ j}$ `(Y i)}) J`

where sets `J` and `s` have the indices of the partitions and the individual blocks of each partition, respectively, `disjoint_family_on` ensures that the indices of the blocks in different partitions are disjoint and `indep_sets p (λi. {Y i}) ⋃`$_{j\in J}$ `(s j)` ensures the independence of the family of blocks `{Y i}` where the indices of the individual blocks are given by the union of `s`. Similarly, we verify the independence of intersection of partitions and the details can be found in [6].

In order to verify the reliability of the series-parallel structure, we need to ensure the independence of the individual blocks. Therefore, we combine the indices of all blocks into a single set using ⋃$_{j\in J}$ `(s j)` to be used with `indep_sets`. To be able to use the reliability of the series structure in this proof, we use Theorem 8 to verify the independence of the unions of partitions of events. This means verifying that the parallel structures are independent, i.e., the probability of intersection of these parallel structures equals the product of the reliability of the parallel structures. Several assumptions related to sets {`s`

**Table 7.** Verified reliability of the series-parallel and parallel-series structures

| Reliability of Series-Parallel Structure | Reliability of Parallel-Series Structure |
|---|---|
| ⊢ ∀p X t s J.<br>indep_sets p<br>(λi. {rv_to_event p X t i}) (⋃$_{j\in J}$(s j)) ∧<br>(∀i. i ∈ J ⇒ s i ≠ {} ∧ FINITE (s i)) ∧<br>FINITE J ∧ J ≠ {} ∧ disjoint_family_on s J ⇒<br>(prob p<br>(DRBD_series<br>(λj. DRBD_parallel<br>(rv_to_event p X t) (s j)) J) =<br>Normal<br>(∏$_{j\in J}$<br>(1 − ∏$_{i\in(s\ j)}$ (real (1 − Rel p (X i) t))))) | ⊢ ∀p X t s J.<br>indep_sets p<br>(λi. {rv_to_event p X t i}) (⋃$_{j\in J}$(s j))∧<br>(∀i. i ∈ ⋃$_{j\in J}$(s j) ⇒<br>rv_to_event p X t i ∈ events p) ∧<br>(∀i. i ∈ J ⇒ s i ≠ {} ∧ FINITE (s i)) ∧<br>FINITE J ∧ J ≠ {} ∧<br>disjoint_family_on s J ⇒<br>(prob p<br>(DRBD_parallel<br>(λj. DRBD_series<br>(rv_to_event p X t) (s j)) J) =<br>1 −<br>Normal<br>(∏$_{j\in J}$<br>(1 − ∏$_{i\in(s\ j)}$ (real (Rel p (X i) t))))) |

i| i ∈ J} and J are required, i.e., these sets are finite and nonempty. Finally, disjoint_family_on ensures that every block has a unique index. The reliability of the parallel-series structure is verified in a similar manner based on the reliability of the parallel structure and the independence of the intersection of partitions of events rather than the union. In addition, it is required that all DRBD events belong to the events of the probability space.

We extend the reliability of the series-parallel structure to verify the reliability of a four-level nested structure, i.e., series-parallel-series-parallel. For this, we have four sets (indexed sets) that determine the structure of the DRBD. We verify the four-level nested structure using two main steps. We first verify the reliability of the outer series-parallel, which requires verifying the independence of the intersection of union of partitions of the DRBD blocks, i.e., the inner series-parallel structures are independent. Then, we verify the reliability of the inner series-parallel structures based on some set manipulation. This way, we can verify even deeper structures, which would require verifying the independence of more nested structures. We use the nested four-level structure to verify the reliability of the series-parallel-series structure as it represents a special case of the series-parallel-series-parallel, where each of the innermost parallel structures has only one block. More details about this proof can be found in [6]. Our formalization follows the natural definitions of parallel and series structures. Moreover, our verified lemmas of independence allow verifying deeper structures, which makes our formalization flexible and applicable to model the most complex systems.

## 4 Applications

To demonstrate the applicability of our proposed DRBD algebra, we formally analyze the reliability of a drive-by-wire system (DBW) [2] and a shuffle-exchange network (SEN) [3] (Fig. 2) to verify generic expressions that are independent of the failure distribution of system components, i.e., we can use different types of distributions to model the failure of components as long as they satisfy the required conditions, such as the continuity. We present here the details of the SEN system due to space limitations and the details of the formal reliability analysis of the DBW system is available at [6].

A SEN is a single-path multistage interconnection network (MIN) that provides the necessary switching in multi-processor systems [3]. It consists of sources (inputs) and destinations (outputs), where only one possible path is available between each source and destination. To increase the reliability of such network,

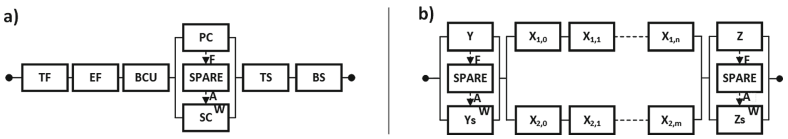



**Fig. 2.** DRBD of: (a) DBW and (b) SEN with spare constructs

additional switching elements are added to provide additional paths between each source and destination. A SEN having two paths between each source and destination is usually called SEN+. The terminal reliability analysis, which is the reliability of the connection between a given source and destination, is usually conducted using static RBDs [3]. However, each source and destination are always connected to single switches, where their failure leads to the failure of the connection. Therefore, we propose to further enhance the reliability of this connection by using spare parts that replace these single switches after failure. Thus, we model the reliability of the modified SEN+ system using DRBDs, as shown in Fig. 2(b), where $Y$ and $Z$ are the main single switches that are connected to the source and destination with their spares $Ys$ and $Zs$, respectively. The parallel structure in the middle represents the reliability model of the two alternative paths between the source and the destination. We formally express the structure function of this DRBD as:

```
Q_SEN = nR_AND (λi. if i = 0 then R_WSP Y Ys_a Ys_d
                    else if i = 1 then ((nR_AND X L1) + (nR_AND X L2))
                    else R_WSP Z Zs_a Zs_d) {0; 1; 2}
```

Thus, the outer series structure is expressed using the `nR_AND` operator over the set $\{0;1;2\}$ as this structure has three different structures; i.e., two spare constructs and one parallel structure, and `L1` and `L2` are the sets that have the indices of the components in the inner series structures. In order to re-utilize the verified expressions of reliability, we verify that the DRBD event of the $\mathtt{Q_{SEN}}$ is equal to a nested series-parallel-series structure to verify a generic expression for the reliability of the SEN+ system:

**Theorem 9.** $\vdash \forall$ `p X Y Ys_a Ys_d Z Zs_a Zs_d t L1 L2.`

```
SEN_set_req p L1 L2 (ind_set [{0}; L1; L2; {3}])
  (ind_set [{0}; {1; 2}; {3}]) {0; 1; 2}
  (event_set[(DRBD_event p (R_WSP Y Ys_a Ys_d) t,0);
             (DRBD_event p (R_WSP Z Zs_a Zs_d) t,3 )] (rv_to_event p X t)) ⇒
(prob p (DRBD_event p Q_SEN t) =
Rel p (R_WSP Y Ys_a Ys_d) t * Rel p (R_WSP Z Zs_a Zs_d) t *
(1 - (1 - Normal (∏_{l∈L1} (real (Rel p (X l) t)))) *
     (1 - Normal (∏_{l∈L2} (real (Rel p (X l) t))))))
```

where `SEN_set_req` ensures that the input sets are finite and nonempty. It also ensures the independence of the input events over the probability space and that they belong to the probability events. `ind_set` and `event_set` generate the proper indices for the blocks in the structure. Their description can be found in [6]. The reliability of the spare constructs can be further rewritten using Theorem 5 given that the required conditions are ensured. The final theorem with the expressions of the reliability of the spare constructs is available in [5]. The proof scripts of the DBW and SEN required around 150 and 1020 lines, respectively, and are available at [5]. Finally, we evaluate, using MATLAB, the reliability of the DBW assuming exponential distribution with failure rates as given in Fig. 3. We also evaluate the reliability of the SEN system (Fig. 3) assuming the same

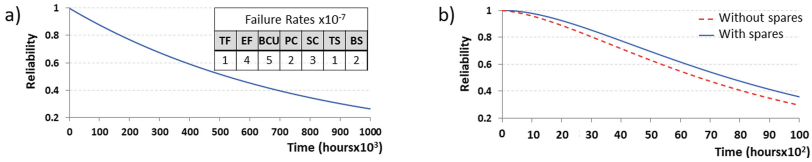



**Fig. 3.** Reliability of (a) DBW (b) SEN with/without spare constructs

failure rate of $1 \times 10^{-5}$ for all switching elements with 16 switching elements in each series structure. We evaluate the SEN reliability without and with spares with a dormancy factor of 0.1. This result shows that considering the spares in the reliability analysis leads to having a more reliable and realistic system than static RBDs that are usually used for the analysis of similar SENs.

To sum up, we are able to provide generic expressions of reliability of the DBW and SEN+ systems that are verified in HOL theorem proving, which cannot be done using other formal tools. These expressions can be instantiated with different failure distributions without the need to repeat the analysis. In addition, we demonstrated that our formalization is flexible and can be used to model more complex systems of an arbitrary number of blocks by implementing its hierarchy using sets that can be instantiated later to model a specific system structure, which is an added feature of our formalized algebra.

## 5 Conclusion

In this paper, we proposed a new algebra to analyze dynamic reliability block diagrams (DRBDs). We developed the HOL formalization of this algebra in HOL4, which ensures its correctness and allows conducting the analysis within a theorem prover. Furthermore, this algebra provides formalized generic expressions of reliability that cannot be verified using other formal tools. This HOL formalization is the first of its kind that takes into account the system dynamics by providing the HOL formal model of spare constructs and temporal operators. The proposed algebra is compatible with the reliability expressions of traditional RBDs as demonstrated by the reliability expressions of the series and parallel structures. It also facilitates extending the verified reliability expressions to model complex systems using nested structures. Finally, we demonstrated the usefulness of this work by formally conducting the analysis of a drive-by-wire and a shuffle-exchange network systems to verify generic expressions of reliability, which are independent of the failure probability distribution of system components. We plan to extend this algebra to include other DRBD constructs, such as load sharing, in order to provide a more complete framework to algebraically analyze DRBDs in HOL.

## References


1. Ahmed, W., Hasan, O., Tahar, S.: Formalization of reliability block diagrams in higher-order logic. J. Appl. Logic **18**, 19–41 (2016). https://doi.org/10.1016/j.jal.2016.05.007
2. Altby, A., Majdandzic, D.: Design and Implementation of a Fault-tolerant Drive-by-wire System. Master's thesis, Chalmers University of Technology, Sweden (2014)
3. Bistouni, F., Jahanshahi, M.: Analyzing the reliability of shuffle-exchange networks using reliability block diagrams. Reliab. Eng. Syst. Saf. **132**, 97–106 (2014). https://doi.org/10.1016/j.ress.2014.07.012
4. Distefano, S.: System Dependability and Performances: Techniques, Methodologies and Tools. Ph.D. thesis, University of Messina, Italy (2005)
5. Elderhalli, Y.: DRBD Formal Analysis: HOL4 Script (2019). http://hvg.ece.concordia.ca/code/hol/DRBD/index.php
6. Elderhalli, Y., Hasan, O., Tahar, S.: A Formally Verified HOL Algebra for Dynamic Reliability Block Diagrams. Technical report, Concordia University, Canada (2019). http://arxiv.org/abs/1908.01930
7. Elderhalli, Y., Ahmad, W., Hasan, O., Tahar, S.: Probabilistic analysis of dynamic fault trees using HOL theorem proving. J. Appl. Logics **2631**(3), 469 (2019)
8. Hasan, O., Ahmed, W., Tahar, S., Hamdi, M.S.: Reliability block diagrams based analysis: a survey. In: Numerical Analysis and Applied Maths, vol. 1648, pp. 850129.1-4 (2015). https://doi.org/10.1063/1.4913184
9. HOL4: (2019). https://hol-theorem-prover.org/
10. Merle, G.: Algebraic Modelling of Dynamic Fault Trees, Contribution to Qualitative and Quantitative Analysis. Ph.D. thesis, ENS, France (2010)
11. Mhamdi, T., Hasan, O., Tahar, S.: Formalization of entropy measures in HOL. In: van Eekelen, M., Geuvers, H., Schmaltz, J., Wiedijk, F. (eds.) ITP 2011. LNCS, vol. 6898, pp. 233–248. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22863-6_18
12. Qasim, M., Hasan, O., Elleuch, M., Tahar, S.: Formalization of normal random variables in HOL. In: Kohlhase, M., Johansson, M., Miller, B., de de Moura, L., Tompa, F. (eds.) CICM 2016. LNCS (LNAI), vol. 9791, pp. 44–59. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-42547-4_4
13. Robidoux, R., Xu, H., Xing, L., Zhou, M.: Automated modeling of dynamic reliability block diagrams using colored petri nets. IEEE Trans. Syst. Man Cybern. **40**(2), 337 (2010). https://doi.org/10.1109/TSMCA.2009.2034837
14. Ruijters, E., Stoelinga, M.: Fault tree analysis: a survey of the state-of-the-art in modeling. Anal. Tools. Comput. Sci. Rev. **15–16**, 29–62 (2015). https://doi.org/10.1016/j.cosrev.2015.03.001
15. Smith, G.: The Object-Z Specification Language, vol. 1. Springer, New York (2012)
16. Xu, H., Xing, L.: Formal semantics and verification of dynamic reliability block diagrams for system reliability modeling. In: Software Engineering and Applications, pp. 155–162 (2007)