Dynamic Dependability Analysis of Shuffle-exchange Networks using HOL Theorem Proving

Yassmeen Elderhalli, Osman Hasan, and Sofiène Tahar

Department of Electrical and Computer Engineering,
Concordia University, Montréal, QC, Canada

{y_elderh,o_hasan,tahar}@ece.concordia.ca

TECHNICAL REPORT

October 2019

Abstract

Dynamic dependability models, such as dynamic fault trees (DFTs) and dynamic reliability block diagrams (DRBDs), are introduced to overcome the modeling limitations of traditional models. Recently, higher-order logic (HOL) formalizations of both models have been conducted, which allow the analysis of these models formally, within a theorem prover. In this report, we provide the formal dynamic dependability analysis of shuffle-exchange networks, which are multistage interconnection networks that are commonly used in multiprocessor systems. We use DFTs and DRBDs to model the terminal, broadcast and network reliability with dynamic spare gates and constructs in several generic versions. We verify generic expressions of probability of failure and reliability of these systems, which can be instantiated with any number of system components and failure rates to reason about the failure behavior of these networks.

1   Introduction

Dependability describes the ability of a system to provide a trusted service [1]. Dynamic dependability models, such as dynamic fault trees (DFTs) [2] and dynamic reliability block diagrams [3], capture the dynamic failure and success dependencies, respectively, among system components, and hence are more suitable in modeling real-world systems. Recently, higher-order logic (HOL) theorem proving has been used in the formal analysis of both models algebraically [4,5], where generic expressions are formally verified that are independent of the failure distributions of system components. This ensures the soundness of the analysis, which is suitable for safety-critical systems. In this report, we use both formalizations in conducting the dynamic dependability analysis of the interconnection network of multiprocessor systems.

With the ongoing demands for intensive processing applications, multiprocessor systems represent one of the solutions that satisfies such demand. Nowadays, such systems are feasible due to their reduced cost and thus it is possible to have systems of hundreds of processors. Multiprocessor systems allow parallel computing, where tasks are executed in parallel with the possibility of interacting with one another when required. This parallel execution highly impacts the overall system performance, such as throughput. However, memory and I/O peripheral resources are shared among processors and thus an efficient data routing among system nodes is necessary to maintain high system performance, reliability and low cost. This is of a great importance, particularly with scientific applications, where a huge number of processors are used, i.e., large-scale multiprocessor systems [6]. Therefore, a dedicated interconnection network is used to connect processors and memory modules, as depicted in Figure 1 [6].
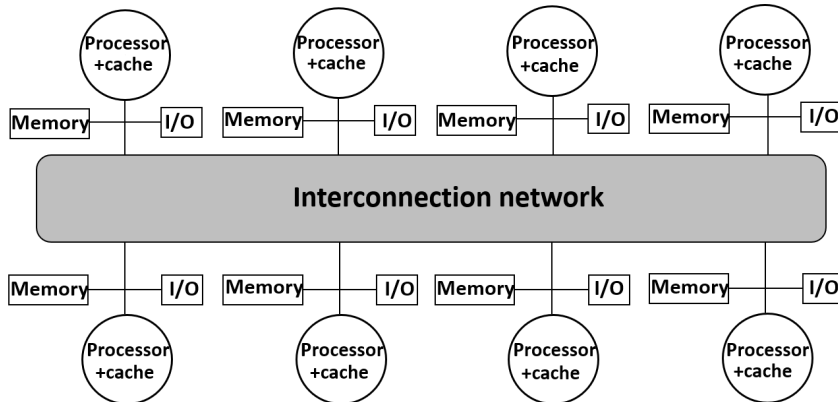
Figure 1: Overview of Multiprocessor System Architecture

The complexity of interconnection networks ranges from simple networks, such as time-shared bus to crossbar switching. The former has a negative impact on the system performance, while the latter has much higher cost as there exists a separate link between each pair of nodes in the systems. For example, for a system of N nodes, i.e., N inputs and N outputs, it is required to have N^2 links or switching elements between each input and output.

Multistage interconnection networks (MINs) are introduced to reduce the number

of required switching elements and hence, reduce the cost while providing better performance than shared-bus networks. The main idea of MINs is to have multiple small stages of crossbar switches that are connected between sources (inputs) and destinations (outputs), which results in a much reduced number of used switching elements. The number of paths available between each input and output determines the category of the MIN. A single-path MIN has only one path to route information between each source-destination pair. A shuffle-exchange network (SEN) is an example of such type of networks. Each stage has log_2N switching elements, where N is the number of inputs and outputs of the network. Usually the switching elements are of size 2×2 to reduce the cost. The number of stages required to establish the single-path MIN is $Nlog_2N$, which is lower than crossbar networks. An 8×8 SEN is shown in Figure 2, where only a single path is available for each input-output pair. However, the reliability of single-path MINs and SENs depends on the switching elements and thus a fault in any of these switches cannot be tolerated.

Enhancing the reliability of MINs is of great importance in order to maintain high system performance. Therefore, redundant switching elements are used to ensure that the network is able to provide the required switching even after the failure of some of these elements [7,8]. Multiple-path MINs are used to increase the fault tolerance and hence the network reliability. SEN+ is a SEN, where an additional stage is added to provide two paths between each input-output pair, as shown in Figure 3. However, even with the additional path, the failure of some switches can lead to the failure of the connection in some situations. Spare parts have been used in [9] to replace switches after failure. However, the analysis was not conducted formally to ensure its correctness.

Studying the reliability of SENs has been an active research area [10–13]. The reliability of MINs are commonly analyzed using simulation or analytically. For example, in [14], Monte Carlo simulation is used to analyze the reliability of SENs. However, as mentioned previously, simulation cannot provide accurate results due to its sampling based nature. Although CTMCs can analytically solve the reliability of MINs [15], they cannot be used with large-scale systems since the state space grows exponentially with the increase in the number of system components. On the other hand, when the complexity of the network increases, reliability bounds provides estimate values for the MIN reliability [16,17]. RBDs have been also used in the analysis of MINs with single and multiple paths. For example, in [18], the reliability of SEN, SEN+ and SEN+2 (a SEN with two additional stages) is modeled using traditional RBDs. Generic expressions of success rates of the switching elements are provided analytically assuming that all these elements have the same failure rates. However, these generic expressions are not formally verified , which may raise questions about its accuracy. Furthermore, dynamic dependencies among system components, like warm spares, are not considered or modeled.

Based on the previous discussion, accurate modeling and analysis of these networks is necessary to capture the dynamic behavior as this will provide the design engineers with some measures that can help enhancing the performance of the entire multiprocessor system. To the best of our knowledge, dynamic dependability analysis using formal methods has not been used with MINs. Therefore, we propose to add spare

switches to replace the critical ones after failure and conduct the analysis of MINs, particularly SENs using our formal dependability framework.
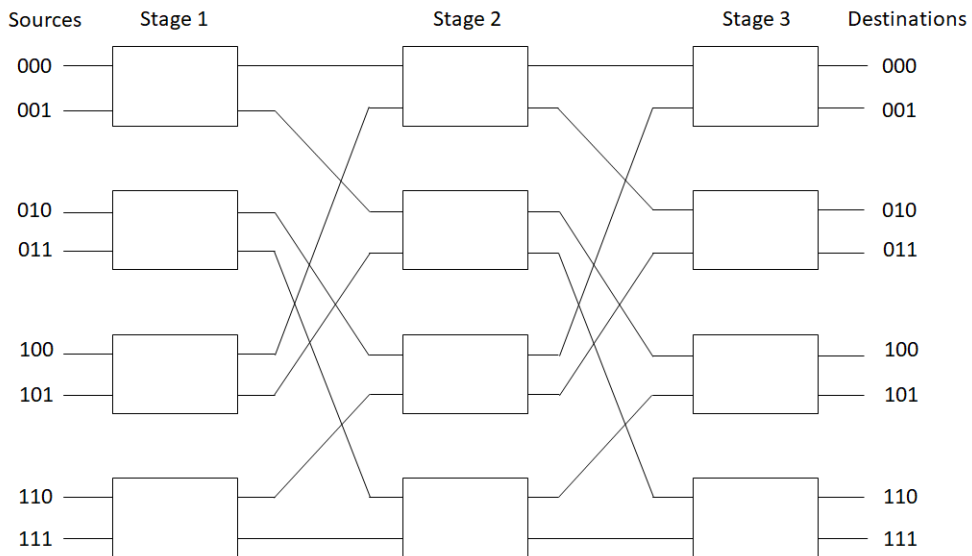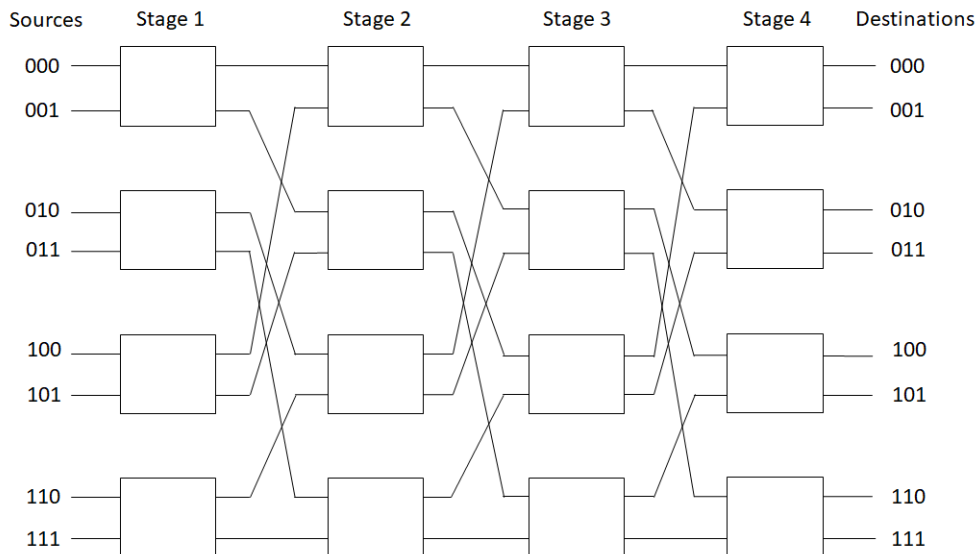

Figure 2: An 8×8 SEN

Figure 3: An 8×8 SEN+

Since the reliability of MINs affects the performance of the overall multiprocessor system, it is required to accurately model and analyze their reliability. In this work, we use both DRBDs and DFTs to model the dynamic reliability of these networks, particularly SEN and SEN+, and conduct the analysis using our framework. In this work, we formally verify the terminal, broadcast and network reliability of SEN and SEN+ in HOL and provide generic expressions of reliability and probability of failure. It is worth noting that the formalization provided in this work uses the HOL theories

(libraries) of DFT and DRBD, which have been developed in [4, 5, 19] and can be accessed from [20, 21].

2 Terminal Reliability Analysis of Shuffle-exchange Networks

The terminal reliability is the reliability of the connection between a given source and destination, i.e., the probability of having a reliable connection between one source-destination pair. We analyze the terminal reliability of the SEN and SEN+ using both DFT and DRBD models.

2.1 DFT Analysis of SEN and SEN+

We model the sources of failure of both SEN and SEN+ using DFTs. We use n-ary gates, which enable verifying expressions of the probability of failure for generic number of system components.

Figure 4 shows the DFT model of the SEN system. Since SENs are single path MINs, the failure of any of the switches in the path between a given source and destination leads to losing the connection. Therefore, adding spare parts will lower the probability of failure. For illustration purposes, we use a spare part to replace the main switch Y after failure. The DFT consists of an n-ary OR gate, which means that the failure of any of the switches, interrupts the connection between the source and the destination.
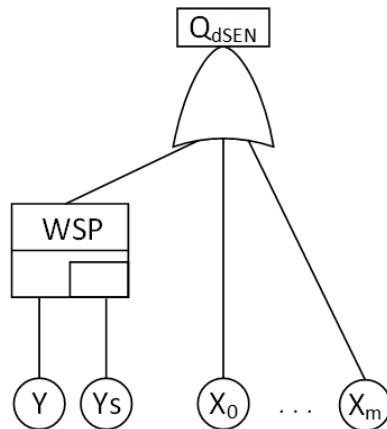

Figure 4: DFT of SEN

Since the top event is an n-ary OR gate, we need first to verify that the `DFT_event` of the n-ary OR is equal to the union of the individual events, as:

Theorem 2.1.
⊢ ∀ p X t s. FINITE s ⇒
  (DFT_event p (n_OR (MAP X (SET_TO_LIST s))) t =
  ⋃$_{i∈s}$ {rv_to_devent p X t i})

where s is a set of numbers that has the indices of the system components. X is a group of random variables that represent the time-to-failure of the switches in the system. We need to recall that n_OR accepts a list of random variables as an argument. Therefore, we create this list using MAP X (SET_TO_LIST s). rv_to_devent, in Theorem 2.1, is similar to the rv_to_event of the DRBD, but it creates DFT events. It is defined as:

Definition 2.1. *rv_to_devent*
⊢ ∀ p X t. rv_to_devent p X t = (λi. DFT_event p (X i) t)

This way, we can use this function to create a group of DFT events for a set of indexed random variables. Then, we verify the probability of the *n*-ary OR gate in a way similar to the probability of the DRBD parallel structure, which is defined as the union of events.

Theorem 2.2.
⊢ ∀ p X t s. s ≠ {} ∧ FINITE s
  indep_sets p (λi. {rv_to_devent p X t i}) s ∧
  (∀ i. i ∈ s ⇒ rv_gt0_ninfinity [X i]) ⇒
  (prob p (DFT_event p (n_OR (MAP X (SET_TO_LIST s))) t) =
  1 - Normal (∏$_{i∈s}$ (real (1 - F$_{X_i}$(t)))))

In Theorem 2.2, it is required that the set of indices, s, to be nonempty and to be finite, which is a realistic condition as in any system the number of components is finite. The last condition of Theorem 2.3, ensures that the random variables of X are greater than or equal to 0 and not equal to $+\infty$, which is required to be able to use the CDF of the random variable as given in [19].

We express the structure function of the DFT of SEN as:

$$Q_{dSEN\_Terminal} = n\_OR \ (MAP \ (λi. \quad if \ i = 0 \ then \ WSP \ Y \ Ys_a \ Ys_d \\ else \ X \ i) \ (SET\_TO\_LIST \ \{0\} \ ∪ \ L)) \tag{1}$$

We notice that the structure of the DFT is defined using the indices in {0} ∪ L. 0 is the index of the spare gate and L has the indices of the rest of the switches in the system.

Finally, we verify the probability of failure of this top event as:

Theorem 2.3.
⊢ ∀ p X Y Ys$_a$ Ys$_d$ t L.
  DISJOINT {0} L ∧ FINITE L ∧ L ≠ {} ∧
  indep_sets p (λi. {event_set [(DFT_event p (WSP Y Ys$_a$ Ys$_d$) t, 0)]
    (rv_to_devent p X t) i}) ({0} ∪ L) ∧
  (∀ i. i ∈ L ⇒ rv_gt0_ninfinity [X i]) ∧

```
(prob p (DFT_event p Q_dSEN_Terminal t) =
1-
(1- prob p (DFT_event p (WSP Y Ys_a Ys_d) t)) *
  Normal (∏_{i∈L} (real(1-F_{X_i}(t)))))
```

where `DISJOINT {0} L` ensures that the indices of the elements are unique. While `FINITE L ∧ L ≠ {}` ascertain that set L, which has the indices, is finite and not empty. Finally, the independence of the events is added using `indep_sets`. Theorem 2.3 can be further rewritten based on the probability of the spare gate [19]. However, the required conditions of the latter should be satisfied, such as the continuity of the distributions. Since we need a group of indexed sets in `indep_sets`, we define a function `event_set` that accepts a list of pairs each of which is composed of a DFT event with its index. This function also accepts the remaining blocks of the DFT that have their indices embedded in a set (that can be generic of any size).

In SEN+, an additional path is added to increase the redundancy in the system. Therefore, for the connection between a given source and a destination to be broken, it is required that these two paths must be disconnected. The DFT of the SEN+ is shown in Figure 5, where two spares are added to replace the main switches Y and Z after failure. Switch Y is the input switch connected to the source and switch Z is connected to the destination. This DFT is composed of three levels of OR of AND of OR gates. Therefore, in order to verify the probability of the top event, we need first to verify that the `DFT_event` of the n-ary AND gate is equal to the intersection of the input events. We formally verify this in HOL as:
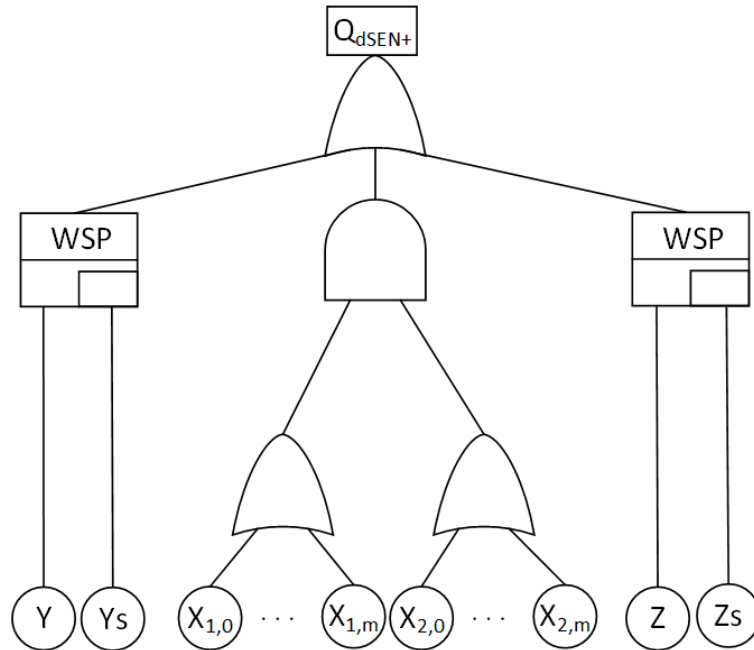

Figure 5: DFT of SEN+ Terminal Connection

Theorem 2.4.
$\vdash \forall$ p X t s. FINITE s $\wedge$ s $\neq$ {} $\wedge$ 0 $\leq$ t $\Rightarrow$
  (DFT_event p
  (n_AND (MAP X (SET_TO_LIST s)))) t = $\bigcap_{i \in s}$ {rv_to_devent p X t i})

Then, we verify the probability of failure of the top event of the AND gate as:

Theorem 2.5.
$\vdash \forall$ p X t s. FINITE s $\wedge$ s $\neq$ {} $\wedge$ 0 $\leq$ t $\wedge$
  indep_sets p (λi. {rv_to_devent p X t i}) s
  ($\forall$ i. i $\in$ s $\Rightarrow$ rv_gt0_ninfinity [X i]) $\Rightarrow$
  (prob p
  (DFT_event p
  (n_AND (MAP X (SET_TO_LIST s))) t) =
  Normal ($\prod_{i \in s}$ (real (F_{X_i}(t)))))

The first three conditions are needed to be able to use Theorem 2.4, while `indep_sets` ensures the independence of the events.

We use Theorems 2.2 and 2.5 to verify the probability of OR of AND of OR, which is required for the probability of the top event. We express the top event of the DFT of Figure 5, Q_{dSEN+} as:

$$Q_{dSEN+\_Terminal} = \text{n\_OR (MAP (λi. if i = 0 then WSP Y Ys}_a \text{ Ys}_d$$
$$\text{else if i = 1 then}$$
$$\text{((n\_OR (MAP X (SET\_TO\_LIST L1))) $\cdot$}$$
$$\text{(n\_OR (MAP X (SET\_TO\_LIST L2)))))}$$
$$\text{else WSP Z Zs}_a \text{ Zs}_d\text{) (SET\_TO\_LIST \{0; 1; 2\}))}$$

(2)

where $\{0; 1; 2\}$ indicates that the OR gate has three inputs with indices 0 for the first spare, 1 for the AND of ORs, and 2 for the second spare. $L1$ and $L2$ has the indices of the switches in the two redundant paths (for the two lower ORs).

The DFT top event can be expressed using union and intersection of events, which can be quite useful in reusing the existing theorems of probability of union of intersections and intersection of unions. We verify this relationship as:

Theorem 2.6.
$\vdash \forall$ p Y Ys$_a$ Ys$_d$ Z Zs$_a$ Zs$_d$ X L1 L2 t.
  FINITE L1 $\wedge$ FINITE L2 $\wedge$
  disjoint_family_on (ind_set [{0}; L1; L2; {3}]) {0; 1; 2; 3} $\Rightarrow$
  (DFT_event p ($Q_{dSEN+\_Terminal}$) t =

$\bigcup$
  {$\bigcap$
    {$\bigcup$

```
    {event_set
       [(DFT_event p (WSP Y Ys_a Ys_d) t,0);
          (DFT_event p (WSP Z Zs_a Zs_d) t,3)]
       (rv_to_devent p X t) i |
      i ∈ ind_set [{0}; L1; L2; {3}] a} | a |
    a ∈ ind_set [{0}; {1; 2}; {3}] j} | j |
  j ∈ {0; 1; 2}})
```

Finally, we verify the probability of failure of Q_{dSEN+}:

Theorem 2.7.
```
⊢ ∀ p X Y Ys_a Ys_d Z Zs_a Zs_d t L1 L2.  0 ≤ t ∧
 SEN_set_req p L1 L2 (ind_set [{0}; L1; L2; {3}])
   (ind_set [{0}; {1; 2}; {3}]) {0; 1; 2}
   (event_set [(DFT_event p (WSP Y Ys_a Ys_d) t,0);
                  (DFT_event p (WSP Z Zs_a Zs_d) t,3)]
        (rv_to_devent p X t)) ∧
 (∀ i.  i ∈ (L1 ∪ L2) ⇒ rv_gt0_ninfinity [X i]) ⇒
 (prob p (DFT_event p Q_{dSEN+_Terminal} t) =
  1 -
   (1 -
    prob p (DFT_event p (WSP Y Ys_a Ys_d) t)) *
    (Normal
     (1 -
       (1 - ∏_{i∈L1} (real (1 - F_{X_i}(t)))) *
       (1 - ∏_{i∈L2} (real (1 - F_{X_i}(t))))) *
    (1 - prob p (DFT_event p (WSP Z Zs_a Zs_d) t)))))
```

where `SEN_set_req` ensures the required conditions of the input sets including that the sets are finite and nonempty. It also ensures the independence of the input events over the probability space. We also define `ind_set` that accepts a list of sets and returns a group of indexed sets. This is required to be able to create the hierarchy of the DFT using sets.

In order to use the above generic probability of failure expressions on a concrete instance of SEN+, we evaluate in MATLAB [22] the probability of failure of the terminal connection of a 128×128 SEN+, where each OR gate of the first level of Figure 5 has 6 inputs. We assume that the failure rate of each switching element is 1×10^{-5}. We evaluate the probability of failure for the SEN+ system without and with spare parts with a dormancy factor of 0.1, as shown in Figure 6. This result shows that considering the spares in the analysis leads to having more reliable and realistic system than the traditional FTs.

2.2   DRBD Analysis of SEN and SEN+

For SENs (single-path MIN), the terminal reliability is modeled as a series RBD. For illustration purposes, we use a spare part to replace the first input switch, and thus
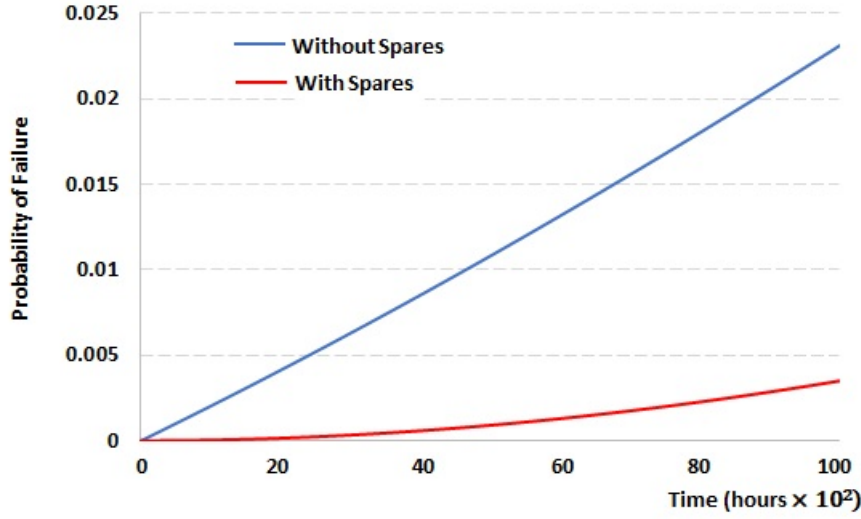
Figure 6: Probability of Failure of the Terminal Connection of a 128×128 SEN+ with and without Spares

increase the reliability. The DRBD of the modified SEN is shown in Figure 7, where Y is the main switch that will be replaced by Ys after failure and the series structure has $m + 1$ elements.
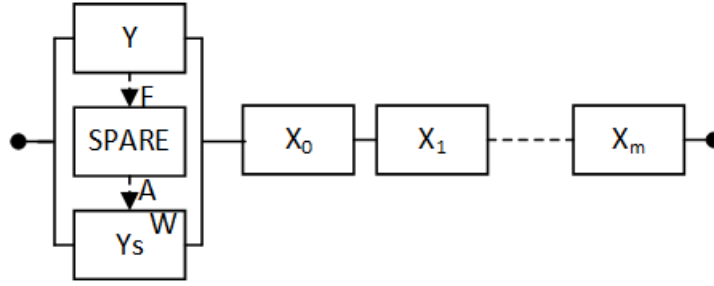

Figure 7: DRBD of SEN

Using the proposed DRBD algebra in [5], we express the structure function of the SEN DRBD as:

$$Q_{\texttt{SEN\_Terminal}} = \texttt{nR\_AND } (\lambda\texttt{i. if i = 0 then R\_WSP Y Ys}_a \texttt{ Ys}_d$$
$$\texttt{else X i) } \{0\} \cup \texttt{L} \tag{3}$$

where X is a group of indexed time-to-failure functions that represent the blocks of the series structure and L is a set with their indices. L can be instantiated with any group of numbers, which makes this function generic to represent the reliability model of any SEN with any size.

Then, we verify that the DRBD_event of $Q_{\texttt{SEN}}$ can be represented using the series parallel structures as:

11

Theorem 2.8.
⊢ ∀ p X Y Ys_a Ys_d t L.
 DISJOINT {0} L ∧ FINITE L ∧ L ≠ {} ⇒
 (DRBD_event p $Q_{SEN\_Terminal}$ t =
  DRBD_series
   (λi. event_set
    [(DRBD_event p (R_WSP Y Ys_a Ys_d) t,0)]
     (rv_to_event p X t) i) ({0} ∪ L))

where DISJOINT ensures that all sets are disjoint. We use event_set and ind_set to create the events, similar to the DFTs. Since we are dealing with a series structure, we only need to specify the heirarchy of the architecture in one direction using {0} ∪ L. We verify Theorem 2.8 using the relationship between nR_AND and DRBD_series verified in [5] and some set-related theorems.

Based on Theorem 2.8, we verify a generic expression for the reliability of the SEN system:

Theorem 2.9.
⊢ ∀ p X Y Ys_a Ys_d t L.
 DISJOINT {0} L ∧ FINITE L ∧ L ≠ {} ∧
 indep_sets p (λi. {event_set [(DRBD_event p (R_WSP Y Ys_a Ys_d) t, 0)]
   (rv_to_event p X t) i}) ({0} ∪ L)⇒
 (prob p (DRBD_event p $Q_{SEN\_Terminal}$ t) =
 Rel p (R_WSP Y Ys_a Ys_d) t * Normal ($\prod_{l \in L}$ (real (Rel p (X l) t))))

In a similar manner, the SEN+ is modeled as a series-parallel-series structure. To further enhance the reliability, we use spare constructs as shown in Figure 8, 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. Therefore, this DRBD consists of a series of two spare constructs and one parallel structure that consists of two series structures.
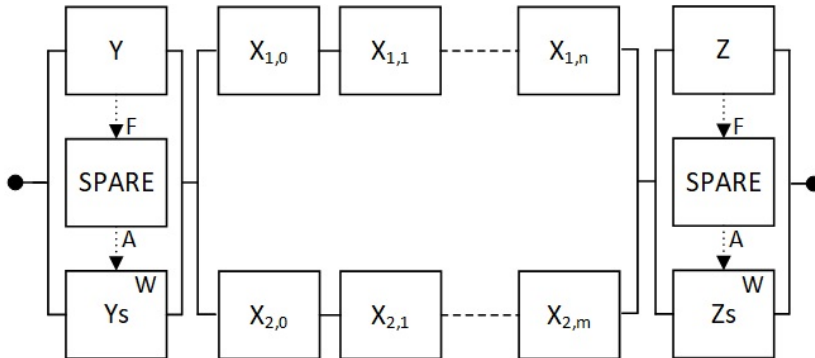

Figure 8: Terminal Reliability DRBD of SEN+

Using our DRBD operators, we formally express the structure function of this DRBD as:

$$Q_{\text{SEN+\_Terminal}} = \text{nR\_AND } (\lambda i. \quad \text{if i = 0 then R\_WSP Y } Ys_a \; Ys_d$$
$$\text{else if i = 1 then } \big((\text{nR\_AND X L1}) + (\text{nR\_AND X L2})\big)$$
$$\text{else R\_WSP Z } Zs_a \; Zs_d) \; \{0; \; 1; \; 2\}$$

(4)

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. In order to re-utilize the verified expressions of reliability, it is required to express this DRBD using the series and parallel structures. Therefore, we verify that the DRBD event of the $Q_{\text{SEN+}}$ is equal to a nested series-parallel-series structure as:

Theorem 2.10.
$\vdash \forall$ p X Y Ys_a Ys_d Z Zs_a Zs_d t L1 L2.
 disjoint_family_on (ind_set [$\{0; 3\}$; L1; L2]) $\{0;1;2\}$ $\wedge$
 FINITE L1 $\wedge$ FINITE L2 $\wedge$ L1 $\neq$ $\{\}$ $\wedge$ L2 $\neq$ $\{\}$ $\Rightarrow$
 (DRBD_event p $Q_{\text{SEN+\_Terminal}}$ t =
  DRBD_series (λj.
    DRBD_parallel (λa.
      DRBD_series (λi.
        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) i)
       ind_set [$\{0\}$; L1; L2; $\{3\}$] a))
     (ind_set [$\{0\}$; $\{1; 2\}$; $\{3\}$] j)) $\{0; 1; 2\}$)

where disjoint_family_on (ind_set [$\{0; 3\}$; L1; L2]) $\{0;1;2\}$ ensures that the sets $\{0;3\}$, $L1$ and $L2$ are disjoint, i.e., each switch has a unique index. Since we are dealing with a series-parallel-series structure, we need three sets to identify the hierarchy of this nested structure. Set $\{0;1;2\}$ in Theorem 2.10 indicates that the outer series structure has three elements, i.e., three parallel structures. ind_set [$\{0\}$; $\{1;2\}$; $\{3\}$] indicates that the first parallel structure has only one series structure with index 0, the second parallel structure has two series structures with indices 1 and 2, and the third parallel structure has only one series structure with index 3. Finally, ind_set [$\{0\}$; L1; L2; $\{3\}$] implies that the first series structure has only one element with index 0, the second and third series structures have an arbitrary number of blocks indexed by $L1$ and $L2$. The last series structure has one element with index 3. We verify Theorem 2.10 using the relationship between the event of `nR_AND` and the `DRBD_series` and the equivalence of the event of the OR with the union of events besides some set-related theorems.

Based on Theorem 2.10, we verify a generic expression for the reliability of the SEN+ system:

Theorem 2.11.
$\vdash \forall$ 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)) $\Rightarrow$
  (prob p (DRBD_event p Q$_{\text{SEN\_Terminal}}$ t) =
  Rel p (R_WSP Y Ys$_a$ Ys$_d$) t * Rel p (R_WSP Z Zs$_a$ Zs$_d$) t *
  (1 −
    (1 − Normal ($\prod_{l\in L1}$ (real (Rel p (X l) t)))) *
    (1 − Normal ($\prod_{l\in L2}$ (real (Rel p (X l) t))))))

where SEN_set_req is the same function that we use with DFTs. We first rewrite the goal using Theorem 2.10, then we use the reliability of the series-parallel-series to verify the final expression. The reliability of the spare constructs can be further rewritten using the probability of the spare construct verified in [5] given that the required conditions are ensured, such as the continuity of the CDFs. It can be noticed that the DRBD and the DFT models possess the same hierarchy represented by the sets of indices, which makes it easy to be used when going from one model to the other.

Similar to the DFT analysis, we evaluate the terminal reliability of a 128×128 SEN+, where each inner series structure of Figure 8 has 6 blocks. We assume that the failure rate of each switching element is 1×10^{-5}. We evaluate the reliability for the SEN+ system without and with spare parts with a dormancy factor of 0.1, as shown in Figure 9.
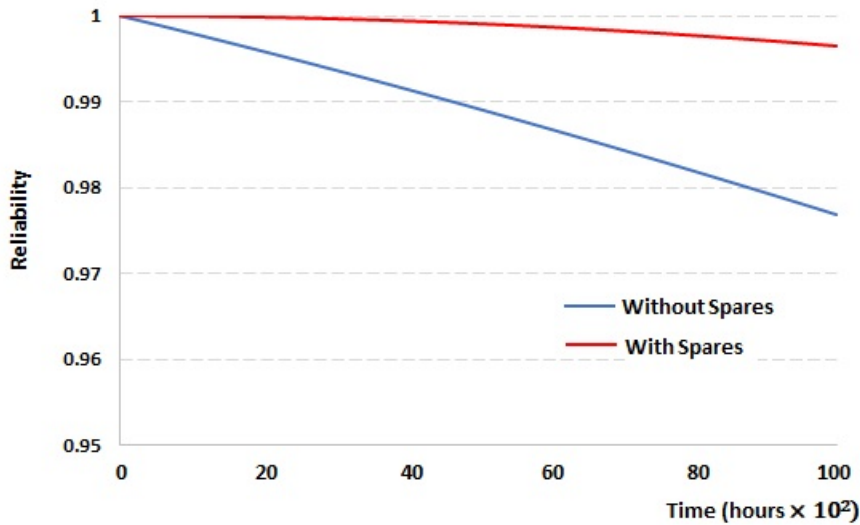

Figure 9: Terminal Reliability of 128×128 SEN+ with and without Spares

3 Broadcast Reliability Analysis of Shuffle-exchange Networks

The broadcast reliability represents the probability of having a working connection between one source and all destinations. This is required when one of the processors in the system needs to transmit information to all destinations in the network. We present in this section, the broadcast reliability of the SEN and SEN+ using both DFT and DRBD models.

3.1 DFT Analysis of SEN and SEN+

Since in SENs there exists a single path between each source and destination, it is required to have a successful transmission through all these paths for a proper broadcast. Therefore, the DFT can be modeled using an OR gate. We further lower the probability of failure by adding an additional spare gate, as shown in Figure 4. However, the number of DFT inputs, which represent the switches, varies between the terminal and broadcast reliability models. For example, consider an 8×8 SEN. The number of inputs for the terminal DFT is 3, i.e., $log_2 8$, while the broadcast DFT requires seven inputs, i.e., $\sum_{i=1}^{log_2 8}(\frac{8}{2^i})$ [18]. Therefore, we can also use Theorem 2.3 for the broadcast, since this theorem is verified for any number of system blocks with their indices in the set s . This highlights the importance of having generic verified expressions for any number of system blocks, which enables the re-utilization of the theorems in different contexts.

The DFT model of the broadcast SEN+ is shown in Figure 10. Its top event is modeled using an OR gate that is connected to a spare gate for the input switch, AND of OR to model the two alternative paths and finally, the rest of the destination switches in order to have a proper broadcast transmission.

We formally express the structure function of the top event as:

$$
\begin{aligned}
\texttt{Q}_{\texttt{dSEN+\_Broadcast}} = &\texttt{ n\_OR (MAP (}\lambda\texttt{i.\ \ if i = 0 then WSP Y Ys}_\texttt{a}\texttt{ Ys}_\texttt{d} \\
&\qquad\qquad\quad \texttt{else if i = 1 then} \\
&\qquad\qquad\quad\quad \texttt{((n\_OR (MAP X (SET\_TO\_LIST L1)))\ \cdot} \\
&\qquad\qquad\quad\quad \texttt{(n\_OR (MAP X (SET\_TO\_LIST L2))))} \\
&\qquad\qquad\quad \texttt{else (n\_OR (MAP X (SET\_TO\_LIST L3))))} \\
&\qquad\quad \texttt{(SET\_TO\_LIST \{0; 1; 2\}))}
\end{aligned}
\tag{5}
$$

The hierarchy of the DFT is divided using the sets of indices. We need to recall that `MAP X (SET_TO_LIST L1)`, `MAP X (SET_TO_LIST L2)` and `MAP X (SET_TO_LIST L3)` are used to create the lists of the group of random variables for the n-ary gates. $L1$ and $L2$ has the indices of the switches in the two alternative paths, i.e., the inputs of the two lower OR gates in the DFT of Figure 10, while $L3$ has the indices of the remaining inputs of the top OR gate. The set $\{0; 1; 2\}$ indicates that the top OR gate has three inputs, which is similar to the terminal DFT model.
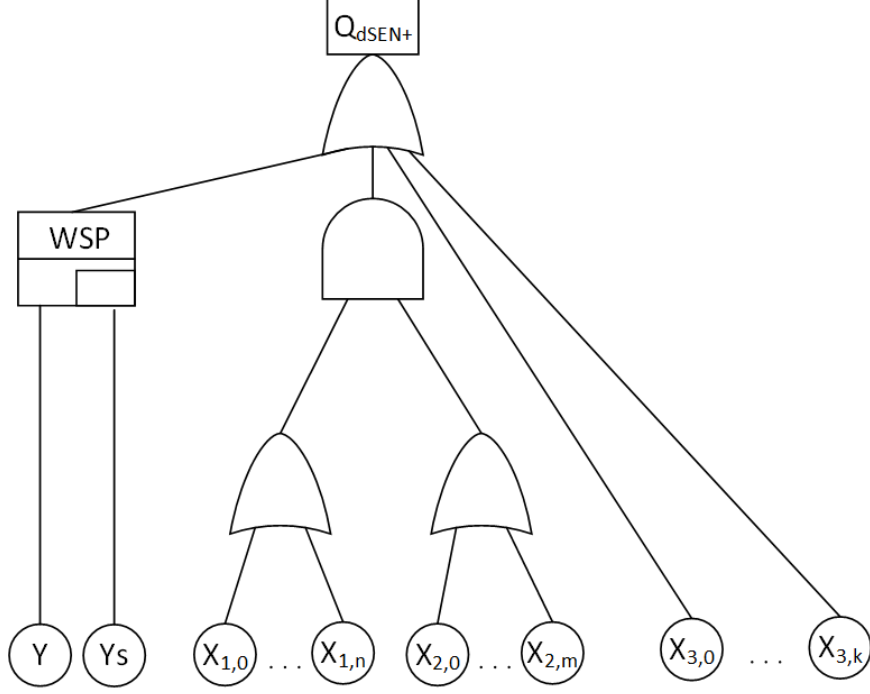
Figure 10: DFT of Broadcast SEN+

We use this structure function to verify the probability of failure of the top event:

Theorem 3.1.
⊢ ∀ p X Y Ys$_a$ Ys$_d$ t L1 L2 L3 s.
  SEN_broad_set_req p L1 L2 L3 (ind_set [{0}; L1; L2; L3])
    (ind_set [{0}; {1; 2}; {3}]) {0; 1; 2}
    (event_set [(DFT_event p (WSP Y Ys$_a$ Ys$_d$) t,0);
     (rv_to_devent p X t)) ∧ 0 ≤ t ∧
  (∀ i. i ∈ (L1 ∪ L2 ∪ L3) ⇒ rv_gt0_ninfinity [X i]) ⇒
  (prob p (DFT_event p Q$_{dSEN+\_Broadcast}$ t) =
   1 -
    (1 -
     prob p (DFT_event p (WSP Y Ys$_a$ Ys$_d$ t)) *
     (Normal
      (1 -
       (1 - $\prod_{i \in L1}$ (real (1 - F$_{X_i}$(t)))) *
       (1 - $\prod_{i \in L2}$ (real (1 - F$_{X_i}$(t))))) *
     Normal ($\prod_{i \in L3}$ (real (1 - F$_{X_i}$(t))))))))

where SEN_broad_set_req ascertains the conditions required for the sets such as finiteness. It also ensures the independence of the events.

    Figure 11 shows the evaluation results of the probability of failure of the DFT of Figure 10 for a 128×128 SEN+. This SEN+ has 63 inputs for each first level OR gate and the top level OR gate has 66 inputs. As with the terminal SEN+, we assume that the failure rate of each switching element is 1×10^{-5} with a dormancy factor of 0.1.
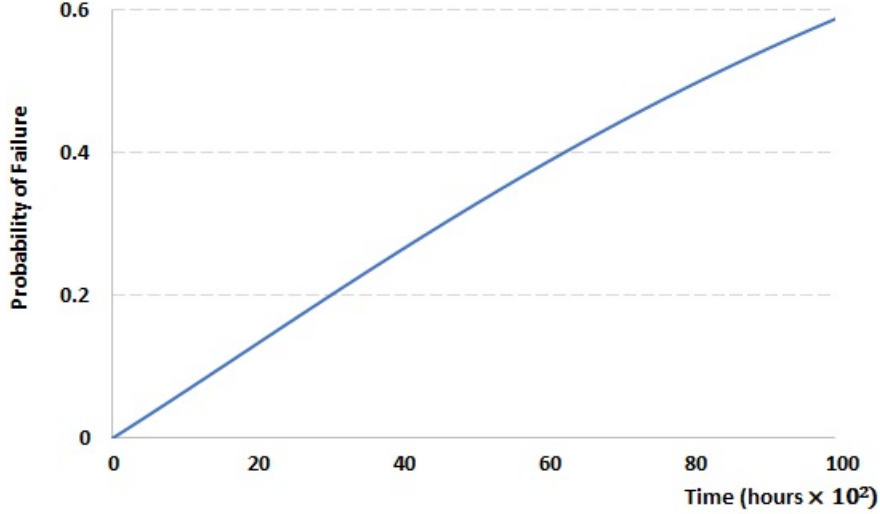
16

Figure 11: Probability of Failure of the Broadcast of a 128×128 SEN+

3.2 DRBD Analysis of SEN and SEN+

Similar to the DFT SEN broadcast model, we can use the model in Figure 7. However, as mentioned previously, the number of the blocks is different. Therefore, we can also use Theorem 2.9 for the broadcast reliability, since this theorem is verified for any number of system blocks using set s.
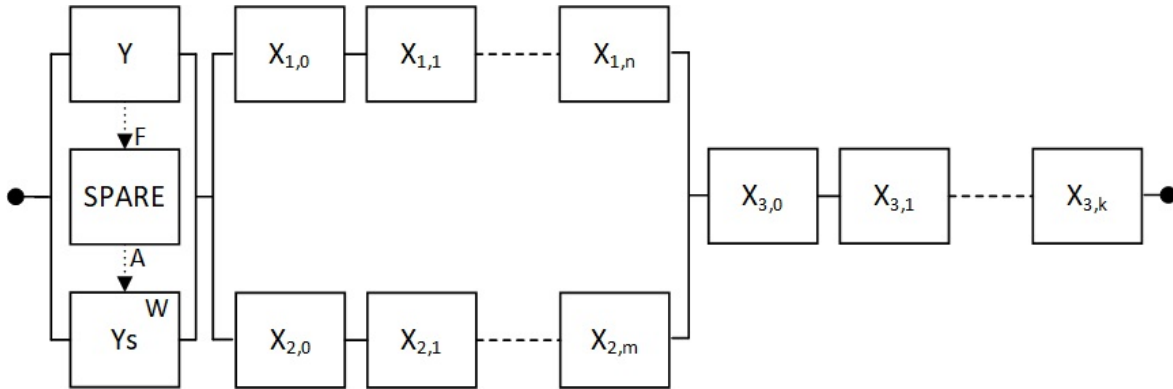

Figure 12: Broadcast DRBD model of SEN+

The DRBD of the SEN+ is depicted in Figure 12. The first block (with the spare) represents the input switch that is connected directly to the source. The failure of this switch will interrupt the broadcast transmission. Therefore, we add a spare part to replace it after failure. The series structure on the right side of the figure models the switches of all destinations, as they are all receiving the transmission. Finally, the parallel-series structure in the middle, represents the two alternative paths that are available for each broadcast transmission. For example, for the SEN+ shown in Figure 3, the number of switches connected to the destinations are four, while each one of the alternative paths has three switches.

17

In order to formally verify the reliability of the broadcast of the SEN+, we first express it using our operators as:

$$Q_{\text{SEN+\_Broadcast}} = \texttt{nR\_AND} (\lambda \texttt{i.} \quad \texttt{if i = 0 then R\_WSP Y Ys}_a \texttt{ Ys}_d$$
$$\texttt{else if i = 1 then } ((\texttt{nR\_AND X L1}) +$$
$$(\texttt{nR\_AND X L2}))$$
$$\texttt{else (nR\_AND X L3)) (\{0; 1 2\})} \tag{6}$$

where $L1$ and $L2$ are the sets that have the indices of the inner series structures of the parallel-series structure in the middle. The set $\{0; 1; 2\}$ indicates that the outer series structure consists of three main components. The first spare construct has index 0, while the parallel-series structure has index 1. Finally, the series structure on the left side of Figure 12 has index 2, and $L3$ has the indices of the blocks in this series structure. We verify the reliability of this DRBD as:

Theorem 3.2.
⊢ ∀ p X Y Ys$_a$ Ys$_d$ t L1 L2 L3.
 SEN_broad_set_req p L1 L2 (ind_set [{0}; L1; L2; L3])
   (ind_set [{0}; {1; 2}; {3}]) {0; 1; 2}
   (event_set [(DRBD_event p (R_WSP Y Ys$_a$ Ys$_d$) t,0);
     (rv_to_event p X t)) ⇒
 (prob p (DRBD_event p Q$_{\text{SEN+\_Broadcast}}$ t) =
 Rel p (R_WSP Y Ys$_a$ Ys$_d$) t * Normal ($\prod_{i \in L3}$ (real (Rel p (X l) t))) *
 (1 - (1 - Normal ($\prod_{l \in L1}$ (real (Rel p (X l) t)))) *
     (1 - Normal ($\prod_{l \in L2}$ (real (Rel p (X l) t))))))

We evaluate the broadcast reliability, in Figure 13, of a 128×128 SEN+, where each inner series structure of Figure 12 has 63 blocks and the series structure on the right hand side of the figure has 64 blocks. We use the same failure rates of 1×10^{-5} for each switching element with a dormancy factor of 0.1.

4 Network Reliability Analysis of Shuffle-exchange Networks

According to [18], the network reliability of SENs can be defined as the reliability of all connections between sources (inputs) and destinations (outputs). In other words, we are looking at the reliability of the overall network. This is usually modeled using RBDs. In this section, we use both DFT and DRBD models in different scenarios to model the reliability of the network.

4.1 DFT Analysis of SEN and SEN+

In the SEN, it is required that all switching elements must work properly in order to maintain a successful behavior of the network. Thus, the system fails with the failure
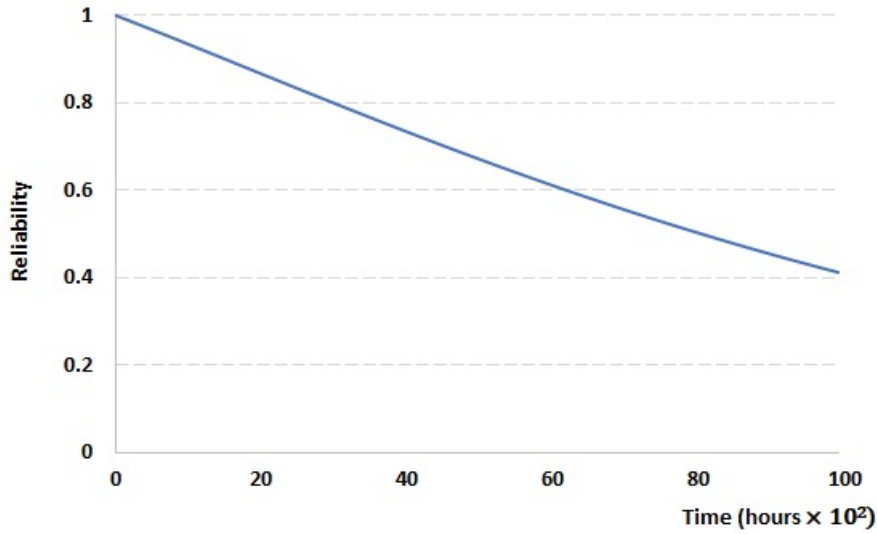
Figure 13: Broadcast Reliability of a 128×128 SEN+

of any of the switching elements. The behavior can be further enhanced by using spares. The DFT of the SEN network can be modeled as in Figure 4. However, to further enhance the system reliability, the reliability engineer may suggest to use more spares to replace the switching elements. Therefore, we present a generic model, where the number of switching elements that have spares is generic, as shown in Figure 14. This model can be also used with both the terminal and broadcast models, when more spares are required.
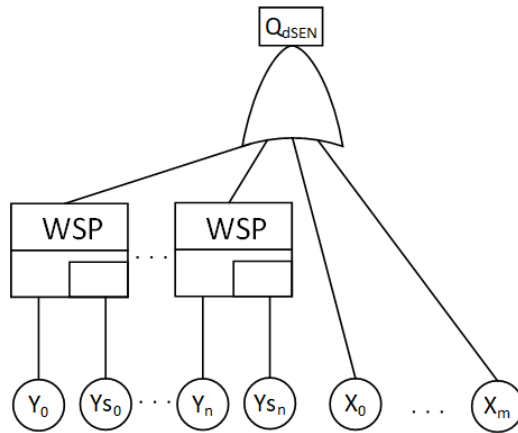
Figure 14: DFT of SEN Network with Multiple Spares

The top event of the DFT of Figure 14 can be expressed using the DFT operators as:

$$Q_{\text{dsSEN\_Network}} = \text{n\_OR (MAP} (\lambda i. \quad \text{if } i \in \text{L1 then WSP (Y i) (Ys}_\text{a} \text{ i) (Ys}_\text{d} \text{ i)}$$
$$\text{else X i) (SET\_TO\_LIST (L1} \cup \text{L2)))}$$

$$(7)$$

We verify the probability of failure of the top event in a similar way to Theorem 2.3, as:

Theorem 4.1.
⊢ ∀ p X Y Ys$_\text{a}$ Ys$_\text{d}$ t L1 L2.
  DISJOINT L1 L2 ∧ FINITE L1 ∧ L1 ≠ {} ∧
  FINITE L2 ∧ L2 ≠ {} ∧
  (∀ i. i ∈ L2 ⇒ rv_gt0_ninfinity [X i]) ∧
  indep_sets p
    (λi.
      {rv_to_devent p
        (λi. i ∈ L1 then WSP (Y i) (Ys$_\text{a}$ i) (Ys$_\text{d}$ i) else X i)
        t i})(L1 ∪ L2) ⇒
  (prob p (DFT_event p Q$_\text{dSEN\_Network}$ t) =
  1−
  Normal
    ($\prod_{i \in L1}$
      (real(1− prob p (DFT_event p (WSP (Y i) (Ys$_\text{a}$ i) (Ys$_\text{d}$ i)) t)))) *
  Normal ($\prod_{i \in L2}$ (real(1−F$_{\text{X}_\text{i}}$(t)))))

where Y, Ys$_\text{a}$ and Ys$_\text{d}$ are groups of indexed random variables that represent the main and spare switches. Theorem 4.1 provides a generic scenario for the SEN, where L1 and L2 can be instantiated with any number of distinct indices that represent the system switches, with and without spares.

The DFT model of the SEN+ network is shown in Figure 15. It consists of a spare gate for one of the switches in the input stage. The rest of the input switches ($X_{1,0}$ - $X_{1,r}$) are connected directly to the n-OR gate of the top event. Therefore, the failure of any of these switches leads to the failure of the network. The series of ANDs and ANDs of ORs are used to model the two available paths. Finally, all destination switches ($X_{4,0}$ -$X_{4,k}$) are required to function and thus they are all connected to the output OR gate. This DFT is composed of three levels; OR of ANDs of ORs, and thus we can use the theorems of union of intersections of unions to verify its probability of failure if the sets of indices are handled properly.

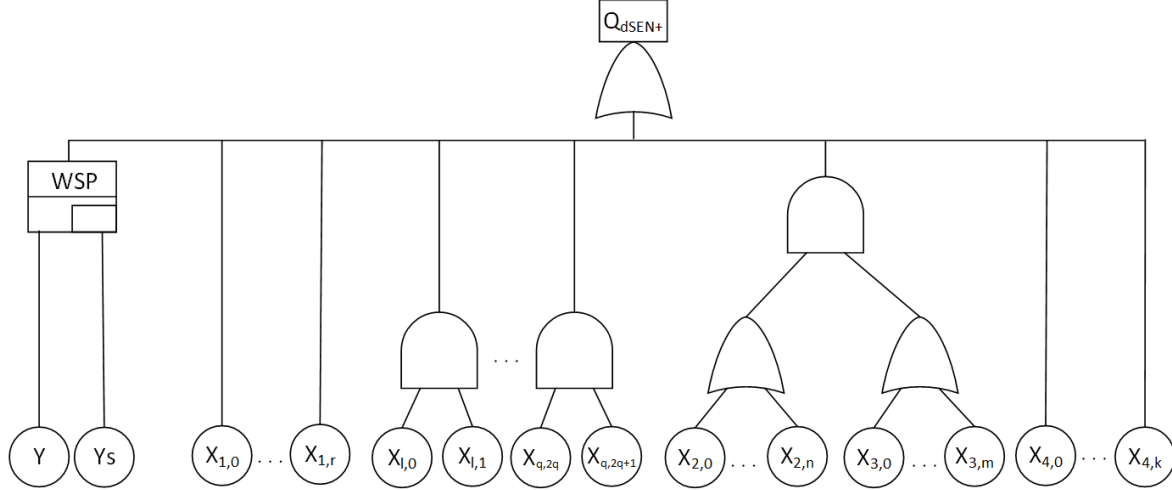We first express the top event using the DFT operators as:

Figure 15: DFT of SEN+ Network

$$
\begin{aligned}
Q_{\texttt{dSEN\_Network}} = \\
\quad \texttt{n\_OR} \\
\quad\quad (\texttt{MAP} \\
\quad\quad\quad (\lambda\texttt{i.} \quad \texttt{if i = 0 then WSP Y Ys}_\texttt{a}\ \texttt{Ys}_\texttt{d} \\
\quad\quad\quad\quad\quad \texttt{else if i = 1 then n\_OR (MAP X (SET\_TO\_LIST L1))} \\
\quad\quad\quad\quad\quad \texttt{else if i = 3 then (n\_OR (MAP X (SET\_TO\_LIST L2))) } \cdot \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \texttt{(n\_OR (MAP X (SET\_TO\_LIST L3)))} \\
\quad\quad\quad\quad\quad \texttt{else if i = 4 then n\_OR (MAP X (SET\_TO\_LIST L4))} \\
\quad\quad\quad\quad\quad \texttt{else (X (2 * i)) } \cdot \texttt{ (X (2 * i + 1)))} \\
\quad\quad\quad (\texttt{SET\_TO\_LIST (\{0; 1; 3; 4\} } \cup \texttt{ L)))}
\end{aligned} \tag{8}
$$

where the spare gate is assigned index 0. The second group of switches has index 1, while the indices of these switches, $X_{1,0}$ - $X_{1,r}$, are in set L1. They are represented as n_OR (MAP X (SET_TO_LIST L1). The output of the AND of ORs is assigned index 3 and is modeled as (n_OR (MAP X (SET_TO_LIST L2))) · (n_OR (MAP X (SET_TO_LIST L3))), which is similar to both the terminal and broadcast models. The group of switches, $X_{4,0}$ -$X_{4,k}$, has index 4 and is represented using n_OR (MAP X (SET_TO_LIST L4)). Thus, we have the indices $\{0; 1; 3; 4\}$ for the outer groups in the DFT. However, the last part of the DFT, which is the series of ANDs in the middle of Figure 15, has a generic number of AND gates and cannot be assigned a specific index. Therefore, we use set L to get a unique index for the output of each AND gate. We use this unique number to create the indices of the inputs of each AND gate. For example, for an index j in set L, we create two indices for the inputs of the AND gate as (2*j) and (2*j+1). This is modeled as (X (2 * i)) · (X (2 * i + 1))) and set L is used with the set of indices in the outer level as (SET_TO_LIST ($\{0; 1; 3; 4\} \cup$ L)). It is important to highlight that the indices of the individual inputs should be unique.

21

We then verify that the `DFT_event` of $Q_{dSEN\_Network}$ is equal to the union of intersection of union of events as in the following theorem:

Theorem 4.2.
⊢ ∀ p L1 L2 L3 L4 L X Y Ys$_a$ Ys$_d$ t.
  FINITE L1 ∧ L1 ≠ {} ∧ FINITE L2 ∧ L2 ≠ {} ∧ FINITE L3 ∧
  L3 ≠ {} ∧ FINITE L4 ∧ L4 ≠ {} ∧ FINITE L ∧
  DISJOINT {0; 1; 3; 4} L ∧
  (∀ i. i ∈ L ⇒ DISJOINT {2 * i; 2 * i + 1} {0; 1; 2; 3; 4}) ∧
  disjoint_family_on
    (ind_set
      [{0}; L1; L2; L3; L4; {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L}])
    {0; 1; 2; 3; 4; 5} ⇒
  (DFT_event p (Q$_{dSEN\_Network}$) t =
   ⋃
    {⋂
      {⋃ {event_set [(DFT_event p (WSP Y Ys$_a$ Ys$_d$) t,0)]
              (rv_to_devent p X t) i |
        i ∈ if a ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {a}
               else ind_set [{0}; L1; L2; L3; L4] a} |
      a ∈ if j ∈ L then {2 * j; 2 * j + 1}
            else ind_set [{0}; {1}; {}; {2; 3}; {4}] j} |
   j ∈ {0; 1; 3; 4} ∪ L}

where the conditions are required to ensure that the sets are finite, nonempty and that at each level of the DFT the indices are unique. It is clear from the theorem how the hierarchy of the DFT is structured using the sets. For example, "if j ∈ L then {2 * j; 2 * j + 1} else ind_set [{0}; {1}; {}; {2; 3}; {4}] j" determines the indices of the second level of the DFT (the ORs) based on the value of j in the outer level. The first part "if j ∈ L then {2 * j; 2 * j + 1}" is for the series of ANDs, while "else ind_set [{0}; {1}; {}; {2; 3}; {4}] j" is for the rest of the parts in the second level. Although some of the parts of the DFT have no intermediate OR gates, like the spare, we implicitly assume that there are OR gates with single inputs to maintain the consistency. The indices of the second level indicates the indices of the output of these gates. This can be obvious for the AND of ORs in Figure 15, where the OR gates have indices 2 and 3. We use an empty set ({}) in the indices of the second level due to the fact that there is no index 2 in the outer level, and thus we assigned an empty set in the second level for this index.

We verify the probability of failure of $Q_{dSEN\_Network}$ as:

Theorem 4.3.
⊢ ∀ p L1 L2 L3 L4 L X Y Ys$_a$ Ys$_d$ t.
  SEN_network_set_req p L1 L2 L3 L4 L
    (λi.
      if i ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {i}
      else ind_set [{0}; L1; L2; L3; L4] i)

```
(λj.
   if j ∈ L then {2 * j; 2 * j + 1}
   else ind_set [{0}; {1}; {}; {2; 3}; {4}] j)
 ({0; 1; 3; 4} ∪ L)
   (event_set [(DFT_event p (WSP Y Ys_a Ys_d) t,0)]
     (rv_to_devent p X t)) ∧
(∀ i.
   i ∈ L1 ∪ L2 ∪ L3 ∪ L4 ∪
     {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} ⇒
   rv_gt0_ninfinity [X i]) ⇒
(prob p
 (DFT_event p (Q_dSEN_Network) t) =
 1 -
 (1 - prob p (DFT_event p (WSP Y Ys_a Ys_d) t)) *
 Normal (∏_{l∈L1} (real (1 - F_{X_l}(t)))) *
 (1 -
   (1 - Normal (∏_{l∈L2} (real (1 - F_{X_l}(t))))) *
   (1 - Normal (∏_{l∈L3} (real (1 - F_{X_l}(t)))))) *
 Normal (∏_{l∈L4} (real (1 - F_{X_l}(t)))) *
 Normal (∏_{j∈L} (1 - real (F_{X_{2*j}}(t) * F_{X_{2*j+1}}(t)))))
```

where `SEN_network_set_req` ensures all the required conditions for the sets to be finite, nonempty and distinct. It also ensures the independence of the input events. It accepts all the sets of the indices of the three levels. The second condition (`rv_gt0_ninfinity [X i]`) ascertains that each element in the group of random variables of X that have their indices in `L1 ∪ L2 ∪ L3 ∪ L4 ∪ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L}` are greater than or equal to 0 but not equal $+\infty$. This condition is required to be able to use the CDF of the random variables.
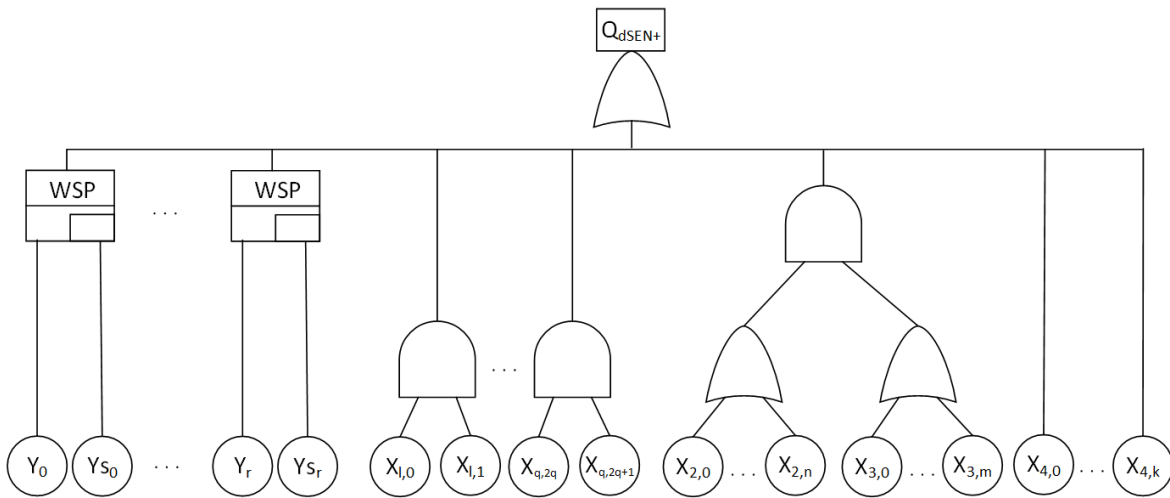

Figure 16: DFT of SEN+ with Multiple Spares

In a similar manner to the SEN network, we provide a generic model where any

23

number of spares can be used for the input switches. The modified DFT is shown in Figure 16. We express the top event using the DFT operators as:

$Q_{\text{dSEN\_Network2}}$ =
  n_OR
   (MAP
     (λi. if i = 0 then WSP (Y 0) (Ys_a 0) (Ys_d 0)
          else if i = 1 then
           (n_OR (MAP X (SET_TO_LIST L1)))   (9)
         else if i = 3 then (n_OR (MAP X (SET_TO_LIST L2))) ·
                     (n_OR (MAP X (SET_TO_LIST L3)))
         else if i = 4 then n_OR (MAP X (SET_TO_LIST L4))
         else (X (2 * i)) · (X (2 * i + 1)))
     (SET_TO_LIST ({0; 1; 3; 4} UNION L)))

where Y, Ys_a and Ys_d are indexed random variables that represent the main and spare parts for each spare gate. We choose to use the same hierarchy of Figure 15, where we assign index 0 for the first spare and the rest of the spares have their indices in set L1. In addition, the model of these additional spares is embedded within X as will be explained shortly.

We verify the probability of failure of the top event as:

Theorem 4.4.
⊢ ∀ p L1 L2 L3 L4 L X Y Ys_a Ys_d t.
  SEN_network_set_req p L1 L2 L3 L4 L
    (λi.
      if i ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {i}
      else ind_set [{0}; L1; L2; L3; L4] i)
    (λj.
      if j ∈ L then {2 * j; 2 * j + 1}
      else ind_set [{0}; {1}; {}; {2; 3}; {4}] j)
    ({0; 1; 3; 4} ∪ L)
    (λi.
      event_set [(DFT_event p (WSP (Y 0) (Ys_a 0) (Ys_d 0)) t,0)]
      (rv_to_devent p X t) i) ∧
  (∀ i.
   i ∈ L1 ∪ L2 ∪ L3 ∪ L4 ∪ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} ⇒
   rv_gt0_ninfinity [X i]) ∧
  (∀ i. i ∈ L1 ⇒ (X i = WSP (Y i) (Ys_a i) (Ys_d i))⇒
  (prob p
  (DFT_event p ($Q_{\text{dSEN\_Network2}}$) t) =
  1 -
  Normal
   ($\prod_{l\in(\{0\}\cup L1}$

24

```
        (real (1 - prob p (DFT_event p (WSP (Y l) (Ys_a l) (Ys_d l)) t))) *
     (1 -
        (1 - Normal (∏_{l∈L2} (real (1 - F_{X_1}(t))))) *
        (1 - Normal (∏_{l∈L3} (real (1 - F_{X_1}(t)))))) *
        Normal (∏_{l∈L4} (real (1 - F_{X_1}(t)))) *
        Normal (∏_{j∈L} (1 - real (F_{X_{2*j}}(t) * F_{X_{2*j+1}}(t)))))
```

where the conditions are similar to Theorem 4.3. However, we add the condition that $(\forall \ i. \ \ i \in L1 \Rightarrow (X \ i = WSP \ (Y \ i) \ (Ys_a \ i) \ (Ys_d \ i))$, which adds the additional spare gates. This way, we can use Theorem 4.3 to verify Theorem 4.4. Set $\{0\} \cup L1$ is used to provide the indices of the spares, including the first one with index 0.

We evaluate the probability of failure of the network DFT, shown in Figure 16, for a 128×128 SEN+. The DFT of this SEN has 32 AND gates in the first level. Each OR gate in the first level has 160 inputs. Furthermore, we assume that all the 64 input switches have spares. Figure 21 shows the evaluated result of the probability of failure, where the failure rates of each switching element is 1×10^{-5} with a dormancy factor of 0.1.
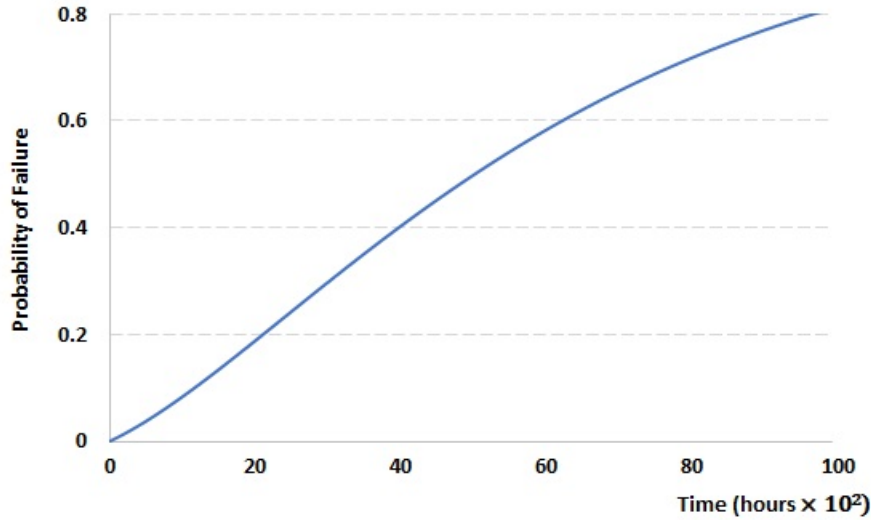

Figure 17: The Probability of Failure of the Network of a 128×128 SEN+

4.2 DRBD Analysis of SEN and SEN+

Similar to the DFT models, we start first with the network reliability model of the SEN. Since it is a single path, it can be modeled using the series DRBD of Figure 7. Thus, we can use Theorem 2.9 to provide a generic expression for its reliability. We provide a generic model in Figure 18, where additional spares are used. This provides a general case where we can choose how many switches can be replaced with spares.

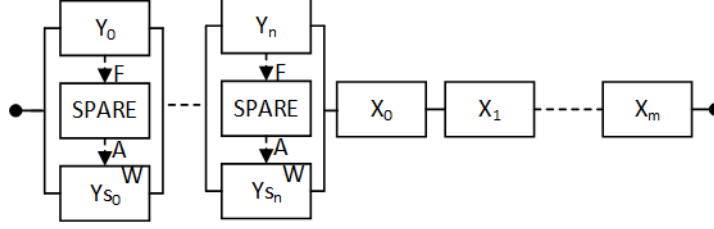We express the structure function of this DRBD using our DRBD operators as:

Figure 18: DRBD of SEN Network

$$\text{Q}_{\text{sSEN\_Network}} = \text{nR\_AND } (\lambda\text{i. if i} \in \text{L1 then R\_WSP (Y i) (Ys}_\text{a}\text{ i) (Ys}_\text{d}\text{ i)}$$
$$\text{else X i) (L1} \cup \text{L2)}$$

$$(10)$$

where `L1` and `L2` provide the indices of the blocks in the series structure for the spare constructs and the remaining blocks, respectively.

Similar to the proof steps of Theorem 2.11, we verify the reliability of the SEN network as:

Theorem 4.5.
```
⊢ ∀ p X Y Ysₐ Ys_d t L1 L2.
 DISJOINT L1 L2 ∧ FINITE L1 ∧ L1 ≠ {} ∧
 FINITE L2 ∧ L2 ≠ {} ∧
 indep_sets p
   (λi. {if i ∈ L1 then DRBD_event p (R_WSP (Y i) (Ysₐ i) (Ys_d i)) t
         else (rv_to_event p X t) i}) (L1 ∪ L2)⇒
 (prob p (DRBD_event p Q_SEN_Network t) =
  Normal
    (∏_{i∈L1}
      (real (Rel p (R_WSP (Y i) (Ysₐ i) (Ys_d i)) t))) *
  Normal (∏_{i∈L2} (real (Rel p (X i) t))))
```

The DRBD of the SEN+ network is modeled in Figure 19, where only one of the switches of the input stage can be replaced by a spare. This DRBD is composed of a series-parallel-series structure. The indices of each level can be treated in a similar manner to the DFT.

We express the structure function using the operators with the same sets of indices of the DFT as:
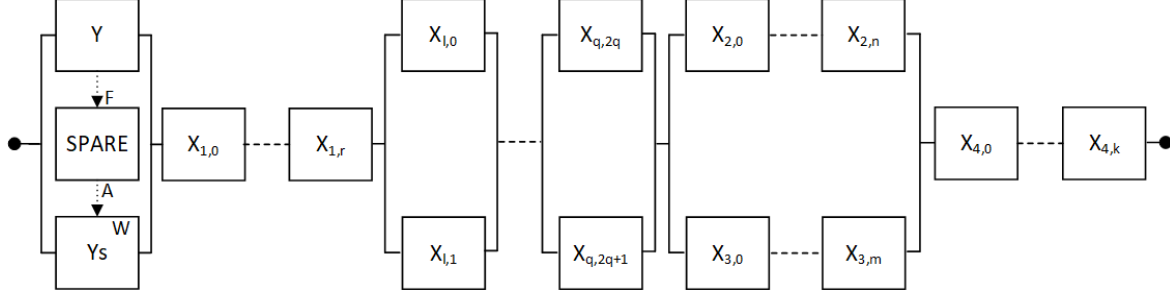
Figure 19: DRBD of SEN+ Newtork

$Q_{\text{SEN\_Network}}$ = nR_AND
```
            (λi.
               if i = 0 then R_WSP Y Ys_a Ys_d
               else if i = 1 then nR_AND X L1
               else if i = 3 then (nR_AND X L2) + (nR_AND X L3)
               else if i = 4 then nR_AND X L4
               else (X (2 * i)) + (X (2 * i + 1)))
            ({0; 1; 3; 4} ∪ L))
```
(11)

Then, we verify that the DRBD_event of this structure can be expressed as a series-parallel-series structure as:

Theorem 4.6.
```
⊢ ∀ p L1 L2 L3 L4 L X Y Ys_a Ys_d t.
  FINITE L1 ∧ L1 ≠ {} ∧ FINITE L2 ∧ L2 ≠ {} ∧ FINITE L3 ∧
  L3 ≠ {} ∧ FINITE L4 ∧ L4 ≠ {} ∧ FINITE L ∧
  DISJOINT {0; 1; 3; 4} L ∧
  (∀ i.  i ∈ L ⇒ DISJOINT {2 * i; 2 * i + 1} {0; 1; 2; 3; 4}) ∧
  disjoint_family_on
   (ind_set
      [{0}; L1; L2; L3; L4;
       {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L}])
      {0; 1; 2; 3; 4; 5} ⇒
  (DRBD_event p
   (Q_SEN_Network) t =
   DRBD_series
     (λj.
        DRBD_parallel
          (λa.
             DRBD_series
               (λi.
                  event_set
```

```
              [(DRBD_event p (R_WSP Y Ys_a Ys_d t,0)]
                (rv_to_event p X t) i)
           ((λi.
               if i ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {i}
               else ind_set [{0}; L1; L2; L3; L4] i) a))
        ((λj.
             if j ∈ L then {2 * j; 2 * j + 1}
           else ind_set [{0}; {1}; {}; {2; 3}; {4}] j) j))
        ({0; 1; 3; 4} ∪ L))
```

Finally, we verify the reliability of the DRBD as:

Theorem 4.7.
```
⊢ ∀ p L1 L2 L3 L4 L X Y Ys_a Ys_d t.
  SEN_network_set_req p L1 L2 L3 L4 L
    (λi.
       if i ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {i}
       else ind_set [{0}; L1; L2; L3; L4] i)
    (λj.
       if j ∈ L then {2 * j; 2 * j + 1}
       else ind_set [{0}; {1}; {}; {2; 3}; {4}] j)
    ({0; 1; 3; 4} ∪ L)
    (event_set [(DRBD_event p (R_WSP Y Ys_a Ys_d) t,0)]
        (rv_to_event p X t)) ⇒
  (prob p
    (DRBD_event p (Q_SEN_Network) t) =
  Rel p (R_WSP Y Ys_a Ys_d) t *
  Normal (∏_{l∈L1} (real (Rel p (X l) t))) *
  (1 -
    (1 - Normal (∏_{l∈L2} (real (Rel p (X l) t)))) *
    (1 - Normal (∏_{l∈L3} (real (Rel p (X l) t))))) *
  Normal (∏_{l∈L4}(real (Rel p (X l) t))) *
  Normal
    (∏_{j∈L}
      (1 -
        real
          ((1 - Rel p (X (2 * j)) t) *
           (1 - Rel p (X (2 * j + 1)) t)))))
```

It is worth mentioning that the conditions of the sets are similar to Theorem 4.3 of the DFT.

Finally, we provide a generic model to have any number of spares that can replace the input switches as shown in Figure 20. We choose to use the same indices of Figure 19 in order to reutilize the verified theorems.

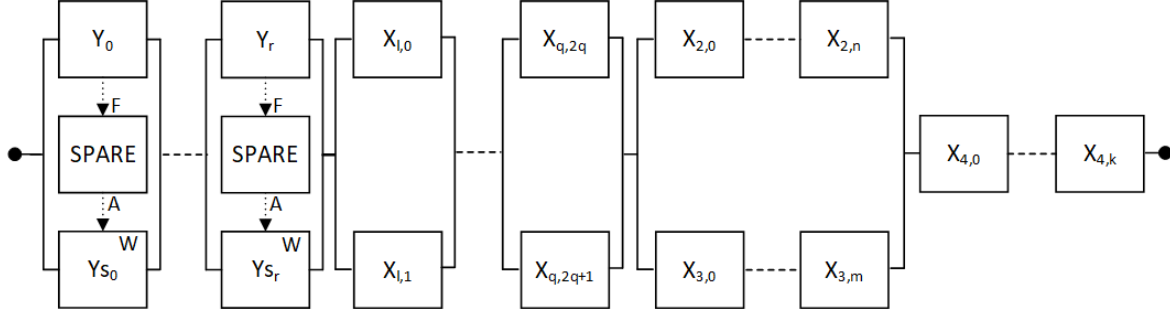We express the structure of the DRBD of Figure 20 as:

Figure 20: DRBD of SEN+ Network with Multiple Spares

$$
\begin{aligned}
\mathrm{Q_{SEN\_Network2}} = \ &\mathrm{nR\_AND} \\
&(\lambda\mathrm{i}. \\
&\quad \mathrm{if\ i = 0\ then\ R\_WSP\ (Y\ 0)\ (Ys_a\ 0)\ (Ys_d\ 0)} \\
&\quad \mathrm{else\ if\ i = 1\ then\ nR\_AND\ X\ L1} \\
&\quad \mathrm{else\ if\ i = 3\ then\ (nR\_AND\ X\ L2) + (nR\_AND\ X\ L3)} \\
&\quad \mathrm{else\ if\ i = 4\ then\ nR\_AND\ X\ L4} \\
&\quad \mathrm{else\ (X\ (2 * i)) + (X\ (2 * i + 1)))} \\
&(\{0;\ 1;\ 3;\ 4\} \cup \mathrm{L}))
\end{aligned}
\tag{12}
$$

where `(Y 0)`, `(Ys`$_a$` 0)` and `(Ys`$_d$` 0)` are indexed groups of random variables that represent the main parts and their spares.

Finally, we use Theorem 4.7 to verify the reliability of this DRBD as:

Theorem 4.8.
⊢ ∀ p L1 L2 L3 L4 L X Y Ys$_a$ Ys$_d$ t.
  SEN_network_set_req p L1 L2 L3 L4 L
    (λi.
      if i ∈ {2 * i | i ∈ L} ∪ {2 * i + 1 | i ∈ L} then {i}
      else ind_set [{0}; L1; L2; L3; L4] i)
    (λj.
      if j ∈ L then {2 * j; 2 * j + 1}
      else ind_set [{0}; {1}; {}; {2; 3}; {4}] j)
    ({0; 1; 3; 4} ∪ L)
    (event_set [(DRBD_event p (R_WSP (Y 0) (Ys$_a$ 0) (Ys$_d$ 0)) t,0)]
      (rv_to_event p X t)) ∧
(∀ i. i ∈ L1 ⇒ (X i = R_WSP (Y i) (Ys$_a$ i) (Ys$_d$ i))) ⇒
  (prob p
    (DRBD_event p (Q$_{\mathrm{SEN\_Network2}}$) t) =
  Normal
  ($\prod_{l \in (\{0\} \cup L1}$

```
   (real (Rel p (R_WSP (Y l) (Ys_a l) (Ys_d l)) t))) *      (1 -
  (1 - Normal (∏_{l∈L2} (real (Rel p (X l) t)))) *
  (1 - Normal (∏_{l∈L3} (real (Rel p (X l) t))))) *
 Normal (∏_{l∈L4}(real (Rel p (X l) t))) *
 Normal
   (∏_{j∈L}
     (1 -
     real
       ((1 - Rel p (X (2 * j)) t) *
        (1 - Rel p (X (2 * j + 1)) t)))))
```

We evaluate the network reliability of a 128×128 as shown in Figure 20. In Figure 20, there are 32 parallel structures that are connected in series. The DRBD has 64 spare constructs, while there are 160 blocks in the inner series structures. Finally, the series structure on the right hand side of Figure 20 has 64 blocks. We assume that the failure rates of each switching element is 1×10^{-5} with a dormancy factor of 0.1.
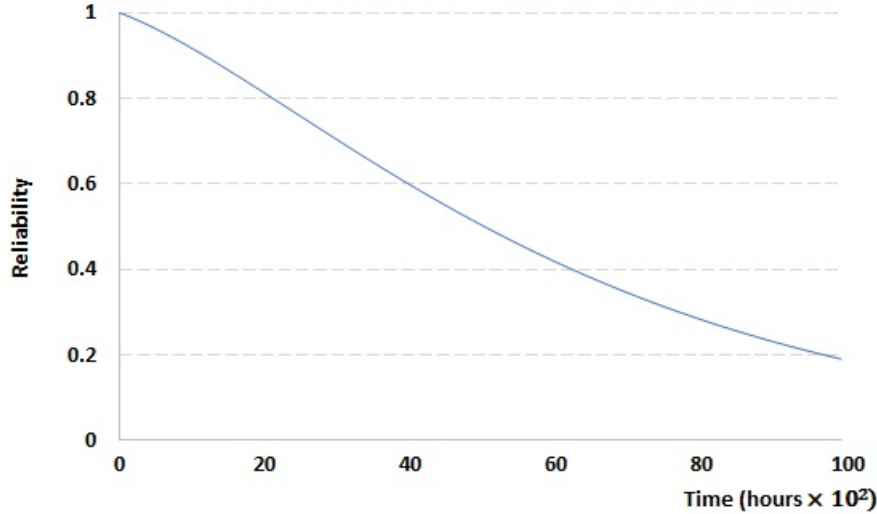

Figure 21: The Network Reliability of a 128×128 SEN+

5   Equivalence of SEN DFT and DRBD Models

In [23], we proposed a methodology for where a DFT model can be formally analyzed using the DRBD algebra and vice versa. To illustrate the utilization of the proposed methodology, we formally verify the equivalence of the DRBD and the complement of the DFT events for both terminal and broadcast reliability of SEN and SEN+. The equivalence of the network models can be conducted in a similar manner. Proving this equivalence allows verifying the probability of one model and directly use the equivalence proof to provide the probability of the other model.

We verify the equivalence of the DRBD and DFT models of the terminal reliability of both SEN and SEN+ as:

Theorem 5.1. *Terminal/Broadcast SEN*
$\vdash \forall$ p X Y Ys_a Ys_d t L.
 FINITE L $\wedge$ ($\forall$ s. ALL_DISTINCT [Y s; Ys_a s; Ys_d s]) $\Rightarrow$
 (DRBD_event p
      (nR_AND
        (λi.
           if i = 0 then R_WSP Y Ys_a Ys_d
           else X i) $\{0\}$ $\cup$ L) t =
  p_space p DIFF
  DFT_event p
    (n_OR
      (MAP
        (λi.
           if i = 0 then WSP Y Ys_a Ys_d
           else X i)
      (SET_TO_LIST ($\{0\}$ $\cup$ L)))) t)

Theorem 5.2. *Terminal SEN+*
$\vdash \forall$ p X Y Ys_a Ys_d Z Zs_a Zs_d t L1 L2.
 FINITE L1 $\wedge$ FINITE L2 $\wedge$
 ($\forall$ s. ALL_DISTINCT [Y s; Ys_a s; Ys_d s; Z s; Zs_a s; Zs_d s]) $\Rightarrow$
 (DRBD_event p
    (nR_AND
      (λi.
          if i = 0 then R_WSP Y Ys_a Ys_d
          else if i = 1 then $\big(\text{(nR\_AND X L1)} + \text{(nR\_AND X L2)}\big)$
          else R_WSP Z Zs_a Zs_d) $\{0; 1; 2\}$) t =
  p_space p DIFF
  DFT_event p
    (n_OR
      (MAP
        (λi.
           if i = 0 then WSP Y Ys_a Ys_d
           else if i = 1 then
               $\big(\text{(n\_OR (MAP X (SET\_TO\_LIST L1)))}\ \cdot$
                 $\text{(n\_OR (MAP X (SET\_TO\_LIST L2))))}$
           else WSP Z Zs_a Zs_d) (SET_TO_LIST $\{0; 1; 2\}$))) t)

   In a similar manner, we verify the equivalence of the DRBD and DFT models of
the SEN+ broadcast reliability as:

Theorem 5.3. *Broadcast SEN+*
⊢ ∀ p X Y Ys$_a$ Ys$_d$ t L1 L2 s.
 FINITE L1 ∧ FINITE L2 ∧ FINITE L3 ∧
 (∀ s. ALL_DISTINCT [Y s; Ys$_a$ s; Ys$_d$ s]) ⇒
 (DRBD_event p
   (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 (nR_AND X L3)) ({0; 1 2}) t =
  p_space p DIFF
  DFT_event p
   (n_OR
    (MAP
      (λi.
           if i = 0 then WSP Y Ys$_a$ Ys$_d$
           else if i = 1 then
                ((n_OR (MAP X (SET_TO_LIST L1))) ·
                 (n_OR (MAP X (SET_TO_LIST L2))))
           else (n_OR (MAP X (SET_TO_LIST L3))))
          ({0; 1 2}))) t)

It is worth mentioning that Theorem 5.1 can be used for the equivalence of the DRBD-DFT models of the SEN in both the terminal and broadcast since they both share the same structure.

Based on these theorems, we can use one model to verify the probability of the other model using the probability of the complement.

6   Conclusion

In this report, we presented the formal dynamic dependability analysis of SEN and SEN+ MINs that form a critical part in the routing process of multiprocessor systems. We provided generic expressions of reliability and probability of failure that are independent of the failure distributions. Furthermore, we verified these expressions for an arbitrary number of system blocks that can be instantiated later to a certain number without the need to repeat the verification process. For instance, we evaluated the reliability and probability of failure using MATLAB for a specific number of system components based on these generic expressions. It is worth mentioning that such sound generic results cannot be obtained using simulation or model checking as the state space should be defined in advance. The proof script of the verification of SEN and SEN+ is available at [24] and it took around 80 hours to be developed.

References

[1] A. Avizienis, J.C. Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

[2] E. Ruijters and M. Stoelinga. Fault Tree Analysis: A Survey of the State-of-the-art in Modeling, Analysis and Tools. *Computer Science Review*, 15-16:29 – 62, 2015.

[3] S. Distefano and L. Xing. A New Approach to Modeling the System Reliability: Dynamic Reliability Block Diagrams. In *Reliability and Maintainability Symposium*, pages 189–195. IEEE, 2006.

[4] Y. Elderhalli, O. Hasan, and S. Tahar. A Methodology for the Formal Verification of Dynamic Fault Trees Using HOL Theorem Proving. *IEEE Access*, 7:136176–136192, 2019.

[5] Y. Elderhalli, O. Hasan, and S. Tahar. A Formally Verified Algebraic Approach for Dynamic Reliability Block Diagrams. In *International Conference on Formal Engineering Methods*, LNCS 11852, pages 253–269. Springer, 2019.

[6] J.L. Hennessy and D.A. Patterson. *Computer Architecture: A Quantitative Approach*. Elsevier, 2011.

[7] R. Aggarwal and L. Kaur. On Reliability Analysis of Fault-tolerant Multistage Interconnection Networks. *International Journal of Computer Science and Security*, 2(4):01–08, 2008.

[8] V.P Kumar and S.M Reddy. Fault-tolerant Multistage Interconnection Networks for Multiprocessor Systems. In *Concurrent Computations*, pages 495–523. Springer, 1988.

[9] M. Jeng and H.J. Siegel. A Fault-Tolerant Multistage Interconnection Network for Multiprocessor Systems Using Dynamic Redundancy. In *International Conference on Distributed Computing Systems*, pages 70–77. IEEE, 1986.

[10] N.A.M. Yunus and M. Othman. Reliability Evaluation for Shuffle Exchange Interconnection Network. *Procedia Computer Science*, 59:162–170, 2015.

[11] F. Bistouni and M. Jahanshahi. Determining the Reliability Importance of Switching Elements in the Shuffle-exchange Networks. *International Journal of Parallel, Emergent and Distributed Systems*, 34(4):448–476, 2019.

[12] N.A.M. Yunus, M. Othman, Z.M. Hanapi, and Y.L. Kweh. Evaluation of Replication Method in Shuffle-Exchange Network Reliability Performance. In *Advances in Data and Information Sciences*, pages 271–281. Springer, 2019.

[13] D.K. Panda, R.K. Dash, A.K. Mishra, and S.K. Mohapatra. Reliability Evaluation and Analysis of Multistage Interconnection Networks. *International Journal of Pure and Applied Mathematics*, 119(14):1729–1737, 2018.

[14] I. Gunawan. Reliability Prediction of Distributed Systems using Monte Carlo Method. *International Journal of Reliability and Safety*, 7(3):235–248, 2013.

[15] S Rajkumar and N.K. Goyal. Review of Multistage Interconnection Networks Reliability and Fault-tolerance. *IETE Technical Review*, 33(3):223–230, 2016.

[16] I. Gunawan. Redundant Paths and Reliability Bounds in Gamma Networks. *Applied Mathematical Modelling*, 32(4):588–594, 2008.

[17] N.A.M. Yunus, M. Othman, Z.M. Hanapi, and K.Y. Lun. Reliability Review of Interconnection Networks. *IETE Technical Review*, 33(6):596–606, 2016.

[18] F. Bistouni and M. Jahanshahi. Analyzing the Reliability of Shuffle-exchange Networks using Reliability Block Diagrams. *Reliability Engineering & System Safety*, 132:97–106, 2014.

[19] Y. Elderhalli, W. Ahmad, O. Hasan, and S. Tahar. Probabilistic Analysis of Dynamic Fault Trees using HOL Theorem Proving. *Journal of Applied Logics*, 2631(3):469, 2019.

[20] Y. Elderhalli. DFT Formal Analysis: HOL4 Script, Concordia University, Canada, http://hvg.ece.concordia.ca/code/hol/DFT_method/index.php (2019).

[21] Y. Elderhalli. DRBD Formal Analysis: HOL4 Script, http://hvg.ece.concordia.ca/code/hol/DRBD/index.php, 2019.

[22] MATLAB 2017a, The MathWorks, Natick, 2017.

[23] Y. Elderhalli, O. Hasan, and S. Tahar. Integrating DFT and DRBD Formalizations in HOL4. Technical report, Concordia University, Canada, 2019.

[24] Y. Elderhalli. Shuffle-exchange Network Formal Dependability Analysis: HOL4 Script, Concordia University, Canada, http://hvg.ece.concordia.ca/code/hol/SEN/index.php, (2019).