Toward Accessibility Enhancement of Dependability Modeling Techniques and Tools

Ann T. Tai [†] Herbert Hecht [†] Kishor S. Trivedi [‡] Bing Zhang [†]

[†] SoHaR Incorporated
Beverly Hills, CA 90211
U.S.A.
Tel: (+1)213-653-4717
E-mail: tai@sohar.com

[‡] Duke University
Durham, NC 27708
U.S.A.
Tel: (+1)919-660-5269
E-mail: kst@ee.duke.edu

Abstract

Fast turnaround time in dependability evaluation is crucial for efficient fault-tolerant system design and dependability of the resulting product since timely feedbacks will allow more iterations for design modification under the constraints of project schedule. Therefore, it is highly desirable to enable system designers to handle and control dependability modeling processes themselves, instead of turning over the problems to reliability/quality-assurance personnel. Although various dependability evaluation techniques and tools have been developed in the last two decades, no adequate attention has been paid regarding how to enable system designers with minimal analytic background to easily employ these techniques and tools. In this paper, we report our experiences on accessibility enhancement for off-the-shelf modeling techniques and tools. In particular, we discuss our approaches to the development of a user-friendly dependability-evaluation workbench which is intended to lead the user to exploit the features and capabilities of the modeling tool SHARPE.

Keywords: Dependability evaluation, modeling techniques and tools, graphical-user-interface, fault-tolerant system design

Submission Category: Practical Experience Report

1 Introduction

Dependability evaluation is an important activity for fault-tolerant system specification, design and maintenance. Moreover, fast turnaround time of dependability modeling process is one of the key factors for the efficiency of those activities and for the dependability of the resulting products since timely feedbacks will allow more iterations for design modification under the constraints of project schedule. In other words, a system designer should be able to quickly get ideas about how the current products (specification, design, etc.) satisfy the requirements and where modifications need to be incorporated. Indeed dependability evaluation can become more efficient and effective if modeling techniques and tools are made easier for system designers to employ such that they can handle and control the evaluation process themselves, instead of turning over the problems to the reliability/quality-assurance personnel. Although various dependability evaluation techniques and tools have been developed in the last two decades, significantly fewer efforts have been devoted to enabling system designers with little analytic background to access those techniques and tools. With the motivation of enhancing accessibility for off-the-shelf modeling techniques and tools, we have developed a dependability-evaluation workbench called SDDS (Software Dependability for Distributed Systems), aimed at fully utilizing the features and capabilities of SHARPE [1, 2] modeling engine. SDDS features a graphical user interface (GUI) with which system designers are permitted, through an *interface language*, to specify models interactively in terminologies they are familiar with. The *translator* in SDDS, which plays a prominent role in leading users toward effective utilization of SHARPE's features and capabilities, converts the high-level specifications into the most appropriate (internal) representations that can be automatically solved by the underlying modeling engine SHARPE. The translation and solution processes are transparent to the user.

Section 2 explains the relationships between SHARPE and SDDS. In Sections 3 and 4, we describe the interface language of SDDS and how the translator leads the user to make best use of SHARPE's features and capabilities, respectively. The concluding section summarizes what we have accomplished and discusses our future work.

2 The Modeling Engine and Workbench

SHARPE (Symbolic Hierarchical Automated Reliability and Performance Evaluator) developed by Sahner and Trivedi is a modeling engine for analyzing hybrid, hierarchical models for a class of performance, dependability and performability models [2]. It provides a textual specification language and solution methods for a variety of model types: series-parallel re-

liability block diagrams, fault trees, reliability graphs, Markov chains, semi-Markov chains, series-parallel directed acyclic graphs, product-form closed queueing networks, and generalized stochastic Petri nets. Furthermore, any hierarchical combination of above model types can be specified and solved.

However, from the perspective of users with little analytic background, a number of SHARPE's useful features may not look user-friendly. First, SHARPE accommodates a variety of model types which facilitate dependability evaluations of fault-tolerant systems in a complimentary manner. For example, while the fault-tree solver handles fault-tolerant systems with both shared and dedicated components among redundant subsystems via allowing explicit specification for a "repeated node", the block-diagram solver emphasizes simplicity and does not deal with such systems. Thus, a non-modeling-expert user who lacks the knowledge about proper model decomposition will have difficulties in selecting the most appropriate model type to represent a particular aspect of a system. Clearly, an improper model decomposition may introduce significant errors in solutions. Second, SHARPE expresses numerical results of dependability measures based on "mixture distribution" which allows various fault-tolerant systems to be characterized by *exponential polynomials* that easily lend themselves to computer manipulation. However, this may cause difficulties for non-modeling-expert users in interpreting evaluation results or intermediate results. For example, a user may have difficulties to understand why the mass at zero (usually corresponding to a system's initial unavailability) is positive when he solves a model hierarchically by passing numerical results from a lower layer to the top layer. Third, although the GSPN solver in SHARPE has the full power of stochastic Petri net, it provides only a small set of library functions, which prevents a non-modeling-expert user from conveniently specifying a model and dependability measures at a high level.

Aimed at making the powerful features of SHARPE accessible to system designers with little analytic background, we have developed a user-friendly dependability-evaluation workbench. In particular, accessibility enhancement is accomplished based upon two major components of SDDS, namely,

1. An interface language that permits the user to interactively specify models and access capabilities of SHARPE using terminologies they are familiar with.

2. A translator which converts a high-level model specification into the most appropriate *internal representation* that SHARPE can automatically solve and ensures the user to utilize the features and capabilities of the modeling engine in an effective way.

The interface language and translator are described in Sections 3 and 4, respectively.

3 The Interface Language

The interface language features the following ingredients which are implemented in *Tcl/Tk*[1] and can be accessed by the user through a GUI:

A set of graphical block-diagram primitives that facilitates hierarchical model specification.

A taxonomy that categorizes those typical fault-tolerant system architectures and guides the user to map a system component to an appropriate type.

A collection of specification templates each of which is customized to a particular architecture type in the taxonomy and directs the user to specify dependability attributes of a model component.

The set of graphical block-diagram primitives includes block, join node, edge and block-attribute specification, as shown in Figure 1. Note that there are three types of blocks, namely, *simple block*, *composite block* and *library block*. The choice for block type will become available when the user selects the icon "block." A simple block represents a simplex component or a subsystem with N-modular redundancy (NMR or k-out-of-n, meaning that k out of the n redundant components must fail for the system to go to a "down" state, which is further discussed in the last paragraph of this section). Whereas a composite block enables the user to conveniently specify a block diagram in a recursive manner and thus facilitates hierarchical model construction. The user is allowed to move up and down in a model hierarchy to inspect and/or modify the specification using icons. (Note that the block diagram shown in Figure 1 is at its top level so the "up" icon is not available.) A library block refers to a "built-in" representation for a fault-tolerant system architecture that is rather complex such as a duplex system accommodating recovery blocks (a system incorporating both hardware and software fault tolerance mechanisms). A library block can be integrated with other (user-specified) blocks to compose a complete block-diagram representation.

To help the user map a system component to an appropriate representation, a taxonomy that categorizes typical fault-tolerant architectures as shown in Figure 2 becomes available on the screen when the user starts to specify a block (through using the "spec" icon). Upon the user's selection, a dependability-attribute specification template that asks for parameter values and success/failure criterion *specific to the chosen type* will pop-up, guiding the user to correctly and completely characterize a model component. For example, if the user selects the type for the block "m1" as a non-repairable simplex subsystem (single memory module)

[1] Tcl/Tk is a software package for developing and using graphical user interface applications in X-Window System.

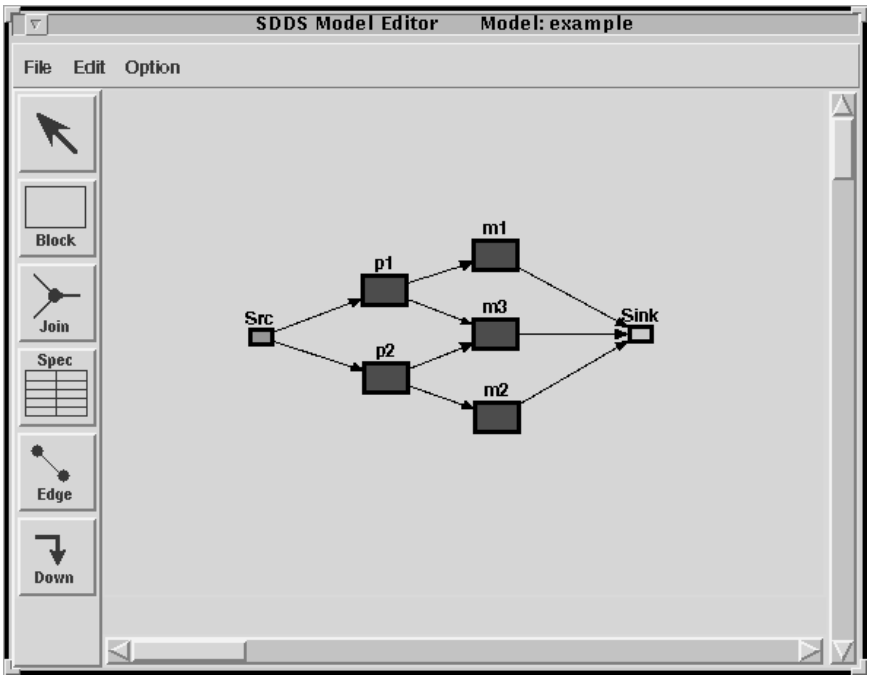
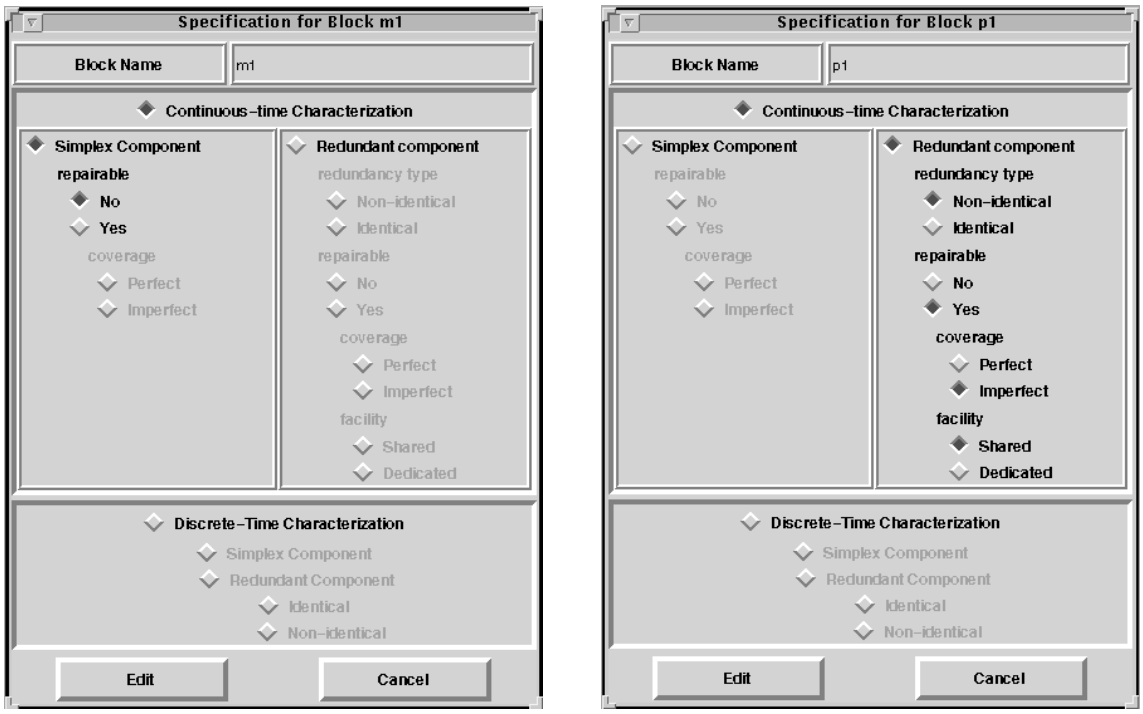


Figure 1: Block-Diagram Level User Input

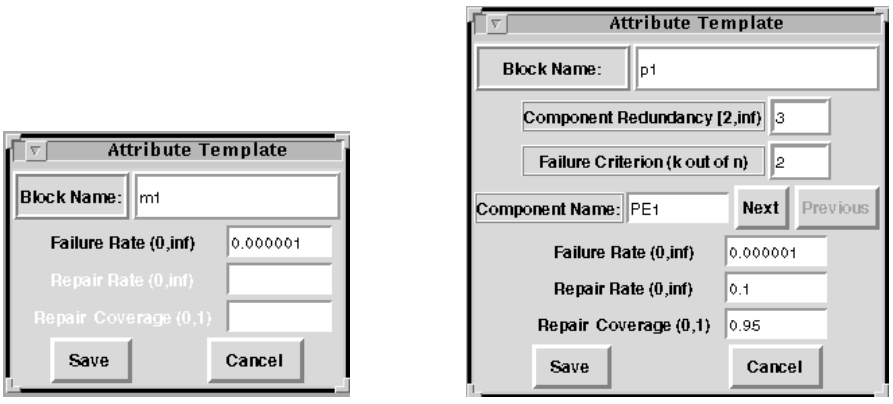
as shown in Figure 2(a), the corresponding template for parameter-value assignment will pop-up as shown in Figure 3(a) (where the parameter-value entries for repair rate and coverage are disabled). Whereas if the user selects the type for the block "p1" as a subsystem with non-identical redundant components (usually corresponding to different processing elements for functional/semantic redundancy) which are repairable with shared repair facility and imperfect repair coverages as shown in Figure 2(b), the corresponding template will ask for repair rate and coverage for each component as shown in Figure 3(b). Thus the combination of the taxonomy and the set of attribute templates facilitates *directed model specification*, avoiding potential errors by an unexperienced user.

It can also be noticed from the figures that, the taxonomy and attribute templates enable the user to access a number of useful capabilities of SHARPE. Among other things, an important feature we let the user to exploit is that SHARPE permits explicit specification for redundancy and failure criterion of a k-out-of-n system. Moreover, the taxonomy (see Figure 2) indicates that, although the non-state-space solvers in SHARPE (e.g., block-diagram and fault-tree solvers) restrict each of the redundant components in a repairable k-out-of-n system to have dedicated repair facility ("independent repair"), SDDS accommodates repairable k-out-of-n systems with shared repair facility for (identical or non-identical) redundant components. This is accomplished by converting the high-level user specification into a GSPN representation (described in the next section).



(a) (b)

Figure 2: Block-Type Taxonomy



(a) (b)

Figure 3: Dependability-Attribute Specification Template

4 The Translator

As mentioned previously, the translator plays a prominent role in ensuring that the user can access and utilize the features and capabilities of SHARPE in an effective way. In particular, the translator is intended to enable users to exploit SHARPE's hybrid/hierarchical modeling capabilities, which is described below.

Among other representation types, system designers are in general most familiar with block diagrams which are usually heavily used throughout a system's life cycle and thus are well suited at the user-input level in SDDS. However, as mentioned in Section 2, the block-diagram solver of SHARPE does not accommodate a system with both shared and dedicated components among redundant subsystems such as the one shown in Figure 1 in which the upper and lower processing elements "p1" and "p2" have dedicated memory modules "m1" and "m2", respectively, while they share the third memory module "m3." On the other hand, the powerful fault-tree solver in SHARPE is able to handle "repeated nodes" (a node that appears in more than one branch in a fault tree), which can be utilized to represent a fault-tolerant system of such type. Therefore, we choose fault tree as the *top-layer internal representation*. Accordingly, by taking the advantage that the fault-tree solver permits explicit specification for repeated nodes, we developed a simple yet efficient recursive translation algorithm. The algorithm exhaustively enumerates all the paths from source to sink in a block diagram such that any block diagram can be translated into a 2-level fault tree [3]. Figure 4 illustrates the fault tree translated from the block-diagram input shown in Figure 1. Further, the fault tree at the top-layer of the model hierarchy may need to be elaborated depending upon the characteristics of each component or subsystem. The translator takes the responsibility to make the decision on which model type (supported by the underlying modeling engine) a node in the fault tree should be converted to. Figure 5 depicts the decision tree for the translator in which rules are driven by the goal of enabling the user to exploit SHARPE's capabilities. It is worth noting that, 1) aimed at better performance, the decision rules are intended to utilize as much as possible the powerful, non-state-space fault-tree solver and, 2) when Markov chain is considered as the candidate for the lower-layer representation, we choose to translate a block into a GSPN representation first instead of directly generating the Markov chain. This is because i) a GSPN representation is simpler and more concise than Markov chain (especially for systems with redundancy), which allows the translator to be less complex and, ii) the GSPN solver in SHARPE can be exploited to carry out the further conversion.

Note also that, while the non-state-space solvers in SHARPE such as fault tree and block diagram allow the user to specify redundant systems with dedicated repair facility for each

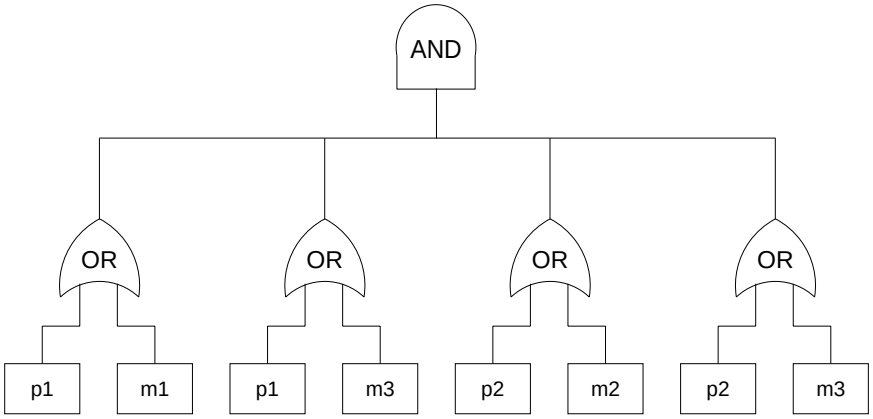


Figure 4: Equivalent Fault-Tree Representation

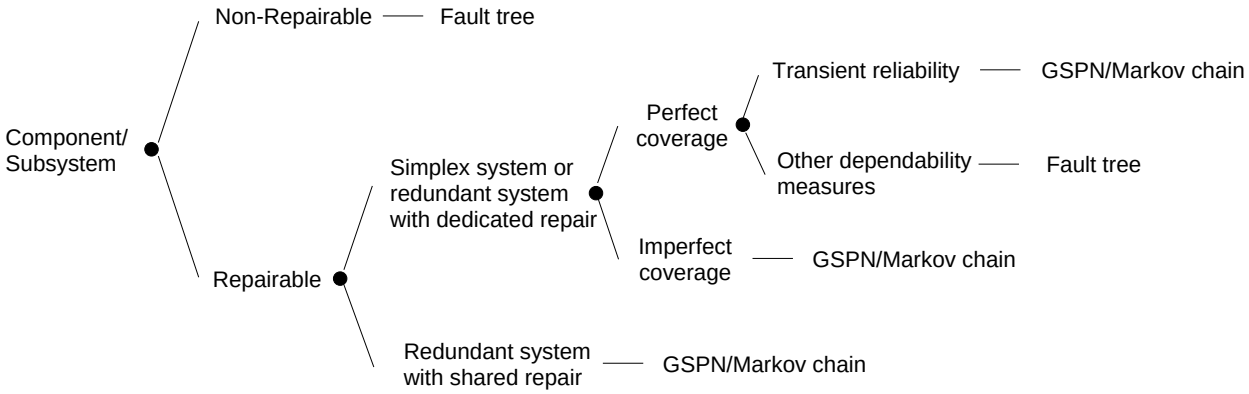


Figure 5: Decision Tree for the Translator

component, evaluation of such systems with shared repair (which is more typical than dedicated repair in real-life applications) in general requires the use of state-space solvers, which could be difficult for a non-modeling-expert user. On the other hand, with the taxonomy and translator's decision tree (see Figures 2 and 5), the user can easily evaluate such systems and needs not to worry about the underlying GSPN/Markov-chain specification and solution. By utilizing the small set of library functions of GSPN, SDDS exploits the full power of the solver to allow the evaluation of redundant systems with non-identical components that have shared, perfect or imperfect repair. Figure 6 depicts the internal GSPN representation generated by the translator for a redundant system consisting of two non-identical-components with shared repair and imperfect coverage. In this figure, a special case in which $k = n = 2$ (i.e., a duplex system) is used for the simplicity of illustration. It can be observed that inhabit arcs are utilized to maintain the order of those non-identical components in a repair queue. For the particular snapshot shown in the figure, the token in the place "q21" is forbidden to enter the place "q22" (corresponding to the front of the repair queue) until the place "q12" (also corresponding to the front of the queue) becomes empty (the first component finishes repair). Figure 7 shows the internal GSPN representation for a more general case (i.e., a triple-modular-redundancy (TMR) system with non-identical components and shared repair; any k-out-of-n system with $1 \leq k < n$ can be represented in a similar manner), where we can see how auxiliary places and immediate transitions are used in order to exploit the library functions available in the GSPN solver such as `prempty(tmr,totalUp)` and `premptyt(t;tmr,totalUp)` (probabilities of the place "totalUp" being empty at steady state and at time t, respectively) for dependability measures.

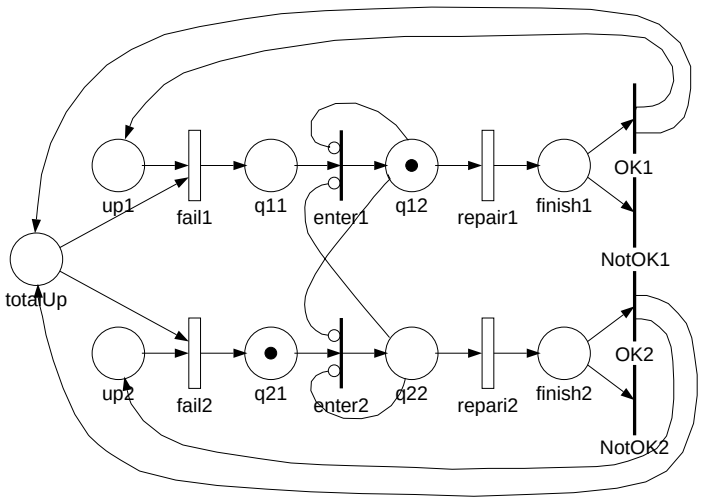


Figure 6: A Duplex System with Non-Identical Components and Shared Repair

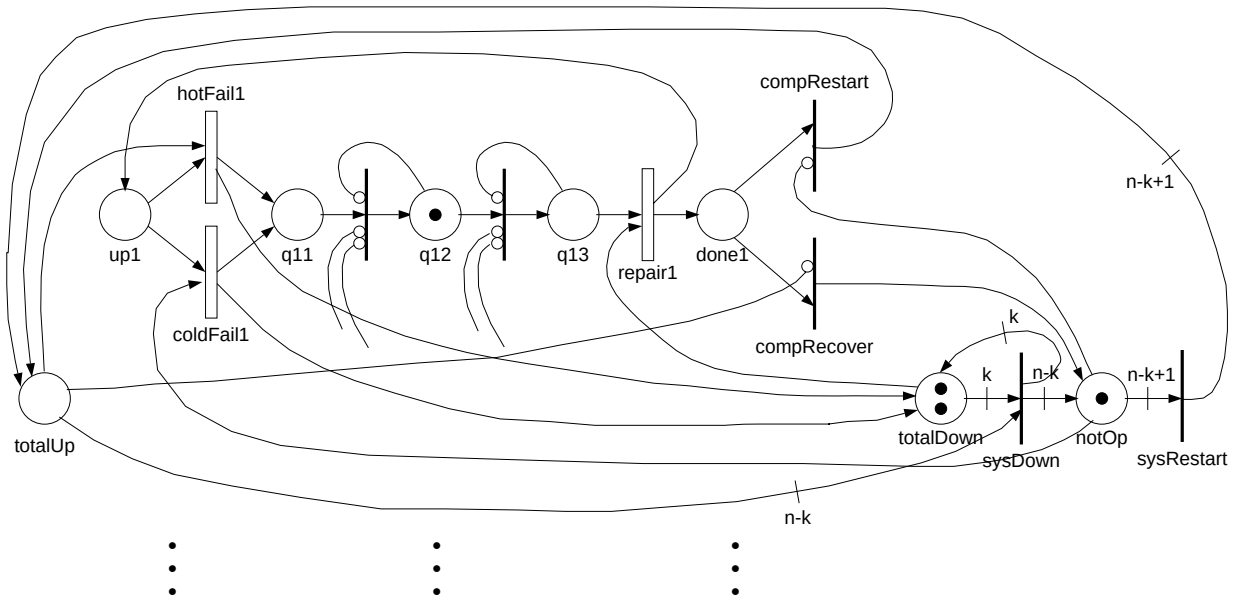


Figure 7: A TMR System with Non-Identical Components and Shared Repair

From the solution speed point of view, the translator is intended to optimize performance by taking advantage of SHARPE's flexible interface between layers in a model hierarchy. For example, although we can take a straight forward fault-tree approach for the transient measures of a system where each of the repairable components has its own repair facility and perfect repair coverage, the translator chooses to convert the block-diagram user specification for such a system into the SHARPE code with which the final solution is obtained by integrating the numerical results from each component system at the top-layer fault tree. Thus by avoiding a non-hierarchical approach that combines the exponential-polynomials (which characterize the components) before numerical evaluation, the solution speed is improved by several orders of magnitude.

As mentioned in Section 2, the output format of SHARPE for dependability measures based on a mixture distribution may not be easy for users with little analytic background to interpret. To circumvent this problem, the interface language and the input/output filters in the translator incorporate in a way so that SDDS is able to accept measure specification and display numerical results in more conventional terms (e.g., unavailability at time t, steady-state instantaneous unavailability, etc.).

5 Conclusion and Future Work

Aimed at enhancing accessibility for off-the-shelf modeling techniques and tools for system designers, we have developed a user-friendly dependability-evaluation workbench SDDS that

is intended to lead the user to effectively utilize the features and capabilities of SHARPE. In particular, we exploit SHARPE's hybrid/hierarchical modeling capabilities in two ways. First, we utilize these capabilities in the design of SDDS itself. That is, while allowing the user to specify a model at block-diagram level, SDDS translates user's input into an internal representation which can be solved by the powerful fault-tree solver and can be further elaborated using other model types depending upon the system characteristics specified by the user. Second, the user language and the translator enable the user to specify a block diagram in a hierarchical manner and utilize the most appropriate model types to elaborate the components in a high-level representation for solutions (the latter is realized in a way transparent to the user). SDDS permits the users with little analytic background to efficiently assess design alternatives by adding, deleting or moving blocks around, modifying success/failure criteria, and increasing/decreasing component redundancies.

Currently, we are enhancing the GUI-level error-checking facility (in addition to our error-avoidance strategies) for model specification, aimed at making dependability evaluation process more dependable. We also plan to extend the capabilities of the translator, based on iterative solution methods, to accommodate repair dependence across (all or a subset of) subsystems. To further enhance accessibility of dependability-modeling techniques and tools, we are motivated to integrate SDDS into one or more computer-aided design environments in the future.

References

[1] R. A. Sahner and K. S. Trivedi, "Reliability modeling using SHARPE," *IEEE Trans. Reliability*, vol. 36, pp. 186–193, Feb. 1987.

[2] R. A. Sahner, K. S. Trivedi, and A. Puliafito, *Performance and Reliability Analysis of Computer Systems An Example-Based Approach Using the SHARPE Software Package*. Boston, MA: Kluwer Academic Publishers, 1995.

[3] A. T. Tai, H. Hecht, K. S. Trivedi, and B. Zhang, "Making dependability evaluation more effective and efficient for engineers," in *Proceedings of the International Workshop on Computer-Aided Design, Test, and Evaluation for Dependability*, (Beijing, China), pp. 145–150, July 1996.