Dependable Systems

Chair

A.M. Tyrrell

Department of Electronics
University of York
Heslington, York, YO1 5DD, England
Tel. + 44 - 1904-432340
Fax: + 44 - 1904-432335
E-mail: amt@ohm.york.ac.uk

The engineering discipline of dependable system design is not a new one, but is probably more important now than ever before. The concept of embedded computer systems in practically every consumer device, medical equipment, transport systems, and communication system makes the design of highly reliable systems critical. There are a number of differing ideas on the concepts of high-reliability computer systems; a number of commonly-used terms in the field of reliable computer systems are:

- Dependability: the property of a computing system which allows reliance to be placed on the service it delivers;
- System failure: occurs when the delivered service deviates from service stated by the specification;
- An error is that part of the system state which is liable to lead to failure;
- A fault is an adjudged cause of an error;
- An error is thus the manifestation of a fault in the system and a failure is the effect of an error on the service.

In order to achieve a dependable computing system, a number of diverse techniques can be used at various stages of the system design. Probably the most successful method of achieving reliable systems is to use a combination of one or more of the following:

- Fault Avoidance: how to prevent, by construction, fault occurrence or introduction;
- Fault Tolerance: how to provide, by redundancy, a service complying with the specification in spite of faults;
- Fault Removal: how to minimize, by verification, the presence of faults;
- Fault Forecasting: how to estimate, by evaluation, the presence, the creation and the consequences of faults.

An important aspect of any system design is an evaluation of its performance, usually against some specification. In dependable computer systems, there are two main measures of dependability:
- Reliability: a measure of the continuous delivery of proper service — or equivalently, of the time-to-failure.
- Availability: a measure of the delivery of proper service with-respect-to the alternation of proper and improper service.

The relationship between the concept of dependability and the means of achieving it, the impairments stopping it and the measures of assessing are shown in Figure 1.

![Figure 1. Relationship between Dependability and its Impairments, Means and Measures](image)

The first paper in this session, by IS. Goseva-Popstojanova and A. Grnarov, deals with the problem of modeling the behavior of a fault-tolerant system employing N-version programming and its operational environment. The failure model used includes both functional failures that are where the output is incorrect, and timing failures. A Markov model is constructed for the N-version system, and a user-oriented model of the operational environment is developed. A random model for failure rate and execution rate is assumed. Results are shown for both functional and timing failures and their effect on the overall system failure probabilities.

The second paper in the session, by O. Benkahla, F. Chevassu, B. Remy, and C. Robach, presents a comparison of two test assignment strategies used in distributed system-level diagnosis. The authors consider distributed system-level diagnosis in a parallel computing environment to be a credible way of providing fault-tolerance to a design. In the paper, quantitative analysis is applied to static and dynamic testing assignment approaches. A process-based model is produced and the performance of the strategies is evaluated when compared to a number of system parameters, including topology, faulty processors, and faulty links. Results of these tests are shown.
In the final paper in the session, by T. Bartha, diagnosis is again considered as a means of providing dependability to a system design. An algorithm is presented that provides efficient approximate diagnosis of massively parallel multiprocessor systems. The algorithm is based on the implication graph representation of the generalized test invalidation model. Results are shown in the paper, illustrating the characteristics of the algorithm.