Computer Code Abstract

SAFE

J. M. Kontoleon

University of Wollongong, Department of Electrical Engineering
Wollongong, New South Wales, Australia, 2500

Received April 24, 1980
Accepted May 31, 1980

1. Program Name and Title: SAFE, a fail-to-safe and fail-to-danger analysis program for nuclear reactor protective systems.

2. Problem Solved: The SAFE program[1] is designed to analyze the fail-to-safe (FS) and fail-to-danger (FD) probabilities of failure to large protective networks, such as those associated with nuclear reactor protective systems.[2] The protective network may include as components (a) sensors, (b) safety lines, and (c) logic units, which have either an *m*-out-of-*n* or a majority voting configuration. Sensors and safety lines may fail in either an FS or FD mode of failure. The overall logic protective network is modeled as a network with three types of nodes and arcs; the nodes specify the components involved in the logic network and the arcs their interconnections. The three types of nodes, namely "input," "buffer," and "logic" nodes are numbered successively, and in that order, to allow a simple description of the logic protective network into the computer. The simulation of unreliable logic units is done by the use of reliable logic nodes and unreliable buffer nodes. It is generally assumed that the three types of nodes are *s*-independent and that they can be in one of the following three states: good, FS, and FD. The program can also be used in the evaluation of the probability of occurrence of the top event in a fault tree, provided that the bottom events are *s*-independent and not mutually exclusive.

3. Method of Solution: The determination of the FS and FD probabilities of failure at the outputs of the various nodes in the network is done iteratively by scanning a Boolean logic-flow matrix A, which describes the interconnections between the various nodes of the network. At each step, one column of A is scanned (this corresponds to the output of a node in the network) to determine whether or not the probabilities of its input events are known (at that point of the solution process). If the probabilities at the input of a buffer node are known, the FS and FD probabilities at its output are determined by treating the buffer node as a two-component system with a two-out-of-two configuration (series system); one component has the known FS and FD probabilities at the input of the buffer node, and the other has the specified pair of FS and FD probabilities for the buffer node. In the case of logic nodes (*m*-out-of-*n* or majority voting) the solution process involves the Boolean method described in Ref. 3; the FS and FD probabilities at the output of a logic node are determined as a special case of the dynamic redundant system analysis (zero frequency of scanning). To deal with the non-identical FS and FD probabilities at the inputs of the logic nodes, the program incorporates the modified algorithms reported in Ref. 4. The scanning of the logic-flow matrix A is systematic, in the sense that the "pattern of scanning" followed in SAFE aims at reducing the required number of iterations. At the end of the above process, the FS and FD probabilities at the output of the logic protective network become known.

4. Related Programs: SAFE incorporates a library subroutine for determining the required processing time.

5. Restrictions on the Complexity of the Problem: The maximum number of logic nodes is limited to 50, the maximum number of buffer nodes is limited to 100 and the maximum number of input nodes is limited to 100. No other restrictions are imposed on the size and complexity of the problem.

6. Computer: Univac 1106.

7. Typical Running Time: Varies widely depending on problem complexity. On the Univac 1106, SAFE analyzes a logic system network with 17 logic nodes, 30 input nodes, and 30 buffer nodes in <3 s.

8. Programming Language: FORTRAN IV.

9. Operating System: Univac Exec 8, Level 36.

10. Machine Requirements: At least 40K of core memory is required.

11. Availability: A software package containing elements required for use of SAFE together with copies of Ref. 1 is on file at the National Energy Software Center, Argonne National Laboratory, 9700 South Cass Ave., Argonne, Illinois 60439. The author of this Abstract will, of course, respond to inquiries and requests.

12. *References:*

[1] J. M. KONTOLEON, "SAFE—A Computer Program for the Analysis of Logic Protective Networks," University of Wollongong (1980).

[2] A. E. GREEN and A. J. BOURNE, *Reliability Technology*, John Wiley & Sons Ltd., London (1972).

[3] J. M. KONTOLEON, *IEEE Trans. Reliab.*, **27**, 2 (1978).

[4] J. M. KONTOLEON, *IEEE Trans. Reliab.*, **29**, 1 (1980).