2

CONF-840914--14

UCRL-91462
PREPRINT

LOGIC FLOWGRAPH MODEL FOR DISTURBANCE ANALYSIS OF A PWR PRESSURIZER SYSTEM

S. GUARRO
D. OKRENT

THIS PAPER WAS PREPARED FOR SUBMITTAL TO
INTERNATIONAL MEETING ON
THERMAL NUCLEAR REACTOR SAFETY

KARLSRUHE, GERMANY

SEPTEMBER 10-13, 1984

Lawrence
Livermore
National
Laboratory

LOGIC FLOWGRAPH MODEL FOR DISTURBANCE ANALYSIS OF A PWR PRESSURIZER SYSTEM*

by

S. Guarro[+] and D. Okrent[++]

+Lawrence Livermore National Laboratory
P.O. Box 808, L-140
Livermore, CA 94550

++School of Engineering and Applied Science
University of California Los Angeles
Los Angeles, CA 90024

UCRL--91402

DE84 017023

ABSTRACT

The Logic Flowgraph Methodology (LFM) has been developed as a synthetic simulation language for process reliability or disturbance analysis applications. A Disturbance Analysis System (DAS) using the LFM models can store the necessary information concerning a given process in an efficient way, and automatically construct in real time the diagnostic tree(s) showing the root cause(s) of occurring disturbances.

A comprehensive LFM model for a PWR pressurizer system is presented and discussed, and the latest version of the LFM tree synthesis routine, optimized to achieve reduction of computer memory usage, is used to show the LFM diagnoses of selected hypothetic disturbances.

INTRODUCTION

In order to implement diagnostic capabilities, a Disturbance Analysis System (DAS) must utilize process models that are at the same time compact and rich in information content.

The models used in the first prototype DASs were developed in the form of cause-consequence diagrams or cause-consequence trees. Both techniques use the same type of binary representation and logic gates employed by fault trees, and are similar to the latter in terms of modeling capabilities. The quite large dimensions of the models resulting from the early attempts to apply these types of representation to whole scale plant systems was indicated by many analysts as a severe hindrance in the development of DASs with extensive diagnostic capabilities.

LFM OVERVIEW

LFM is a new methodology intended to provide a more efficient way of constructing process models for use in diagnosis oriented disturbance analysis systems. At the foundation of this method is the derivation of graph models for the processes to be analyzed. As in the "digraph method"[1] the LFM models include the fundamental units of nodes and edges, which are used to represent respectively process variables and

*This work was supported by the U.S. NRC under a Memorandum of Understanding with the U.S. Department of Energy.

causality network, which expresses the fundamental physical relations of direct cause and effect existing in a process, and the condition network, which represents in a formally defined and organized way the conditions whose occurrence may change or modify the course of causality flow in the causality network.

A detailed description of the LFM representation rules can be found in References 2 and 3, while a more synthetic account is given in Reference 4. We use here the simple scheme of Fig. 1 to show an example of some essential LFM features. In this figure the U and V nodes represent continuous variables. These are process variables or parameters that can vary over a continuous range, reduced in LFM to 5 discretized states (0 = normal, + 1 = moderate deviations in positive or negative direction, ± 10 = large deviations). The C node on the other hand represents a truly binary process variable or parameter. U and V are shown to be linked by a causality connection expressed by a causality edge and by a multiple gain box (MGB). The +1 gain value in the MGB signifies that the connection is normally one of direct proportionality from U to V. However, the graph also shows through the diamond shaped text box (TB) that the binary variable C may have a conditioning influence on the relation between U and V. More specifically, when the condition expressed by the equality $C = \bar{1}$ is verified, U has no longer any influence on the value(s) to be taken by V. This type of formal representation is very effective in showing how binary variables, usually associated with primary level faults or with the action of engineered protection devices, can affect the causality relations that link process continuous variables and parameters to one another. LFM is also advantageous in that it condenses in one model the representation of both process success and failure logics, including the effect of feedback and feedforward actions.

After being derived and stored in their condensed-information format, the LFM models can be routinely analyzed by computer to produce fault tree structures for reliability analysis purposes. By additional utilization of the instrument signals coming from the actual process modeled, the same computer routine can be employed in a DAS to produce diagnostic trees for the identification of the root cause(s) of an existing disturbance. This procedure is well suited for DAS implementation since it does not require any analyst's or operator's mediation and can thus be performed on-line. Tests performed on LFM utilization in disturbance analysis showed that a diagnosis can be obtained by the DAS computer one second or less from the start of a disturbance.

PRESSURIZER MODEL

The pressurizer, together with the control and protection devices attached to it, constitutes an essential system in a PWR plant. The complexity of the functions it must perform, in keeping the primary system pressure within the working range and in allowing for the volumetric expansion and contraction of the primary coolant mass, makes the development of a reasonably complete LFM pressurizer model a quite challenging task, one that can seriously test the method capabilities. We review briefly the controls and protections that are typically employed in such a system.

The following devices can intervene in regulating the pressure for control and/or safety purposes: a) safety valves (safety), b) power operated relief valves (PORVs)(control/safety), c) proportional sprays (control), d) proportional heaters (control), e) backup heaters (control).

Pressurizer level, on the other hand, is regulated by properly adjusting the charging flowrate from the chemical and volume control system (CVCS). This can be done by controlling the speed of a positive displacement pump or by throttling a valve on the discharge line of a centrifugal pump (when this alternative charging mode is being used.

In the derivation of the LFM model, the modeled range of pressure and level is the one between the high and low pressure trip set-points and above the low level trip set-point, which deliberately limits the modeling effort to transients before the occurrence of reactor shutdown.

Within the selected pressure range, it was necessary to arrive at a definition of the discrete penta-valued set needed in LFM for representation of the pressurizer pressure (PP) "continuous variable." Figure 2 illustrates the choice that was made in regard to this. In the selected scheme, the PORV setpoint determines the boundary between the +1 and +10 values, whereas the midpoint between the backup heater energizing and de-energizing set-points is used as a boundary between the -1 and -10 values. The separations between the 0 and +1 values, and between the -1 and 0 values, correspond to the start-point of the spray flow demand program ramp, and to the midpoint of the proportional heater demand program ramp respectively. Different choices are possible. The set-up just illustrated, however, provide a sufficiently balanced representation of the "normal" and "upset" conditions within the modeled range.

Figure 3 shows two portions of the pressurizer model that was ultimately developed. Section a represents some of the principal thermal-hydraulic interactions with the paths of the protective and control actions affecting the pressurizer pressure and pressurizer level parameters. Section d shows the details of the level control system. The remaining portions of the model can be found in Reference 3 together with the necessary aids for its detailed interpretation. It is important to notice that, due to the considerable complexity of the physical reality to be represented, it is necessary to break down physical interactions into fundamental composing parts. For instance, the driving mechanisms for variation in the system pressure PP are assumed to be either produced by a direct outflow of steam (SOF) or by volumetric effects (VPE) that cause steam compression or expansion and which are induced by variations in the water level. In addition, pressure changes may be induced by changes in the balance exchange flow (BEF) between the water and steam phases in the pressurizer. BEF normally acts as a corrective agent on either of the other two variables just mentioned above, but is also capable of directly inducing variations in PP. The BEF variable is driven by the combined action of the proportional sprays (variable PSF), the proportional heaters (variable PHA) and backup heaters (variable BHA), and is also influenced by other factors such as the pressurizer pressure itself and the degree of pressurizer water subcooling (variable PWS). To describe the complete interactions between these variables the "special input box" (SIB) operators S1 and S2 are used together with the other LFM standard operators. These are equivalent to multi-state decision tables representing the correspondence between BEF and its input variables PHA, PSF, and BHA. The assumptions for modeling this correspondence derive from knowledge of the relative capacities of the heaters and sprays.

DIAGNOSTIC AND RECOVERY TREES

References 2 and 3 illustrate how the computer program TRIC (Tree Instantaneous Constructor) implements the LFM modeling "grammar" and a complete set of "tracing rules" to allow derivation of logic trees from the flowgraph models. To derive a fault or success tree, TRIC only needs as input a definition of the tree top event in the form (variable) = (value) (for example: V = + 10). If the program is run on-line on a process computer (as would be the case in a DAS application) process instrumentation readings will also be used as inputs, to only allow derivation of tree branches corresponding to the actual events (among all those that could in theory produce the top event). When this latter procedure is used to determine the causes of a process upset, the tree produced by the LFM automated analysis is called a "diagnostic tree."

Diagnostic trees for two different disturbances are presented here. The first hypothesized disturbance is one that affects the PLCS (pressurizer level control system). While the PLCS is in the centrifugal pump regulating valve mode (control option CO = $\bar{0}$), it is assumed that a drift in the level controller setpoint causes a transient to be initiated, resulting in a moderate lowering of the pressurizer level (PLD = -1). When the disturbance is well under way, different observable variables are affected and assume perturbed values. Figure 4 shows the diagnostic tree developed by TRIC when taking the event PLD = -1 as the top-event and the "observed" values of the other variables just mentioned as "boundary conditions" for the given disturbance. These observable conditions are marked by a dot in Fig. 3 for identification by the reader. It should, however, be understood that other observable conditions, utilized to exclude non-active tree branches from the diagnostic derivation, do not appear in the diagnostic tree itself.

The second hypothetical disturbance with which the pressurizer model was tested is a transient in which a stuck-open power-operated relief valve (RVUO = $\bar{1}$) causes the pressurizer pressure to fall low (in the LFM -10 range). Secondary effects of this are the actuation of the proportional and backup heaters and the disactivation of the sprays, in an attempt by the PPCS (pressurizer pressure control system) to contrast the course of the transient and arrest the observed decrease in the system pressure. The top event PP = -10 was analyzed by TRIC with the use of the appropriate boundary conditions given by the observable events resulting from the occurrence, and the resulting diagnostic tree is shown in Figure 5.

It is worthwhile to notice that the significant part of the tree, in terms of disturbance diagnosis, is the one on the right side under the SOF = +10 event, and shows the disturbance root cause RVUO = $\bar{1}$. The left side (event BEF = +1, etc.) only describes conditions that result from, or accompany, the disturbance, and which are to be shown for a better comprehension of the actual occurrence.

It was mentioned before that LFM permits the derivation of both fault and success trees from the same flowgraph. The ability to derive success trees can be advantageously used in disturbance analysis to identify recovery actions after a disturbance has been identified and diagnosed. For example, to obtain from TRIC a "recovery tree" for the disturbance just discussed above, one may set the top variable PP equal to 0 (which is the "default", unperturbed LFM value for any continuous variable), and adjust accordingly the values of the other observable values on which PP may have direct or indirect influence. Thus the values of the variables BHA and PHA have to be modified into 0's for consistency with the new value assumed for PP. All the other observable variable values produced by the disturbance are, however, kept as boundary conditions. The LFM routine can then identify possible actions that may suppress the undesired effects of the disturbance root cause(s). The tree obtained in this fashion is partially shown in Figure 6. The actual tree derived by TRIC includes development of events like VPE = 0 and BEF = 0, which are only of secondary interest and therefore not shown here. The desired recovery action can be seen at the low left end of the tree, indicated by the event BVS = $\bar{1}$ (which means: PORV block valve secured), 'ANDED' with the primary branch containing the fault event RVUO = $\bar{1}$.

The example given above demonstrates the feasibility "in principle" of the use of LFM-derived success trees to identify needed recovery action. Different strategies can be envisioned to make this process as efficient as possible, so that for instance the LFM routine could automatically avoid the development of "useless" branches such as the ones omitted from the tree in Figure 6, and could also expressly emphasize the identified "recovery action" in some way appropriate for ready interpretation by the operator.

As a factor relevant to the actual on-line applicability of LFM in disturbance analysis, it is noted that, throughout the testing done with the pressurizer model, the developed fault or success trees were produced by the TRIC code in times of the order of 1 sec on an IBM 370/3033 computer.

CONCLUSIONS

This paper has discussed the application of a new approach called the Logic Flowgraph Methodology to a fairly complex system, for the purpose of automatically producing fault or success trees. The computer routine based on LFM is presently operational and capable of performing this task, be it for reliability or disturbance analysis applications. The routine itself requires about 160K of computer memory on an IBM 370/3033. The most recent version has been partially optimized to reduce array storage. As a result, the pressurizer model discussed here requires only an additional 160K. The previous code version required the same amount of array memory for a system model, presented in Reference 4, which had less than 1/3 the number of LFM modeling elements.

Since in the area of reliability and risk analysis many proven and consolidated methods exist and are routinely used, the major emphasis of research for LFM implementation was placed in the disturbance analysis - automatic diagnosis and recovery identification area. We think that the results presented and discussed in the previous sections are promising, and confirm the potential of the method for disturbance analysis applications. Of course, before real implementation, it would be necessary to further test the methodology and the models with real on-line, rather than simulated, disturbances.

Open to definition remain the possible different strategies by which a user may want to utilize the methodology within the scope of an integrated disturbance analysis system. The choice of such strategies is expected to be influenced by contingent practical considerations regarding a specific application area, rather than by aprioristic theoretical arguments.

It is finally noted that for a user, LFM involves in a sense the learning of a new "language." In practical application to complex systems, it will also require intimate knowledge of these systems. Consequently, the skills of trained practitioners will be needed for successful utilization.

REFERENCES

1. S. A. Lapp, G. J. Powers: "Computer Aided Synthesis of Fault-Trees", IEEE Trans. on Reliability, April 1977.

2. S. Guarro, D. Okrent: "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", Ph.D Dissertation, UCLA, June 1983.

3. S. Guarro, D. Okrent: "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", UCLA - ENG report, to be published.

4. S. Guarro, D. Okrent: "Logic Flowgraph Methodology for use in Disturbance, Reliability and Risk Analysis", Proc. of 7th Intl. Conf. on Structural Mechanics in Reactor Technology, Chicago, IL, August 1983.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

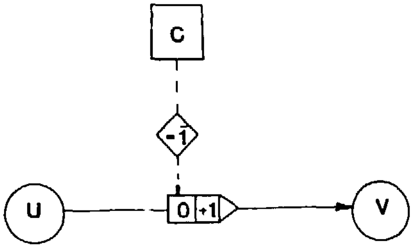


Fig. 1 Example of LFM Representation

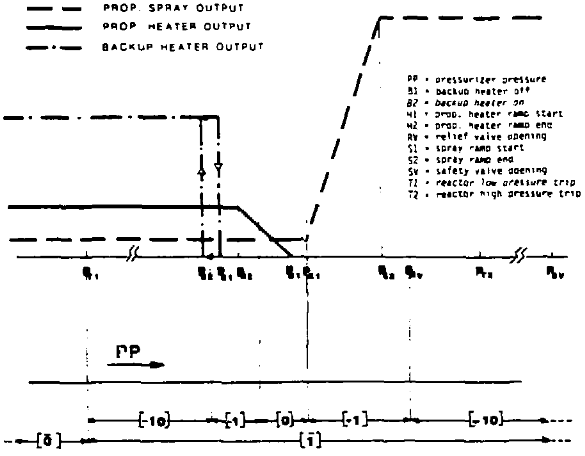
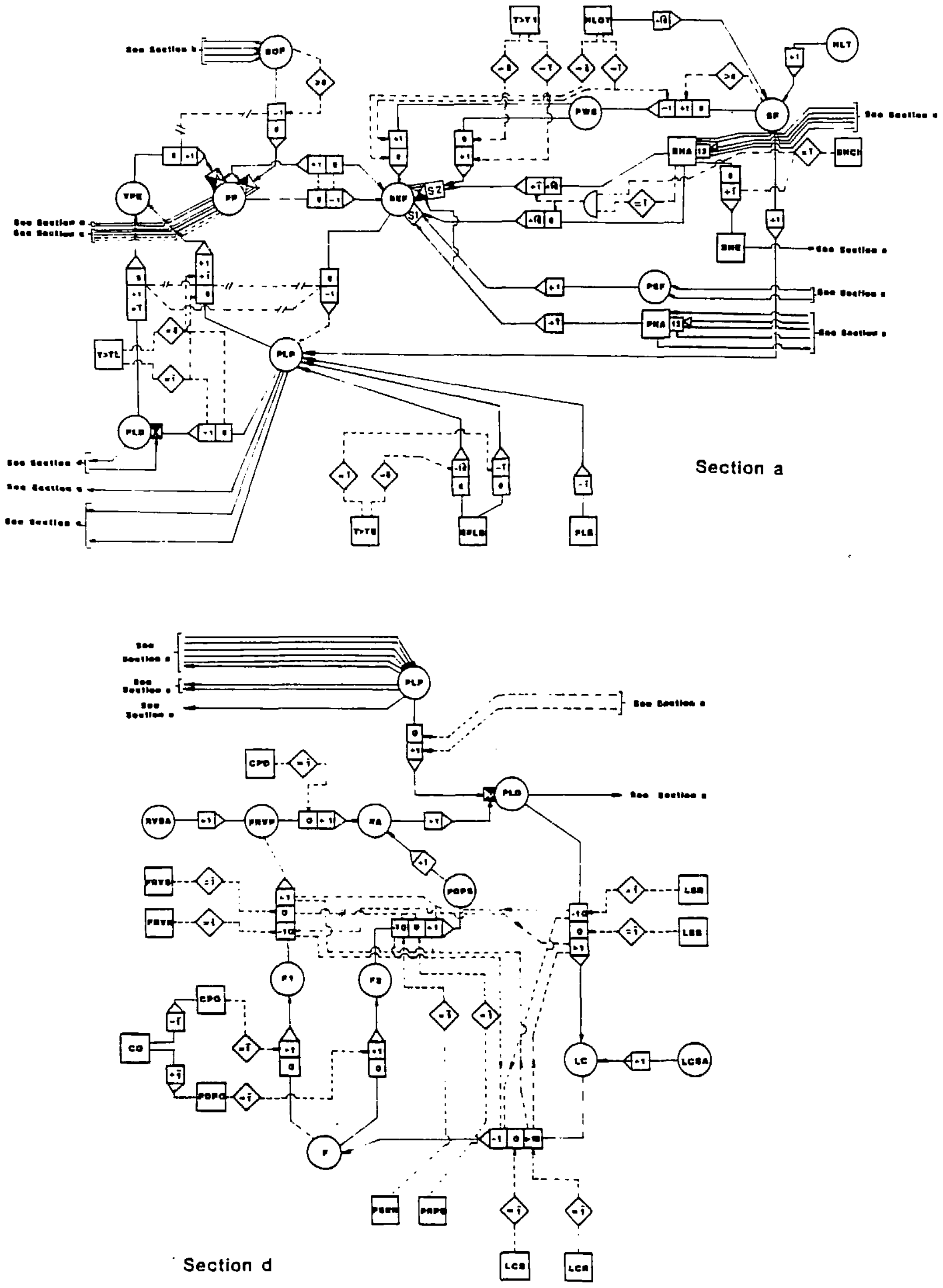


Fig. 2 Discretization of Pressurizer Pressure (PP) Range



Section a

Section d

Fig. 3 LFM Pressurizer Model

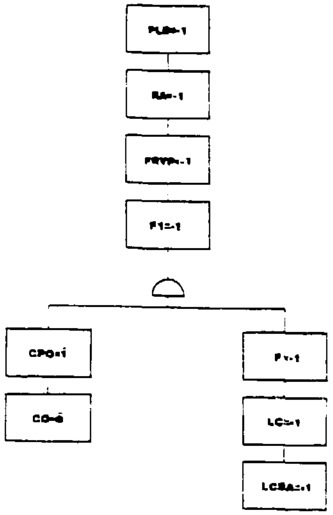


Fig. 4

Pressurizer Level Diagnostic Tree

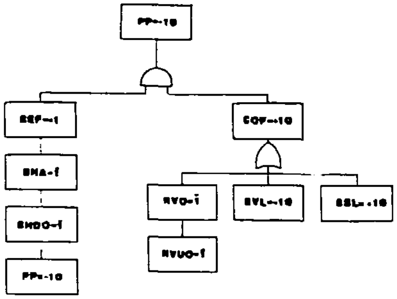


Fig. 5

Pressurizer Pressure Diagnostic Tree

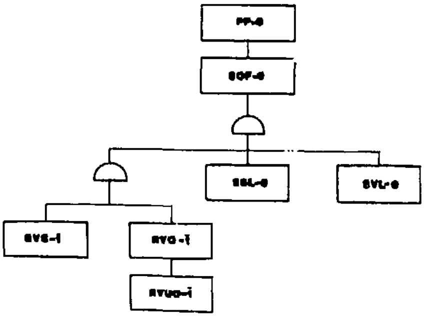


Fig. 6

Pressurizer Pressure Recovery Tree