CONF-841105--17

CONF-841105--17

DE84 014685

A Methodology for Validation of Safety Parameters and Fault Identification*

Constantine P. Tzanos

Reactor Analysis and Safety Division
Argonne National Laboratory
Argonne, Illinois 60439

*Work performed under the auspices of the U.S. Department of Energy.

A Methodology for Validation of Safety Parameters and Fault Identification

The reliability of plant control and protection is strongly dependent on the reliability of the plant instrumentation system. The experience from the operation of nuclear power plants has shown that erroneous and contradictory instrument signals confuse the operator and delay corrective action. The same experience has also shown that about 10% of the total unplanned shutdowns are due to instrument failures[1]. Plant safety as well as plant availability can be enhanced by improving the reliability of instrument information.

A methodology has been developed that provides validation of safety-significant plant parameter measurements, plant state verification, and fault identification in the presence of many instrumentation failures (including multiple common-cause failures). This paper presents the basic features of this methodology and some results of its application to a reference LMFBR plant.

All the plant parameters can be grouped into a number of sets, such that each of these sets contains a minimum number of parameters that are sufficient to define the system state. Such a set is called "minimum system state definition set." From any minimum system state definition set of measured parameters analytic measurements can be generated for all the remaining measured parameters utilizing the analytic models that describe the system. If it is known that all the measurements contained in the minimum system state definition set are correct, the analytic measurements of the remaining parameters generated by this set can be compared with their direct measurements. If there are direct measurements that are not consistent with their analytic measurements, the sensors that generated these measurements must have failed. Thus, the comparison of analytic and direct measurements provides data validation as well as fault identification. However, it cannot be assured that all direct measurements contained in a minimum system state definition set are correct if at least one of the analytic measurements, generated by this set, is not consistent with its direct (sensor) measurement. Therefore, to validate all the system parameters, at least one consistent "minimum system validation set" must exist, i.e., a set that consists of one minimum system state definition set plus one more parameter whose value can be analytically generated from the minimum system state definition set.

Although for validation of all system parameters the existence of a consistent minimum system validation set is a necessary condition, this condition is not always sufficient. If all the sensors of a minimum data validation set are stuck at consistent indications, or some of them have failed such that still consistent indications are obtained, these failures cannot be identified and any conclusions of validation will be erroneous. However, since the probability for the occurrence of such an event in a large number of sensors measuring different plant parameters at different parts of the plant is extremely small, this condition is considered also sufficient. The assumption that this condition is necessary as well as sufficient, is the basis of the methodology discussed in this paper. However, if it is desired, additional checks can be imposed to strengthen the sufficiency of this condition.

Based on the above discussion, the problem of data validation and fault identification is reduced to a search for a consistent minimum system validation set. The algorithm of this search is divided in two levels: (a) the local level, and (b) the plant-wide level. At the local level, validation of the primary, intermediate, and feedwater flows is first sought by using local instrumentation information and the methodology of analytic redundancy discussed in Refs. 2 and 3. More specifically, a given flow is validated if at least two measurements are consistent. Analytic flow measurements are generated by using the pump similarity, the pump power usage, and pressure drop correlations [3]. If validation of one or more of the flow parameters fails at this level, its validation is sought at the plant-wide level.

In this paper, only the steady-state part of the plant-wide level will be discussed. At this level, the search for a minimum system validation set starts by generating analytic power measurements utilizing the primary, intermediate, and water loop parameters. These analytic measurements and the direct power measurements (from neutron flux measurements) are compared for consistency. If all of them are consistent, all the measurements used for their generation are valid, and the search proceeds to the next validation time interval. If all of them are not consistent, there are three possible cases: three are consistent, two are consistent, all are inconsistent. The search proceeds by examining only the possible minimum validation sets that arise from one of these three cases. Failure to find a minimum validation set means that either there are more failed sensor sets than required to validate

the system state or the system is under a transient. Then, the search proceeds with analyses using transient system models.

To keep the computation time within the requirements of an on-line data validation system (validation interval of the order of one second) fast running models have been developed for the core, the intermediate heat exchanger (IHX), and the steam generator.

This methodology was applied to a reference LMFBR plant to determine the maximum number of failed sensor sets (each set measures the same parameter) that could be tolerated in validating the following plant-wide parameters: reactor power (Q), reactor inlet and outlet coolant temperatures (T_{IC} and T_{OC}, respectively), intermediate heat exchanger (IHX) inlet and outlet secondary coolant temperatures (T_{IS}, T_{OS}), steam generator feedwater temperature (T_W), steam temperature (T_S) and pressure (P_S), as well as primary, intermediate, and feedwater flows (G_p, G_I, G_W). In addition to these parameters, the assumption was made that the following parameters were also measured: pump speed, pump electrical power input, feedwater control valve stem position, pressure drop across the feedwater valve, pump discharge and suction pressure, pressure at two additional locations in each heat transport loop (primary, intermediate, water), and steam flow. The results of this application show that validation of the flow parameters at the local level would fail if more than eight sensor sets had failed. If flow validation at the local level had failed, validation of the plant state would fail if more than four sensor sets from those measuring plant-wide parameters had failed. However, even in this case, depending on the failed sets of sensors, some plant parameters and the state of part of the plant can be validated.

In summary, a methodology has been developed for on-line validation of safety-significant plant measurements, plant state verification, and fault identification. The implementation of this methodology can significantly improve plant safety and availability. For example, as discussed in Ref. 4, the application of this methodology can improve the unavailability of the reactor scram initiation function by one to two orders of magnitude.

References

1. S. L. Basin, et al., "Characteristics of Instrumentation and Control System Failures in Light Water Reactors," EPRI NP-443, Electric Power Research Institute (August 1977).

2. C. H. Meijer, et al., "On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytic Redundancy," EPRI NP-2110, Electric Power Research Institute (November 1981).

3. O. L. Deutsch, et al., personal communication.

4. C. P. Tzanos, "Reactor Shutdown System Unavailability Improvement by Using a System of Continuous Data Validation," Trans. Am. Nucl. Soc. 46 (June 1984).