This summary is of technical quality
and accuracy that reflects credit on
the RAS Division

Reactor Shutdown System Unavailability Improvement by Using a System of Continuous Data Validation*

Constantine P. Tzanos

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

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.

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

Reactor Shutdown System Unavailability Improvement by Using a System of Continuous Data Validation

Dominant accident sequences in LMFBRs are characterized either by failure of reactor scram or failure to remove the decay heat. The frequency of failure-to-scram accident sequences is proportional to the unavailability of the reactor shutdown system (RSS).

The RSS can be divided into an electrical subsystem and a mechanical subsystem. The electrical subsystem includes all the components from the sensors through the scram breakers. Its function is to cut off the power supply to the control rod drives. For LWRs it is believed that the mechanical subsystem is much less likely to fail than its electrical subsystem. Also, all the events, excluding the Browns Ferry partial failure to scram, that have occurred in operating LWRs and had the potential to cause a scram failure involved failures of the electrical subsystem. The Browns Ferry event involved failure of the scram discharge volume which does not have a counterpart in the LMFBR RSS.

The objective of this work is to show that the unavailability of the scram initiation function of the RSS can be significantly reduced by using a system of continuous data validation and manual scram as a redundant and diverse means of cutting off the power supply to the control rod drives. A continuous data validation system that can be used for that purpose is currently under development at Argonne National Laboratory and is envisioned to operate as follows. Direct sensor measurements of safety-important parameters are fed to the system every few seconds. These direct measurements and "analytic" measurements generated in real-time from an analytic plant model are compared for consistency. Through this comparison, instrumentation and other plant component failures can be identified, and validated values of safety-important parameters can be generated even in the presence of a significant number of instrumentation common-cause failures.

Such a data validation system can be used to generate promptly a scram signal whenever the plant safety parameters exceed their limiting values, or whenever the plant state cannot be determined (validation failure) due to a large number of instrumentation failures. Thus, the data validation system can be used as a means of scram signal generation that is redundant and diverse to the part of the conventional RSS electrical subsystem that extends from the sensors through the scram logics. Consequently, the contribution of this part of the electrical subsystem to its unavailability can be significantly reduced. However, the contribution of common-cause failures in components following the scram logics would not be affected. This contribution is significant. For example, the Salem event was due to common-cause failure of the scram breakers.

In LMFBRs, and especially pool LMFBRs, for anticipated transients other than loss of offsite power and positive reactivity insertion, if failure to generate an automatic scram signal does not generate a pump trip, there is significant time available for manual scram if the operator receives early enough a validated scram signal. For example, in the event of loss of main feedwater and failure to scram, if primary flow is available, the sodium saturation temperature is reached in ~30 min. in a pool LMFBR and in ~10 min. in a loop LMFBR. In the absence of validated data, due to the significant economic implications of a spurious scram, the operator faces the dilemma of a spurious scram or an accident due to scram failure. Emergency operating instructions of commercial LWRs stress avoidance of manual actions before failure of automatic actions has been verified. The operator is instructed to verify prevailing conditions by using multiple indications (i.e., alarms, charts, indicating lights, gauges, and other instrumentation). From this discussion it is clear that the reliability of manual scram can greatly be enhanced if a scram signal is generated for the operator by a reliable data validation system. This system and the operator can be used as a means of reactor scram initiation that is independent of common-cause failures in the entire electrical subsystem of the RSS (from the sensors through the scram brakers).

To estimate how much the unavailability of the RSS scram initiation function can be reduced if a data validation system is used, the following analysis was performed.

For operating PWR plants, frequencies of 0.16 and 0.02 per reactor-year have been estimated for loss of offsite power and uncontrolled rod withdrawal, respectively [1]. For commercial LWRs, the NRC staff has estimated a frequency of seven ATWS significant transients per year [2]. In EBR-II [3], the average frequency of scram for the last six years was 6.5 events/year. Loss of offsite power and uncontrolled rod withdrawal contribute only ~2.6% to a frequency of seven ATWS significant events per reactor-year. Thus, for more than 97% of the events there is adequate time for manual scram if a validated scram signal is available to the operator. Moreover, if loss of offsite power causes inherently loss of power to the control rod drives, only uncontrolled rod withdrawal events are of concern and the above percentage increases to 99.7.

At this stage, a detailed design for a data validation system is not available. Gai _et al_. [4], have estimated an unavailability of 2×10^{-3} for the plant computer system of the Waterford III nuclear power plant. This system, which consists of two redundant computers, seems to have basic similarities with a data validation system. In Ref. 5, a conservative estimate of 3×10^{-6} has been obtained for the unavailability of the primary and secondary systems of an LMFBR power plant design.

The unavailability Q of the RSS scram initiation function can be written as:

$$Q = \frac{f}{F} \times q_e + \left(1 - \frac{f}{F}\right) \times q_e \left(q_d + P_o\right) \qquad (1)$$

where

f = frequency of events that do not allow adequate time for manual scram

F = frequency of ATWS significant transients = 7/yr

q_e = unavailability of the RSS electrical subsystem = 3.0×10^{-6}

q_d = unavailability of the data validation system = 2×10^{-3}

P_o = probability of operator failure to initiate scram

Equation (1) was used to obtain the following unavailability estimates

Time (min.)	f/F	P_o	Q	$3 \times 10^{-6}/Q$
5	0.026	0.002	9.0×10^{-8}	33
5	0.003	0.002	2.1×10^{-8}	145
15	0.026	0.001	8.6×10^{-8}	35
15	0.003	0.001	1.8×10^{-8}	169
30	0.026	0.0005	8.4×10^{-8}	36
30	0.003	0.0005	1.6×10^{-8}	185

The P_o values of 0.0005, 0.001 and 0.002 correspond to 30, 15, and 5 min. of available time for operator action, respectively [6]. These results show that the unavailability of the scram initiation function can be reduced by one to two orders of magnitude. For these estimates, the conservative assumption was made that if no data validation system is available P_o = 0.0. This probability is expected to be greater than zero, especially for the longer time intervals and whenever scram failure is not caused by multiple instrumentation failures. However, even in these cases the unavailability of scram initiation is further reduced if validated data is provided to the operator. Moreover, due to the large uncertainties in common-cause failure rates and the probabilities of successful operator action, regardless of the actual magnitude of the expected reduction, a data validation system provides assurance that manual scram will be effective and a substantial credit for operator action is warranted.

References

1. A. S. McClymont and B. W. Poehlman, "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients," EPRI NP-2230, Electric Power Research Institute (1982).

2. "Anticipated Transients Without Scram for Light Water Reactors," NUREG-0460, Vols. 1, 2, 3 (1978), Vol. 4 (1980).

3. W. H. Perry, Experimental Breeder Reactor II, Private Communication (1983).

4. E. Gai et al., "Availability Studies for Waterford III Plant Computer System," R-1495, The Charles Stark Draper Laboratory, Inc. (August 1981).

5. C. P. Tzanos, N. A. Hanan, and A. G. Adamantiades, "An Assessment of the Core Degradation Frequency in a Typical Large LMFBR Design for Internal Accident Initiators - A Comparison with PWR Predictions," Nucl. Technol., 63, 309 (1983).

6. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, U.S. Nuclear Regulatory Commission (1980).