Annals of Nuclear Energy 62 (2013) 326–332

Contents lists available at SciVerse ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence

A.C. Cilliers *

North West University, School for Mechanical and Nuclear Engineering, Hoffman Street, Potchefstroom, North West 2530, South Africa

ARTICLE INFO

Article history:
Received 14 June 2012
Received in revised form 24 June 2013
Accepted 26 June 2013
Available online 24 July 2013

Keywords:
Nuclear power plant
Fault detection
Fault isolation
Fault characterisation
Plant diagnostics
Plant simulator

ABSTRACT

Early fault identification systems enable detecting and diagnosing early onset faults or fault causes which allow maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

We have shown (Cilliers and Mulder, 2012) that detecting faults early during transient operation in NPPs is possible when coupled with a reliable reference to compare plant measurements with during transients. We have also shown (Cilliers, 2013) that by correlating the fault detection information as received from distributed systems it is possible to diagnose the faults in terms of location and magnitude.

This paper makes use of the techniques and processes developed in the previous papers and apply it to a case study of the Three Mile Island accident. In this way we can determine how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

1. Introduction

With the availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection and diagnosis (Cilliers et al., 2011; Cilliers and Mulder, 2012; Cilliers, 2013).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.
2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper functions as a benchmark of the first objective described by Cilliers and Mulder (2012) and the second objective described by Cilliers (2013), with a following paper presenting the third objective. In these papers we have shown that fault detection and diagnoses in this manner is indeed possible without relying on statistical models of fault signatures. The effectiveness of the system lies in the use of accurate mathematical models of the plant combined with conventional deterministic reactor protection principles. In this paper a case study is done on the Three Mile Island (TMI) accident.

For the purposes of the research a PC based nuclear power plant simulation software, PCTRAN was used, PCTran is a product of Micro-Simulation Technology (MST) Inc. it performs nuclear power plant transients and accident simulations on a personal computer (MST Inc., 2007). The most important advantage of PCTRAN is that it can be operated easily and is capable of running faster than real time (Po, 1981).

The TMI accident can be considered as a watershed moment in the nuclear industry which led to numerous safety analyses and advances following. The event itself has been studied to determine the exact sequence of events (Hochreiter and Robinson, 2004) as

* Tel.: +27 829202954; fax: +27 866648796.
E-mail address: cillliean@eskom.co.za

0306-4549/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.anucene.2013.06.037

well as the cause and mistakes made (Cummings, 1980). Other research was done on preventing the deterioration of the situation in the direct aftermath of the accident (Gonzalez and Gagliardo, 1980).

The event has also been used as case studies such as that of Le Bot (2004) that illustrated their point of view through the analysis of the TMI accident in 1979. Analysis of this accident allowed them to validate their positions regarding the need to move, in the case of an accident, from the concept of human error to that of systemic failure in the operation of systems such as a nuclear power plant. Their retrospective analysis of the TMI accident showed that the operators' mode of operation resulted from an overall logic, reflecting emergency operation logic upon which the design of the operating system was based. It helps to get out of the deadlock reducing the TMI accident either to a commissioning error of the type 'Inappropriate shutdown of the safety injection' or to an error of diagnostic and misrepresentation of the situation. The main theme of the research is acknowledging that although operator actions was to blame for the accident after a minor plant fault occurred, the real problem was the limited information available to the operators and that automated actions would have resulted in the same effect. They conclude by stating:

"The operating system did not foresee the means that were actually necessary to fulfill the mission required by the situation".

The work by Le Bot (2004) is very relevant to the research in this paper as we focus on manipulating measurement data combined with detailed models of the plant to increase the available information to the operator or system.

2. The TMI accident sequence of events

The event occurred at 04:00 on 28 March 1979. At the time, routine maintenance was being carried out on the ion-exchange system for feed water polishing. The accident was caused as a result of two block valves in the auxiliary feed water pump pressure lines that had been left closed after maintenance work had been conducted on the lines 2 days prior to the accident. The fault was initiated when the primary feedwater pump failed. Failure of this main pump stopped the main feed flow and caused reactor trip and low steam generator level. This should not have caused an accident as the auxiliary feedwater supply system should continue to supply feedwater to the steam generators. With the two block valves closed, the feedwater supply was cut off completely (Cummings, 1980).

This prevented feed water from entering one of the steam generators and so reduced the plant's ability to evacuate heat from the core. Because of the rise in temperature in the core, the Reactor Coolant System (RCS) pressure increased, which caused the power-operated relief valves (PORV) to open. Once the pressure had been reduced, the pressure relief valve failed to reseat and a leak occurred corresponding to a small break LOCA.

The closed auxiliary feed water block valves were discovered closed after 8 min and opened. This should have enabled the steam generators (SGs) to evacuate the heat correctly from the core, and the accident would have been prevented.

The small break LOCA caused by the leaking PORV was only discovered two and a half hours later, by which time the accident was well under way. Due to fault trigger (the closed block valves in the auxiliary feed water pressure lines) being corrected and the PORV indication light in the control room indicating that it had been de-energised, the operators did not expect a small break LOCA, and since the plant was already in a recovery transient from the accident, it was difficult to recognise unexpected behaviour of the plant. In fact, when the safety injection system started operating automatically after 2 min, the operators switched it off, believing that it would overfill the pressuriser (Hochreiter and Robinson, 2004).

It would be valuable to test the plant diagnostic system in these conditions. The event can be split into two distinct phases. The first phase is the blocking of feedwater flow to one SG, and the second phase the PORV stuck open after relieving pressure. The valves involved in these two causes are depicted in Figs. 1 and 2.

3. Cause 1: feedwater supply block to steam generator

The closed feedwater block valves caused a large fault that was detected within 114 s on the RCS high pressure setpoint by the conventional plant protection system. The affected control systems during this phase of the accident were the:

- Pressuriser level control
  - o Control: pressuriser letdown flow larger than expected.
  - o Measurement: pressuriser level higher than expected.
- RCS pressure control
  - o Control: pressuriser spray operation larger than expected.
  - o Measurement: pressuriser pressure higher than expected.
- SG pressure control
  - o Measurement: SG pressure increase larger than expected.
  - o Measurement: SG pressure higher than expected.
- SG Level control
  - o Measurement: SG level lower than expected.

Making use of dynamic setpoints and control operations operating beyond the expected operations the fault is detected within 4 s, with the combination of systems correlating to an "Inadvertent closure of secondary loop isolation valve" in Table 7.1 reached within 56 s as depicted the following figures.

Fig. 3 depicts the pressuriser level and feed flow, indicating an almost immediate rise in level with the pressuriser level control system following with increased letdown flow in an attempt to reduce the pressuriser level. The increase in pressuriser level is a direct effect of the reduced heat evacuation capability of the steam generators which resulted in increased pressure in the RCS and subsequent increased pressuriser level. Fig. 4 depicts the increase in RCS pressure and the activation of the pressuriser spray after 35 s in an attempt to reduce the pressure.

In the secondary coolant loop the effect of the blocked auxiliary feedwater flow resulted in an immediate drop in SG level due to the continuation of steam being removed from the SG without the coolant being replaced. The reduced capacity for heat evacuation caused an increase in coolant temperature and pressure. The reduced level and increased pressure in the affected SG is depicted in Fig. 5.

During the accident the closed auxiliary feedwater block valves were discovered after 8 min (480 s) and opened by which time the reactor was already tripped. Although the use of the PDS would detect and characterise the fault within 56 s, it is accepted that closing of the valve could still take some time. For this reason we assume that even with the use of the plant diagnostic system the opening of the valve could have occurred 480 s after the fault was initiated.

The reactor SCRAM event due to high RCS pressure after 114 s coincided with the opening of the power-operated relief valve (PORV) with the intention of reducing the RCS pressure. The PORV should have remained open only temporarily until the pressure was sufficiently reduced, but after the PORV was de-energised it remained stuck open. The stuck open PORV is considered to be the start of the second phase of the accident.

4. Cause 2: power-operated relief valve failure

When the auxiliary feedwater block valves were opened and since the reactor was already tripped the plant was expected to