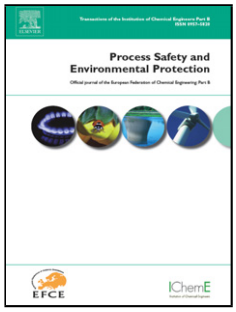


Title: An Inherently Fail-Safe Electronic Logic Design for a Safety Application in Nuclear Power Plant

Authors: Srikantam Sravanthi, R. Dheenadhayalan, K. Devan, K. Madhusoodanan

PII: S0957-5820(17)30222-7
DOI: http://dx.doi.org/doi:10.1016/j.psep.2017.07.008
Reference: PSEP 1110

To appear in: *Process Safety and Environment Protection*

Received date: 11-2-2017
Revised date: 16-3-2017
Accepted date: 6-7-2017

Please cite this article as: Sravanthi, Srikantam, Dheenadhayalan, R., Devan, K., Madhusoodanan, K., An Inherently Fail-Safe Electronic Logic Design for a Safety Application in Nuclear Power Plant.Process Safety and Environment Protection http://dx.doi.org/10.1016/j.psep.2017.07.008

# An Inherently Fail-Safe Electronic Logic Design for a Safety Application in Nuclear Power Plant

Srikantam Sravanthi[*, 1, 2], R. Dheenadhayalan[2], K. Devan[2] and K. Madhusoodanan[2]
Homi Bhabha National Institute[1]
Indira Gandhi Centre for Atomic Research[2]
Kalpakkam, Tamilnadu-603102, India.
*sravanthisrikantam.445@gmail.com

Highlights

- Inherently fail-safe electronic logic circuit is proposed and implemented with very low unsafe failure probability.
- It is achieved by processing the inputs as synchronized pulses rather than static digital levels.
- A prototype circuit is built to verify Failure Mode Effect Analysis and results are presented in paper.
- Unsafe failure probability is calculated.
- This method can be extended to similar industrial control involving combinational circuits

**Abstract**: In this paper, an inherently fail-safe electronic logic circuit is proposed. Further, it's investigated for safety critical application in a nuclear power plant with a very low unsafe failure probability requirement. The application involves control circuit for operation of solenoid valves based on the plant state, wherein the de-energization of certain solenoid valves is considered as a safe state. The inherent fail-safeness is achieved by processing the inputs as synchronized pulses rather than static digital levels. Pulse transformers are used at specific locations in the circuit so that energy transition to subsequent stages of the circuit is seized in case of a failure in the previous stage. Such pulse processing is selectively applied to those parts of the circuit for which fail-safe behavior of final control elements is expected. A Failure Mode Effect Analysis (FMEA) is performed for the circuit to systematically ensure that failure of components in postulated modes will result in the fail-safe state. A prototype circuit is built to verify the results obtained from FMEA. The inherency in the circuit is shown to possess a very low unsafe failure probability and quantitatively it is shown. The proposed technique is suggested as a diverse method to control, redundant instrumentation provisions usually provided for safety critical application. This method can be easily extended to similar industrial control involving combinational circuits with modifications.

**Keywords-Inherently fail-safe, pulse processing and unsafe failure probability.**

## I. INTRODUCTION

The Prototype Fast Breeder Reactor (PFBR) is (500MWe sodium cooled) under construction at Kalpakkam, India. During normal operation, the heat generated in the core is removed with dedicated heat exchangers and converted to electrical energy. After the reactor is shut down, the decay heat is removed with Operation Grade Decay Heat Removal (OGDHR) system predominantly using normal heat removal path. During the unavailability of OGDHR, the decay heat is removed with Safety Grade Decay Heat Removal (SGDHR) system. The reactor core is immersed in a large sodium pool. SGDHR consists of four sodium loops each with 8 MWt capacity. In each loop, the heat transfer from sodium pool to the SGDHR loop takes place through a sodium to sodium heat exchanger dipped into the pool (DHX). This heat will be