RULES AND DIRECTIVES
BRANCH
USNRC

As of: June 25, 2013
Received: June 21, 2013
Status: Pending_Post
Tracking No. 1jx-8614-goun
Comments Due: August 16, 2013
Submission Type: Web

PUBLIC SUBMISSION

2013 JUN 25 AM 9: 42

RECEIVED

Docket: NRC-2013-0089
Design-Specific Review Standard for the mPower Design

5/14/2013
78 FR 28258
1

Comment On: NRC-2013-0089-0001
mPower Design-Specific Review Standard

Document: NRC-2013-0089-DRAFT-0002
Comment on FR Doc # 2013-11394

Submitter Information

Name: Thomas Koshy
Address:
Division of Nuclear Power | Department of Nuclear Energy |International Atomic Energy Agency Box 100, 1400 Vienna
Vienna, Austria,
Organization: IAEA

General Comment

7.1.5 DIVERSITY AND DEFENCE IN DEPTH
II ACCEPTANCE CRITERIA

Requirements 1A Compliance (Addition of consideration)
The Clause 5.6 in IEEE Std. 603-1991/2009, Independence, addresses independence between redundant portions of a safety system (clause 5.6.1), between safety systems and the effects of design basis events (clause 5.6.2), and between safety systems and other systems (clause 5.6.3). The Emergency Core Cooling System and Reactor Protection System should be independent in electric power supply and control systems as illustrated in the IEEE Std. 603 1991/2009 (Annex A, Figures A-2 and A-3) should be demonstrated to be free from any common cause failures..

Reasons
The figures clearly indicate Emergency core cooling (ECCS) and reactor trip to be separate systems and designate 1E power supply for ECCS and different kind of power supply for reactor trip with fail safe features to cause a trip when the conditions exceed operational limits.
The separation is needed to prevent the common cause failures that could potentially propagate into preventing reactor trip and spreading into emergency core cooling actuations systems. Diversity is essential NRC Information Notice 2009-03 SOLID STATE PROTECTION SYSTEM CARD FAILURE RESULTS IN SPURIOUS SAFTY INJECTION ACTUATION AND REACTOR TRIP describes an event at North Anna

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add: Y. Malave (yxm)

J. Starefos (jls1)

Station where a Diode failure caused main feed water system isolation, reactor trip, ECCS actuation and control system prevented resetting Safety Injection signal from the control room. The licensee staff had to rush and locally detach some relays and pull fuses to de-energize circuits to prevent over filling the pressurizer. If ECCS sensors and controls were separate, pressurizer over filling would not be a prompt challenge. While this condition caused the trip and ECCS actuation, it could have possibly caused the opposite or its undesirable combinations. This condition clearly calls for removing any sharing of control sys

Attachments

NRC-mpower-ipwr-7-2comment-Koshy

7.1.5 DIVERSITY AND DEFENCE IN DEPTH

II ACCEPTANCE CRITERIA

Requirements 1A Compliance (Addition of consideration)

The Clause 5.6 in IEEE Std. 603-1991/2009, Independence, addresses independence between redundant portions of a safety system (clause 5.6.1), between safety systems and the effects of design basis events (clause 5.6.2), and between safety systems and other systems (clause 5.6.3). The Emergency Core Cooling System and Reactor Protection System should be independent in electric power supply and control systems as illustrated in the IEEE Std. 603-1991/2009 (Annex A, Figures A-2 and A-3) should be demonstrated to be free from any common cause failures..

Reasons

The figures clearly indicate Emergency core cooling (ECCS) and reactor trip to be separate systems and designate 1E power supply for ECCS and different kind of power supply for reactor trip with fail safe features to cause a trip when the conditions exceed operational limits.

The separation is needed to prevent the common cause failures that could potentially propagate into preventing reactor trip and spreading into emergency core cooling actuations systems. **Diversity is essential** NRC Information Notice 2009-03 SOLID STATE PROTECTION SYSTEM CARD FAILURE RESULTS IN SPURIOUS SAFTY INJECTION ACTUATION AND REACTOR TRIP describes an event at North Anna Station where a Diode failure caused main feed water system isolation, reactor trip, ECCS actuation and control system prevented resetting Safety Injection signal from the control room. The licensee staff had to rush and locally detach some relays and pull fuses to de-energize circuits to prevent over filling the pressurizer. If ECCS sensors and controls were separate, pressurizer over filling would not be a prompt challenge. While this condition caused the trip and ECCS actuation, it could have possibly caused the opposite or its undesirable combinations. This condition clearly calls for removing any sharing of control systems, process parameter sensors, or power supply between ECCS and reactor Trip system..

An over voltage event is described in IN 2006-18: "Significant Loss of Safety-Related Electrical Power at Forsmark Unit 1, in Sweden" IN 2006-18 supplement was issued on August 10, 2007This is a plant event where a common cause disabled 2 of the 4 uninterruptible power supplies (UPSs)and caused two relief valves to stay open (undesirable failure mode), disabled two of the emergency diesel generators, and lost half of the control room indications. The other two UPSs had the same vulnerability but serendipitously remained available and avoided core damage. The lesson to be learned is the common mode failure vulnerability of power supplies. The Fukushima event further magnifies the common mode failures of power supplies. Therefore, power supply and control system diversity is needed to separate Reactor trip system and ECCS actuation. For example: A DC powered control system logic for ECCS and AC-from UPSs for reactor trip system could bring diversity.

Mr. Thomas Koshy, Head

Nuclear Power technology Development| Division of Nuclear Power | Department of Nuclear Energy |International Atomic Energy Agency Box 100, 1400 Vienna, Austria Email: **T.Koshy@iaea.org**