Nuclear Engineering and Design 339 (2018) 225–234

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

Sensitivity analysis of APR-1400's Reactor Protection System by using RiskSpectrum PSA

Muhammad Zubair*, Ahmed Ishag

Department of Mechanical and Nuclear Engineering, University of Sharjah, Sharjah 27272, United Arab Emirates

ARTICLE INFO

Keywords:
Reactor Protection System
Probabilistic Safety Assessment
RiskSpectrum
Reliability enhancement

ABSTRACT

The Advanced Pressurized Water Reactor (1400) offers greater power output than its predecessor, the Optimized Power Reactor (OPR-1000), hence required increased reliability and design limitations of its protection systems to be licensed for commercial operation. One of these systems is the Reactor Protection System (RPS), a set of subsystems and methods designed to fortify the integrity of the reactor. Compromise of RPS safety could stem from possible failures of subsystems, natural hazards, inadequate application of mitigation measures or human error. Probabilistic Safety Assessment is an effective and indispensable part of Nuclear Safety that is used within the assessment of RPS reliability. Alongside other techniques, it incorporates the use of fault-tree analysis to determine failure rates of top-events, but it requires input data in the form of initiating events. Unfortunately, accurate data on initiating events is hard to obtain and therefore, the use of conservative values was the norm in most studies. This signifies the importance of studying a handful of values around these conservative values. This paper focuses ontheAPR-1400 and aims to investigate the most promising elements to improve the reliability of its Reactor Protection System (RPS). The study was carried out using Risk Spectrum PSA, a tool used in more than 50% of nuclear reactors around the world. From 171 initiating events, trends and case studies for the 3 most sensitive elements in RPS were constructed and discussed. CCF-TCB, Operator and CC-DOP were found to be the most potent events in reducing RPS failure probability. This research should give an insight on how to tackle RPS-enhancements for future designs of Nuclear Power Plants.

1. Introduction and background

In the light of famous nuclear accidents, the bar to improve on nuclear safety standards continues to rise with every successful generation of nuclear power plants, to primarily ensure public safety (European Atomic Energy Community, 2006). TheAPR-1400 features enhanced power output as well as safety margins compared to its predecessor, the OPR-1000 (Goldberg et al., 2011; WNN, 2013). Various technical reports that discuss the suitability of the APR-1400 for commercial use were produced. One of them was made by Korea's Atomic Energy Research Institute (KAERI), a reliability analysis technical report solely focused on the Reactor Protection System (RPS) of the APR-1400 (Varde et al., 2003). The technical report contained 44 pages of the RPS's fault-tree. The main purpose of the report was to model the digital protection system of the APR-1400. This was done by highlighting critical components and functions of RPS to assess its reliability, which also had to include other related factors in the system, such as importance analysis and human error reliability. It was stated that the APR-1400 offers numerous advantages by incorporating digital-technology, such as increased precision of set-points, drift-free operation (better fuel-fission reactivity-control) and online self-diagnosis checks. Additionally, the APR-1400 adopted defense-in-depth safety principles including diversity, component-redundancy and alleviated fault-tolerance to achieve lower failure probabilities. This is a standard advantage over previous analog-protection designs.

RPS contains digital components known as the 'Digital Plant Protection System' (DPPS), aimed to monitor the power plant and intervene in case of a critical failure or abnormal situation. Since RPS is designed to protect the reactor, all factors that may affect the integrity of the reactor are catered for as well in the system. Therefore, in addition to DPPS, RPS also includes shutdown devices with the terms of Control Element Drive Mechanisms' (CEDMs) and 'Common Cause Failures' (CCF). CCF includes human errors as well as natural disasters and their countermeasures (See Fig. 1).

When it comes to quantifying software methods in the nuclear industry, the USNRC and other regulatory bodies did not certify a specific method (Varde et al., 2003), but the general direction strongly suggests to treat the matter probabilistically (Dahll et al., 2007; Chu et al.

* Corresponding author.
E-mail address: mzubair@sharjah.ac.ae (M. Zubair).

https://doi.org/10.1016/j.nucengdes.2018.09.019
Received 23 July 2018; Received in revised form 10 September 2018; Accepted 18 September 2018

Nomenclature

APR-1400	Advanced Pressurized Water Reactor (1400 MW_e)
RPS	Reactor Protection System
OPR-1000	Optimized Water Reactor (1000 MW_e)
DPPS	Digital Plant Protection System
CCF	Common Cause Failures
FTA	Fault-tree Analysis
PSA	Probabilistic Safety Assessment
ACT	Actuation Logic
AM	Auto & Manual tip
CCF-TCB	Common Cause Failure of Trip Circuit Breakers
CCF-DOP	Common Cause Failure of Digital Output Module
LCL	Logical Coincidence Logic

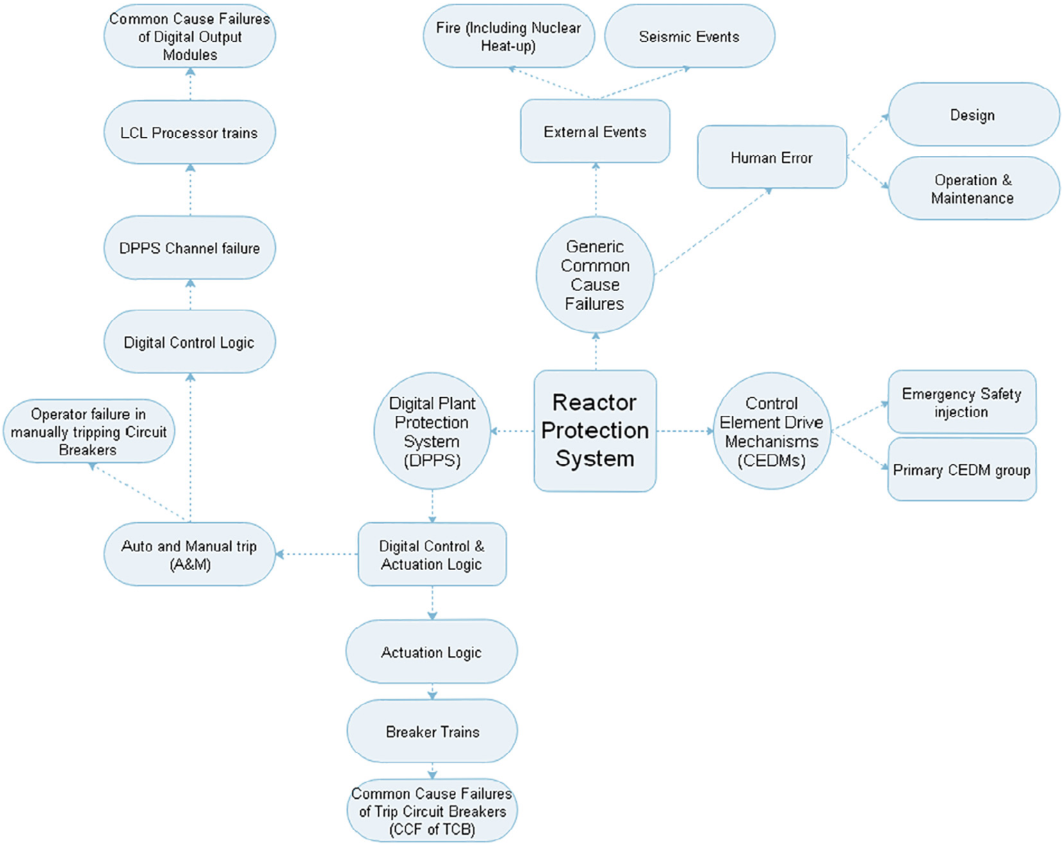
Common Cause Failures of Digital Output Modules
LCL Processor trains
DPPS Channel failure
Digital Control Logic
Operator failure in manually tripping Circuit Breakers
Auto and Manual trip (A&M)
Fire (Including Nuclear Heat-up)
Seismic Events
External Events
Human Error
Design
Operation & Maintenance
Generic Common Cause Failures
Digital Plant Protection System (DPPS)
Reactor Protection System
Control Element Drive Mechanisms (CEDMs)
Emergency Safety injection
Primary CEDM group
Digital Control & Actuation Logic
Actuation Logic
Breaker Trains
Common Cause Failures of Trip Circuit Breakers (CCF of TCB)

Fig. 1. Simplified map of APR-1400's Reactor Protection System and dependencies.

(2009)), involving the use of Fault-tree Analysis (FTA).

FTA incorporates Boolean logic to merge a number of basic events, to deduce the likelihood of an event that could take place with respect to these basic events. A basic yet common example, is to see the likelihood of waking up in the morning, with basic events including functional alarm(s) and people to assist with breaking the state of sleep. FTA is used in safety/reliability engineering to depict how complex systems could fail, with emphasis on the most effective ways to increase total reliability of these systems. FTA is utilized in various sectors, such as nuclear power (Vesely et al., 1981; Us, 1984), pharmaceuticals (Idaho National Laboratory, 2012), chemical processes (Center for Chemical Process Safety, 1999; Center for Chemical Process Safety, 2008; U.S. Department of Labor, 1994), systems of social service (Lacey and Peter, 2011), aerospace (Goldberg et al., 1994), and many others.

Fault trees are composed by connecting conventional logic gates (e.g. AND & OR gates) to events, in such a way that these trees would reflect the system at hand. A combination of events that cause the top event is often called a Cut Set. If a Cut Set is basic, where its removal would alter the top event, that Cut Set is then called Minimal Cut Set (MCS). With focus on MCSs, various analyses can be made, including Importance Measures.

Importance Measures are used to carry out Sensitivity studies, which are used to quantify total risk based on inputs or initiating events. Some of the dominantly used importance measures are risk reduction and Fussell-Vesely (FV) (USNRC, 1994). Keeping in view the initiating events that could cause a system to fail, risk reduction would set an initiating event's failure probability to zero, to observe the total decrease in the failure probability of the system. On the other hand, FV measures percentage-contribution of MCSs to total risk, as long as these MCSs contain initiating events that could contribute to the failure of the system (Idaho National Laboratory, 2012).

1.1. Importance measures

The most commonly used Importance Measures are Risk Achievement Worth (RAW), Risk Reduction Worth (RRW) and Fussel-Vesely (FV) (Dimitrijevic and Chapman, 1996).

RAW or RIF is a factor that represents the increase in risk, with the assumption or knowledge that equipment is guaranteed to fail. Which translates into the greatest increase in risk if most vital equipment fails. Mathematically, it is calculated as:

$$RIF = \frac{Risk\ \ @unavailability = 1}{Measured\ \ baserisk}$$

RRW or RDF is the opposite of RAW. This factor illustrates the reduction in risk with the guarantee that equipment will not fail. In other