Reliability Engineering and System Safety 138 (2015) 21–30

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A systematic framework to investigate the coverage of abnormal operating procedures in nuclear power plants

Jinkyun Park*, Wondea Jung

Korea Atomic Energy Research Institute (KAERI), Daejeon, Republic of Korea

ARTICLE INFO

Article history:
Received 18 March 2014
Received in revised form
8 August 2014
Accepted 15 January 2015
Available online 2 February 2015

Keywords:
Single point vulnerability
Human performance
Abnormal operating procedure
Coverage investigation

ABSTRACT

It is evident that the reliability of complex socio-technical systems, such as NPPs (nuclear power plants), is very critical for public safety. For this reason, the DID (defense-in-depth) concept has been adopted as a core principle to ensure the operational safety of NPPs. Regarding this, the provisioning of AOPs (abnormal operating procedures) is essential for implementing the DID concept. Unfortunately, since most AOPs were developed based on operational experience, it is not easy to investigate their coverage in a systematic manner. Therefore, in this study, a framework to identify the coverage of AOPs is proposed based on a SPV (single point vulnerability) model. As for the initial validation of the suggested framework, the coverage of OPR1000 (optimized power reactor 1000 MWe) units operating in the Rep. of Korea is analyzed. As a result, it is revealed that their coverage is about 63%. In addition, it is confirmed that one of the component failures distinguished from the proposed framework actually triggered an unexpected reactor trip event in an OPR1000 unit. Therefore, it is possible to expect that the proposed framework can be used as a practical tool to enhance the coverage of AOPs.

1. Introduction

The safety of complex socio-technical systems, such as NPPs (nuclear power plants), off-shore industries, and marine transportation systems, is very important because the consequence of any accident can result in a dramatic casualty toll including massive deaths and/or injuries, significant environmental damage and tremendous financial losses. For example, the Fukushima accident clearly demonstrated the result of a severe accident in an NPP [5,9]. In addition, 167 people were killed due to the Piper Alpha accident that occurred in an off-shore oil production platform located in the North Sea [33], and the Exxon Valdez accident caused irrecoverable environmental damage from the huge amount of oil spilled into the bay [27]. Therefore, various kinds of countermeasures that are helpful for enhancing the operational safety of these systems have been studied for many decades. From the point of view of the safety of NPPs, the core principle to identify these countermeasures is the implementation of a DID (defense-in-depth) concept [38].

According to the IAEA [12], the DID concept "consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant." (p. 4) In this regard, a five-level structure shown in Table 1 has been generally considered from the design of NPPs [12].

The objective of each DID level can be accomplished by many different ways. For example, one of the representative countermeasures for *DID Level 3* is the provision of EOPs (emergency operating procedures) to control accidents within the scope of a design basis while SAMGs (severe accident management guidelines) is a typical means to achieve the objective of *DID Level 4* [12].

Of them, it is promising that the most effective strategy to implement the DID concept is to prevent the initiation of an event that is able to jeopardize the operational safety of NPPs from the very beginning. In this context, Ma and Jiang [23] categorized various kinds of fault detection and diagnosis methods based on IAEA documents illustrating that potential faults in NPPs can be classified into six types [14,15]: (1) instrument steady state performance degradation, (2) instrumentation channel dynamic performance degradation, (3) faults in equipment, (4) loose parts in reactor coolant system, (5) anomalies in reactor core, and (6) plant transients. Accordingly, diverse applications (such as instrument monitoring, equipment monitoring, loose part monitoring, and

* Correspondence to: 1045 Daedeokdaero, Yuseong-Gu, Daejeon, 305-353, Republic of Korea. Tel.: +82 42 868 2186.
E-mail address: kshpjk@kaeri.re.kr (J. Park).

http://dx.doi.org/10.1016/j.ress.2015.01.013
0951-8320/

Nomenclature

AIMS-PSA	Advanced Information Management System for PSA
AOP	abnormal operating procedure
BDBA	beyond design basis accident
BE	basic event
CAP	corrective action program
CEDMCS	control element drive mechanism control system
DBA	design basis accident
DID	defense-in-depth
DIF	difficulty, importance and frequency
DNBR	departure from nucleate boiling ratio
EOP	emergency operating procedures
FMEA	failure modes and effects analysis
FT	fault tree
FTA	fault tree analysis
FTREX	fault tree reliability evaluation expert
HMI	human machine interface
IAEA	International Atomic Energy Agency
KAERI	Korea Atomic Energy Research Institute
MCS	minimal cut set
MCSC	MCS criticality
MUX	multiplexer
NIM	network interface module
NPP	nuclear power plant
PSA	probabilistic safety assessment
OE	operating experience
OPIS	operational performance information system for nuclear power plant
OPR1000	optimized power reactor 1000 MWe
PCS	plant control system
RCP	reactor coolant pump
SAMG	severe accident management guidelines
SME	subject matter expert
SPV	single point vulnerability

Table 1
DID levels with the associated objectives; reproduced from IAEA [12].

Level	Objectives
1	Prevention of abnormal operation and failures
2	Control of abnormal operation and detection of failures
3	Control of accidents within the design basis
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents
5	Mitigation of radiological consequences of significant releases of radioactive materials

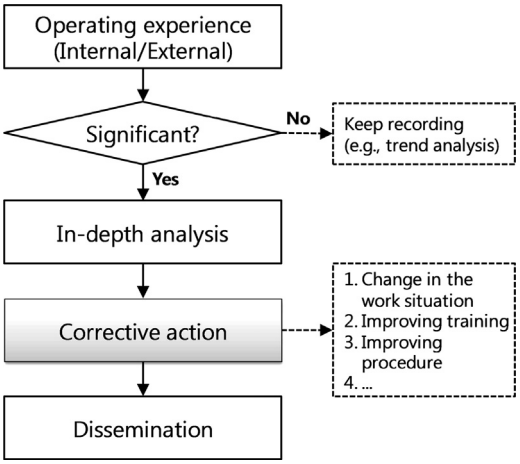

Fig. 1. Simplified CAP process; reproduced from IAEA [16].

Table 2
Three levels of event significance; reproduced from EPRI [7].

Level	Investigation Type	Selected example
Critical	Root cause investigation	• Unit trip or major loss of MWs • Safety incident (fatality or lost time injury) • Significant reportable environment incident
Important	Apparent cause evaluation	• Startup failures • Safety incidents resulting in recordable injury • Reportable environmental incidents
Minor	Trend	• Equipment reliability issues • Near miss

transient monitoring) to detect these faults correspond to promising countermeasures to implement the *DID Level 2*.

However, even though each fault is successfully detected and isolated (i.e., recognizing its location), there are times when a series of manual actions should be conducted in order to lead the abnormal condition of NPPs to a normal condition. For this reason, most NPPs provide a large volume of AOPs (abnormal operating procedures), through which human operators are able to effectively identify the list of actions to be done and how to actually conduct them [10,17,22]. This implies that AOPs should have a sufficient coverage so that human operators are able to determine the required actions to cope with a given abnormal condition. If not, the operational safety of NPPs may be degraded owing to the breach of the *DID Level 2*. From this concern, it is not easy to ensure the sufficient coverage of AOPs because most of them were developed based on the review of historical data (e.g., OE; operating experience). In order to clarify this claim, let us consider Fig. 1 that shows the simplified process of the CAP (corrective action program) reproduced from IAEA [16].

As shown in Fig. 1, the first step of the CAP process is to collect an event that has occurred in either a home plant (i.e., internal event) or other NPPs (i.e., external event). Of them, if there are significant events that have a potential for affecting the operational safety of the home plant then an in-depth analysis should be followed in order to identify their root causes. In this light, although each NPP can use its own standard, EPRI [7] suggested decision criteria for three levels of event significance with the associated investigation methods (Table 2).

For example, when an event of which the significance belongs to the *Critical level* and *Important level* has occurred, it is necessary to identify its cause by using a root cause analysis and an apparent cause analysis (i.e., a kind of a brief process to discover plausible