Engineering Failure Analysis 47 (2015) 117–128

Contents lists available at ScienceDirect

Engineering Failure Analysis

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

Learning how to learn from failures: The Fukushima nuclear disaster ☆

Ashraf Labib [a,*,1], M.J. Harris [b,2]

[a] University of Portsmouth, UK
[b] University of Manchester, UK

ARTICLE INFO

Article history:
Received 8 July 2014
Received in revised form 20 September 2014
Accepted 6 October 2014
Available online 23 October 2014

Keywords:
Fukushima
Hydrogen explosion
Common mode failure
Loss of cooling
Fault tree

ABSTRACT

Analysis of the Fukushima nuclear reactor disaster will show how to learn from failures using multi-models. This type of analysis can enrich the modelling of causal factors, provide insight into policy making and support decisions for resource allocations to prevent such disasters.

The analysis presented here is based on a workshop on learning from failures in which participants were first given a brief about the related theory, then an introduction to the analytical techniques that can be used such as FTA, and RBD. They were then given a brief in the form of a narrative of the accident derived from investigation reports and divided into small groups tasked to analyse the disaster and to present their recommendations both orally and in a written report.

All the participants were asked to follow a certain presentation format. Firstly there would be a technical account of the sequence of events that would be based on research of greater depth than provided in the initial summary, one related more to the scope of their analysis.

This would be followed by a review of the consequences of the accident, a presentation of their multi-model analysis of the event and a summary of generic lessons and recommendations to prevent future failures of such systems. Finally, collective feedback, focused on the generic lessons gained, was offered.

1. Introduction

In the wake of the Fukushima disaster few investigation reports, aimed at explaining the accident and outlining the lessons learnt, have been published. Most notably, it has been suggested that in the nuclear power industry, probabilistic safety assessment (PSA) is under-utilised. A report of the Japanese government to the International Atomic Energy Agency (IAEA) observed that "… *PSA in risk management has not always been effectively utilised in the overall reviewing processes or in risk reduction efforts at nuclear power plants*" [28]. Moreover, the British Office of Nuclear Regulation (ONR) final report on Fukushima commented that "*This* [under-utilisation of PSA in the nuclear power sector] *is an important lesson, … effective use of PSA could have helped to prevent accidents like that at Fukushima escalating and deal with them should they occur*" [37]. In

☆ This research builds on and extends previous work presented at the PSAM Conference, 2014, and in chapter 9 of Labib [18].
* Corresponding author.
1 Professor.
2 Visiting Senior Lecturer.

http://dx.doi.org/10.1016/j.engfailanal.2014.10.002
1350-6307/

the same report the final recommendations include "*The circumstances of the Fukushima accident have heightened the importance of Probabilistic Safety Analysis for all nuclear facilities that could have accidents with significant off-site consequences*". Also responding to the Fukushima disaster George Apostolakis of the United States Nuclear Regulatory Commission (NRC), has argued that "*probabilistic risk assessment (PRA) can support a more holistic, performance-based safety case, with an appropriate emphasis on systems and components that are shown to contribute the most to technological risk*" [1]. Others have also supported the use of PRA approaches in the nuclear industry [24,17]. In this paper the Fukushima disaster is analysed and a hybrid modelling approach, using PSA-related techniques, is developed. It is hoped that through the provision of an example of PRA/PSA tools used to analyse Fukushima disaster, such analysis can lead to the realisation of a learning culture within organisations and governments.

Although the literature on organisational learning has been well established since the seminal work of Cyret and March [7,5], the literature in the field of learning from rare events of high severity is largely multi-disciplinary and fragmented [29,27]. A reason for its being treated as marginal to the mainstream research has probably been the perception that such a field of research was a statistical outlier [19]. Also, there have been few text books on this topic, other than those of Turner [34] on man-made disasters and Kletz [15] on learning from accidents. The fragmentation of the topic has been reflected in the variety of its names, e.g. Learning from Incidents, Learning from Disasters, Learning from Major Events and Near Misses, and Learning from Crises. Recently, however, there has been a revival of interest and research activity, the Journal of Safety Science dedicating an issue to learning from events and near-misses [6] and another to learning from accident reports [9], The Journal of Contingencies and Crisis Management running an issue on learning from crises and major accidents [8] and The Journal of Organization Science publishing a special on rare events and organisational learning [19]. Also recently published have been reviews of the literature on learning from incidents, accidents and disasters [21,22,20,10]. In a recent work by Saleh et al. [30], an excellent analysis of a failure of a defense-in-depth (a concept originated in nuclear industry), was studied and applied to the case of BP Texas refinery accident.

After the Three Mile Island and Chernobyl accidents research in learning from failures has resulted in recommendations, for becoming learning organisations, specifically addressed to the nuclear power sector [11]. Unfortunately, these have not been matched with guidance on how this could be achieved [35]. One unique feature of nuclear power plants is that they are initially designed for a very long operational life, typically sixty years. This poses major challenges such as those of having to cope with technical developments, new safety requirements and sustaining skills and competencies, over two or three generations of staff [35].

The following section is a narrative summarising the abundance of information in the literature on the Fukushima accident. It is suggested that, the disaster having happened a while ago, a primary data collection would be of lower quality, as memories have faded and key observers have dispersed, and a secondary data analysis (which is a proven and widely used research method) is therefore employed for structuring the problem. This also offers the possibility of triangulating sources and easy checking by other researchers. The same narrative was provided in the workshop conducted by the first author. The participants were then divided into groups, each of which was required to scrutinise the literature to find more evidence about the disaster and utilise reliability engineering and decision science techniques in order to analyse the failure and make recommendations. The background of the participants were practitioners from different industries such as oil and gas, power and nuclear power generation. They workshop was part of a masters class related to learning from failures. They were also initially provided with the theoretical background of the tools used in the analysis such as FTA and RBD.

1.1. The evolution of the disaster

On 11 March 2011 Japan suffered its worst ever recorded earthquake, known as the Great East Japan Earthquake. It was classified as a seismic event of magnitude 9.0, with maximum measured ground acceleration of 0.52 g (5.07 m/s^2). The epicentre was 110 miles E.N.E. from the Fukushima-1 reactor site, where Reactor Units 1, 2 and 3 were operating at power. On detection of the earthquake all the units shutdown (tripped) safely.

Initially, on-site power was used to provide essential post-trip cooling. About an hour after shutdown a massive tsunami, generated by the earthquake, swamped the site and took out the AC electrical power capability. Sometime later, alternative back-up cooling was also lost. With the loss of these cooling systems Reactor Units 1 to 3 overheated, as did a spent-fuel pond in the building containing Reactor Unit 4. This resulted in several disruptive explosions, because the overheated zirconium-containing fuel-cladding reacted with water and steam and generated a hydrogen cloud which was then ignited. Major releases of radioactivity occurred, initially to air but later via leakage to the sea. The operators struggled to restore full control.

This was a serious nuclear accident, provisionally estimated to be of Level 5 on the Nuclear Event Scale (INES), a figure which was later amended to a provisional Level 7 (the highest category). The Japanese authorities imposed a 20 km radius evacuation zone, a 30 km sheltering zone and other countermeasures. Governments across the world watched with concern and considered how best to protect those of their citizens who were residents in Japan from any major radioactive release that might occur [36].

Some have commented on reports of plant damage caused by the earthquake itself, concluding that the loss of effective cooling for the reactors stemmed directly from the earthquake rather than the subsequent tsunami. However, the information available about the emergency cooling systems, and analysis of the circumstances, do not support such a hypothesis [37].

This case study is a good example of a double-jeopardy, where the combination of earthquake and tsunami caused destruction on a scale that was not anticipated in the initial design specifications. For example, the plant was protected