Fusion Engineering and Design 84 (2009) 1521–1524

Contents lists available at ScienceDirect

Fusion Engineering and Design

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

Safety analysis of ITER failures and consequences during maintenance☆

T. Pinna [a,*], A. Natalizio [b]

[a] ENEA-Frascati, Via E. Fermi 45, I-00044 Frascati, Rome, Italy
[b] ENSAC Associates Ltd.,87 Markland Dr., Toronto, Ont. M9C 1N4, Canada

ARTICLE INFO

Article history:
Available online 20 January 2009

Keywords:
Safety analysis
Maintenance
ORE
ITER

ABSTRACT

This study has been a first attempt at identifying potential worker overexposure situations during machine maintenance operations. The results indicate potential areas, or situations, where worker overexposure may be possible [A. Natalizio, T. Pinna, Safety analysis of failures and consequences during maintenance, ENEA Report, FUS-TN-SA-SE-R-170, June 2007, Frascati, Italy].

The key findings obtained are as follows. Firstly, we have found no machine maintenance operations where the risk of worker overexposure is considered significantly large that immediate design attention is needed.

Secondly, the most significant risk of worker overexposure is due to airborne releases of radioactivity from cooling water pipes and tubes that may not have been fully drained and dried, when they are cut, or inadvertently opened, by workers (frequency of pipe-cutting activities could be significantly high).

Thirdly, the risk of overexposure from human error could also be significant. This varies from mistaking the machine sector, to mistaking the component to be maintained. This is analogous to working on a live electrical circuit, when it is believed to be dead (disconnected from the power source) because the worker has mistakenly selected the wrong circuit—a look-alike one. Similarly, consider the situation of a worker mistakenly preparing to work on a cooling water circuit that is still at pressure and temperature, instead of the one that has been drained and dried. The more look-alike situations there are in the facility, the greater the probability of committing this type of error.

Fourthly, when consideration is given to human error, we believe that the aggregation of different diagnostics in the same port enhances the probability of human error. At the moment, these risks cannot be quantified. The task of quantifying those risks in the future should be considered.

Finally, the transport of activated in-vessel components, including components of plasma-heating and current-drive systems, in non-shielded casks, could carry with it a significant risk of worker overexposure. In the context of ALARA, this approach requires a specific study to justify its use.

Concluding, it is important to note that by having identified the possibility of an overexposure situation does not mean that it is probable. The calculation of probability awaits further studies of this nature, when the design reaches a more detailed level.

1. Introduction

The task objective was to perform an evaluation of proposed maintenance activities, documented by the ITER (International Tokamak Experiment Reactor) project, to identify mishaps (situations) that have the potential to lead to a radiation overexposure of workers involved in the maintenance operations. The evaluation covers maintenance activities in the following areas of the ITER facility: the tokamak cooling system vaults, the port cells, and the tokamak hall during movements of the in-vessel component transportation casks [1]. More specifically, the task objective was to identify a list of reference situations that may require to be studied in detail as a part of a future study.

The purpose of this work was to support the preliminary safety case to be made to the licensing authority with respect to occupational radiation exposure, and specifically off-normal situations—i.e., those that are not included in the normal Occupational Radiation Exposure (ORE) studies that have been performed to date. It must be noted, however, that, in the overall scheme of things, at this particular point in time, such studies can be equally useful, if not more so, to the project than to the licensing authority. To the licensing authority, this study demonstrates that important ORE issues are being addressed very early in the project life, so that solutions to potential problems are easier to find and implement, whereas, to the project, it provides an early warning of potential issues to be addressed. The identification and discussion of potential issues should provide documented evidence to the licensing

☆ Presented to the 25th Symposium on Fusion Technology.

* Corresponding author.
E-mail address: pinna@frascati.enea.it (T. Pinna).

0920-3796/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.fusengdes.2008.12.021

authority that the ALARA (As Low As Reasonable Achievable) process is in place and not being ignored. It is important to note that this is early stage ORE analysis and the end is far from sight. Nevertheless the direction is right, because, even the initial part of ORE analysis that has been performed to date has caused the project to rethink some aspects of the design.

2. Background

Ideally, to perform this study requires significant project documentation, particularly on the maintenance activities and how they are to be performed. In reality, however, very little information was available, at the time of the study. Moreover, the little that was available was mostly conceptual—i.e., the maintenance activities are known only at the concept level.

In the absence of the necessary maintenance information, required to perform this task, we needed to modify the anticipated evaluation methodology to cope with the reality of the situation. Accordingly, we used the Work Breakdown Structure (WBS) as the basis for this study. The evaluation methodology is described in the following section.

3. Methodology

In an attempt to demonstrate to the licensing authorities that, with respect to maintenance incidents, all bases have been covered, we have used a methodology that is both systematic and comprehensive. We have used the WBS to identify all key components and systems that need to be maintained. For each WBS unit, we have attempted to identify the sources of radiation that could be mobilized during a maintenance mishap. When a source of radiation was identified, we then attempted to identify the sources of energy that could lead to the mobilization of the radioactive material. Accordingly, when a source of radiation and energy are present simultaneously, there exists the potential for a radiation overexposure during a maintenance mishap. The last step, then, was to identify the possible mishaps that could lead to the overexposure.

Experience from nuclear power plants indicates that radiation overexposures do occur and can account for a few percent of the annual exposure [2]. Experience also indicates that there are three categories of events that can lead to unplanned radiation exposure. They are:

- Failures in administrative procedures, which allow planned work to be performed in areas with unmarked radiation hazards;
- Failures in executing maintenance or test procedures properly, which result in the creation of a hazardous situation; and
- Failures of components, which lead to radioactive releases inside the work area.

The first two are due to “human error”, while the last is due to hardware failures, or malfunctions. The nuclear power plant experience indicates that human error is the largest contributor to unplanned events and unplanned exposures.

The focus of the study was thus human error during maintenance activities. Clearly, before any maintenance is performed in a nuclear facility, there must be an approved work plan. Part of the approval process is a review by different disciplinary groups to ensure that the proposed work can be performed safely and that the radiation risks have been made as low as reasonably possible. Specifically, such approved procedures would prevent maintenance work to be performed on the pressure/vacuum boundary of a system that is pressurized/depressurized, for example. Similarly, if the system to be worked upon is connected to a pressurized/depressurized system, then the valves isolating the pressurized/depressurized system would be required to be closed and locked in the closed position during the maintenance work. These are clearly trivial examples, and are used only to illustrate the type of considerations that are given to work plans.

Nevertheless, as noted above, experience from the nuclear industry has shown that even under such well-planned and managed conditions human error is still possible. According to nuclear industry experience, typical human errors include:

- Failure to execute the maintenance procedures properly (i.e., failure to close an isolation valve);
- Failure to identify the correct system (i.e., the tritium supply system is selected instead of the deuterium supply system); and
- Failure to identify the correct component (i.e., when there are multiple components on the same system).

Nuclear industry experience has shown that through the use of quality improvement processes, which include well-planned procedures and worker training, human error can be significantly reduced, but not totally eliminated. Therefore, from a worker safety perspective, and regulatory perspective, when evaluating potential worker overexposures, it is necessary to assume that if an error can be committed, it will be committed. Once the consequences of the error have been properly assessed, the acceptability of such consequences will depend, in part, on the frequency associated with the consequences. The detailed evaluation of consequences, and associated frequencies, for potential overexposures identified by this study, will be undertaken in future studies.

Excluded from this study are unrelated failures—i.e., random failures occurring elsewhere, which might cause elevated radiation fields in the workplace being considered. In other words, the maintenance worker may be following the procedure perfectly, with no error, but an equipment failure elsewhere, or the error of another worker elsewhere, may cause him/her an overexposure. These situations are rare and complex to evaluate systematically and comprehensively.

4. Maintenance

The continued functioning of the tokamak with an acceptable level of availability and reliability requires a well-planned maintenance program. Such a maintenance program would have the following elements: daily checks, annual maintenance and periodic maintenance. The purpose of the daily checks is to confirm that critical components are operating within the specified range of performance. The purpose of annual maintenance is to replace consumable components and to check whether the system can continue to function properly during the following year. Finally, the purpose of periodic inspection is to check major components for pressure/vacuum boundary integrity. The first two are commonly referred to as routine maintenance, and the latter as in-service inspection.

Occasionally, equipment fails between maintenance periods and must be repaired. This is commonly referred to as unplanned maintenance. In most cases, the procedure for repairing, or replacing, a failed component is the same as that used for preventative maintenance—i.e., the planned maintenance procedure. In some cases, however, there are no planned maintenance procedures, because the component is designed to not require maintenance. Therefore, when such a component fails, it represents a special situation, and procedures have to be developed and approved after the fact. Clearly the evaluation of such situations is beyond the scope of this study.

It is the stated objective of the ITER project that, once the vacuum vessel is sufficiently activated, all in-vessel maintenance,