Reliability Engineering and System Safety 126 (2014) 153–165

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Evaluation of risk impact of changes to surveillance requirements addressing model and parameter uncertainties

S. Martorell [a,*], M. Villamizar [a], I. Martón [a], J.F. Villanueva [a], S. Carlos [a], A.I. Sánchez [b]

[a] Department of Chemical and Nuclear Engineering, Polytechnic University of Valencia, Valencia, Spain
[b] Department of Statistics and Operational Research, Polytechnic University of Valencia, Valencia, Spain

ARTICLE INFO

Article history:
Received 14 May 2013
Received in revised form
9 January 2014
Accepted 11 February 2014
Available online 18 February 2014

Keywords:
PRA
Surveillance requirements
Technical specifications
Risk evaluation
Model and parameter uncertainty

ABSTRACT

This paper presents a three steps based approach for the evaluation of risk impact of changes to Surveillance Requirements based on the use of the Probabilistic Risk Assessment and addressing identification, treatment and analysis of model and parameter uncertainties in an integrated manner. The paper includes also an example of application that focuses on the evaluation of the risk impact of a Surveillance Frequency change for the Reactor Protection System of a Nuclear Power Plant using a level 1 Probabilistic Risk Assessment. Surveillance Requirements are part of Technical Specifications that are included into the Licensing Basis for operation of Nuclear Power Plants. Surveillance Requirements aim at limiting risk of undetected downtimes of safety related equipment by imposing equipment operability checks, which consist of testing of equipment operational parameters with established Surveillance Frequency and Test Strategy.

1. Introduction

Safe operation of Nuclear Power Plants (NPP) depends on Technical Specifications (TS), so that TS are part of the Licensing Basis (LB) to operate a NPP. They were established taking into account mainly deterministic criteria. The development of Probabilistic Risk Assessment (PRA) and its application since the early 80s to analyze TS changes has brought the opportunity to review TS consistency from a risk viewpoint, i.e. evaluation of risk impact of changes on plant safety on the basis of the risk information provided by the PRA. In particular, main attention has been paid to the role of the Surveillance Frequency (SF) as part of Surveillance Requirements (SR) and of the Completion Time (CT) as part of Limiting Conditions for Operation (LCO).

In August 1995, the US Nuclear Regulatory Commission (NRC) adopted a final policy statement on the expanded use of PRA methods in nuclear activities that includes the following [1]. The use of the PRA technology and associated analyses (e.g. sensitivity studies, uncertainty analyses and importance measures) should be used in all regulatory matters to the extent supported by the state-of-art in PRA methods and data and in a manner that complements the NRC's deterministic approach. PRA evaluations in support of regulatory decisions should be as realistic as practicable. The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments.

The Nuclear Community has been encouraging the use of PRA to support a risk-informed decision-making framework [2]. In this context, the NRC issued the first draft of Regulatory Guide RG 1.174 in 1998 [3], which remains a major milestone in the NRC initiative to risk-inform the regulations on changes to LB. RG 1.174 introduces the five principles of the risk-informed decision-making to be used for making decisions regarding plant-specific changes to LB. The fourth principle states: “When proposed changes result in an increase in core damage frequency or risk, the increases should

Abbreviations: AS, Automatic scram; B, Birnbaum importance measure; CCF, Common cause failure; CDF, Core damage frequency; CM, Corrective maintenance; CRMS, Control room manual scram; CT, Completion time; FCDE, Final core damage equation; FFNCT, Fraction of failures no covered by testing; FV, Fussel–Vesely importance measure; GAM, Generalized additive model; HEP, Human error probability; ICCDP, Incremental conditional core damage probability; ILERP, Incremental conditional large early release probability; LB, Licensing basis; LCO, Limiting condition for operation; LERF, Large early release frequency; MTBRT, Mean time between reactor trips; MCS, Monte Carlo sampling; NRC, Nuclear regulatory commission; NPP, Nuclear power plant; PFD, Probability of failure on demand; PM, Preventive maintenance; PRA, Probabilistic risk assessment; PWR, Pressurized water reactor; RAMS, Reliability availability maintainability and safety; RAW, Risk achievement worth importance measure; RPS, Reactor Protection System; RRW, Risk reduction worth importance measure; SA, Sensitivity analysis; SIL, Safety integrity level; SR, Surveillance requirement; SF, Surveillance frequency; TI, Test interval; TS, Technical specifications

* Corresponding author.
E-mail address: smartore@iqn.upv.es (S. Martorell).

http://dx.doi.org/10.1016/j.ress.2014.02.003
0951-8320

be small and consistent with the intent of the Commission's Safety Goal Policy Statement". This principle is the one we are concerned with in this paper. Risk and risk increase are quantified using PRA, i.e. using the Core Damage Frequency (CDF) derived from a level 1 PRA and/or the Large Early Release Frequency (LERF) derived from a level 2 PRA. The Guide defines acceptable ranges of values for the possible increase in CDF and LERF. It also recognizes that the scope, level of detail and technical acceptability of the PRA should commensurate with the application. Caruso et al. [4] presents an approach for using risk assessment in risk-informed decisions on plant-specific changes to licensing basis that is based on the first draft of RG 1.174.

Since then, the risk-informed process introduced in RG 1.174 has evolved into a suite of regulatory guides and NUREG reports that define an integrated approach to risk-informed regulation [3,5–10]. Nowadays, there are draft versions of Revision 3 to RG 1.174 (DG-1285) and Revision 2 to RG 1.177 (DG-1287). RG 1.174 [3] presents a framework umbrella for using PRA in risk-informed decision-making on specific changes to licensing basis, while RG 1.177 [5] proposes a more specific approach that focuses, in particular, on plant specific changes to TS, e.g. LCO and SR, which are parts of the licensing basis as introduced early in this section.

The original US NRC policy statement in 1995 and the first drafts of RG 1.174 and RG 1.177 in 1998 already established that all sources of uncertainty must be identified and analyzed such that their impacts are understood. Prior work in this field has already faced the problem of addressing uncertainties in reliability and risk based decision making on changes to licensing basis and particularly to TS [11–18]. However, comprehensive guidance on the systematic treatment of epistemic uncertainties associated with the specific use of the PRA in risk-informed decision making of changes to LB has expanded mainly in the last years [8,19–20]. Moreover, no specific guidance has been proposed yet for the treatment and analysis of epistemic uncertainties particularly in evaluating the risk impact of changes to TS based on the use of the PRA; therefore, there was a need of adapting the generic guidance for LB changes to this particular PRA based application. This was the aim of the work published in Refs. [21–23], which show the origins of a methodology that has evolved into the integrated approach proposed in this paper.

This paper presents the framework and proposes three steps based approach, i.e. risk modeling, risk assessment and risk analysis, for the evaluation of risk impact of changes to Surveillance Requirements in TS based on the use of the PRA, which includes identification, treatment and analysis of model and parameter uncertainties in an integrated manner. It is coherent with the integrated approach to risk-informed decision-making defined by the suite of guides and reports introduced above.

The paper is organized as follows. Section 2 introduces an overview of a Nuclear Power Plant Technical Specification paying attention to the role of the Surveillance Requirements and Surveillance Frequency. Section 3 presents the framework for the evaluation of risk impact of changes to Technical Specification addressing uncertainties while Section 4 presents three steps based approach proposed for the evaluation of the risk impact of a SR change addressing model and parameter uncertainties. Section 5 presents the results of the example of application that focuses on the evaluation of risk impact of a change to Surveillance Frequency of the Reactor Protection System of a Pressurized Water Reactor Nuclear Power Plant using a level 1 PRA at power and considering internal events only, i.e. adopting the CDF as risk measure. Section 6 presents the concluding remarks.

2. Role of surveillance requirements

Fig. 1 shows a schematic view of typical Technical Specification (TS) of a safety system of a Nuclear Power Plant (NPP), which consists of several sections, being Limiting Condition for Operation and Surveillance Requirement the only ones relevant herein. The Reactor Protection System (RPS) of a Pressurized Water Reactor is considered. The RPS consists of two redundant channels.

TS Applicability covers operational modes 1–5, which ranges from full power operational mode to cold shutdown. In particular, TS for RPS during NPP operation at full power, i.e. during Operational Mode 1, require operability of two redundant channels. Then, Actions are required when one channel is found inoperable, which normally involves management of risky configurations, adoption of compensatory measures and Completion Time, transitions, and end states. Unavailability of the RPS normally obeys two circumstances: (1) forced; i.e. entering the LCO to restore the operability of the faulty equipment, or to perform whatever form of corrective maintenance (CM), (2) scheduled or unforced; i.e. entering the LCO under a scheduled activity, for example to perform preventive maintenance (PM) or testing the RPS. On the other hand, SR is intended to demonstrate operability of RPS, imposing the functional tests of redundant channels with an established period, i.e. Surveillance Frequency, and test strategy.

Therefore, Surveillance Requirement involves periodic tests, e.g. monthly or quarterly. Test interval is established by means of Surveillance Frequency. The primary purpose of testing is to assure that equipment of safety systems normally in standby will be operable when needed in case of accident. By testing equipment, failures can be detected that may have occurred since the last test or the time when the equipment was last known to be operational.

The positive effect of testing is its capability to detect hidden failures and this way limiting the risk of undetected downtimes of the safety component, i.e. the "test-limited" risk, which depends on the equipment unreliability characteristics, i.e. equipment failure rate, and the Surveillance Frequency, i.e. test interval. However, some tests may have an adverse impact on safety because of their undesirable effects, i.e. "test-caused" risk, such as for example test errors causing plant transients, wear out of equipment due to testing, etc. Often, a very important adverse effect is the one called the detected downtime effect that represents the time the equipment is out of service for testing. Thus, this adverse effect depends on the testing characteristics of the equipment. In particular for the RPS, Surveillance Requirements impose a reconfiguration of the system when the main equipment is being tested, which consist of connecting additional equipment to minimize such downtime effect. Also TS, throughout their LCO, establishes the maximum Completion Time of equipment to limit this detected downtime effect.

In general, the undesirable effects will be reduced if the SF is decreased, because then fewer tests will be conducted. By reducing the SF we also can obtain the additional benefit of reducing resources on testing. However, an important disadvantage here is that the fault-exposure time, i.e. the time during which the component will be subject to hidden failures during standby, will correspondingly increase as the SF decreases, i.e. the positive effect of the test limiting risk of undetected downtimes is reduced as well.

NPP safety systems consist of a number of redundant and diverse trains, each one consisting of highly reliable equipment, normally in standby, which must perform the intended safety function. Test Strategy establishes the grouping of equipment undertaken the test simultaneously, e.g. a full train, and the scheduling of the tests of the several groups, each group consisting of equipment in one of the redundant trains. Normally, the same SF applies to equipment of the redundant trains. However, the test-limited risk will depend of the relative scheduling of the tests of the redundant trains, i.e. the test strategy. Often, standard PRA quantification of the test-limited risk assumes that the relative test times of redundant components follow no specific schedule and are randomly placed with regard to one another. By staggering the