Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 92 (2007) 1435–1447
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Importance measures and genetic algorithms for designing a risk-informed optimally balanced system

Enrico Zio[a], Luca Podofillini[b,*]

[a]Department of Nuclear Engineering, Polytechnic of Milan, Via Ponzio 34/3, 20133 Milan, Italy
[b]Paul Scherrer Institute, CH-5232 Villigen PSI, Switzerland

Received 30 May 2006; received in revised form 12 September 2006; accepted 14 September 2006
Available online 13 November 2006

Abstract

This paper deals with the use of importance measures for the risk-informed optimization of system design and management. An optimization approach is presented in which the information provided by the importance measures is incorporated in the formulation of a multi-objective optimization problem to drive the design towards a solution which, besides being optimal from the points of view of economics and safety, is also 'balanced' in the sense that all components have similar importance values. The approach allows identifying design systems without bottlenecks or unnecessarily high-performing components and with test/maintenance activities calibrated according to the components' importance ranking. The approach is tested at first against a multi-state system design optimization problem in which off-the-shelf components have to be properly allocated. Then, the more realistic problem of risk-informed optimization of the technical specifications of a safety system of a nuclear power plant is addressed.

Keywords: Importance measures; Risk-informed optimization; Genetic Algorithms; Technical specifications; Multi-objective optimization

1. Introduction

The general goal of risk-informed applications is to make requirements on operation and maintenance activities more risk-effective and less costly by better focusing on what is risk-important [1–6]. To this aim, importance measures (IMs) are used to quantify the risk- or safety-significance of components or, more generally, basic events, according to specific views of their role within the system [6–8].

This paper proposes a risk-informed approach to system design and management in which the information provided by the importance measures is incorporated in the formulation of a multiobjective optimization problem to drive the design towards a solution which, besides being optimal from the points of view of economics and safety, is also 'balanced' in the sense that all components have similar importance values, without bottlenecks or unnecessarily high-performing components, and test/maintenance activities are calibrated according to the components' importance ranking.

The paper is organized as follows. In Section 2, the risk-informed optimization problem is formulated and the proposed "balancing" objective function is introduced, along with the motivations which lead us to use Genetic Algorithms (GAs) for the optimization [12]. In Section 3, a simple case study is presented in which a multi-state system [9] has to be designed selecting off-the-shelf multi-state components. The problem is purposely built in such a way that the search space is small enough that the Pareto-optimal solutions can be identified by crude enumeration and evaluation of all possible alternatives. This allows the direct verification of the approach. The aim of the application is to show how the proposed optimization approach can be used at the system design stage in order to

Abbreviations: AFW, auxiliary feedwater; GA, Genetic Algorithms; HPIS, high pressure injection system; IMs, importance measures; LPIS, low pressure injection system; MCS, minimal cut sets; PWR, pressurized water reactor; RWST, refueling water storage tank; S&M, surveillance and maintenance; TI, test interval; TS, technical specification; VCT, volume control tank

*Corresponding author.
E-mail addresses: enrico.zio@polimi.it (E. Zio), luca.podofillini@psi.ch (L. Podofillini).

0951-8320/$ - see front matter
doi:10.1016/j.ress.2006.09.011

limit over-performances and bottleneck effects. Then, in Section 4, a more realistic problem is addressed regarding the risk-informed optimization of the technical specifications regulating the component's inspection intervals of a safety system of a nuclear power plant, the high pressure injection system (HPIS) of a pressurized water reactor (PWR) [14]. Conclusions are provided in Section 5.

2. The "balanced" optimization problem

The general goal behind risk-informed applications is to rationally manage and improve the safety and economical performance of complex systems and plants [1–6].

In practice, the analyst is typically faced with the challenge of simultaneously achieving several targets (e.g. low costs, high revenues, high reliability, low accident risks). Typically, the targets related to the economical performance and those related to the safety performance may very well be in conflict so that the final choice is necessarily a compromised solution.

Formally, the problem may be cast within an optimization framework in which a vector $\boldsymbol{y}$ of N_f objective functions, e.g. the system unreliability, unavailability, risk, profit, is to be optimized [14]:

$$y = f(\gamma) = (f_1(\gamma), f_2(\gamma), \ldots, f_{Nf}(\gamma)) \tag{1}$$

subjected to a vector $\boldsymbol{g}$ of N_g constraints:

$$g(\gamma) = (g_1(\gamma),\ g_2(\gamma), \ldots, g_{Ng}(\gamma)) \leqslant 0, \tag{2}$$

where $\boldsymbol{\gamma}$ is the vector of the decision variables encoding a particular system design and/or maintenance strategy.

A driving principle for risk-informed applications is that of the consistency of resources allocation: information related to the risk contributors is to be used to focus resources and regulations on what is risk-important while avoiding unnecessary expenditures, constraints and regulatory burdens on what is risk-unimportant [1–6]. In this perspective, importance measures (IMs) are used to quantify the risk- or safety-significance of components or, more generally, basic events [6–8]. Different definitions of IMs have been proposed and used, according to different views of the role of components within a system. The definitions of some frequently used IMs are summarized in Appendix A, for convenience.

The risk-consistent use of information from IMs is twofold [6]. From one side, the classical focus is on the high-significance risk group, for effectively reducing the risk associated to plant operation by prioritizing inspection and maintenance procedures and/or allocating redundancies and/or more reliable components for the most risk-relevant units. On the other side, the lowest risk contributors, which were paid less attention in the past, become relevant for identifying unnecessary expenditures and regulatory burdens and for rendering operation and maintenance procedures more efficient. In this dual perspective, a standard risk-informed application concerns the relaxation of requirements imposed on components and events of low risk significance, after having verified that relaxing these requirements results in at most only small risk increases, well within the allowed margins [1–6].

From the risk-consistency principle, it follows that a desirable system property is that of being 'balanced' with respect to the risk contributions of its components: for example, operation and maintenance activities should be stressed for high-importance components, with the effect of reducing their contribution to the system risk, whereas they should be relaxed on low-importance components, with the effect of increasing the system profit, albeit at the expense of a controlled increase of their contribution to the system risk.

This paper investigates the effect of introducing an "importance balancing" objective in the multiobjective optimization problem formalized by Eqs. (1) and (2). More specifically, in addition to the usual safety- and profit-related optimization targets, the following importance balance function b_I is considered, with reference to a generic importance measure I:

$$b_I = \frac{1}{\sigma_I} = \frac{1}{\sqrt{(\bar{I}^2 - \bar{I}^2)}}; \quad \bar{I}^2 = \frac{1}{n}\sum_{j=1}^{n} I_j^2; \quad \bar{I} = \frac{1}{n}\sum_{j=1}^{n} I_j. \tag{3}$$

Note that if the importances I_j, $j = 1, 2, \ldots, n$, were the same for all components then $\sigma_I = 0$ and $b_I = \infty$, i.e. the system is fully balanced, free of bottlenecks or overly-reliable components.

Concerning the multiobjective problem, a common way to tackle it is that of focusing the optimization on a single objective constituted by a weighed combination of some of the targets while imposing some constraints to satisfy other targets and requirements [10]. This approach, however, introduces a strong arbitrariness in the a priori definition of the weights and constraints levels associated to the subjective homogenization of physically different targets, usually all translated in monetary terms. A more informative approach is one which considers all individual targets separately, aiming at identifying a set of solutions which are equivalent in absence of an assigned ranking of the various objectives [10]. Each member of this set is better or equal to the others of the set with respect to some, but not all, of the targets. Differently from the single objective approach the set identified by the multiobjective approach provides a spectrum of 'acceptable' solutions among which a compromise may be found.

In this work, the multiobjective approach is espoused.

Concerning the actual multiobjective optimization algorithm, practical risk-informed applications often involve a search among a large number of potential alternatives so that the problem becomes NP-hard, and thus difficult to tackle with classical optimization methods, e.g. of the gradient–descent kind [10]. Moreover, these methods encounter severe difficulties when the objective functions to be optimized are embedded in a complicated computer code from which differential information is not easily retrieved. This is the case of the realistic, detailed models