Reliability Engineering and System Safety 145 (2016) 329–340

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Developing probabilistic safety performance margins for unknown and underappreciated risks

Allan Benjamin [a,*], Homayoon Dezfuli [b], Chris Everett [c]

[a] Independent Consultant, Albuquerque, NM, USA
[b] Office of Safety & Mission Assurance, NASA Headquarters, Washington, DC, USA
[c] Information Systems Laboratories, Inc., Rockville, MD, USA

ARTICLE INFO

Available online 30 July 2015

Keywords:
Probabilistic
Safety performance margin
Safety performance requirement
Safety threshold
Safety goal
Unknown risk
Underappreciated risk

ABSTRACT

Probabilistic safety requirements currently formulated or proposed for space systems, nuclear reactor systems, nuclear weapon systems, and other types of systems that have a low-probability potential for high-consequence accidents depend on showing that the probability of such accidents is below a specified safety threshold or goal. Verification of compliance depends heavily upon synthetic modeling techniques such as PRA. To determine whether or not a system meets its probabilistic requirements, it is necessary to consider whether there are significant risks that are not fully considered in the PRA either because they are not known at the time or because their importance is not fully understood. The ultimate objective is to establish a reasonable margin to account for the difference between known risks and actual risks in attempting to validate compliance with a probabilistic safety threshold or goal. In this paper, we examine data accumulated over the past 60 years primarily from the space program, and secondarily from nuclear reactor experience, aircraft systems, and human reliability experience to formulate guidelines for estimating probabilistic margins to account for risks that are initially unknown or underappreciated. The formulation includes a review of the safety literature to identify the principal causes of such risks.

1. Introduction

1.1. Concern about the underestimation of safety risk

Probabilistic safety requirements currently formulated or proposed for complex systems such as space systems and commercial nuclear reactors depend on showing that the probability of loss (e.g., loss of crew, loss of vehicle, loss of mission, loss of core integrity, loss of public life or health) is below a specified safety threshold or goal. There has been concern that proof of compliance with such requirements depends heavily upon the ability of probabilistic risk assessment (PRA) to accurately predict these loss probabilities. To determine whether or not a system meets the probabilistic safety thresholds and goals set by systems engineering or by executive management, it is necessary to consider whether there are significant risk scenarios[1] that are not fully considered in the system's PRA either because they are not known at the time or because their importance is not fully understood. This evaluation must be performed throughout the project timeline, even when the system is still in the concept stage.

Risk model completeness has long been recognized as a challenge for synthetic[2] methods of risk analysis such as PRA as traditionally practiced [1]. These methods are generally effective at identifying system failures that result from combinations of component failures that propagate through the system due to the functional dependencies of the system that are represented in the risk model. However, they are typically ineffective at identifying system failures that result from unknown or underappreciated (UU) risks, frequently involving complex intra-system interactions that may have little to do with the intentionally engineered functional relationships of the system.

* Corresponding author.
E-mail addresses: asbenja@q.com (A. Benjamin), hdezfuli@nasa.gov (H. Dezfuli), ceverett@islinc.com (C. Everett).

[1] The terms "risk scenario" and "risk" are taken to be synonymous for purposes of this paper. Identification of a risk scenario, or risk, involves identification of a set of present conditions, a possible future departure from expectation, and a resulting consequence. Evaluation of the risk scenario, or risk, involves an estimation of the probability of occurrence of the departure and the severity of the consequence.

[2] By "synthetic methods," we mean methods that produce estimates of loss probabilities by explicitly constructing a scenario set and summing risk contributions to obtain an estimate of aggregate risk.

http://dx.doi.org/10.1016/j.ress.2015.07.021
0951-8320/

For example, underappreciated scenarios were operative in both the Challenger and Columbia space vehicle disasters. In the Challenger accident, O-ring blow-by impinged on the external tank, leading to tank rupture and subsequent loss of crew. In the Columbia accident, insulating foam from the external tank impacted the wing leading edge reinforced carbon–carbon (RCC), puncturing it and allowing an entryway for hot plasma upon reentry into the Earth's atmosphere. Because of the complex interactions involved in such scenarios, they tend not to be revealed by subsystem testing. Full-up testing has the potential to reveal them, but the cost of full-up testing in as-flown environments is generally too high to allow a quantity of tests that would demonstrate low probabilities of occurrence.

1.2. The importance of realistic safety performance margins

Traditionally, safety performance policies in the space, nuclear reactor, and nuclear weapon sectors have encouraged the use of PRA but have not required margins to be considered when determining whether or not calculated probabilities of loss of crew, mission, core integrity, etc., fall within specified thresholds or goals [2–4]. These policies are in sharp contrast with policies for certain other measures of performance, such as cost, schedule, mass, and technical capabilities (e.g., thrust, range, or operating life), where providers are routinely required to apply margins or reserves that conform to specified standards. The lack of margin requirements for probabilistic safety performance measures has been seriously questioned by the NASA Aerospace Safety Advisory Panel (ASAP), whose 2014 annual report to the NASA Administrator and to the Congress [5] included the following admonition: "Great care must be exercised by all stakeholders to remember that actual risk for the SLS [Space Launch System] and Orion, especially during early operations, could be significantly higher than the calculated or 'advertised' risk, and a healthy margin should be maintained between the PRA risk assessment calculated numbers and the minimum acceptable safety threshold." The ASAP report also noted, in reference to our earlier work preceding this paper, that "the NASA System Safety Handbook, Volume 1, System Safety Framework and Concepts for Implementation, NASA SP-2010-580, Section 3.1.1.4, calls for programs to allow a 'management reserve' or margin between the PRA-calculated risk (Probability of Loss of Crew) and the maximum acceptable risk for the program (the threshold specified by the decision authority)."

Not accounting for margins in the evaluation of safety performance is tantamount to assuming that the UU risks are small compared to risks that are known and fully understood. Such an assumption is not only counter-intuitive but also introduces a substantial cognitive risk: the risk that decision makers will assume that a system meets all thresholds and goals within an acceptable tolerance when in fact it does not. Thus, as the ASAP has stated, it is critical that a rationale for safety performance margins be developed and that this rationale be incorporated into standards of practice.

1.3. Relationship between unexpected cost overruns and unexpected safety performance risks

We wish to explore whether safety risks are being systematically underestimated in large-scale, complex programs, but before doing so, it is instructive to consider how cost risks tend to be systematically underestimated in such programs. The latter may provide insights about the former.

Following are some examples of large cost overruns that have occurred for various space programs[3]:

- In the Apollo program, when President Kennedy first chartered the Moon landing in 1962, the preliminary cost estimate was $7 billion (about $53 billion in today's dollars). An itemized NASA estimate in early 1969 put the total run-out cost at $24 billion (about $160 billion in today's dollars), a factor of 3 times the original estimate.
- For the Space Shuttle, the expected total cost of the program was estimated to be $7.45 billion in 1970 (about $46 billion in today's dollars). The actual total cost of the program was $196 billion as of its retirement in 2011 (about $210 billion in today's dollars), a factor of 4.6 times the original estimate.
- The total cost of the Hubble Space Telescope program was originally estimated at $1.1 billion in 1980 (about $3.2 billion in today's dollars). The actual total cost in 2010 was about $10 billion (about 10.7 billion in today's dollars), a factor of 3.3 times the original estimate.
- According to the Government Accounting Office [6], the anticipated total life cycle cost of the James Webb Space Telescope has escalated from $1.6 billion in 1996 ($2.5 billion in today's dollars) to $8.8 billion in 2013 ($9.1 billion in today's dollars), a factor of 3.6. GAO's report warns of further possible cost increases before launch in 2018 because of diminishing cost and schedule reserves.

Researchers at the Jet Propulsion Laboratory [7] have reported, based on an analysis of 34 NASA missions (see Fig. 1), that the tendency to underestimate total costs occurs regardless of the size of the project and that "[cost] reserve estimation accuracy has not improved in the last 20 years." Various reasons have been proffered for such systematic underestimation of cost risks. In 2012, for example, a report by the NASA Inspector General [8] highlighted the following four main factors for unexpected cost and schedule growth:

- a culture of over-optimism (i.e., a positive "can-do" attitude that has paradoxically made NASA both technically innovating and susceptible to cost overruns)
- the technological complexity inherent in most NASA projects
- unstable funding, both in terms of the total amount of funds dedicated to a project and the timing of when those funds are disbursed to the project
- a decrease in the number of smaller projects on which aspiring managers can gain hands-on experience

Earlier in 2009, the NASA Advisory Council noted the following set of contributory factors[4]:

- inadequate definitions prior to agency budget decision and to external commitments
- optimistic cost estimates/estimating errors
- inability to execute initial schedule baseline
- inadequate risk assessments
- higher technical complexity of projects than anticipated
- changes in scope (design/content)
- inadequate assessment of impacts of schedule changes on cost
- annual funding instability
- eroding in-house technical expertise
- poor tracking of contractor requirements against plans
- reserve position adequacy
- lack of probabilistic estimating
- "go as you can afford" approach

[3] Figures quoted were obtained from wikipedia.

[4] (see website www.nasa.gov/pdf/314880main_AFC_KSC_NCA_Feb-5-2009.pdf)