International Journal of Disaster Risk Reduction 6 (2013) 59–66

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

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

Exploring the limits of safety analysis in complex technological systems

D. Sornette [a,*], T. Maillart [b], W. Kröger [c]

[a] Department of Management, Technology and Economics, ETH Zurich, Scheuchzerstrasse 7, CH-8092 Zurich, Switzerland
[b] Department of Humanities, Social and Political Sciences, ETH Zurich, Ramistrasse 101, CH-8092 Zurich, Switzerland
[c] Risk Center, ETH Zurich, Scheuchzerstrasse 7, CH-8092 Zurich, Switzerland

ARTICLE INFO

Article history:
Received 26 July 2012
Received in revised form
2 April 2013
Accepted 3 April 2013
Available online 23 April 2013

Keywords:
Probabilistic safety assessment
Power law distribution
Cascades
Criticality
Nuclear safety

ABSTRACT

From biotechnology to cyber-risks, most extreme technological risks cannot be reliably estimated from historical statistics. Therefore, engineers resort to predictive methods, such as fault/event trees in the framework of *probabilistic safety assessment* (PSA), which consists in developing models to identify triggering events, potential accident scenarios, and estimate their severity and frequency. However, even the best safety analysis struggles to account for evolving risks resulting from inter-connected networks and cascade effects. Taking nuclear risks as an example, the predicted plant-specific distribution of losses is found to be significantly underestimated when compared with available empirical records. Using a novel database of 99 events with losses larger than \$50 000 constructed by Sovacool, we document a robust power law distribution with tail exponent $\mu \approx 0.7$. A simple cascade model suggests that the classification of the different possible safety regimes is intrinsically unstable in the presence of cascades. Additional continuous development and validation, making the best use of the experienced realized incidents, near misses and accidents, is urgently needed to address the existing known limitations of PSA when aiming at the estimation of total risks.

1. Introduction

Most innovations are adopted on the premise that the upside gains largely make up for the downside short- and long-term risks, in particular through the adoption of safety measures aiming at preventing or mitigating potential losses. But innovations are often disruptive and, by essence, break new ground. This implies that history is a poor guide for risk assessment due to the novelty of the technology and the corresponding insufficient statistics. For highly technical enterprises for which full scale experiments are beyond reach (such as the Internet and smart grid technologies and associated cyber-risks, technological and population growth and climate change, financial innovation and globalization and the dangers of systemic banking crises), engineers resort to simulation techniques and scenario-based analyses.

To be concrete, we restrict our discussion to the nuclear industry, which has been a leader in the development of state-of-the-art safety analysis, with outstanding efforts aimed at preventing incidents from becoming major accidents. For this, *probabilistic safety assessment* (PSA) has been developed as a decision support tool aiming at ensuring a high level of plant safety limiting the risks of possible release of radioactivity. PSA consists in developing fault and event tree models to simulate accidents, their different triggers and induced scenarios, their severities as well as their estimated frequency [1,2]. When performed as an on-going process continuously refined using the information of new examples, plant-specific safety analysis has proved very useful for the implementation of ever better safety barriers, keeping the advantages of the

[*] Corresponding author.
E-mail addresses: dsornette@ethz.ch (D. Sornette), tmaillart@ethz.ch (T. Maillart), kroeger@ethz.ch (W. Kröger).

2212-4209/\$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijdrr.2013.04.002

technology while reducing its undesirable dangers. PSA is a well-established discipline with growing applications in support of rational decision-making involving important technological and societal risks.

The article is organized as follows. Section 2 presents a brief description of the PSA methodology. Section 3 describes the main predictions of PSA with respect to the plant specific "core damage frequencies" and the "large early release frequencies", before comparing them quantitatively with the database of losses per event constructed by Sovacool [18], with special care to demonstrate the robustness of the reported power law distribution. Section 4 introduces and analyzes a simple conceptual model of cascades of failures that allows us to rationalize the discrepancy between predicted and realized losses. Section 5 concludes.

2. Brief description of probabilistic safety assessment (PSA)

PSA provides nuclear plant-specific information on risk metrics at three sequential levels of end states (levels 1–3). Level 1 corresponds to the assessment of the risk of a core damage (core damage frequency or CDF). Level 2 assesses the size of radioactive releases from the reactor building, in the event of an accident (large early release frequency or LERF), in order to develop accident management strategies and identify potential design weaknesses in reactor containment buildings. Core damage frequency (level 1) and large early release frequency (level 2) are regarded as representative surrogates to steer design and operations of systems towards achieving quantitative and qualitative safety goals. Level 3 evaluates the impact of such releases on the public and the environment and is used mainly for emergency planning. In the nuclear domain, PSA Levels 1 and 2 are required to support regulatory activities in most countries (e.g., in the US since 1995 to complement the deterministic approach within the framework for risk informed regulation). The PSA methodology has developed into national and international guidelines (for an history of PSA, see for instance in Ref. [3, Chapter 2.4] and in Ref. [4, Chapter II-b]). International guidelines are presented in Refs. [5–7] (for the later, see http://www-ns.iaea.org/standards/ for updates and revisions). This has resulted in widely established and used codes, such as SAPHIRE 8 (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations), MELCOR (see for instance Ref. [8]) and MACCS2 (MELCOR Accident Consequence Code System, Version 2).

Since many years, PSA is not thought to represent the true risks and to become generalized across sectors, countries and events without considerable adjustments. PSA is mainly thought of as a platform for technical exchanges on safety matters between regulators and the industry, among peers, between designers and operators [9]. PSA provides a rigorous and methodical way to steer towards measures to achieve safety goals by efficient use of resources and measures. PSA is a fairly well developed mature methodology, although diversely implemented and used in different countries, in particular in the choice of internal and external events that are included in the analysis.

The basic methodology of PSA is based on logic trees and human reliability analysis (HRA) incorporating unintentional failures only, with the uncertainty analysis being restricted to data variation that assumes traditional (Normal) distributions. Common cause failure (CCF) analysis is included by point estimates on fractions of the system, with rare event approximations and cut-sets with cut-off values for the quantification of fault trees and binning techniques to cope with the large number of sequences. PSA uses in general the assumption that a nuclear power plant is essentially a closed system, even under catastrophic accident conditions. There are considerable weaknesses concerning the neglect of cascades and the transformation of PSA modeling to consider the nuclear power plan as an open system with strong interactions with its environment as well as to include the importance of local conditions, in particular under severe accident conditions. PSA is limited to single units embedded in an ideal environment, in which a safety culture is assumed to be ensured, and for which atmospheric transport and dispersion dominate (thus neglecting other pathways). This has implications for the conclusions, when the nature of the triggering event (earthquakes, flooding/tsunamis) affect large areas, and/or other sources of radiation (spent fuel pool) exist, which are currently neglected. There is also limited feed of accident insights back into PSA methodology as well as few new approaches and models developed in other sectors and fields that influence PSA.

3. Confronting PSA with reality

3.1. *Understanding the predictions of PSA*

Probabilistic safety assessment is seldom used for communication but, in reality, it is sometimes used to support political decisions, within the public debate and by actors other than the nuclear industry such as the insurance industry. And this naturally raises the issue of the possible gaps between the occurrence of accidents, public perceptions and the predictions of PSA.

In order to frame correctly the discussion on how to use PSA to estimate risk surrogates such as core damage frequency (CDF) and large early release frequency (LERF), we stress again that the basic methods of PSA levels 1 and 2 use fault/event trees, human reliability analysis (HRA) and common cause failure (CCF), to model plant and operator behavior according to principles of reductionism in a plant specific way limited to single units. In this way, PSA models failure of safety systems using linear semi-dynamic causal chains, with binning techniques and many approximations allowing quantification. And severe accident management guidelines (SAMG) are taken into account in such framework, as long as they are planned and trained.

PSA level 3 studies are relatively rare, and uses of PSA to estimate risks for the public are mostly based on levels 1 and 2 studies, which make assumptions about population behavior, take deterministic (early) and stochastic (late cancer effects) into account for submersion, inhalation and ingestion exposure pathways. They are site-specific but extend the calculations of consequences to large distances