Safety Science 99 (2017) 140–155

Contents lists available at ScienceDirect

Safety Science

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

Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job?

Hans J. Pasman *, William J. Rogers, M. Sam Mannan

Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX 77843, United States

ARTICLE INFO

Article history:
Received 11 November 2016
Received in revised form 17 January 2017
Accepted 20 January 2017
Available online 1 February 2017

Keywords:
Process hazards
Consequence analysis
Hazard identification
Risk management

ABSTRACT

Much has been written about the value of risk assessment, in particular the quantified version, QRA, here considered in the context of industrial processing oil, gas, and chemicals. It is plagued by mistrust due in part because estimated uncertainties are generally not included. QRA is done for predictive purpose, to design risk reducing measures, and to base safety decisions on, but many major accidents occur according to scenarios not foreseen in the analysis. Yet, QRA forces us to think. Predicting what can happen under specified conditions is the most elementary step in better safety. So, we must improve the methods and in particular to model sensitive uncertainties and establish confidence limits about our predictions. The present paper will review in short the state of affairs, and it will summarize recent contributions shedding light of what is currently wrong with QRA. The paper will further present for the various aspects and steps to be done in a QRA directions, in which progress is being made and where promising possibilities may appear. The latter are according to the opinion and the scope of the authors, so hopefully there is much more! Anyhow, due to complexities of socio-technical systems a QRA will require more effort, so to keep it practical large scale application of computerization will be a must. And, to improve trust in QRA we must acknowledge variability and quantify the uncertainties as we see them; in addition, there will be hidden uncertainties, which gives reason to think in resilience terms too.

1. Introduction

1.1. Context and purpose of this paper

This contribution is made to the special issue of Safety Science under the heading "Risk Analysis Validation and Trust in Risk Management". The article is written from the point of view of predictive risk assessment with respect to industrial processes involving hazardous materials. This is with regard to the entire system of raw materials supply, conversion processes, storage, and product transportation. It also includes the storage and use of fuels in energy systems. It all poses a risk if process control is lost and/or process materials are inadvertently released from their containment. Such release can cause explosion, fire, and the dispersion of toxic clouds presenting a risk to health and life of workers, the public in the vicinity of the event location, and damage to assets and to the environment.[1] *Risk analysis* is performed both with respect to onshore and offshore installations. The analysis must lead to *assessment* and *decision making* about whether a risk can be tolerated.

More than 40 years ago with scale-up of the oil-based process industry the often disastrous accidents prompted risk analysis studies to determine distances to a risk source at which risk was judged sufficiently low. At first, these studies were conducted on the initiative of governmental authorities to enable decision making in view of *land use planning*, or stationary source siting as it is expressed in the U.S., because of possible threat to neighbors. But, where it became interesting to determine the effect of process and equipment options, in general the effect of risk reducing measures, optimal plant lay-out, vulnerability analysis in view of security, and planning of emergency response, companies also initiated studies on complex cases on their own. In a number of countries, e.g., in Europe, risk assessment became mandatory to perform as part of a *safety report* for obtaining a license to operate in case nature and corresponding amounts surpassed specific thresholds. After the Piper Alpha disaster in the North Sea in 1988, for offshore installations this developed to a '*safety case*'.

Although it is occurring in a quantitative fashion only in a limited number of countries, the analysis objective is control of risk and if needed to reduce it to at least a tolerable level, or even more

* Corresponding author.
E-mail address: hjpasman@gmail.com (H.J. Pasman).

[1] Assessment of environmental damage had for a long time in integral process risk assessments a low priority compared to human injury but this changed as a result of legislation, e.g., in Europe beginning with the Seveso II Directive in 1996 and even more since Seveso III Directive in 2012.

http://dx.doi.org/10.1016/j.ssci.2017.01.011
0925-7535/

desirable to an acceptable level. *Risk management* concerns the whole of analysis, weighting cost/benefit of measures and decision making. In case of onshore plant, the European Seveso Directive requires a safety report that "*should contain details of the establishment, the dangerous substances present, the installation or storage facilities, possible major-accident scenarios and risk analysis, prevention and intervention measures and the management systems available, in order to prevent and reduce the risk of major accidents and to enable the necessary steps to be taken to limit the consequences thereof*". Offshore installation owners/operators must prepare a 'safety case'. The term is borrowed from British defense requirements and, e.g., defined in a UK Defence Standard (DS 00-56, 2007) as "*a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment*". The EU Offshore Safety Directive (2013) requires from operators/owners that "*risk assessments and arrangements for major accident prevention should be clearly described and compiled in the report on major hazards*".

Risk assessments are performed in the design stage and at intervals of several years may be updated for the current state. Study detail and degree of quantification depends on the study's purpose and the complexity of the situation. Over time, the safety demand to reduce the chance of a fatality or a serious loss of containment in an industrial operation rose to become virtually zero. Apart from public pressure, companies realizing that cost of accident is high, put more emphasis on foresight and pro-active measures. This may appear from the continuously improving safety records of major companies (e.g., Pasman et al., 2015), although even in the best performing companies preventable accidents may still occur. An example of the latter is the 2014 Shell Moerdijk MSPO2 explosion (DSB, 2015). As a result of this overall trend, in recent years in the industry interest has developed in *operational risk assessment*. By nature, this will be for continuously changing situations, so the assessment must be *dynamic* instead of previously for a *static* situation. The objective may be to follow based on detection of *weak signals* relatively slow degradation processes, such as corrosion, to enable predictive maintenance, or change in safety culture requiring organizational measures, but it may also be to follow the real-time risk level of a process operation. Also, because of advances in sensor technology, the installation of process safety performance indicators to measure the quality of the safety management system, safety culture surveys, and the growth of digitization enabling large volumes of data to be stored, processed, merged, and analyzed, in the future *dynamic risk assessment* will become commonplace (Villa et al., 2016). Hence, it is useful to examine and evaluate the quality of the methodology and to see where improvements are needed.

1.2. Scrutiny of risk assessment results consistency

The methodology of risk analysis as such has been borrowed in the late 1960s, early 1970s from the nuclear community. The knowledge build-up and methodology with respect to the specific risks of process industry evolved quickly in the 1980s and as recent articles and conference papers show, it is still further developing. The three basic questions posed in the early days of risk assessment by Kaplan and Garrick (1981), consist of a systematic search for *what can go wrong*, with *what likelihood*, and *how severe the consequences*. Certainly, at the beginning much of risk analysis remained purely qualitative and comparative, so that at least risk ranking could be achieved. For the majority of applications in industry this is still the case distinguishing 'green' as safe, 'orange' as it may be unsafe, and 'red' as unsafe. Next, semi-quantitative solutions were derived by estimating orders of magnitude of consequences and probability values of events. Layer of protection analysis in its early-on application is an example. Yet, in the context of a regulatory application of a license to operate a plant, or in complicated situations for engineering an adequate design, a full quantification to QRA (quantitative risk assessment) became required forcing intense analysis of a case and including more detail.

After context of scope, system definition, tools, and assessment, criteria for a quantified analysis are fixed, as shown in Fig. 1 the three questions translate into the following six detailing steps: (1) process hazard analysis leading to hazard identification and resulting in scenario definitions, (2) calculation of physical effects of a mishap scenario and potential damage consequence distribution (the whole is called consequence analysis), (3) determination of a scenario probability distribution, (4) risk distribution as the combination of consequence and probability distributions, (5) considering risk reduction measures, (6) final risk tolerability and acceptance assessment (risk appraisal). Some countries, such as the Netherlands, introduced a fixed criterion for acceptable, involuntary posed risk of being killed by the risk source per unit of time: e.g., 10^{-6} per year, others defined certain physical effect thresholds, such as toxic concentrations, blast intensity or fire radiant heat levels (see e.g., Pasman et al., 2015, Chapter 2). As values diminish with distance to a risk source, both types of criteria can be shown as contours around the risk source.

In the second half of the 1980s the EU became a sponsor of risk analysis research projects, initially with emphasis on heavy gas dispersion and vapor cloud explosion. This was to further develop knowledge and, consistent with the Seveso directives, to prevent major hazard accidents, to facilitate and to harmonize application procedures in the Member States. Because risk results of different groups often varied by orders of magnitude, there have been two EU benchmark projects to compare risk figures based on a given plant. In both cases this concerned an ammonia storage plant.

As reported by Amendola et al. (1992) under management by the EU Joint Research Centre, eleven teams from different countries participated in the first project from 1988 to 1990. Two main, so-called Working Phases were defined, the first a complete risk analysis, while in the second a guillotine pipe fracture leak scenario was given. The result of the first phase showed risk figures differing over 2–4 orders of magnitude depending on distance to the risk source (the largest, the closest). There were differences in scenario definition, leak modeling, dispersion concentration, and in addition uncertainty in NH_3 toxicity vulnerability as a function of concentration. In phase 2, which should have been much less uncertain, risk values still spread over 6 orders of magnitude at larger distance of the risk source, although concentration figures differed by only 2 orders. So, it became clear that the spread in risk value derived from consequence analysis and probability estimates a factor to reckon with. This project was followed in 1994 by a pure comparison of ten well known gas dispersion models as described by Brighton et al. (1994). The model parameters had been 'calibrated' to the same large scale test results. Yet, the results differed by a factor 2–3. This all prompted the EU project SMEDIS (Scientific Model Evaluation of Dense Gas Dispersion) described by Duijm et al. (1997). The goal was to separate the 'black sheep from the whites' by following a structured procedure (protocol) examining and categorizing the model with respect to its application (type of terrain etc.), physics (completeness, assumptions), user aspects, verifying the coding, and validating it against selected large-scale tests.

The second multi-team benchmark project, called ASSURANCE, came about a decade after the first. Lauridsen et al. (2002) reported the findings of a full risk analysis on the same type of ammonia plant, this time conducted by seven in risk analysis highly skilled teams. It was hoped, of course, that reproducibility would have