COMPUTER-AIDED HAZARD LIFECYCLE-ORIENTED SAFETY ENGINEERING: CONCEPT AND FUNCTIONAL REQUIREMENTS

Igor .A. Kirillov[1], Alexander V. Panasenko[2], Igor E. Lukashevich[1], Alexey I. Lobanov[3]
[1] Russian Research Centre "Kurchatov Institute", Moscow, 123182, Russia
[2] Central Research Institute of Machine Building, Korolev, 121439, Russia
[3] Moscow Institute of Physics and Technology, Dolgoprudny, 141700, Russia

Abstract

As well as in the nuclear and offshore oil applications, the computer-aided quantitative safety analysis, physico-chemical modeling and detailed numerical simulation of the hazardous phenomena (constituents of accident) or evaluation of inventory properties (reactivity or energy potential) can be valuable engineering techniques to improve the Chemical Process Industries safety. Concept of hazard life cycle is introduced in addition to the known process and design lifecycles. Report describes a hazard lifecycle-oriented approach to safety engineering of the chemistry- or energy-loaded industrial processes and units. Proposed generalized framework invites the safety-concerned experts not limit oneselves to estimate the macroscopic ("post-accident") consequences, required by acting legislation, but to analyze the causes of, to reveal the critical conditions and criteria for, to simulate the basic driving mechanisms of the hypothetical accidents at the micro- ("pre-") and mesoscopic ("in-accident") scales (stages). The modeling and simulation results, obtained with the hazard lifecycle perspective in mind, can also be indispensable for digital prototyping and virtual testing of the "inherently-safe" designs. The functional requirements for integrated simulation software, targeted to practical implementation of the proposed approach, are discussed on the base of experience, obtained in Kurchatov Institute.

Keywords

Chemical process, Safety engineering, Life cycle, Multi-physics phenomena, Numerical simulation, Computer-aided, Reaction analysis and modeling, Integrated software tools.

Introduction

Idea - to use a computer-aided analysis and modeling of the hazardous multiphysics phenomena (for example, reactive runaway in multiphase, mechanically stirred reactor, gaseous dispersion, detonation, etc.) as one of the tools to improve a chemical process safety – has a relatively long history (see, e.g., Rotman, 1996; Pitt, 1996; Kirillov, 1996; Preston, 1997; Dimitriadis, 1997).

Important role, which process modeling plays within the process lifecycle, and the appropriate problems, associated with a phenomenon-oriented modeling, were discussed by Eggersmann (2001) and Hackenberg (2001). The focus of their analysis was on the process engineering applications (design, control, operation), which take place under "normal" operational conditions. Process safety was just mentioned. In contrast to data-centric view, which is specific to stand-alone software modeling packages, the RWTH team advocates a lifecycle-centric view on the computer-aided process modeling (Marquardt, 2000). Exploration of topic was performed within a two-dimensional coordinate system, which comprises the process/product lifecycle and design lifecycle.

Nearly at the same time, Kirillov (2000a) analyzed the ways to improve effectiveness of safety analysis, modeling and simulation of the hazardous processes for complete range of the operational ("normal") and accident ("abnormal") regimes at different stages of the process and design lifecycles. It was argued that the today's situation of "information disunity" - inability to share, re-use, store,

communicate and manage the safety-related data, models, patterns of "good safety practice" – can be overcame by integration of the available and future safety analysis tools to a common information grid of the chemical process engineering work via creation of the unified standards for data and model exchange.

Attention was brought to importance of the *quantitative* modeling and simulation methods, which used for safety analysis along with and in addition to the widely accepted *qualitative methods* - like hazard identification, screening and assessment (HAZMAT, HAZOP, FMEA, FTA, ETA, PHA, etc.), using of accident databases (MHIDAS, FACTS, MARS, etc.), re-use of the past experiences by case-based reasoning, evaluation of the human, organizational, management, software and the other non-physical factors.

Discussion of advanced physico-chemical modeling and detailed (chemical kinetics, CFD, structural dynamics) numerical (finite elements, finite differences, etc.) simulation of the hazardous phenomena and estimation/ recovery of the inventory properties (material and energy) was concentrated on the *deterministic* aspects of the safety problems. The results of deterministic simulation are the engineering base and initial data input for the subsequent *probabilistic* safety analysis and risk management measures. Abbreviation CASAMS (**C**omputer-**A**ided **S**afety **A**nalysis, **M**odeling and **S**imulation) was proposed for an emerging research domain - using computer- and IT-based physico-chemical analysis, numerical modeling and computer simulation of the accident phenomena in safety engineering of the chemical processes and reaction technologies.

The main goals of the present report are - 1) to show a key difference between the scope of process modeling for the "normal" and "abnormal" conditions of the industrial chemical processes via introducing of an innovative concept of hazard lifecycle; 2) to explain a distinction between today's generally accepted consequences-centric safety engineering approach and a proposed hazard lifecycle-centered safety engineering framework (more shortly – hazard lifecycle safety engineering); 3) to discuss the functional requirements for an "ideal" integrated software, which is capable to perform safety analysis throughout the whole domains of the process, design and hazard lifecycles.

Concept of the Hazard Lifecycle

For modeling of unit, plant or enterprise under "normal" (designed or expected or wishful within specified range) conditions it is enough to work inside the two-dimensional conceptual plane, where the *process/product* and *design lifecycle* axes are present only (see Hackenberg, 2001).

Computer-aided analysis, modeling and simulation of the safety-related issues under "incident" or "accident" conditions require at least a three-dimensional conceptual space, which includes an additional hazard *lifecycle* axis (see Fig. 1).

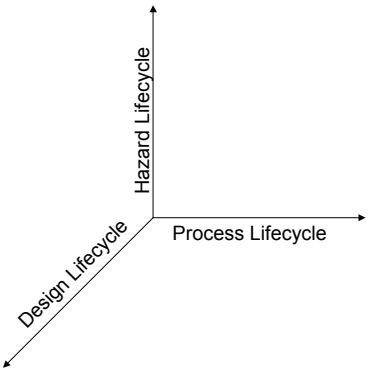

Figure 1. Basic lifecycles in safety engineering of chemical processes

We define the *hazard lifecycle* as a set of the business, R&D, regulatory and other processes, performed by different organizations and experts, from the chemical reactivity estimation to emergency plan preparation. Hazard lifecycle is a virtual representation (model) in engineering activity of an accident in real world. Each accident scenario can be treated from viewpoint of either a single or the multiple interrelated hazard lifecycles. Each hazard lifecycle can have a different nature, mechanism and run on the different spatial and time scales (see Fig. 2).

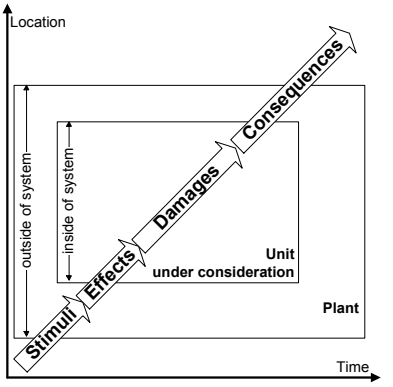

Figure 2. Basic stages of the hazard lifecycle

Within the *hazard lifecycle* it is possible to delineate the following four key stages (see Fig. 2) – 1) "Stimuli": latent (or "sleeping") hazard existence, critical conditions and precursors formation, initial disturbance (internal fluctuation or external initiating event) onset; 2) "Effects": embryonic (micro- and mesoscopic) competition between promoters and inhibitors, stochastic or regular launching and full-scale development of a harmful macroscopic process, initiating of another dangerous process; 3) "Damages": degradation, breakdown or collapse of the

protective barriers or system boundary due to the separate or simultaneous combined effects; 4) "Consequences": release, dispersion and sedimentation of toxic agents, mechanical collapse, fire, injuries, etc.

Impetus for hazard evolution can be related with the different nature-driven (lighting, tornado, etc.) phenomena, human-driven activity (unintentional improper control or management procedures at technological accident, malevolent actions at terrorist act), or technology- or business-driven processes (ageing, etc.).

Effects can include the mechanical (impact, penetration, etc.), physical (shock or blast wave in gases, tension in solids, boiling in liquids, etc.), chemical (reactive or thermal runaway, deflagration, etc.) or mixed processes, which possess the harmful properties.

Consequences-centric vs. Hazard Lifecycle-oriented Safety Engineering

Currently dominated approach to safety engineering of the major accident at hazardous chemistry- or energy-loaded process plants, storage facilities or transport systems can be named as a *consequences-centric*. It means that the safety-concerned stakeholders (society, industry, R&D community, government) are, in first turn, targeted on prevention or mitigation of the consequences of accidents.

Authority directives in the industrially developed countries obligate to assure a socially acceptable risk of the hypothetical accident consequences.

The existing R&D hazards analysis tools are also designed for the "post-accident" consequences analysis. They are based on postulated (safety analyst-defined) accident scenarios, and do not deal with the actual physico-chemical processes, which run inside of system under consideration and whose unrestricted (by process operator or protective technical system) evolution results in the accident occurrence. Today the modeling and simulation tools specifically aimed to "pre-accident" and "in-accident" stage for chemical process units are absent. Their roles in the rare known cases are played by the general-purpose CFD and structural codes, supplied with specific data on material properties or specific process models. On the other hand, examples of the nuclear industry (after the TMI and Chernobyl accidents) and offshore oil/gas industry (after accident at continental shelf) convinced us that using of advanced physico-chemical modeling is feasible, effective and valuable.

Let's consider an example case – gas-air explosion at chemical plant. For standard "consequences-centric" safety analysis, an impetus or initiating event is a rupture of feeding pipeline, for example. Effects: 2-phase release from hole in pipe, atmospheric dispersion over plant boundaries, formation of explosive gas-aerosol mixture, ignition and vapor cloud explosion. Damages: blast-induced structure crush, heat loads for human skin, etc. Consequences: property losses, human injuries.

In terms of the proposed hazard lifecycle concept the mentioned safety analysis deals with "external" or "post-accident" hazard lifecycle and do not analyses an "internal" or "pre-accident" hazard lifecycle. However, if a safety expert will restrict (either due to unwillingness or due to absence of the appropriate tools) oneself to the mentioned "external" hazard lifecycle, it will never be possible to him to make a sound engineering judgment – how safe is this reactor under given boundary and initial conditions? What are the key, specific operational parameters or material properties inside of reactor, which trigger the self-accelerating process of accident?

Stimuli in "internal" hazard lifecycle can be – wrong actions of worker, terrorist act, loss of steel strength due to ageing or hard weather conditions, etc. Effects: deflagrative explosion of combustible mixture inside of pipe; blast wave strengthening due to multiply reflections; formation of the sub-critical microcracks, induced by dynamic loads from blast wave; propagation of super-critical cracks in pipe wall. Consequences: mechanical (brittle or viscous) rupture of steel pipe and macroscopic hole formation. These consequences are the physical causes (or stimulus) of the "external" hazard lifecycle.

In contrast to the consequences-centric viewpoint, we guess that computer-aided safety engineering with the whole hazard lifecycle perspective in mind can be beneficial and useful for a process safety improvement. The computer-aided analysis, modeling and simulation of the driving forces, critical conditions, criteria, promoters or inhibitors of accident evolution can provide more effective and accurate digital prototyping, more creative and predictive virtual testing and more responsible decision making on safety-related issues.

Functional Requirements for CASAMS Tools

Implementation of the proposed hazard lifecycle-oriented framework requires an advanced functionality for the CASAMS workflow. The key requirements, revealed and used during development of the CASAMS tools (Chemical WorkBench – computer-aided reaction engineering software, CADYC – reactive CFD library, VRECA – Virtual Reality Engineering Content Analyzer) in Kurchatov Institute, are the following:

1. to be *user-friendly* to all participants in a hazard lifecycle process (i.e. design engineers, managers, safety analysts, emergency planners, etc.) and to provide an easy-to-comprehend media for visual modeling of the safety problems and cognitive visualization (in easy to human perception form) of the simulation results (as in VRECA – see Lukashevich, 2001).
2. to support *phenomenon-driven* (Kirillov, 1996; Pasanen, 1998) approach, enabling both "unit-operation"-based modeling and simulation of the *multiphysics* phenomena at the different spatial and time scales.
3. to communicate with the GIS (location), CAD/ CAM/CAE (geometry, topology, initial

and boundary conditions), grid generation (Finite Elements for structural and thermal analysis, Finite Volumes or Finite Differences for reactive CFD analysis) systems.

4. to use both the *detailed* (multi-step, finite rate), *reduced* and *one-step* (global) *kinetics* models for chemical reactor or reactive CFD modeling (as in Chemical WorkBench software – see Kirillov, 2000b).
5. to use the *embedded, extendable databases* for the (a) thermodynamic properties of individual chemical species, (b) elementary reaction rate constants, (c) kinetic mechanisms and the *knowledge bases* for recovery of unknown (from experiment) thermochemical and kinetic parameters.
6. to perform modeling with a *variable granularity* (level of detail), i.e. detonation parameters modeling can be made either by lumped-parameter thermodynamic Chapmen-Jouget model (as in ChemBench software) or by 1-dim (chemical kinetics and Euler gasdynamics) Zeldovich-Neuman-Doring model (as in CADYC reactive CFD software library – see Panasenko, 1999).
7. to perform both the *empirical-based* and *"from-first-principles"* computer modeling.
8. to support the *multiple views* of phenomenon or property under consideration, including textual, geometric, structural, physical, chemical information, etc.

Conclusions

Innovative concept of the hazard lifecycle is introduced to describe a peculiarity of safety-concerned mathematical modeling and simulation of the "abnormal" processes under accident conditions throughout a whole set of the process and design lifecycles.

In order to improve the quality, accuracy, predictive power and efficiency of computer-aided safety engineering work it is proposed to transfer from the consequences-centric to the hazard life-centered framework.

Functional requirements are enumerated for the computer-aided safety analysis, modeling and simulation (CASAMS) of the hazardous phenomena and estimation / recovery of the inventory properties (material and energy). These features are essential for cost-effective and user-friendly digital prototyping and virtual testing of the "inherently safe" designs, robust and comprehensive reengineering and investigation of the governing parameters, critical conditions, competitive mechanisms and overall evolution of the real or hypothetical accidents.

Acknowledgments

The authors are grateful to the four anonymous referees for their valuable comments and stimulating suggestions.

References

Dimitriadis V.D., Shan N., Pantelidis C.C. (1997). Modeling and safety verification of discrete/continuous processing systems. *AIChE Journal*, v.43/4, 1041-1059.

Eggersmann M. , et.al. (2001). Applications of Modeling – A Case Study from Process Modeling. *Technical Report LPT-2001-20.* Lehrstuhl fur Prozesstechnik, RWTH, Aachen, September.

Hackenberg J., et.al. (2001). Lifecycle Modeling Support – Concepts and Software. In: Panreck K., Dorrescheit F. (eds.). *Simulationstechnik, 15. Symposium in Paderborn*, September 11-24.

Kirillov I.A. (1996). Smart simulation technology: innovative computer modeling approach for hydrogen vehicle safety. In: *Proc. of the Seminare Franco-Russe Inter-Academies des Sciences on L'HYDROGENE DANS TRANSPORTS*. Paris, Septembre 25-26, 353-361.

Kirillov I.A. (2000a). Embed Safety into Chemical Process Engineering and Reaction Technologies. *2000 AIChE Spring National meeting; Session: [141] - Challenges for Design in Practice*. Atlanta, Georgia, March 6, oral report and paper number 141c.

Kirillov I.A. et.al. (2000b). Rapid Modeling and Estimation of Hydrogen Safety Issues using "Chemical WorkBench" Integrated Simulation Software, *ACHEMA 2000.* Frankfurt am Main, May 22-27.

Lukashevich I.E. (2001). Virtual Reality Engineering Content Analysis Tool for the Industrial Safety Applications. In: *Safety in Oil and Gas Industries*, Russian Ministry of Emergency Conference, Moscow, December 18-20.

Marquardt, W., et.al. (2000). Perspectives on lifecycle process modeling. In: Malone M.F., Trainham J.A., Carnahan B. (eds.). *Foundations of Computer-Aided Process Design,* AIChE Symp. Ser.323, 96, 192-214.

Rotman D., Kemezis P., Hunter D. (1997) Computers in CPI: tying it all together. *Chemical Week,* v. 28, 22-24.

Panasenko A.V., et.al. (1999). Development of software components library CADYC for modeling of reactive gas-dynamics in the scientific, industrial and ecological applications. *10th International Conference on Computational Mechanics and Modern Applied Software Systems*. Pereslav-Zalessky, June 7-12.

Pasanen A., et.al. (1998). Phenomenon Driven Process Design Methodology: Tool Support. *CHISA'98*, Prague, August 23-28.

Pitt M.J., Flower J.R., BenEmhmmed M.K. (1996). Computer simulation of safety and environmental hazards of process deviations. *IchemE Research Event*, v.1, 391-393.