CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648139

How Can We Improve HAZOP, Our Old Work Horse, and Do More with Its Results? An Overview of Recent Developments

Hans J. Pasman*, William J. Rogers

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, Texas 77843-3122
hjpasman@gmail.com

All risk management starts in determining what can happen. Reliable predictive analysis is key. So, we perform process hazard analysis which should result in scenario identification and definition. Apart from material/substance properties, thereby, process conditions and possible deviations and mishaps form inputs. Over the years HAZOP has been the most important tool to identify potential process risks by systematically considering deviations in observables, by determining possible causes and consequences, and, if necessary, suggesting improvements. Drawbacks of HAZOP are known; it is effort intensive while the results lack completeness and are used only once. Repeat of the exercise is required at several stages of process build-up, and when the process is operational, it must be re-conducted periodically.
There have been many past attempts to semi-automate the HAZOP procedure to ease the effort of conducting it, but lately new promising developments have been realized enabling also the use of the results for facilitating operational fault diagnosis. There are several factors enabling and supporting these improvements. In the first place there are now decades of experience with HAZOP. Secondly, system science and artificial intelligence provide methods that even with present-day laptop computing power provide equipment ontological and classifying structuring (computer aided process engineering, CAPE) and enable identification of causal relations by learning causal structures from data. This paper will review the directions in which improved automation of HAZOP is going and how the results, besides for risk analysis and design of preventive and protective measures, also can be used during operations for early warning of upcoming abnormal process situations. The latter will enhance operator's situation awareness and will guide operators more efficiently to causes. Thereby, use is made of advanced methods of process simulation and data treatment. Freeing manpower for HAZOP-ing of operations may allow HAZOPs of non-routine activities such as start-ups, shutdowns, and turnarounds in which a relatively large fraction of accidents happen because of greater uncertainty due to wider ranges of potential upset consequences and reduced control as a result of non-routine activities.

1. Introduction

The HAZOP study emerged in the early 1970s at ICI in developing new processes. The incentive was optimizing operability of a process. But recognizing hazards when process variables deviate from the design intent and what to do to prevent a mishap already in design or later in operation became the main purpose. HAZOP is performed as a team effort under experienced chairmanship on the basis of process information derived from piping & instrumentation diagrams (P&ID), flow sheets, material data sheets, and general basic knowledge. In a review paper on HAZOP methodology Dunjó et al., 2010 described the evolution of the method, compared the HAZOP study with other process hazard analysis methods and presented a brief overview of the various attempts to semi-automate the method. As HAZOP focuses on physical process deviations, known weaknesses of the method are possible undetected design, construction and material deficiencies, and lack of representation of human error in the process operation. But also the unreliability of a HAZOP team is an issue. Baybutt, 2015a and b devoted recently much attention to this subject. In the first paper, entitled: "A critique of the Hazard and Operability (HAZOP) study", the weaknesses of the method are elucidated. Teams may miss scenarios, after-thoughts may be neglected, participants may become

Please cite this article as: Pasman H., Rogers W., 2016, How can we improve hazop, our old work horse, and do more with its results? an overview of recent developments, Chemical Engineering Transactions, 48, 829-834 DOI:10.3303/CET1648139

complacent, the process may be complex, the terms used may be confusing, and the studies can be prolonged diminishing focus. Considering the right and complete design intents, process parameters, guide words, initiating events, and operability scenarios may flaw. Full technical coverage and right documentation may fail. Baybutt's second article formulates competency requirements for HAZOP team members.
Regarding the relatively long time a team is involved in conducting a HAZOP study of a plant, the effort required is quite intensive. Depending on plant size it may take 1 to 8 weeks for a team of at least five members. When HAZOP after commission of the plant must be repeated every five years the accumulating cost will be significant.
Summarizing: Three improvement directions worth investigating translate in the following questions:

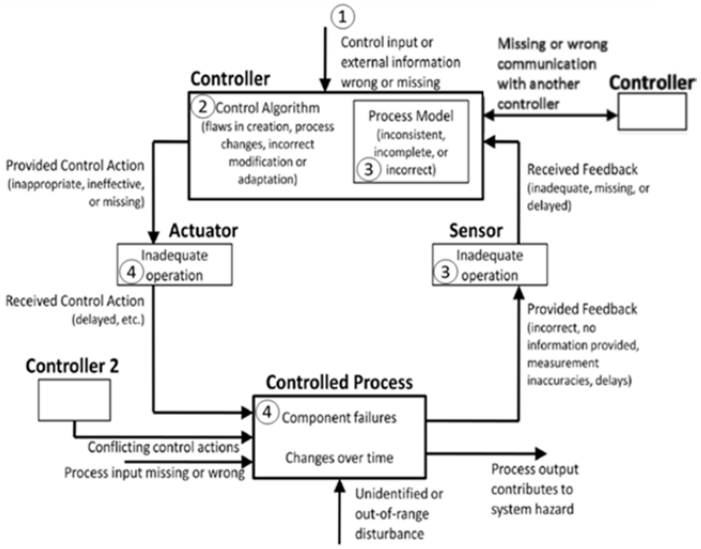
a. Can the reliability of the identification method of hazards and possible scenarios be improved?
b. Can the efficiency of the method be enhanced by making use of information technology?
c. Can the yield of the effort be strengthened by applying the results for other purposes?

In the remainder of the paper we shall address these questions by reviewing recently published work.

2. Reliability improvement

In a simplified sense, for development of scenarios of cause-consequence chains we may encounter the so-called Donald Rumsfeld's four quadrants of 'knowns' (K) and 'unknowns' (U), namely: K-K, U-K, K-U, and U-U. Here, 'known' means a possible scenario recognized and defined, and 'unknown' a potential scenario as an overlooked possibility. The latter may also concern a branch or final part of a scenario: one may underestimate consequences such as escalation and domino effects. Hence, the fields apt to improve the first step of risk analysis and the follow-on possible conception of risk reducing measures are the latter three combinations containing the 'unknowns'. U-K means a possible scenario is not recognized in the team, but awareness of its existence is known by others. The U-K quadrant is fuzzy in the sense that thoroughness of applying the HAZOP procedure, optimizing the team composition, longer thinking, process simulation, networking in the branch, and application of the DyPASI similarity algorithm (see Paltrinieri et al., 2013) for querying accident data bases can diminish the number of unknown knowns. Known unknown scenarios are those where one presumes a scenario of cause-consequences, but there is no certainty about its reality. Also in this case process simulation providing causal relations for fault propagation may help.
In Pasman, 2015, an overview table is given of HAZOP automation attempts over the last 20 years that aimed besides for efficiency also for reliability. Therefore, the attempts made use of a large variety of process simulation models. This paper does not allow an extensive explanation of the different models, so only a brief description will be given. Early attempts made use of directed graphs (directed edges and nodes), representing flow and operational variables. Signed digraphs were used in which the plus or minus signs at the edges stand for reinforcing or diminishing influences, while later a guideword workspace layered digraph allowed a three-dimensional influence structure offering even more flexibility. More sophisticated is the use of coloured Petri nets which for instance are used to represent logistics. The places nodes have a state and contain tokens which move to a next place upon a firing trigger of a transition node. The node colour is associated with a specific property/value. The trigger can be an event, or a fixed or random chosen time lapse. Quite a few of above attempts have been initiated by Venkatasubramanian at Purdue, see, e.g., Zhao et al. 2005. More recently, a further sophistication occurred by the application of the Multi-level Flow Model (MFM), originally developed for simulation of nuclear power plant installations. MFM shows equipment objectives (source, transport, storage) and functions (sink, barrier, balance), and it describes in combination with, e.g., HYSYS the interactions of mass, energy, and information flows, combined to flow structures (see Wu, 2014). An example of MFM will be described in the next Section. Finally, in 2012 Rodriguez and De La Mata went again a step further, describing the D-higraph model which is more intuitive and insightful than MFM. Besides the MFM features, D-higraph shows the plant's controls. For difficult scenarios Aspen Plus will be required.
Obviously, unknown-unknowns are the real problem. There can be unforeseen external and internal threats, which may trigger a scenario no one anticipated. Only a resilient organization and plant will be able to neutralize such a threat to an extent that depends on the nature of the threat, and vulnerability and recoverability of plant, process and organization. Resilience is better as a topic of a different paper, though.
A *System approach*, as strongly advocated by Leveson, 2011 and Venkatasubramanian, 2011 will in principle lead to a complete inventory of possible scenarios, albeit that the definition of the system boundaries will result in restriction. The narrower these boundaries are delimited, the less threats from outside the system will be taken into account. In Blended Hazid, or BLHAZID for short, by Cameron and his group (see Seligmann et al., 2012) the system consists of plant, people and procedures with connecting information streams and is called a functional system framework. The tools in BLHAZID are classic: besides HAZOP for identifying functional failure scenarios, FMEA (failure mode and effect analysis) is conducted in partly overlap to account for

component failures and their consequences. This combination and modeling a larger degree of component detail allowed by use of smart P&ID (see next section) will certainly result in a higher degree of completeness.



The STPA guide word queries for each control loop are four, as illustrated in the figure by the circled numbers which refer each to one of the queries below:

1. Control action provided?
2. Control action unsafe?
3. Action too early, too late, or out of sequence?
4. Action stopped too soon or applied too long?

Figure 1. System approach control loop queries as proposed by Leveson, 2011 and later publications (2015).

By considering safety as emergent from a system and keeping an adequate safety level as a control problem, Leveson developed the system theoretic process analysis (STPA) tool with four HAZOP-like queries, as shown in Figure 1, which include time as a parameter and guarantee completeness. This fully different way of looking at a process could develop to the ultimate solution.

3. Increasing efficiency

If one goes into the depth and detail of a plant installation a main problem is handling (storing, retrieving) the many data. The number of scenarios runs in the thousands. In Blended Hazid the handling of a myriad of scenarios has been solved, see Seligmann et al., 2012 and Seligmann, 2011. For STPA a start has been made by Thomas, 2013 in applying rigorous parameter definitions and structuring the problem.
Another aspect is making use of the process, and plant equipment data embedded in the modern smart layered P&IDs, which speed up the analysis. Because of different CAD systems, this is another IT challenge.
Third is the use of query generating engines. For enabling automation, initially a knowledge or expert system software tool consisting of a knowledge domain/experience rule base indexed for retrieval/re-use and a reasoning/inference system shell (JAVA) was applied. The tool generates deviations and contains rule-based trees linking process specific attributes, via process parameters, and deviations to causes and consequences. Instead of pure rule based, a further step is case based reasoning (CBR); CBR is to apply on similar cases (stories), which beside rules contain context, e.g., process system ontology. Instead of a static system an artificial neural network (ANN, complex neuron node directed graph structure) has been tried, which is dynamic in the sense it has learning ability for adaptation to a similar but new case. Today, a genetic algorithm may be used for optimization of the adaptive weighting.
Individual performance claims have been made in which some results were quite disappointing, but no systematic round-robin of comparing various machine assisted HAZOP results are found with those obtained by human teams. Also, no systematic overall effort measurements have been published. Developing a simulation model for a process and a knowledge base/reasoning engine is not a sinecure. To make progress, a round-robin comparison should have priority.

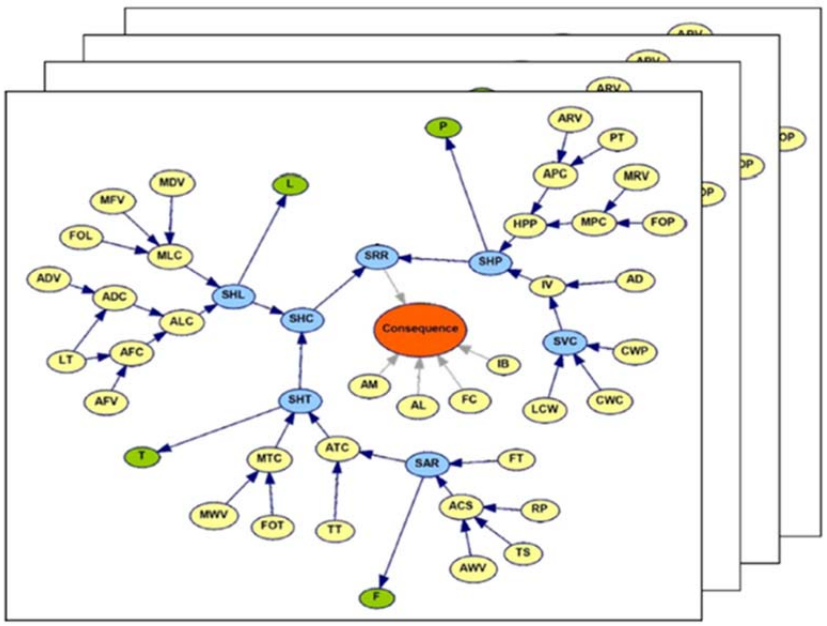
4. Applying results for alternative purposes

HAZOPs are performed to verify plant safety from an operability point of view before operations start and to check after certain intervals of, e.g., five years whether results are still adequate and not degraded by modifications. However, once results have been stored in computer compatible form, such as in Blended Hazid, then given a process upset more or less instantaneously a causal graph or rather cause-implication diagram can be produced. This was shown by Németh and Cameron, 2013 at the previous LP symposium.

Besides verification of HAZOP study and supporting hazard identification audit and design, these authors mention also operator training as possible re-use application of the results outside the actual process. However, when available on-line in the control room and connected to the SCADA system much more is possible as causation of developing upsets can be more easily diagnosed. This on-line use can help to prevent trouble, restore normal state before alarms are triggered, or at least facilitate investigation afterwards.
Meanwhile, two groups of researchers independently published results of an on-line application of HAZOP results for the purpose of keeping a process within its safe envelope before an alarms-trigger state is reached. To that end both apply historical process data but in a completely different way. Both also apply dynamic Bayesian network to connect actually measured process variable data to equipment malfunction causes hidden for the operator at the time the upset develops. In the following a synopsis of both works will be given.

4.1 Historical data via operator experience

Naderpour et al., 2015 published three articles on the same approach but for different cases. Here will be described the one on treatment of a solvent containing the very toxic residue of methomyl product, of which the main part was centrifuged off in a previous process step. The solvent treatment consisted of decomposing the toxic substance to below 0.5% at 135 °C and 1.4 bar by recirculating the residue mixture through a reactor vessel. The solvent is first steam heated to a temperature at which the rates of exothermal reactions become significant and thereafter must be water cooled. The hazard is a run-away with spread of toxic fumes.
The operators were interviewed about safe ranges of the SCADA observed variables: a low, normal (half full), and high liquid fill level (L); a very low, low, and normal recirculation flow (F); a normal and high temperature (T); and a normal, high, and very high pressure (P). From this information for each variable a triangular or trapezoidal fuzzy membership function was construed, but used as probability distribution. Consequence (C) severity levels of run-away were defined and expressed on a 5-point scale from negligible to catastrophic and probability (Pr) from very unlikely to very likely. The fuzzy risk product of C and Pr ranged from non-acceptable via tolerable to acceptable. The tolerable non-acceptable (TNA) level shall initiate action. Based on HAZOP results seven abnormal situations were defined. For each abnormal situation the equipment components were identified failure of which can cause the situation. These dependencies were mapped and quantified in a Bayesian net (BN) as shown in Figure 2 and made dynamic by updating the observables L, T, P and F at each time step. When reaching the TNA risk level at a developing abnormal situation, operators are alerted. They can read from their panel at which node(s) this occurs and by looking at the BN they can see the components influencing that node(s). The component with the highest failure probability is the most likely cause.



Abnormal situations (S):

SVC: vent condenser failure, decomposition gases entering vapour stream to flare, while by solids deposition the flow blocks increasing pressure.

SHL: high liquid level, L

SAR: abnormal recirculation (hi or lo), F

SHP: high pressure, P

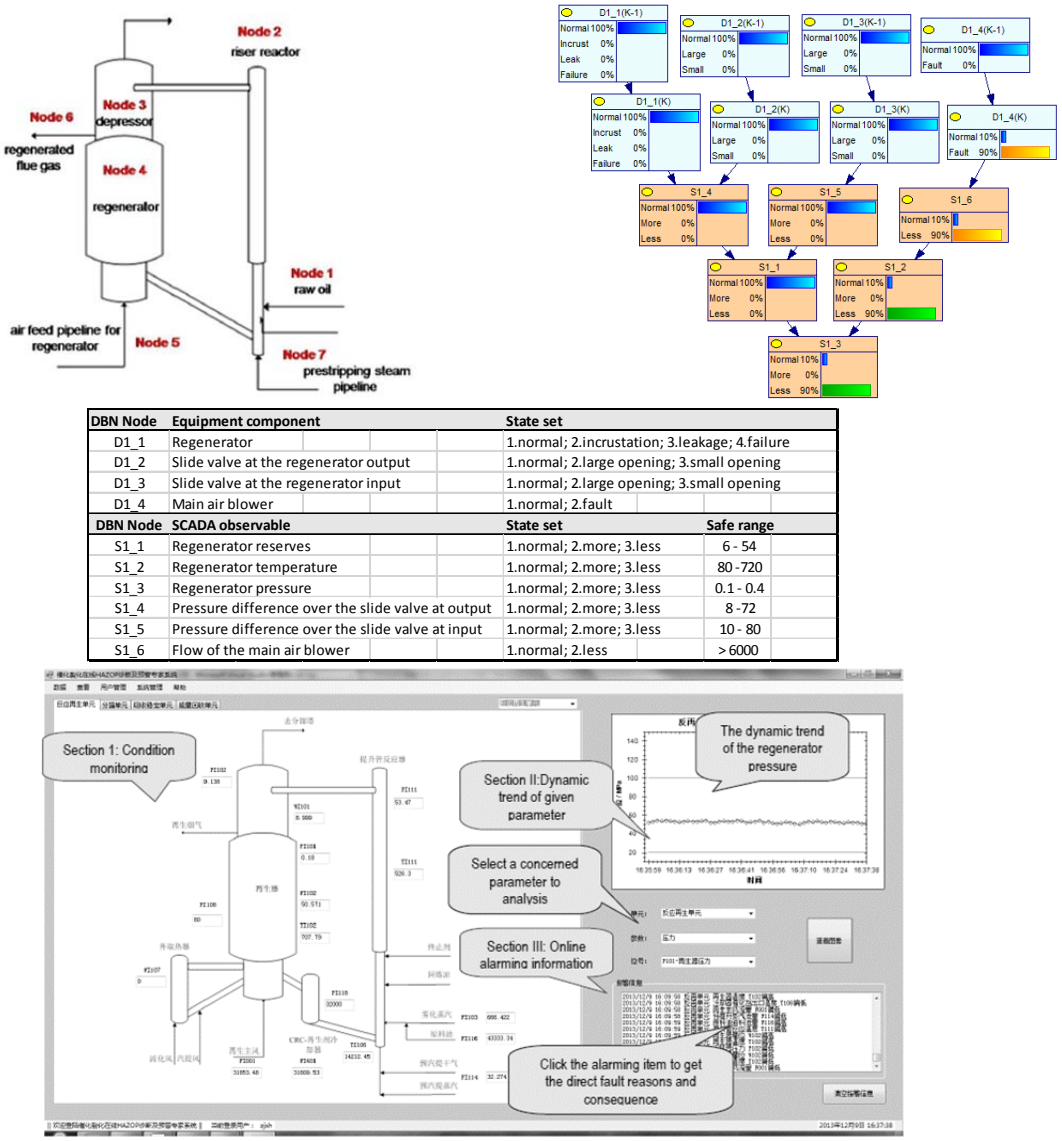
SHT: high temperature, T

SHC: high concentration of methomyl by feeding at too low temperature. Possible runaway at heating the mixture to normal temperature.

SRR: runaway reaction

Figure 2. Dynamic Bayesian net of possibly failing (hidden) components of residue treating reactor causing abnormal situations after Naderpour et al., 2015. Observables L, T, P, and F provide updated evidence for each time step. Operator is alerted when risk level reaches Tolerable Non-Acceptable. A corresponding change in an abnormal situation node value indicates the direction the faulty component should be sought. The consequence of run-away can be mitigated by air monitoring, alarming, fire cannons, and ignition barriers.

4.2 Historical data via SCADA (System control and data acquisition)



DBN Node	Equipment component	State set
D1_1	Regenerator	1.normal; 2.incrustation; 3.leakage; 4.failure
D1_2	Slide valve at the regenerator output	1.normal; 2.large opening; 3.small opening
D1_3	Slide valve at the regenerator input	1.normal; 2.large opening; 3.small opening
D1_4	Main air blower	1.normal; 2.fault

DBN Node	SCADA observable	State set	Safe range
S1_1	Regenerator reserves	1.normal; 2.more; 3.less	6 - 54
S1_2	Regenerator temperature	1.normal; 2.more; 3.less	80 -720
S1_3	Regenerator pressure	1.normal; 2.more; 3.less	0.1 - 0.4
S1_4	Pressure difference over the slide valve at output	1.normal; 2.more; 3.less	8 -72
S1_5	Pressure difference over the slide valve at input	1.normal; 2.more; 3.less	10 - 80
S1_6	Flow of the main air blower	1.normal; 2.less	> 6000

Figure 3. An impression of the work of Hu et al., 2015. On top left: Fluidized Catalytic Cracking Unit with the catalyst regenerator as the large vessel at left, and at right the riser reactor, connecting piping and designated HAZOP nodes; on top right is the Dynamic Bayesian net with its nodes specified in the legend table below the net. The net is an adaptation for the situation of main air blower failure D1_4 between time steps K-1 and K. At the bottom is reproduced the main interface of their Intelligent Online Early Warning System, IOEWS.

Based on HAZOP results, Hu et al, 2015, drafted several possible Bayesian nets describing the cause-consequence chains potentially existing and relating equipment failures with observable deviations. For each net the K2-algorithm, developed for medical diagnosis, was applied and the Bayesian Information Criterion (BIC) calculated while adding sections of historical data about abnormal situations until BIC was constant. The best net yields the highest BIC value. The node variable probability density functions are also derived from the data. Next, by feeding actual observable values at each time step the temporal function was obtained, and the net made dynamic. A forward-backward recursive algorithm yields inference of a likely cause of an upset.
The authors presented as an example the catalyst regenerator part of a Fluidized Catalytic Cracking Unit (FCCU), see Figure 3. This regenerator burns coal deposits on the catalyst with air fed at the bottom. The HAZOP study considered two possible deviations from design: air flow low (possibly caused by the anti-surge valve opened; or the main fan shut down; also the main fan entrance filter net choked with adsorbate; filter sucked into the pipeline reducing the primary air flow; or the flow control valve faulty) and air flow stops (due to

compressor fails). In the Bayesian net the moment at time step K is shown, when at K-1 all equipment was still running normal. But at time K, node S1_6 (flow of main air blower) went into alarm state ‘less’, by inference clearly showing as likely cause node D1_4, the main air blower system. The example is rather simple, but it shows the potential.

5. Conclusions

Based on recent literature we can conclude the following with respect to the three questions posed in the introduction: (a). From the methods reviewed, once fully developed BLHAZID working with smart P&IDs offers at this time the best perspective for improving the reliability of scenario identification as well as, (b). improving the efficiency of the team operation of HAZOP (and FMEA). DyPASI will be of general help, and in the longer term the holistic system control loop approach of STPA may further add to completeness. The human and organizational aspects of scenarios will need much further study. At a certain stage a cooperative HAZOP round robin would be a must. (c) To enlarge effectiveness, HAZOP study results can be utilized in operations to alert personnel in real-time for a developing upset and through causal graph facilitate fault diagnosis. Examples were shown of two different approaches. Hence, several developments are underway, but it will take considerable time to achieve their full potential.

References

Baybutt, P., 2015a, A critique of the Hazard and Operability (HAZOP) study. Journal of Loss Prevention in the Process Industries 33, 52-58.

Baybutt, P., 2015b, Competency requirements for process hazard analysis (PHA) teams. Journal of Loss Prevention in the Process Industries 33, 151-158.

Dunjó, J., Fthenakis, V., Vílchez, J.A., Arnaldosa, 2010, J., Hazard and operability (HAZOP) analysis. A literature review. Journal of Hazardous Materials, 173, 19–32.

Hu, Jq., Zhang, Lb., Cai, Zs., Wang, Y., Wang, Aq., 2015, Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework. Process Safety and Environmental Protection, 97, 25–36.

Leveson N.G., 2011, Engineering a safer world, systems thinking applied to safety. The MIT Press, Boston MA; 608 pp., ISBN-10:0–262-01662-1, ISBN-13:978-0-262-01662-9.

Leveson N.G., 2015, A systems approach to risk management through leading safety indicators, Reliability Engineering and System Safety, 136, 17–34.

Naderpour M., Lu J., Zhang Gq., 2015, An abnormal situation modeling method to assist operators in safety-critical systems. Reliability Engineering and System Safety, 133, 33–47.

Németh E., Cameron I.T., 2013, Cause-Implication Diagrams for Process Systems: Their Generation, Utility and Importance, Chemical Engineering Transactions, 31, 193-198, DOI: 10.3303/CET1331033.

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., Cozzani, V., 2013, Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. Journal of Loss Prevention in the Process Industries, 26, 683-695.

Pasman H.J., Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals, A System Perspective for Assessing and Avoiding Low-Probability, High- Consequence Events. Butterworth Heinemann, Copyright © 2015 Elsevier Inc., 2015, ISBN: 978-0-12-800057-1.

Rodriguez M. and De La Mata J.L., 2012, Automating HAZOP studies using D-higraphs, Computers and Chemical Engineering 45, 102– 113.

Seligmann B.J., Németh, E., Hangos, K.M., Cameron, I., 2012. A blended hazard identification methodology to support process diagnosis. J. Loss Prev. Process Ind. 25, 746–759.

Seligmann B.J., 2011, A Functional Systems Framework and Blended Hazard Identification Methodology to Support Process Diagnosis, Ph.D. Dissertation, School of Chemical Engineering, University of Queensland, Australia.

Thomas J., 2013, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis. Ph.D. Dissertation, Massachusetts Institute of Technology, Boston MA.

Venkatasubramanian V., 2011, Systemic failures: challenges and opportunities in risk management in complex systems. AIChE Journal; 57(1), 2–9.

Wu J., Zhang L., Lind M., Hu J., Zhang X., Jensen N., Bay Jørgensen S., Sin G., 2014, An integrated qualitative and quantitative modeling framework for computer assisted HAZOP studies, AIChE Journal, 60 (12), 4150–4173.

Zhao C., Bhushan M., and Venkatasubramanian V., 2005, PHASUITE: An Automated HAZOP Analysis Tool for Chemical Processes, Part I: Knowledge Engineering Framework, Process Safety and Environmental Protection, 83(B6), 509–532; Part II: Implementation and Case Study, ibidem 533-548.