MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

HAZOP: Our Primary Guide in the Land of Process Risks: How can we improve it and do more with its results?

Hans Pasman† and William Rogers
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University
College Station, Texas 77843-3122
†Presenter E-mail: hjpasman@gmail.com

Abstract

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 are used only once. The exercise must be repeated 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. This paper will review the directions in which improved automation of HazOp is progressing 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.

Introduction

All of process safety thinking must start with obtaining a perfectly complete inventory of hazard potentials and mechanisms through which hazards can emerge and through event scenarios cause damage. It is only after one realizes what can happen either in design or in an operational stage that measures can be taken and effective risk controls organized and installed. Hence, it depends on knowledge of the materials involved and their properties both of process fluids and containment. It further requires a clear mental image of process mechanisms, based on relevant physics, chemistry, and their interactions, probable wear, tear, and degradation processes.

Besides, and this may be even more important, it needs imagination of human and organization failure in all stages: in design, construction, operation and maintenance, and later decommissioning. Practice shows there exists a myriad of possible, unintended, and unforeseen interaction mechanisms potentially forming cascading cause-consequence chains, which may escalate in consequence severity. That is why for the human brain imagining and defining what can go wrong soon becomes overwhelming and complex. Systematic methods of approach by people with insight, experience, and knowledge are the only way to tackle such complexity and provide support for humans to manage engineering systems and their organizations.

In fact, some fifty years ago this was reason that methods such as HAZOP (Hazard and Operability Study) and FMEA (Failure Mode and Effect Analysis) emerged and became so wide-spread. HAZOP involves functional process dynamics and is considered the primary approach for event scenario generation, while FMEA is seen as additional because it concerns static equipment reliability issues adding information on equipment failure probability and possible effect. HAZOP occurs by systematically assessing the effects of process variable deviations from design intention applying the information of a Process Flow Sheet (PFS) and/or a Piping and Instrumentation Diagram (P&ID). In the US HAZOP is a cornerstone of Process Hazard Analysis demanded by OSHA's PSM, the Process Safety Management's rule, and in Europe of the risk assessments required by the Seveso directives. Basically, it requires teams performing brainstorming exercises on what can happen section by section of an installation or particular equipment. HAZOP focusing on the process operation and checking possible deviations from design intent and their effects, FMEA analyzing equipment components and investigating possible failures, failure modes, and their effects. It is clear that one needs a team with representation of different disciplines to capture as much as possible all potentially possible mishaps. The team members need all their experience to do a good job and the team leader in particular needs insight and overview. Baybutt [1] described recently the competency required by members of such teams. For good performance he recommends installing a competency management program, because there are many topics to cover.

Here, we can see already limitations appearing. Brainstorms take time, much time. The exercises require experienced people, who may be badly needed in other areas, perhaps their regular jobs. Brainstorming is tiring and after a morning session productivity in the afternoon will be much lower, so the recommended procedure is to restrict sessions to half-a-day per day. Hence, the exercises are costly, and guarantee that all possibilities have been reviewed cannot be given. In addition, due to changes in process operations and equipment over time there is a tendency to require a repeat of HAZOPs every five years.

In another article this year Paul Baybutt [2], from his experience, presented a critical review of the various weaknesses and failures a HAZOP study can suffer from. These are many of very different types. So, even if with much effort a HAZOP study has been accomplished there remains uncertainty whether all important scenarios have been defined. Therefore as part of a system approach, monitoring and learning from system behavior beyond the HAZOP, including near misses and upsets, is crucial to identify previously overlooked scenarios and also identify newly developed scenarios as the system changes with time.

The results of a HAZOP serve to formulate improvement actions. They can also be used as input to risk analysis, if so required. The latter can be kept relatively simple as a LOPA (Layers of Protection Analysis) or can be performed in an extensive form as a detailed QRA (Quantified

Risk Assessment), but that is all. HAZOP results are not used in daily operations. Operators in the actual process have usually no insight in and sometimes no access to the HAZOP results regarding their plant and must build-up their own experience from mishap scenarios.

From the above we can extract two questions:
- Can we be complacent and continue to repeat the same HAZOP procedure we performed in the 1970s, or is it possible with the present knowledge and advanced computer tools to perform a more efficient and effective job?
- Is it possible to make more effective use of the HAZOP results in routine operations, apply it to swiftly track down the cause of mishaps, and even add possible scenarios based on experience? And so improve cause diagnosis, risk assessments, and design of risk controls as well?

In the next sections we shall review first attempts to computerize HAZOP followed by considering how ideally HAZOP can be extended to the whole process system, which includes plant, people, and information flows. Then we shall briefly describe computational aids to boost the efficiency of scenario generation and to obtain a higher degree of scenario identification completeness. Next, it will be shown how smartly stored result data can be re-used in different ways. One of the applications will be automated alerting and information for faster diagnosis of root causes of a process upset by tracing the possible cause-consequence chains. Early knowledge of causes may also improve maintenance effectiveness.

Attempts to semi-automate HAZOP

In 2010, Dunjo et al. [3] provided an overview of the literature on HAZOP as it appeared over the years. Comparisons have been made of HAZOP with other Process Hazard Analysis techniques such as Action Error Analysis, FMEA, and Fault Tree Analysis. Already early on it became clear that one of HAZOP's weaknesses is lack or representation of human error and organizational failure. Plant computerization as, e.g., the introduction of Programmable Electronic Systems was one of the drives to extend the scope of HAZOP, but most research effort went into attempts to reduce the time and effort to spend on HAZOPs by computer support and automation. Administrative computer support for suggesting deviations to the team and keeping track of results is obvious and straightforward, but real automation attempts started in the late 1980s with, in the forefront, Frank Lees at Loughborough University (Parmar and Lees [4]) applying a rule-based approach. One year later Heino et al. [5] at VTT in Finland published the development of a more advanced rule-based expert system for HAZOPs. Many other attempts with knowledge-based systems followed. In the mid-1990s, the work of Venkat Venkatasubramanian and coworkers [6] at Purdue University became quite known by going a step further and applying process simulation with the digraph process flow simulation technique in addition to an expert system.

Trevor Kletz, who had been with other ICI-engineers at the cradle of HAZOP in the early to mid-1960s, while discussing in 1997 what HAZOP can do and fails to do in case of a computerized plant, addressed also HAZOP automation and was impressed by the results obtained at Purdue [7]. However, he also warned about conditions not readable from a P&ID but known to a team, and brought up by at least one team member, which may constitute a serious hazard if no countering measure would be taken.

In his 2015 published book, Hans Pasman [8] presented a brief compilation of automation efforts of the last twenty years. With some adaptation this compilation is reproduced here in Table 1.

Table 1 Various, relatively recent approaches to support and to (semi-) automate HAZOP

1995	Vaidhyanathan and Venkatasubramanian [9]	*Digraph* based HAZOP. Digraph is in mathematical graph theory a directed graph. A digraph consists of nodes connected by directed edges or arcs. In process application it is qualitatively modeling material and information flows initiating or undergoing change.
1996	Vaidhyanathan and Venkatasubramanian [10], [11]	HAZOPExpert is a *DiGraph* (HDG) model-based, object-oriented, intelligent system for automating HAZOP. The *expert system* is provided with semi-quantitative reasoning that is checking, whether in case of loss of containment, conditions surpass the auto-ignition threshold and whether a spill presents a toxicity risk. It further checks the adequacy of protective devices and ranks consequences.
1998	Srinivasan and Venkatasubramanian [12]	HAZOP applied to batch processes (with additional challenges compared to continuous process of operator procedures and actions, and discrete process steps). This is realized by *Timed Petri Net* representation of the batch process and Digraph to represent causal relations between process variables in sub-tasks. A Petri Net consists of Place and Transition nodes connected by directed arcs. It models some type of resources (material, information etc.) by tokens which on a certain signal or time lapse changing a place's state by the transition and move from one place to another. In combination with the earlier *expert system* work it constituted the Batch HAZOPExpert.
1999-2000	McCoy et al. [13], [14]	Software system HAZID consisting of several modules: AutoHAZID is the heart of the system. The description is quite detailed. It has at the start a configuration checker after the program read in the plant description and built a Signed DiGraphs (SDG) of the process units. It further has a qualitative effects module. The HAZOP emulation module was developed in the earlier STOPHAZ project. It is *a rule based inference engine* generating scenarios. VTT (Finland) contributed with a fluid library and fluid rules distinguishing feasible from infeasible scenarios. Fault propagation was modeled by means of SDG. The output is filtered to remove redundant information.
1997-2000	Khan and Abbasi [15], [16]	Development of a procedure to speed up 'HAZOP-ing': optHAZOP, followed by development of a *knowledge-based inference engine* software tool enabling automation. The tool consists of a general and a process specific part. It generates deviations and contains rule-based trees linking process specific attributes, via process parameters, and deviations to causes and consequences. Renamed from TOPHAZOP to EXPERTOP.
2005	Zhao, Bhushan, and	Software system PHASuite: Instead of Digraph, the process is

	Venkatasubramanian [17]	now represented by *Colored Petri Net* (CPN, tokens of different types have different colors), but the Petri Net also represents the methodology to perform the HAZOP. The process is abstracted to two levels: operation and equipment, which have been functionally linked. Knowledge is externally stored in layered operation and equipment models in a structured database, which can be approached by a user via Knowledge Builder. A *Case Based Reasoning Engine* (CBR – stories containing knowledge/experience learned by previous exercises) operating on the two-levels and on two-layers (CPN with below a safety model) performs the automated HAZOP. Application is again to pharmaceutical batch processes, more difficult to HAZOP than continuous ones. Gain in time spent is about 50%.
2008-2009	Cui et al. [18]; Zhuhao et al. [19]	As an extension of the Digraph method of Vaidhyanathan and Venkatasubramanian [10], [11], a *Layered DiGraph* (LDG) expert system was proposed. The Digraph is now three-dimensional, which enlarged the flexibility and knowledge storage capability. Each layer or workspace is associated with a guideword. The workspaces contain nodes representing variables interconnected by (unsigned directed) arcs, implying that the deviation in the 'parent' node determines the direction of deviation in the 'child'. Linked nodes can also be in different workspaces. The authors claim that a higher degree of completeness of HAZOP scenarios is achieved. Later the same group developed *PetroHAZOP*, an expert system but this time it is learning by *Case Based Reasoning* (see PHASuite above), while like in [17] it is making use of CAPE ontology for process systems (CAPE is computer aided process engineering, see Morbach et al. [26] and for application in HAZOP, Zhao et al. [27]; ontology is explicit specification of conceptualization here built as an taxonomy). A case consists of problem/situation, solution, and outcome description. A new problem is judged on similarity by an algorithm based on predefined indexes. It is thus highly domain dependent. It functions in the Chinese petrochemical industry with 900+ cases. A future effort was announced to combine the two approaches.
2009	Rahman et al. [20]	Further development of Khan and Abbasi's EXPERTOP to ExpHAZOP+ with some added features as an enhanced GUI (Graphical User Interface) and a selection method for an equipment node. It also added an update possibility of the knowledge base and introduced a unique *fault propagation algorithm*, identifying downstream causes and consequences from an identified upstream event.
2010 2014	Rossing et al. [21] Wu et al. [22]	*Multi-level flow modeling* (MFM), developed by co-author Lind in the early 1990s, is applied to describe the plant goal - function structure. MFM can be used at various abstraction levels, applies

		symbols (of which a few resemble Petri Net ones) for objectives (source, transport, storage) and functions (sink, barrier, balance), and it describes the interactions of mass, energy, and information flows, combined to flow structures. Also, symbols are available for functions as management, decision and actor action. Further, a set of means-to-ends relations (with symbols for produce, producer product, maintain, and mediate) and causal roles (with condition, agent, participant symbols) describe dependencies between functions. The interconnected flow structures to achieve a goal are represented graphically. Combined with a rule based causal reasoning engine, and quantitative dynamic simulation (with e.g., HYSYS) MFM can generate fault/cause and consequence trees/paths for a given deviation in a system function, and with a goal reasoning engine goal trees. The different trees can be used in reasoning to develop counteraction plans. The whole is called MFM workbench, see Figure 1. After process variable deviations have been specified the workbench facilitates HAZOP as a functional assistant by diagnosing the causes of abnormal situations. It does not have the aim of automating HAZOP. The concept is further elaborated, extensively described, and demonstrated on an offshore three-phase separator case by Wu et al. [22].
2012	Rodriguez and De la Mata [23]	*D-higraphs* are another way of modeling a process including controls. Developed in the late 1980s, D-higraphs represent in yet another way states (blobs, being a function effected by an actor - a machine - with an optional condition as a Boolean variable) and transitions (edges). Hence, D-higraphs combine in their representation function and equipment/structure, so it is more intuitive as there is more direct correlation with the real installation than in case of MFM. Distinction is made between mass, energy, and information edges. There are process (green), control (orange), and mixed (blue) blobs. The edges can be triggered or fired resulting in state changes. A blob can contain other (sub-) blobs and can also be partitioned to represent an OR-statement. Causal rules have been established. The system description is in three layers: structural, behavioral, and functional. Deviations are coded and the reasoning engine is constructing cause and consequence trees. For comparison the same distillation unit was ‘HAZOP-ed’ as Rossing et al. did. The D-higraph HAZOP assistant results were not different.
2012	Hu, Zhang and Liang [24] Hu, Zhang and Wang [25]	Having in mind prognosis for enabling predictive maintenance to prevent process upset a HAZOP method was developed assisted by a *Dynamic Bayesian Network* (DBN). A Bayesian network is a probabilistic acyclic graphical network consisting of nodes representing stochastic variables connected by edges or arcs representing conditional dependencies. The net models cause-

		consequence chains. Application was for a gas turbine plant where wear, fouling, and corrosion lead to faults. A DBN showing time sequenced changes was chosen because process faults due to degradation have often multiple propagation paths to different effects, some of which propagating to adjacent parts. This may lead to fault coupling and disaster. A DBN can represent these interactions in space and time by conditional probabilities. Degradation of components is modeled by a distribution, e.g., Weibull. Observable variable values can be obtained from the SCADA (Supervisory Control and Data Acquisition) system. Then, DBN-HAZOP can predict failure by not directly observable causes before it occurs.

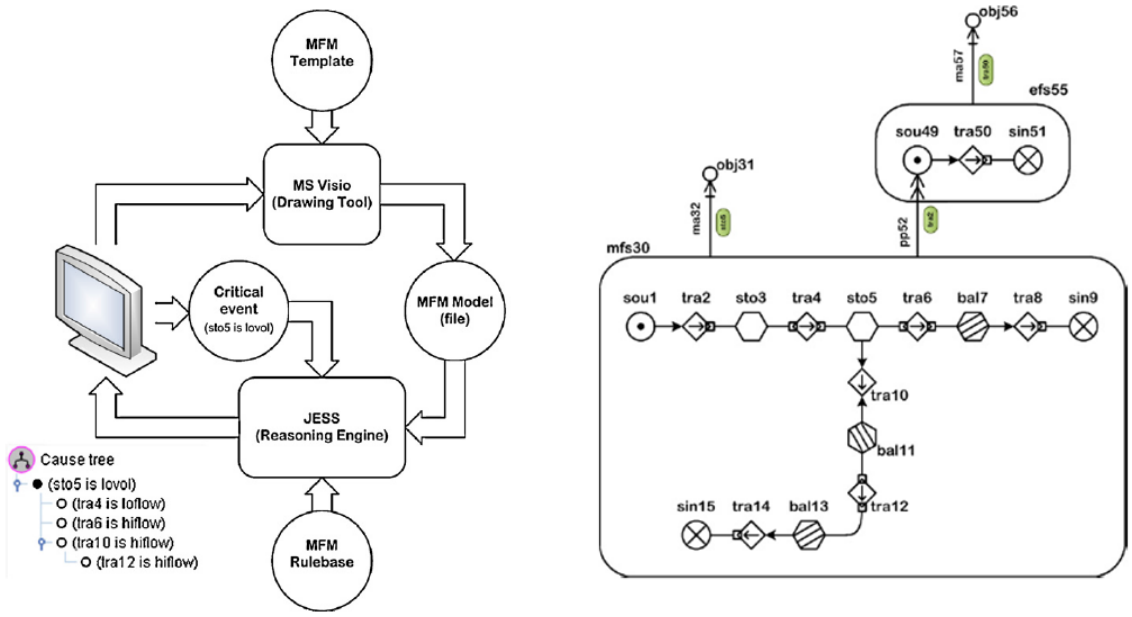


Figure 1. Multi-Flow-Model (MFM) Workbench functional HAZOP assistant developed by Rossing et al. [21]. On the right side a MFM sample is shown of the reflux part of an advanced distillation column design by the Danish Technical University (DTU) with component functions (e.g., tra = transport), flow structure, causal roles, and so-called means-ends. JESS means Java Expert System Shell. Left below is a cause tree derived from MFM.

Summarizing: automation is achieved by applying qualitative modeling and reasoning by expert system. Models range from relatively simple Digraphs to more sophisticated process simulation enabling revealing up- and downstream causes and consequences. Expert systems are rule-based inference engines or case based reasoning ones; the former must be fully programmed ahead of tackling a task, while the latter, given experience in a domain, learn further by doing (e.g., via neural networks of genetic algorithms). For the various attempts, Pasman [8] also tried to compare the effort needed to run a system and to assess their relative improvement over a team HAZOP-ing without a computer tool. However, comparisons can only be rather superficial; no round-robin has ever been organized. There are pluses and minuses with respect to the effort of conducting a case. The modeling will require quite some time, D-higraph more than MFM, but

both are less than the effort to develop an expert system not supported by a model. We shall consider the DBN approach for early warning in more detail in Section 5. Rather poor results of the SDG automated HAZOP system HAZID are reported by McCoy et al. [13], [14]. Roughly 10 - 30% of scenarios identified by the system were judged correct and useful. Others claim much better results.

The holistic system's approach: top-down and bottom-up

Scenario identification is an Achilles heel of risk assessment of designs and start-ups. Many accidents occurred according to scenarios never be thought of in the analysis early-on. Data mining algorithms, though, enable making much better use of existing accident/incident data bases. Paltrinieri et al. [28] showed by applying a similarity algorithm how data bases more effectively can be searched for scenarios fitting conditions and constraints by an actual situation being investigated. Findings can be structured as a bowtie of causes, a critical event, and consequences. They called the approach Dynamic Procedure for Atypical Scenarios Identification (DyPASI) and suggested its use for supplementing scenarios in risk assessment. Of course while running a plant, operators would be able to add possible scenarios based on their experience. The question is whether this is actually done in practice.

In 2011, MIT Professor Nancy Leveson in her book [29] clearly showed it will never be possible to identify all possible upsets and mishaps due to failing equipment, people, and software with all their possible interactions without considering the system as a whole and considering safety as a control problem. Safety is a system's emergent property. The system here is the sociotechnical system consisting of all hierarchical levels from the operational level (work floor) up to the president or prime minister on its way up passing the company's board. The levels connect through information flows: directional from top to bottom and feedback in return. Each level controls the one below. This holds for both the design stage and the operational one. Of course, extent of detail increases strongly in the direction of the work floor. The operational level controls the equipment in a number of parallel control loops, which themselves can contain control sub-loops. Accountability for the whole will be strongest at the board level.

According to Leveson, for safety focus shall be laid on a system's behavioral safety constraints. She developed a method to investigate accidents based on her approach called STAMP (System-Theoretic Accident Model and Processes) able not only to find the linear cause-consequence chains starting at a failing component but also to uncover complex mechanisms such as coincidences and faulty interactions of perfectly correct functioning components. Hence STAMP identifies systemic failures because of gaps in a system's risk control. From this method is derived STPA (System-Theoretic Process Analysis) which is her version of Process Hazard Analysis (PHA). For STPA one needs first to define the system with its boundaries and hierarchical levels, and then to define unacceptable losses, which enable determining the hazards to the system. Next is defining the safety constraints (instead of failure events) as those variable value combinations that form the borderlines of a system's safe state. Constraints can be physical (p, T, flow), organizational (e.g., procedural), or social (think of acceptable risk limit). Then, guide words will be applied on control loops. The guide word queries for each control loop are four, as illustrated in Figure 2:

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?

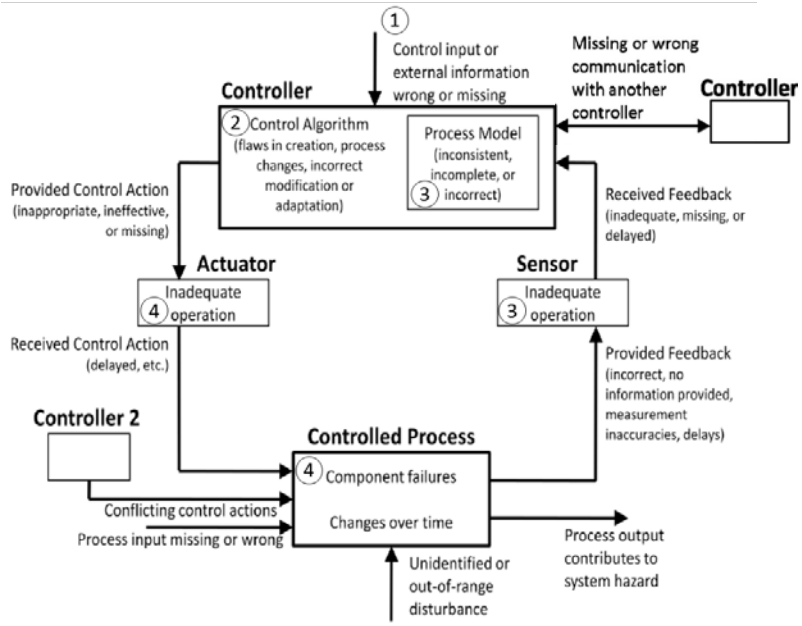


Figure 2. Generic STPA (system-theoretic process analysis) control loop to identify upset scenarios and to ensure safety according to the system approach launched by Nancy Leveson [29]. The circled figures refer to the four guide word queries mentioned in the text.

Although in principle all possible losses of control can be found, STPA functions in practice well when considering the system top-down. If one however tries to apply it on a low level and to build it bottom up to the system as a whole one becomes easily lost in a myriad of details. Thomas [30], at the time one of Leveson's Ph.D. students, laid a foundation for a computational tool coping with details but this must be further developed. A brief example of his method has been described in Pasman [8].

Ian Cameron's Blended Hazid approach (Seligmann et al. [31]) is also considering the whole system of plant, people, and procedures, but it is based on methods we are familiar with namely HAZOP and FMEA. The strength of BLHAZID is the computational aid, which shall be described in the next section.

Computer tools to facilitate HAZOP and store its results

Blended Hazid, or BLHAZID for short, has been described in a number of publications, e.g., [31], [32]. Briefly, the crux of the method is the computer storable semantics in which characterizing process variables, component capabilities, guide words, and the triplets of causes, deviations, and their impacts can be described. HAZOP results in functional failures (FF) and FMEA in component failures (CF). These failures combine in the triplets as (FF, FF, FF), (CF, FF, FF), (CF, FF, CF), (FF, CF, FF), (CF, CF, FF). Analyzing a plant results in thousands of triplets. Computer storage however enables generating for an abnormal situation a *causal graph*. The graphs visualize how an upset in a particular observable process variable can be caused by showing the propagation of faults in a causal chain tracing back to usually a multiple of possible root causes. The stored data generating the graphs can be used for verifying the PHA results. In

operational use it will guide an operator to a possible cause in the case of a process upset, or alternatively to train operators and make them aware of what could happen and how to respond. And finally the stored data will be a basis for later when again a HAZOP must be performed.

Much effort has been spent on reading by computer smart Piping and Instrumentation Diagrams (P&ID) in which much embedded information on functions of components, process conditions, control structures, and the like. According to Németh et al. [34] an intelligent P&ID provides input as a result of functional layering of equipment (mass/energy inventories, process lines, instrumentation and control, and sub-layers). Upon decomposition of the system, (semi-) automatically component function classification and design intent is obtained. This enables grouping in sections with distinct function, which will speed-up the BLHAZID exercise significantly. To make the BLHAZID software compatible with the different P&ID software packages took time. Other data are extracted from Material Safety Data Sheets (MSDS), flow sheets, procedures, and other sources.

As mentioned in Table 1, Zhao et al. [27] discussed the role process engineering ontology can have in automated HAZOP as applied in PHASuite. Ontology is defined as a hierarchical framework of concept descriptions within a certain domain. It has the structure of a taxonomy but the descriptions define the concept items. The ontology for process engineering purposes has been developed within the CAPE, computer aided process engineering, cooperation. CAPE was initiated in the late 1980s as a project with many contributors in a working party of the European Federation of Chemical Engineering, EFCE. Much information can be found on CAPE in the ESCAPE symposia series in Europe. Bogle and Cameron [35] discuss CAPE tools for off-line process simulation, design, and analysis.

Early diagnosis of process upsets using HAZOP results

Due to the measured variables at many different locations in a process with corresponding set points for an alarm to be triggered and the coupling of the chemical and physical mechanisms in a process, once an upset develops many alarms will annunciate and/or start sounding. Alarm flooding is undesired and often leads to confusion of the operator's team. Under time pressure finding the right action for response can introduce errors, may worsen the situation and may even lead to severe accidents, as has been shown in the past. Of course, safety instrumented functions or more passive layers of protection may be present to shut down and reduce consequences, but this all leads to a smaller or larger extent of economic damage.

Also, by distinguishing various types of alarms with different priorities and defining alarm clusters of related variables, alarm flooding can be limited but not eliminated. Therefore, it would be desirable to detect a developing upset in an early stage and by tracing the cause to redress the situation before the process variables start exceeding the safety envelope and even before alarms are triggered, as illustrated by Hu et al. in Figure 3. Information on causes also is useful for optimizing test and maintenance schedules. Hence, the problem is to deduce from observables, the pattern of measured process variables, hidden possible causes in the running process for the operator's eye.

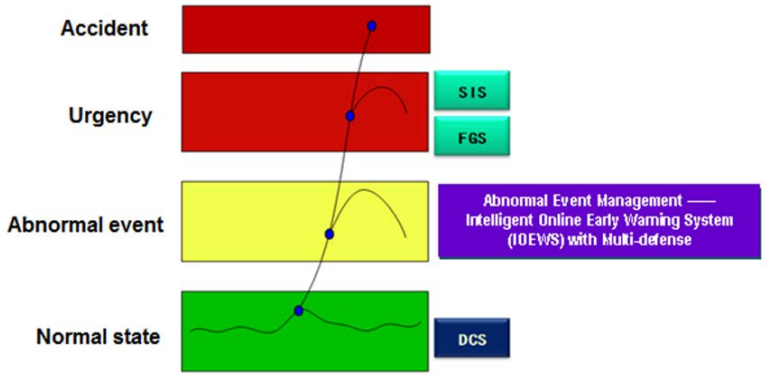
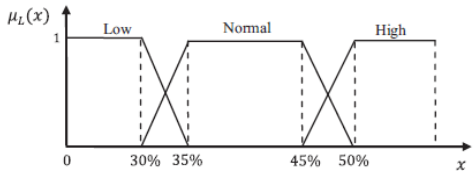


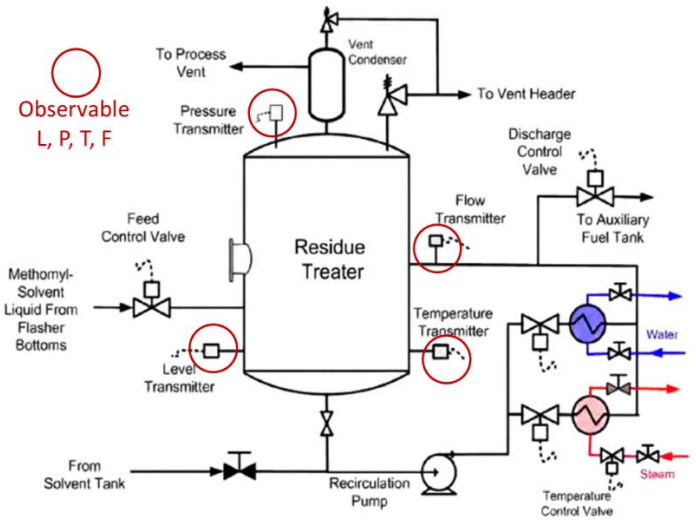
Figure 3. Early warning resulting in abnormal event management before the protective systems become activated, emergency shutdown must occur or an accident happens according to Hu et al. [39].

The BLHAZID causal graphs can help to find a cause more quickly, but in case of developing an abnormal situation it is still the operator who must detect the deviation, to take action by calling-up the relevant graph, and make a selection from the presented root causes. In the past year two approaches have been published to automate detection of an upset via measurement of increased risk level. Both make use of HAZOP results and both apply the Dynamic Bayesian Network (DBN) technique but are quite different in DBN implementation. A key point is the definition of possible abnormal situations. Both approaches make use of historical data. However, the first by Naderpour et al. [36], [37], [38] does that through operator experience and focuses on improved operator situation awareness. Experience with the process is elicited and absorbed by fuzzy logic via a linguistic gradation scale. The second by Hu et al. [39] takes historical process data and applies an algorithm developed in the artificial intelligence community to select the best DBN to enable tracing hidden causes from an input of observables. Both approaches shall be briefly described.

1). Naderpour et al. published the method in three journals. In two papers [36], [37] the example given was inspired by the CSB investigation [40] in the 2006 explosion of a vapor cloud released from an overheated 2000-gallon mixing tank containing a highly flammable liquid of which the temperature had to be maintained within a specific interval. The third [38] was actually motivated by the CSB investigation [41] of a run-away pressure vessel explosion in 2008. This concerned the treatment of a solvent containing the very toxic residue of methomyl product, of which the main part was centrifuged off in a previous step. The solvent treatment consisted of decomposing the toxic substance at an appropriate elevated temperature by recirculating the residue mixture through a reactor vessel until it is below a certain percentage. This third example will be used to illustrate the approach of Naderpour et al.

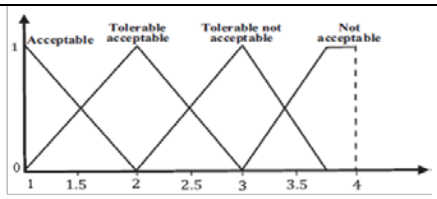


Level membership function example



Probability/Severity	Negligible	Minor	Medium	Major	Catastrophic
Very likely	TNA	TNA	NA	NA	NA
Likely	TA	TNA	TNA	NA	NA
Even	A	TA	TNA	NA	NA
Unlikely	A	A	A	TNA	NA
Very unlikely	A	A	A	TNA	TNA

Risk matrix: TNA Tolerable-Not Acceptable



Fuzzy product of probability and severity

Figure 4. *Left* is shown the reactor. Circled are sensor locations; *on top right* is an example of the fuzzy membership of the observable level, in the *middle* the decision risk matrix and at the *bottom* the resulting fuzzy risk level range. Adapted after Naderpour et al. [38].

The residue methomyl product in the solvent must be reduced to below 0.5% before the solvent can be burned. This occurs via decomposition into gaseous products in a 50% full tank at 135^{o}C and 20 psig (1.4 bar overpressure). To start the reaction the mixture is heated with steam; and following the reaction cooling water removes reaction heat, as shown in Figure 4. The operator monitored four process variables: the liquid level in the residue treating reactor, the recirculation flow, the temperature of the liquid, and the vessel pressure. The operators were asked to give limits on what they would call a low, normal, and high 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 fuzzy membership functions for each variable were constructed, but used as probability distributions. Next, with the aid of HAZOP results seven abnormal situation were defined, of which the first three are independent and the other four are dependent on others:

- SVC: situation of vent condenser failure allowing decomposition gases to enter the vapor stream entering the flare. By solids deposition this flow could be blocked increasing pressure in the vessel.
- SHL: situation of high liquid level
- SAR: situation of abnormal recirculation (hi or lo)
- SHP: situation of high pressure
- SHT: situation of high temperature
- SHC: situation of high concentration of methomyl in the residue in case the liquid had been heated first to 135^{o}C but for some reason cools then below 130^{o}C. In such case the incoming high concentration in the feed is not quickly decomposed, and by accumulation the concentration increases. To avoid runaway at reheating the mixture, the concentration should be measured and the heating adapted.
- SRR: situation of runaway reaction

The dependencies of the situations on equipment components causing an abnormal situation were determined, so that a Bayesian causal relations net could be constructed in which the

component failure probabilities are embedded (see Figure 5). The main threat is the runaway, SRR. There are four consequence reducing measures, called safety barriers, in case SRR occurs: an air monitor (triggers at concentration >1 ppm), an alarm, an ignition barrier, and several fire extinguishing cannons. The whole is configured as a time-step Dynamic Bayesian Network (DBN) with the components as the dynamic nodes and the observables as static nodes. At each time step the four SCADA observables: P, T, F, and L input their current value converted to a membership as a probability of the (static) nodes. The net is then evaluated and the probability of a consequence calculated.

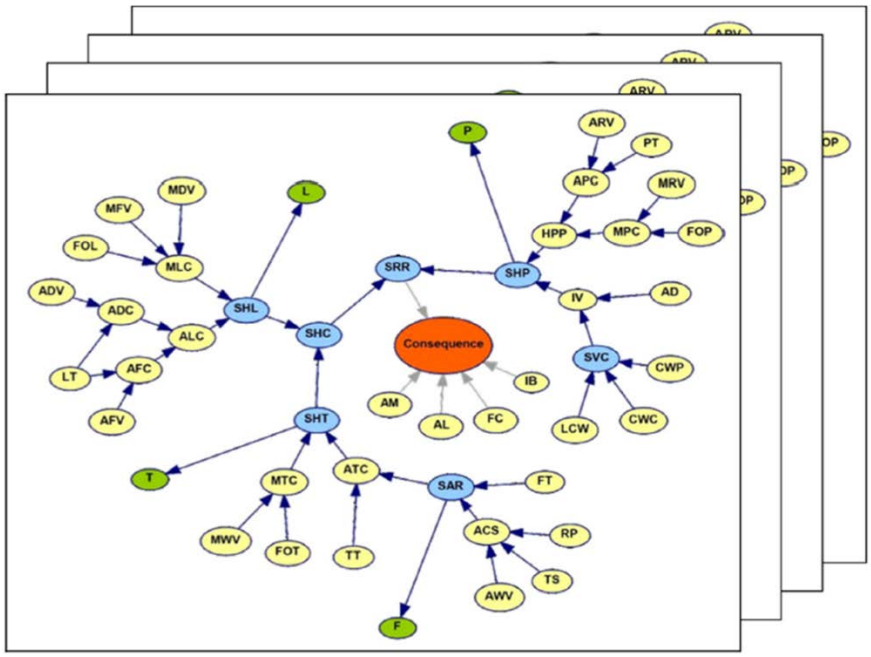


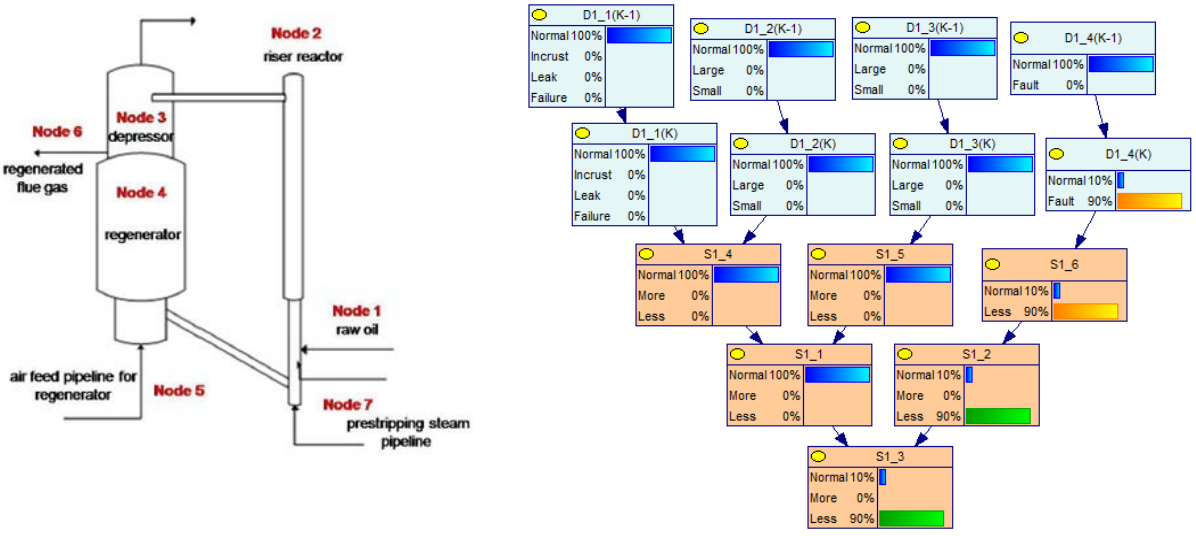
Figure 5. Dynamic Bayesian net of possibly failing (hidden) components of residue treating reactor causing abnormal situations of SAR, and/or SHT, SHL, SHC, SVC, SHP, and SRR (see text for these latter acronyms) after Naderpour et al. [38]. Observables L, T, P, and F provide updated evidence for each time step. Operator is alerted when risk level reaches TNA (see Figure 4). From the change in abnormal situation, nodes follow in the direction that fault should be pursued.

The consequence of a runaway can exhibit itself at six levels of severity, and corresponding damages were expressed in dollar units (up to $\$10x10^6$; for the calculation of risk the consequence range is taken in units of 10^6 from 0 - 10.). Six different types of damage with different loss amounts are represented in the consequence node as separate states (but the paper does not make clear how that is taken into account, other than in case of SRR, loss is $3x10^6$, which appears to be the average of the six types). Also operational losses are specified and included when it does not come all the way to a runaway but there is just a situation of high pressure, temperature, or concentration (up to $\$10^4$). Component failure probabilities range from 10^{-1} to 10^{-6} per year. The crux is further that both fuzzy consequence (C) and probability (Pr) are expressed on a 5-point scale. The combinations of C and Pr for decision-making are shown in a risk matrix resulting in four risk levels defined as acceptable (A), tolerable acceptable (TA), tolerable not-acceptable (TNA) and not-acceptable (NA). This produces the fuzzy risk graph

with a range of 0 – 4; TNA is at risk level 3. When risk increases to level 3, the operator is alerted.

While running the reactor, at each time step fuzzy multiplication of current C and current Pr values based on the observables yields the current risk level. Given the definitions reaching the level TNA, a developing abnormal situation is still in an early stage when an alerted operator can diagnose and take corrective action. The situation as reflected in the DBN can be followed in real time on an operator panel. Because the alert arrives ahead of process alarms, an acute problem is then still quite some time away. Possible causes follow from observed affected abnormal situation nodes or of their combinations. This early warning information will provide clues to possible component failures connected to affected situation nodes. The model enables a sensitivity analysis on the parameters showing most hazardous situations are a high pressure, and even more so, a high pressure and high reactor liquid level. An example is given of a high pressure resulting from a high concentration due to a cooling water isolation valve that was inadvertently closed (node CWC connected to SVC in Figure 5). All details of the network are not revealed.

2). Hu et al. [39] followed a different approach. They worked on a continuous process, a Fluidized Catalytic Cracking Unit (FCCU). Pre-operational HAZOP results were used for revealing and tracking fault propagation paths, and possible coinciding of faults and associated consequences. But for finding causes of abnormal situations, the information from HAZOP results is not sufficiently comprehensive and reliable. Equipment failures may be not specified by HAZOP (although BLHAZID which includes FMEA will be less suffering from this deficiency). To solve this lacuna, historical data on abnormal situations were collected revealing observable deviation patterns and causes. The so-called K2-algorithm, developed in the mid-1990s for the purpose of artificial intelligence and medical diagnostics [42], [43] and the Bayesian information criterion (BIC) [43] indicating the likelihood of a model found, were applied to derive the most probable Bayesian network structure describing the dependencies. As a further step using the historic data the probability density functions of the network parameters were extracted. Turning the static Bayesian network into a dynamic one (DBN) also the temporal dependencies of failing components can be accounted for. A two-step forwards-backwards algorithm (see Murphy [44]) is applied in order to infer probable fault root causes by failing



DBN Node	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	**Component**	**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

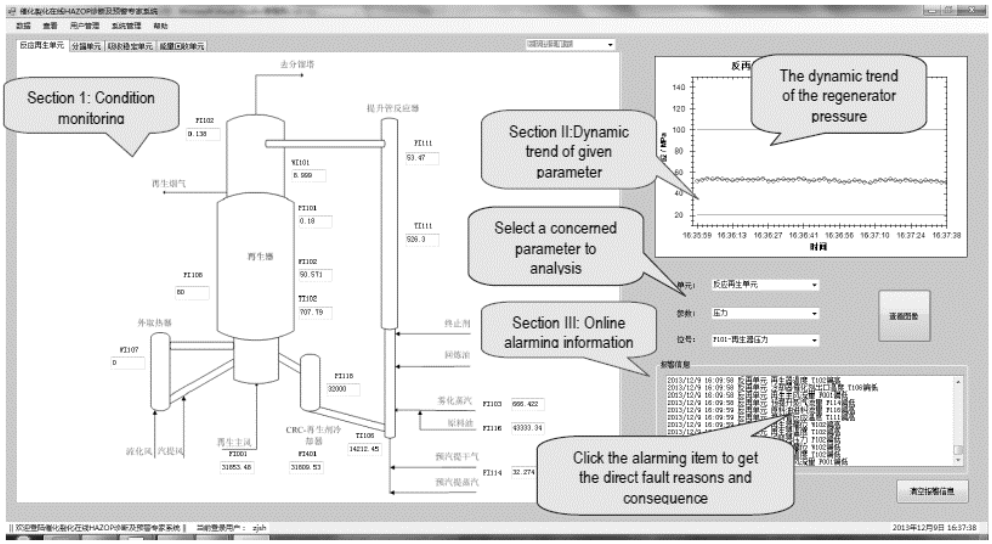


Figure 6. An impression of the work of Hu et al. [39]. *On top left*: Fluidized Catalytic Cracking Unit with the catalyst regenerator as the large vessel at left, and at right the riser reactor, connecting piping and designated HAZOP nodes; *on top right* is the Dynamic Bayesian net with its nodes specified in the 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.

equipment components hidden for the operator. Given the observed process variables sequence of the operating unit up to and including time *t*, a forwards inference calculation will yield the probability of state transitions of components at time *t*, given the state at *t*-1. Next, a backwards calculation will produce a predicted probability of the observed variable values at time *t*+1 and recursively later, given the state of components at *t*. Once a significant deviation is found, an alert is presented showing the most probable causes.

Hu et al. [39] described a case representing part of an FCCU, namely the catalyst regenerator in which coal deposits on the catalyst are burned with air flowing in at the bottom of the regenerator vessel. The partial HAZOP results show that two deviations can appear: air flow low and air flow stops. The latter is due to a failing compressor but the former has five possible causes:

- The main fan shut down;
- Anti-surge valve has opened;
- The main fan entrance filter net has been choked with adsorbate;

- Filter is sucked into the pipeline reducing the primary air flow;
- The flow control valve is faulty.

Based on the HAZOP results a number of DBN structures were configured. From the historical data 100,000 samples with fault data were extracted and with the K2 algorithm and BIC the DBN structure with the highest score was selected and the probability densities of the network parameters were derived. In the course of time while operating the unit, further updating is possible. The FCCU and a DBN representation are shown in the top of Figure 6, in the middle a table with DBN node designations (dynamic D is a component possibly failing as a 'hidden' cause, and static S are observable process variables) and at the bottom a reproduction of the interface of the Intelligent Online Early Warning System, IOEWS developed by Hu et al. [39]. The starting point of a run is all normal. In the example presented after some time, K, both regenerator temperature and air flow dropped below the safe threshold and the alarm was triggered. However, all other process variables had normal values. From the DBN output followed immediately that D1_4, the flow of the main air blower, must be the problem. It was concluded that the most probable causes are failure of the blower or a partly shut down valve in the air pipeline. Following this diagnosis, a field operator was instructed to examine the blower system.

Conclusions

HAZOP is an elementary building stone for plant and process safety. It is, however, not free of deficiencies and weaknesses, which mainly are due to human lack of insight, inattentiveness, and carelessness. Moreover, once accomplished its results are used only once for decision-making and are not used in operations. It is further labor-intensive and requires costly expertise. In addition, accidents often occur in non-routine activities such as start-ups, shutdowns, and turnarounds because of greater uncertainties due to wider ranges of potential upset consequences and reduced control as a result of non-routine activities. Freeing expertise for HAZOP-ing this kind of activities will therefore be useful.

A holistic system approach and considering safety as a control problem including dysfunctional interactions of healthy components and including human and organizational factors will result in the most effective methods for analyzing what can go wrong in a complex plant. However, supporting software to deal with a myriad of details still lacks. In due time this approach will enable a comprehensive predictive analysis: Leveson's System-Theoretic Process Analysis.

Full automation of HAZOP will be beyond any capability; semi-automation will be very useful, but results of attempts so far have not become common good. Recently, there are further developments. Progress in computing power and information technology enable a higher efficiency in handling and processing data. This enables connecting to computer aided designs and extraction of flow sheets and piping and instrumentation diagrams (P&IDs). Relatively simple process simulation models emerge that will help to guide and structure scenario thinking. Rule-based or possibly even better case-based reasoning engines will assist in generating possible deviations from design intent and scenarios. Encoding and storing results, as in BLHAZID of Cameron and coworkers, will enable re-use for different purposes such as verifications, operator training, and operational use.

Recently there have been two relatively successful demonstrations of operational use of HAZOP results for early warning in case of abnormal situations. The first is limited to a desk study of a hazardous process in which a Dynamic Bayesian Net (DBN) is developed using HAZOP results and operator experience with the process interpreted as linguistic variables in fuzzy logic. Actual process variable value deviations in abnormal situation are fed to the DBN and at a given risk level the operator is alerted and guided by the DBN to potential causes for the measured increase in risk.

The second example of a functioning fluidized catalytic cracking unit (FCCU) employs beside HAZOP results process historical data and applies sophisticated algorithms to construct the best fitting DBN with corresponding probability parameters. In case of abnormal situations the system automatically alerts and also here the operator is guided to where one or more likely causes are revealed. The FCCU example shown looks rather simple, but more complex situations can be envisaged.

These examples dramatize the potential for an operator early warning system capability to alert of faults in progress but in time for actions to identify causes and reduce risk of upset outcomes. This capability can be developed for great advancement in operational use of HAZOP results. The cost of such a program should be dwarfed by significantly reduced costs of fewer or averted upsets. Additional progress toward implementation can be achieved through collaborative projects with industrial data collected and analyzed to test cost effectiveness and to optimize the method.

References

1. Baybutt, P., *Competency requirements for process hazard analysis (PHA) teams*. Journal of Loss Prevention in the Process Industries 33 (2015) 151-158.
2. Baybutt, P., *A critique of the Hazard and Operability (HAZOP) study*. Journal of Loss Prevention in the Process Industries 33 (2015) 52-58.
3. Dunjó, J., Fthenakis, V., Vílchez, J.A., Arnaldosa, J., *Hazard and operability (HAZOP) analysis. A literature review*. Journal of Hazardous Materials, 173 (2010) 19–32.
4. Parmar, J.C., Lees, F.P., *The propagation of faults in process plants: hazard identification (Part I), Reliability Engineering 17 (1987) 277–302; The propagation of faults in process plants: hazard identification for a water separator system (Part II).* Reliability Engineering 17 (1987) 303–314.
5. Heino, P., Suokas, J., Karvonen, I., *An expert system in process design—analysis of process safety and reliability, in: IEEE AI '88*. Proceedings of the International Workshop on Artificial Intelligence for Industrial Applications, 1988, 225–231.
6. Venkatasubramanian, V., Zhao, J., Viswanathan, Sh., *Intelligent systems for HAZOP analysis of complex process plants*. Computers and Chemical Engineering, 24 (2000) 2291–2302.
7. Kletz, T.A., *Hazop--past and future*. Reliability Engineering and System Safety 55 (1997) 263-266.
8. 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.

9. Vaidhyanathan, R. and Venkatasubramanian, V., *Digraph-based models for automated HAZOP analysis*. Reliability Engineering and System Safety 50 (1995) 33-49.
10. Vaidhyanathan, R. and Venkatasubramanian, V., *A semi-quantitative reasoning methodology for filtering and ranking HAZOP results in HAZOPExpert*. Reliability Engineering and System Safety 53 (1996) 185-203.
11. Vaidhyanathan, R. and Venkatasubramanian, V., *Experience with an Expert System for Automated HAZOP Analysis*. Computers chem. Engng Vol. 20, Suppl., (1996) pp. S1589-S1594.
12. Srinivasan, R., and Venkatasubramanian, V., *Petri Net-DIGRAPH Models for Automating HAZOP Analysis of Batch Process Plants*. Computers chem. Engng Vol. 20, Suppl., (1996) pp. S719-S725.
13. McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P., and Heino, P.M., *HAZID, A Computer Aid for Hazard Identification; 1. The STOPHAZ Package and the HAZID Code: An Overview, the Issues and the Structure*. Trans IChemE, (Process Safety and Environmental Protection), 77B (1999) 317-326.
14. McCoy, S. A., Wakeman, S. J., Larkin, M.L., Chung, P. W. H., and Rushton, A. G.. *HAZID, a computer aid for hazard identification: 4. Learning set, main study system, output quality and validation trials*. Process Safety and Environmental Protection, 78 (2) (2000) 91–119.
15. Khan, F.I., and Abbasi, S.A., *TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner*. J. Loss Prev. Process Ind. 10 (1997) 333-343.
16. Khan, F.I., and Abbasi, S.A., *Towards automation of HAZOP with a new tool EXPERTOP*. Environmental Modelling & Software 15 (2000) 67–77.
17. Zhao, C., Bhushan, M., and Venkatasubramanian, V., *PHASUITE: An Automated HAZOP Analysis Tool for Chemical Processes, Part I: Knowledge Engineering Framework*. Process Safety and Environmental Protection, 83(B6) (2005) 509–532; *Part II: Implementation and Case Study*. ibidem 533-548.
18. Cui, L., Zhao, J., Qiu, T., & Chen, B., *Layered digraph model for HAZOP analysis of chemical processes*. Process Safety Progress, 27(4) (2008) 293–305.
19. Zhao, J., Cui, L., Zhao, L., Qiu, T., & Chen, B. *Learning HAZOP expert system by case-based reasoning and ontology*. Computers & Chemical Engineering, 33(1), (2009) 371–378.
20. Rahman, Sh., Khan, F., Veitch, B., Amyotte, P., *ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis*. Journal of Loss Prevention in the Process Industries 22 (2009) 373–380.
21. Rossing, N.L., Lind, M., Jensen, N., Jørgensen, S.B., *A functional HAZOP methodology*. Computers and Chemical Engineering 34 (2010) 244–253.
22. Wu, J., Zhang, L., Lind, M., Hu, J., Zhang, X., Jensen, N., Bay Jørgensen, S., Sin, G., *An integrated qualitative and quantitative modeling framework for computer assisted HAZOP studies*. AIChE Journal, 60 (12) (2014) 4150–4173.
23. Rodriguez, M. and De La Mata, J.L., *Automating HAZOP studies using D-higraphs*. Computers and Chemical Engineering 45 (2012) 102– 113.

24. Hu, J., Zhang, L., Liang, W., *Opportunistic predictive maintenance for complex multi-component systems based on DBN-HAZOP model*. Process Safety and Environmental Protection 90 (2012)376–388.
25. Hu, J., Zhang, L., and Wang, Y., *A Systematic Modeling of Fault Interdependencies in Petroleum Process System for Early Warning*. WCOGI2014, The 5th World Conf. of Safety of Oil and Gas Industry 1061598, June 8-11, 2014, paper OS8-4 1061598, Okayama, Japan.
26. Morbach, J., Yang1, A., Marquardt, W., *OntoCAPE—A large-scale ontology for chemical process engineering*. Engineering Applications of Artificial Intelligence 20 (2007) 147–161.
27. Zhao, C., Bhushan, M., Venkatasubramanian, V., *Roles of Ontology in Automated Process Safety Analysis.* Computer Aided Chemical Engineering, 14 (2003) 341–346.
28. Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., Cozzani, V., *Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool*. Journal of Loss Prevention in the Process Industries, 26 (2013) 683-695.
29. Leveson N.G. *Engineering a safer world, systems thinking applied to safety*. The MIT Press; 2011 608 pp., ISBN-10:0–262-01662-1, ISBN-13:978-0-262-01662-9.
30. Thomas J., *Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis*. Ph.D. Dissertation, Massachusetts Institute of Technology, April 2013.
31. Seligmann, B.J., Németh, E., Hangos, K.M., Cameron I.T., *A blended hazard identification methodology to support process diagnosis*. Journal of Loss Prevention in the Process Industries 25 (2012) 746-759.
32. Seligmann, B.J., *A Functional Systems Framework and Blended Hazard Identification Methodology to Support Process Diagnosis*. Ph.D. Dissertation, School of Chemical Engineering, University of Queensland, Australia, 2011.
33. Németh, E., Cameron, I.T., *Cause-Implication Diagrams for Process Systems: Their Generation, Utility and Importance*. Chemical Engineering Transactions, 31, (2013) 193-198, DOI: 10.3303/CET1331033.
34. Németh, E., Hockings, K., O'Brien, C., & Cameron, I.T., *Knowledge representation, extraction and generation for supporting a semi-automatic blended hazard identification method*. In CHEMECA 2009: The 39th Australasian chemical engineering conference, (2009). On CD, paper # 227 (pp 10.).
35. Bogle, I.D.L. & Cameron, D., *CAPE tools for Off-line Process simulation, Design and Analysis, in Software Architectures and Tools for Computer Aided Process Engineering*. B. Braunschweig and R. Gani (Editors), 2002 © Elsevier Science b.v., 373-392, ISBN-13: 978-0444549815, ISBN-10: 0444549811.
36. Naderpour, M., Lu, J., Zhang, Gq., *A situation risk awareness approach for process systems safety*. Safety Science 64 (2014) 173–189.
37. Naderpour, M., Lu, J., Zhang, Gq., *An intelligent situation awareness support system for safety-critical environments*. Decision Support Systems 59 (2014) 325–340.
38. Naderpour, M., Lu, J., Zhang, Gq., *An abnormal situation modeling method to assist operators in safety-critical systems.* Reliability Engineering and System Safety 133 (2015) 33–47.
39. Hu, Jq., Zhang, Lb., Cai, Zs., Wang, Y., Wang, Aq., *Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework*. Process

Safety and Environmental Protection, in Press, Corrected Proof, Available online 7 April 2015, doi:10.1016/j.psep.2015.02.003.

40. U.S. Chemical and Hazard Investigation Board, *Investigation Report, Confined Vapor Cloud Explosion, CAI, Inc. and Arnel Company Inc., Danvers, MA, Nov.22, 2006*, Report No. 2007-03-I-MA, May 2008
41. U.S. Chemical and Hazard Investigation Board, *Investigation Report, Pesticide Chemical Runaway Reaction, Pressure Vessel Explosion, Bayer Cropscience, LP. Institute, West-Virginia, August 28, 2008*, Report No. 2008-08-I-WV, January 2011.
42. Cooper, G. and Herskovits, E., *A Bayesian method for the induction of probabilistic networks from data*. Machine Learning, 9 (1992) 309-347.
43. Heckerman, D., *A Tutorial on Learning with Bayesian Networks*. March 1995 (Revised November 1996), Microsoft Research Technical Report MSR-TR-95-06, http://research.microsoft.com/en-us/um/people/heckerman/tutorial.pdf.
44. Murphy, K.P., *Dynamic Bayesian Networks: Representation, Inference and Learning*. Ph.D. Dissertation, University of California Berkeley, Fall 2002, http://www.cs.ubc.ca/~murphyk/Thesis/thesis.html.
45.