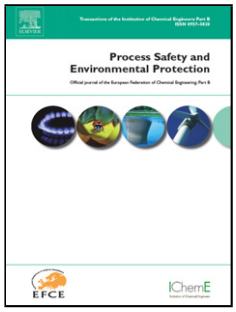
Accepted Manuscript



Title: Process Hazard Analysis, Hazard Identification and Scenario Definition: Are the conventional tools sufficient, or should and can we do much better?

Authors: Ian Cameron, Sam Mannan, Erzsébet Németh, Sunhwa Park, Hans Pasman, William Rogers, Benjamin Seligmann

PII: S0957-5820(17)30030-7
DOI: http://dx.doi.org/doi:10.1016/j.psep.2017.01.025
Reference: PSEP 965

To appear in: *Process Safety and Environment Protection*

Received date: 25-11-2016
Revised date: 21-1-2017
Accepted date: 25-1-2017

Please cite this article as: Cameron, Ian, Mannan, Sam, Németh, Erzsébet, Park, Sunhwa, Pasman, Hans, Rogers, William, Seligmann, Benjamin, Process Hazard Analysis, Hazard Identification and Scenario Definition: Are the conventional tools sufficient, or should and can we do much better?.Process Safety and Environment Protection http://dx.doi.org/10.1016/j.psep.2017.01.025

Process Hazard Analysis, Hazard Identification and Scenario Definition

Are the conventional tools sufficient, or should and can we do much better?

Ian Cameron[a], Sam Mannan[b], Erzsébet Németh[a], Sunhwa Park[b], Hans Pasman[b1], William Rogers[b], Benjamin Seligmann[c]

[a] *School of Chemical Engineering, The University of Queensland, Brisbane, Queensland, Australia*
[b] *Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chem. Eng., Texas A&M University, College Station, TX, USA*
[c] *Department of Chemical Engineering, Curtin University, Perth, Western Australia, Australia*
[1] Corresponding author, *E-mail address*: hjpasman@gmail.com

Highlights

- The weakest link in risk assessments is hazard identification/scenario definition.
- Existing methods, such as HAZOP and FMEA, do not guarantee completeness.
- Attempts to semi-automate HAZOP on plant do not seem to be fully satisfactory.
- Only a system approach can provide completeness on plant, people, and procedures.
- New possibilities are reviewed including an operational use of HAZID results.

Abstract

Hazard identification is the first and most crucial step in any risk assessment. Since the late 1960s it has been done in a systematic manner using hazard and operability studies (HAZOP) and failure mode and effect analysis (FMEA). In the area of process safety these methods have been successful in that they have gained global recognition. There still remain numerous and significant challenges when using these methodologies. These relate to the quality of human imagination in eliciting failure events and subsequent causal pathways, the breadth and depth of outcomes, application across operational modes, the repetitive nature of the methods and the substantial effort expended in performing this important step within risk management practice. The present article summarizes the attempts and actual successes that have been made over the last 30 years to deal with many of these challenges. It analyzes what should be done in the case of a full systems approach and describes promising developments in that direction. It shows two examples of how applying experience and historical data with Bayesian network, HAZOP and FMEA can help in addressing issues in operational risk management.

Keywords: Process hazards; hazard identification; HAZOP automation; scenario generation

1. Introduction

All safety considerations start with recognizing possible hazard events, hence the necessity of hazard identification (HI) via process hazard analysis (PHA). Hazard identification has the objective of defining all possible (*non possumus*) scenarios or sequences of events in which a hazard with its associated chance of realization will generate risks to people, assets, environment or corporate reputation. The potential causing the hazardous situation can reside within the system for a long time or could result from a set of temporal conditions.

PHA is a basic step towards risk assessment and risk management of a technical system and its process. Throughout the history of process design and operation much was learned by trial and error. Today, properties of materials are not regarded as a problem but 50 years ago they were. Many test methods did not yet exist. Phenomena such as runaway or vapor cloud explosion were unknown. Although sound knowledge of the material properties is a first requirement for a PHA, a *conditio sine qua non,* we shall assume for this paper that it is adequately represented, and we shall focus on finding out "*how things can go wrong*".

Early-on, it became already clear that an individual person is not able to think of all possible ways a mishap can occur. The first more or less formal method to evaluate plant process safety was application of a *checklist* based on experience. It required investigating properties of substances, reaction patterns, equipment hazards, safety devices, storage and loading, plant layout, emergency planning and the like. Another, even less formal and perhaps older method is *'What-if?'* For example: what-if valve V1 is shut, while it should be open?

Subsequently, a systematic, scenario oriented method appeared, which was designated Hazard and Operability Study (HAZOP). According to a paper in the 1971 Newcastle Major Loss Prevention in the Process Industries Symposium by Houston (1971) of Imperial Chemical Industries (ICI.), UK, in the case of a new design, safety was initially judged by "how well it will work". As existing codes of practice fell short, for a new design an "Operability Study" was undertaken. Based on a flow sheet, and later a Piping & Instrumentation Diagram (P&ID), a team of experts systematically examined line by line for possible process deviations, and if one was found, what would cause it, and what would be the consequence. Process deviations from design intent were investigated following a brief checklist of guide words, such as More, Less, etc., with the main ones as we know them from today's HAZOP (Hazards and Operability).

In his 1997 article on HAZOP, Trevor Kletz (1997), also in ICI at the time, mentioned more details. The HAZOP inception was in 1963/64 on a new phenol plant design minimized with respect to capital cost, and the team that should operate the plant was given the assignment to perform a 'Critical Examination'. The latter was known at the time as a formal method asking questions, what is achieved, what else could be achieved, what should be achieved, how, when, and who has achieved it. A team of three worked three days a week for four months and found many operating problems and hazards. It later turned out that elsewhere in ICI the same critical examination technique had been applied before. From this, HAZOP as a formal method emerged and conquered the chemical process world and beyond to across a large variety of design activity. However, even in the first journal publication Lawley (1974), also at ICI, it was separately called the Operability study method and the Hazard analysis method. The method became formalized and an extensive literature evolved on how to efficiently apply it. Dunjo et al. (2010) has summarized the history, the literature of how best to perform HAZOP, as well as the attempts to include human failure and other aspects and applications.

Another systematic method that found general application is Failure Mode and Effect Analysis (FMEA) to which Criticality Analysis (FMECA) can be added to increase its rigor. The method started in 1949 as

a military procedure in MIL-P-1629 “Procedures for Performing a Failure Mode, Effects and Criticality Analysis”. Navy-Air converted it to standard MIL-STD-1629 in 1974, being further developed to version A in 1980. The method was applied in design in aerospace and then spread to other industries. Basically, from a piece of equipment the failure modes and their effects shall be identified, subsequently the causes and controls to prevent, and actions to be executed. FMECA, although applied basically as a reliability engineering tool according to the standard, found application too in maintainability, safety analysis, survivability and vulnerability, logistics support analysis, maintenance plan analysis, failure detection, and isolation sub-system design. Hence, where HAZOP is oriented towards operational function as seen in the systems states of temperature, pressure, flow and the like, FMEA is centered on component function and failure. These two methods overlap.

There are many more identification methods created for specific system purposes. These include approaches such as Taylor’s action error analysis (Taylor, 2013), which is a kind of HAZOP on potential operator errors, or sneak analysis developed for electronic circuitry fault finding. A huge range of human factors methods have been developed over the last 25 years (Stanton et al., 2005). However, these methods have generally never reached the level of application in the process industries as have HAZOP and FMEA.

Meanwhile, in many countries, major hazard facilities and other process installations are required by law to not only perform hazard identification before the start of operations but also on a regular, repeating basis such as 5 years for the life of the installation. This requirement signifies the importance of the activity. Missing a scenario and therefore not being prepared to prevent and counter the undesirable outcomes may lead to disaster.

In summary, process hazard analysis (PHA), hazard identification (HI) and scenario definition form the cornerstone of the safety management system, and this is a team effort based on knowledge, experience, and human imagination of what can go wrong. In the next section we review the limitations of current methods due to the considerable effort, expense and the potential weaknesses in human imagination. Following that, we formulate some research questions and ways to improve hazard identification and to enhance the effectiveness and efficiency of the effort.

This paper was inspired by two CET published conference papers for the 15th International Symposium on Loss Prevention and Safety Promotion in the Process Industries 2016 in Freiburg, Germany, respectively, the one of Pasman and Rogers (2016) and that of Cameron, Németh and Seligmann (2016).

2. Current challenges and limitations

In considering the question:

“Are the conventional tools sufficient, or should and can we do much better?”,

it is helpful to discuss what is meant by “sufficient”, and what constitutes “much better”.

First, in relation to ‘*sufficiency*’ or meeting stated needs, practical application of techniques, such as HAZOP or FMEA, over many decades have certainly given excellent insights into the integrity of process designs and important operational aspects. However, these techniques have often been judged as not meeting needs for a variety of reasons, which are inherent in the methodologies and the particular manner in which they are applied. This is particularly evident in major accident reviews where deficiencies in HI were regarded as a major contributing factor in the accident.

The shortcomings can include: a lack of breadth and depth of analysis, a lack of team diversity and imagination, tedium, exhaustion, effort and expense, effective capture and communication of outcomes, follow through to final consequences, poor prioritization of associated risks, handling

multiple operating modes, interaction with people and procedures, and the effectiveness of outcomes on decision making as HI outcomes are passed across various organizational groups (Kletz, 2009). All these issues can diminish the '*sufficiency*' of the method and its applications: in some cases, with disastrous outcomes.

Second, there appears little objection against the idea that we should be doing better than the current situation. Past development efforts have focused on some of these issues with varying degrees of success. Others have stalled due to internal policies and procedures of companies that do not wish to disrupt existing practices and who remain to be convinced of the benefits of change.

Third, it is evident that with a growing focus on life cycle perspectives, accompanied by significant advancement in information and communications technologies (ICT), there are many opportunities to "*do much better*". Exploiting systems thinking and ICT advancements can drive beneficial change. What follows discusses these issues.

Since HAZOP is the main tool to identify scenarios, we focus on its limitations. In the first place there is the limitation in effort capacity. Conducting a HAZOP is labor intensive. To not lose focus, a team of five should work only half days on a project. Each P&ID requires about 5×20 hours, and for a plant depending on size 1 to 6 weeks may be required for a HAZOP. As this must be performed in the design stage, once more before commissioning, and every five years after being in operation, the effort and costs add up. Meanwhile the results usually sit on a shelf and are not used in day-to-day operations; this also reduces its cost effectiveness.

Serious, however, are the limitations due to the range of personnel abilities and the quality of effort that can lead to the missing of key hazard scenarios. Paul Baybutt (2015a) in one of his numerous recent articles on PHA topics described the many different types of weaknesses and failures a HAZOP study can suffer from. Baybutt mentions as first contribution the weaknesses due to lack of imagination and creativity of the team members, not taking time to self-reflect, misunderstanding of the terms, and exhaustion. Further, there are weaknesses in design intent coverage as it appears from the P&ID and other information presented, as well as ambiguities in the definitions of related process parameters and their lack of completeness. There may be weaknesses in the identification of deviations resulting in confusion, because a deviation is not a cause but an intermediate effect of which the cause must be inferred and the impact must be deduced, whereas a combination of guide words on a parameter may generate different deviations. Some deviations may result only from a combination of guide words, while sometimes different guide words lead to the same deviation. Also, a small deviation may cause a large, more significant deviation, so the impact must be thought through to the final consequence. Guide words may be too restricted, which could lead to initiating events missed and in turn to scenarios not identified. On the other hand, deviations will also identify hazards that will be of little concern, although focusing only on the known major hazards may lead to overlooking not well known but yet serious hazards under certain conditions. Chemical reactivity hazards need not be triggered by a common deviation and are of a special kind. Process changes after a HAZOP has been completed may lead to a nasty surprise. Incomplete description of scenario elements in the HAZOP report may have consequences for measures to be installed. In a further article Baybutt (2015b) discusses competency requirements for HAZOP team members.

So, even if with much effort a HAZOP study has been accomplished, there remains uncertainty in the completeness of defined important scenarios, being those conditionally leading to significant upset outcome consequences. Yet, the number of possible scenarios is finite. Therefore, as part of a system approach, monitoring and learning from system behavior in the operational stage beyond the HAZOP, including unusual behavior, near misses, and upsets, is crucial to identify previously overlooked

scenarios and also to identify newly developed upset scenarios as the system continually changes with time.

In FMEA or FMECA similar weaknesses *w*ill exist. A thorough analysis assumes sound knowledge of the failure modes of equipment components and the effects these can bring about. A failure mode is the observable effect of a failure, which is a failure to perform an intended function. It shall not be confused with an underlying or root cause as the cause of the failure is often elsewhere in the system or deeper down in the component. Focus bias on lower frequency, large severity consequences shall be avoided, because high occurrence rates of effects with smaller severities can cumulatively lead to larger significant risk. For evaluating a FMEA score a risk priority number (RPN) is derived, which contains not only severity and occurrence rate but also failure detection probability. Uncertainty in RPN can be estimated from uncertainties estimated for each of severity, occurrence rate, and failure detection probability.

The previous leads to three questions:

- How can we improve the effectiveness of hazard identification and scenario definition?
- How can we enhance the efficiency of the effort?
- Would it be possible to use the hazards analysis findings in the operational stage and be able to correct and augment through operational experience?

In Section 3 of this paper automation attempts in the last two decades will be briefly reviewed, while in Section 4 new approaches will be described, and in Section 5 two recent examples of operational use of HAZOP results will be summarized.

3. HAZOP automation attempts

Computer assistance of a PHA team has already a long history. Several commercial guidance programs are available, such as ABS Consulting LEADER^{TM} and Dyadem (AcuTech Consulting Group) PHA-Pro. These administrative support software programs will alleviate the task of a HAZOP team but will not replace it.

Attempts to automate HAZOP started in the mid-1980s with Parmar and Lees (1987), applying a rule-based approach, and Cameron (1986) using expert systems based on Prolog. A little later this was followed by Heino et al. (1988), who used a more advanced rule based expert system making use of the artificial intelligence progress in those days. It consisted of a knowledge base of IF-THEN rules and an inference engine generating the deviations. Quite a few automation developments, mostly following the same principles, have been summarized by Dunjo (2010). A step forward has been to include a simulation model of the process to check effects and stimulate the imagination. Figures 1 and 2 show the significant developments since 1995 towards semi-automated HAZOP. The figures and text are based on contributions selected first by Pasman (2015) and further completed for this article. All of these developments make use of simulation models of various kinds. Figure 3 is in a way a continuation of the history of Figure 2. A rather special one is the Multi-level Flow Model (MFM) of Rossing et al. (2010) presented in Figure 4 showing a functional type modeling approach.

3.1 Khan and Abbasi, and Rahman et al. (1995-2009)

Figure 1 represents how Khan and Abbasi, and later Khan and coworkers developed semi-auto-mated HAZOP. In 1995, the initial step of this progression was to develop HAZEXPT for the fundamental HAZOP knowledge-base (Khan and Abbasi, 1997a). This knowledge base consisted of process-specific and process-general components. Having developed the knowledge-base, they proposed the optHAZOP study procedure to increase efficiency by eliminating repetitive tasks. At the same year, in 1997, to enable HAZOP automation, TOPHAZOP (Khan and Abbasi, 1997b) advanced in a systematic

way with three structures (knowledge-base, inference engine, and user interface). TOPHAZOP generates deviations and contains rule-based trees linking to process specific attributes, via process parameters, and deviations to causes and consequences. Through EXPERTOP (Khan and Abbasi, 2000) and ExpHAZOP+ (Rahman et al. 2009), the three structures evolved further to a user-friendly environment and larger database. ExpHAZOP+ added an updated feature to the knowledge base and introduced a unique *fault propagation algorithm*, identifying downstream causes and consequences from an identified upstream event.

3.2 Venkatasubramanian and coworkers (1990-2005)

The progression path of contributions by Venkatasubramanian and coworkers with semi-automatic HAZOP is shown in Figure 2. The purpose was also to reduce routine and repetitive tasks regarding HAZOP analysis. However, Venkatasubramanian and Vaidhyanathan (1994) began early-on with the concept of propagation of relevant disturbances downstream to different HAZOP nodes. Srinivasan and Venkatasubramanian (1996) also considered batch processes thoroughly dealing with process procedures. As a prototype of this development, HAZOPExpert was put forward with a systematic framework: Knowledge-base, Inference engine, and Graphical User Interface. The HDG (HAZOP DiGraph) model was proposed to qualitatively represent causal structures of chemical process systems graphically, and a more user-friendly environment was created. Subsequent to the HDG model, a semi-quantitative reasoning approach was introduced to reduce ambiguity in the analysis with the previous qualitative methodology; the expert system was provided with the semi-quantitative reasoning that is checking, whether in the case of loss of containment, conditions surpass the auto-ignition threshold, and whether a spill presents a toxicity risk. The semi-quantitative reasoning further checks the adequacy of protective As follow-on to continuous processes, Batch ExpertHAZOP evolved for batch processes applying Petri Net modeling, which represents tasks regarding procedures and time-intervals. Venkatasubramanian et al. (2000) presented a summary and evaluation of the work done so far. Finally, in 2005 the highly-qualified software tool, PHASuite was launched as an automatic HAZOP analysis by combining the previous steps with new methodologies (e.g., the Colored Petri-Nets and Batch Plus®).

3.3 STOPHAZ project (1999-2000) [McCoy et al., 1999; McCoy et al., 2000]

The software system HAZID consists 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 reads in the plant description and builds 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, which 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.

3.4 Cui et al. (2009-2010), and Zhao et al. (2009)

As an extension of the methods, in particular for 'non-routine HAZOP analysis' of Vaidhyanathan and Venkatasubramanian (1996a; 1996b), Cui et al. (2009 and 2010) and Zhao et al. (2009) proposed the Layered Digraph Model (LDG), LDGHAZOP with Smart Plant P&ID (SP P&ID®, Intergraph) embedding many process and equipment data, and PetroHAZOP, as shown in Figure 3. 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 in Zhao et al. (2005) use is made of CAPE (Computer Aided Process Engineering) ontology for process systems. Ontology means in this context a hierarchical structure of concepts describing the entities in the domain explicitly. CAPE is explained, e.g., by Bogle and Cameron (2002).

A case in Case Based Reasoning consists of a problem/situation, solution, and an outcome description. A new problem is judged on similarity by an algorithm based on predefined indexes. It is thus highly domain dependent. The system functions in the Chinese petrochemical industry with 900+ cases. A future effort was announced to combine the two approaches mentioned above.

3.5 Rossing et al.(2010); Wu et al.(2014)

The Multi-Flow-Model (MFM) approach described by Rossing et al. (2010) was developed by co-author Lind in the early 1990s for nuclear power plants and 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 symbols) for objectives (source, transport, storage) and functions (sink, barrier, balance). MFM also describes the interactions of mass, energy, and information flows, which are combined to flow structures. Symbols are available for functions as management, decision, and actor action. Further, a set of so-called means-ends relations (with symbols for produce, producer product, maintain, and mediate) and causal roles (with condition, agent, participant symbols) describe dependencies among functions. The interconnected flow structures to achieve a goal are represented graphically. Combined with a rule based causal reasoning engine, and a quantitative dynamic simulation with for example HYSYS, MFM can generate fault/cause and consequence trees/paths for a given deviation in a system function, and with a goal reasoning engine to generate goal trees. The different trees can be used in reasoning to develop counteraction plans. The produced causal tree suggests causes of a deviation. The system is called the MFM workbench, as seen in Figure 4. 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 fully automating HAZOP. The concept is further elaborated, extensively described, and demonstrated on an offshore three-phase separator case by Wu et al. (2014)

3.6 Hu, Zhang and Liang (2012); Hu, Zhang and Wang (2014)

Having in mind prognosis for enabling predictive maintenance to prevent process upsets, 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. An 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 often have multiple propagation paths to different effects, some of which are propagating to adjacent parts. This propagation 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, such as Weibull. Observable variable values can be obtained from the SCADA (Supervisory Control and Data Acquisition) system. Then, DBN-HAZOP can predict failure by inference rather than directly observing causes before failure occurs.

3.7 Rodriguez and De la Mata (2012)

D-higraphs are yet another way of modeling a process including controls. Developed in the late 1980s, D-higraphs represent in 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 both function and equipment/structure, so it is more intuitive as there is more direct correlation with the real installation than in the case of MFM. A distinction is made among 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 and coworkers had previously done. The D-higraph HAZOP assistant results were the same.

3.8 Conclusion for semi-automated HAZOP

Full-automation has never been achieved, but by applying qualitative process modeling and through reasoning by expert system semi-automation has been possible. Process models range from relatively simple digraphs to more sophisticated process simulation approaches enabling the disclosure of up- and downstream causes and consequences. Expert systems used are either rule-based inference engines, or case based reasoning ones. When rule-based, they must be fully programmed for a task; in contrast, given experience in a domain, case-based ones continue learning by modeling via neural networks of genetic algorithms.

It would be desirable to determine the quality gained by automation and the reduction in effort. Fair comparisons, though, are hardly possible. The modeling of a process will require quite some time, for example D-higraph requires more effort than MFM, but both are less than the effort to develop an expert system not supported by a model. McCoy et al. (1999; 2000) applying the signed digraph approach for the HAZOP system named HAZID, reported the rather poor result of roughly 10 - 30% of scenarios, identified by the system, as assessed to be correct and useful. Other researchers claimed better results.

It can be concluded that to make progress, a *round robin* must be held. This would require defining a test case just as for the Tennessee Eastman process in control theory, but here for HAZOP-ing a real plant is required to compare the performance of conventional HAZOP teams with promising semi-automated systems. The number of statistically needed trials will depend on the magnitude of differences found, but the larger the number of trials the lower the uncertainty in the result.

4 New extended systems methods

4.1 Why a system approach

Many accidents have occurred according to a scenario that no one had conceived. Clearly, scenario identification is the Achilles heel of risk assessment. It should be considered an important initial step to be followed by continuous or frequent monitoring to track system behavior and to respond and learn from periodic unusual system behavior. This is identified as newly developed scenarios paths, as the system changes with time, resulting in new failure outcomes. In process safety with the present experience of "black swans", low probability but high consequence severity events are extremely rare Taleb (2010). This is because following many such accidents information emerges from investigations to show that such outcomes should have been conditionally foreseen and therefore were not "black swans". Problematic are the coincidental confluences of rare conditions, the so-called "perfect storms", causing disaster as described for a case of a tragic shipwreck by Sebastian Junger (2012) and remarked by Elisabeth Paté-Cornell (2012). Nobel Prize winner economics, psychologist Daniel Kahneman (2011) in his book 'Thinking, Fast and Slow' attributes the missing of scenarios by analysts to the effect of WYSIATI, or rather What You See Is All There Is. In other words, when asked to generate one, there is a certain scenario one thinks of first and due to the laziness of what Kahneman calls our

System 2[2], the rational thinking, no other scenario will come to mind. This is apart from effects that we don't like to think of what can go wrong, and the 'it will not happen to us' attitude, which is an example of certainty seeking where there is no certainty. We avoid certainty delusion by investigating, learning from, and making adjustments following near misses and unusual system behavior that show new scenarios with potential upset outcomes developing as the system changes with time.

Process Flow Failure Mode (PFFM) analysis

A certainly more comprehensive alternative method to HAZOP is the Process Flow Failure Modes (PFFM) analysis developed in Canada and first published by Ego and MacGregor (2004), not using the name and acronym PFFM at that time. In brief, the method is a structured, systematic 'What-if' technique following the direction of flow. MacGregor skilled in HAZOP gained more than a decade of further experience with PFFM, describing the method in MacGregor (2013) and reporting recently (MacGregor, 2016) about three cases in which HAZOP results are compared with PFFM. The results show that PFFM yields many more scenarios. Averaged over three in-depth cases, PFFM found twice as many scenarios as HAZOP and in addition within a shorter time spent on the exercise. Some scenarios that were not in a HAZOP could, when realized, have a disastrous effect. A number of reasons are given. In the first place PFFM is intuitive and starts the scenario development with a possible cause, then in thinking moves on to a potential consequence (an uncontrolled loss of containment, LoC), and identifies whether adequate controls are present to prevent this LoC and if not give a recommendation. To enable this, from a P&ID a somewhat simpler, so-called safeguarding flow diagram (SFD) is derived and as in HAZOP divided in sections or nodes (with the flows indicated in different colors). The SFD contains more information than a process flow diagram (PFD) though. All stream deviations and equipment in a process plant of which failure has an effect on the process are given with the possible failure modes in a master list assembled over a period of more than 15 years. Incoming flows in a section may show deviations up or down of pressure, temperature, flow rate or concentration outside the design envelope. Flows exiting a node are queried for blockage and reversing. Prior to the team meeting one determines in flow direction which equipment failures or operator errors will disturb the process and collects the causes contained in the list to prepopulate a worksheet. The analysis in the subsequent team meeting follows again the direction of flow to a next component (valve, pump etc.) considers the causes in the worksheet, if detected adds additional ones, evaluates potential consequences and controls (safeguards/barriers, such as pressure relief or check valves) and so proceeds from section to section. This method hinges on the list of causes assembled over many years of experience and which therefore can be considered as a check-list. Hence, it is a good step forward but does not guarantee completeness. Of course, a highly experienced HAZOP team with specialized knowledge of a certain type of plant may have an even longer "checklist". Even if that checklist is not written down, they may do better than PFFM.

Need of a scenario database and inclusion of non-continuous operations

We avoid certainty delusion by investigating, learning from, and making adjustments following near misses and unusual system behavior that show new scenarios with potential upset outcomes developing as the system changes with time. But that assumes we have a data base system of potential scenarios that can be easily updated in the operational stage. This should include the start-up, shutdown and turnaround operations of continuous processes. A high fraction of total accidents occurs during these non-continuous activities. Batch operation manipulations repeat themselves rather well

[2] According to Kahneman and his late colleague and friend Amos Tversky, System 1 is the old cave man part of our brain warning us for instant hazard. The rational prefrontal cortex part of System 2 is slow and energy-intensive. It also shows that we have a problem understanding the concept of probability, and among others easily under-or overestimating risk depending whether the probability is high or low.

so there is a one-time HAZOP that is useful, but successive turnarounds of continuous processes may be similar but not the same. There are few studies on these non-continuous or transient operations, but one that is providing a HAZOP-type procedure is by Ostrowski and Keim (2010). The guide words are in this case: who, what, when, and how long. The team will search for deficiencies in the sequence of actions potentially leading to higher consequences, evaluate whether procedural control is sufficient and if needed the team will recommend to improve the procedures followed in the operation and will suggest phrases.

Dynamic Procedure for Atypical Scenarios Identification (DyPASI)

Cues can trigger our imagination. This can be due to recent experiences or observations. In that connection brainstorming helps, as a suggestion by one will cue another. In this context also the concept of DyPASI (Dynamic Procedure for Atypical Scenarios Identification) shall be mentioned as developed by Paltrinieri et al. (2012) with results shown in bowtie diagrams. By applying a similarity algorithm Paltrinieri et al. (2013) showed how accident data bases can be more effectively searched for possible hazard scenarios given a process with its materials, conditions, and dimensions. With the developing abundance of data, and with methods such as data and text mining, effective search will become much more common.

Socio-technical system

The previous sections showed that improvement of conventional methods is possible but the only fundamentally right way to try avoiding the mentioned failure of scenario prediction is a holistic, rigorous system approach. In that respect the socio-technical system must be considered, as it represents, in the context of work, the interaction of people, individually and in teams, within an organization and its levels, engaged in operating and managing a technical installation. The first to describe the socio-technical system regarding work safety in some detail was Jens Rasmussen (1997). He depicted it as a number of hierarchical layers with government at the top, followed by regulating authority and associations, then company board level, management, staff, and finally a work level.

Such a system is however complex as the many possible interactions are not immediately clear to an observer. In a convincing way, Johansen and Rausand (2014) argued though, that complexity is not a system property but is perceived by us as such due to our limitation to capture the system's many possible interactions. Interactions are cause-effect chains in a safety context, which usually are linear and single, but there may be parallel chains, splits, and mergers leading to non-linear effects, even tightly coupled and resulting in fully surprising consequences. Hence, one needs conceptually to decompose a system and unravel the interactions to capture all the possibilities that are not intended and which may constitute a hazard. Such an approach is called reductionism, and it can certainly work well in a static situation. But, as complexity science is postulating, this approach will not fully cover and predict a complex adaptive/dynamic system. A larger organization with all interactions of, and among people, procedures, and plant behaves seemingly like a living organism. Not by chance, it has been biologists that have done the ground-breaking work in complexity theory. In such systems depending on conditions small changes at certain spots and times may trigger through feedback an instability possibly leading to an emerging unexpected systemic failure. This kind of non-linearity is hard to identify and the 2007/8 financial collapse has already been often mentioned as an example.

The socio-technical system concept has been expanded to design and maintenance by Nancy Leveson (2011) at MIT and published in her many articles over the last 15 years and summarized in her book 'Engineering a Safer World', as seen in Figure 5. She applied the approach to develop a new accident analysis model, STAMP (System-Theoretic Accident Model and Processes), and a hazard investigation and scenario identification tool derived from STAMP, called STPA (System-Theoretic Process Analysis). The latter shall be able to analyze hazardous non-linear cause-effect interactions in a system, for

example giving rise without notice under certain, unforeseen conditions to dysfunctional interaction of humans, organizational units, and technical components, which are each functioning perfectly as designed. STPA will further be described in the next sub-section. This will be followed by describing a different system-based methodology developed by Cameron et al. (2008) and coworkers at The University of Queensland in Australia, co-author of this article, from a CAPE perspective. This methodology is called Blended Hazard Identification, or BLHAZID for short.

4.2. System-Theoretic Process Analysis, STPA

Nancy Leveson looks at a system from a control point of view. Safety of a system is therefore emergent, and an accident is a failure of system control. For STPA the system shall be defined with its boundaries and hierarchical levels. Next, unacceptable losses will be identified as well as the safety constraints within which the system is operating safely. In other words, instead of failure events the variable value combinations are defined that form the borderlines of a system's safe state. Such constraints can be physical such as pressure, temperature or flow, organizational (e.g., procedural), or social (think of acceptable risk limit). Control loops will be on all levels of the system, down to the component parts. Guide words can then be applied to control loops. The guide word queries for each control loop are four, as presented in the center of Figure 6 with corresponding examples.

The hazards identified this way shall include not only operational failures but also design error, software flaws, human and organizational failures, and faulty sub-system and component interactions. The parameter 'time' in queries 3 and 4 reveal also chemical failure. STPA looks therefore very promising as a generally applicable and comprehensive tool to identify hazards. The magnitude of the hazard and the potential damage it can cause can for a risk assessment be calculated in the conventional way by consequence analysis. However, in safety the 'devil is in the detail' and a plant consists of many details. Although John Thomas (2013) made a start in designing a software infrastructure to handle details, it will require much development work to make STPA practical. Domino effects due to blast, fragments/projectiles, and/or jets/flooding originating from a primary event should in a risk assessment be handled in a subsequent analysis.

4.3. Blended Hazard Identification (BLHAZID)

A blended hazard identification methodology BLHAZID applied to process systems as published by Seligmann et al. (2012) blends two different types of HAZID methods: the function-driven and component-driven approach exemplified by HAZOP and FMEA respectively. A foundational conceptual framework, called the Functional Systems Framework (FSF) (Cameron et al., 2008; Seligmann et al., 2010) was developed and used to classify and understand the fundamental concepts of hazard identification methods, thus providing a consistent framework for how to identify their fundamental elements and blend them.

The FSF represents the way function arises in complex processes from the interplay of capabilities associated with plant, people and procedural components (called P3). In the FSF, the capability is "the ability to affect the states of the system", the function is "the intended effects of the capabilities". These concepts provide the base for understanding and building up the function and other important properties such as resilience of the system. The FSF describes the structure–function–goal relationships within a process system and is shown in Figure 7.

The function-driven analysis investigates how the intended function of the system is lost or degraded, while the component-driven analysis considers failures in the structure, that is, the components, and seeks to ascertain the effects of these failures on the system function. Function-driven and component-driven HAZID approaches are both complementary and overlapping (both identify failure causation in the same system). Failure events and their causes and implications are fundamentally the

same no matter which method is used to identify them. Also, certain failure events are more easily identified with particular methods.

The BLHAZID workflow has 3 main steps: (i) decomposing the system into subsystems, as the analysis is done at subsystem level; (ii) functional failure analysis looks for deviations from intended functions, their causes and implications; (iii) component failure analysis identifies failures in each component of the subsystem and elicits the causes and effects of component failures on the function of the system. During the analysis, four types of failures are identified: functional failures, component failures, environmental failures, and part failures. Causality relations are described as triplets, and the structure built into the triplets provides an opportunity to transform the BLHAZID result into HAZOP-like tables. More details about the BLHAZID methodology are given in Seligmann et al. (2012).

A structured language has been developed in order to express the knowledge used and generated in the BLHAZID method so that this knowledge can be effectively reused for a number of applications, including fault diagnosis. A so-called generic knowledge base is established to store static knowledge, like equipment class related failure modes with their failure mode causes, local implications, and failure rates in different operation modes. The content of the generic knowledge base is utilized as an a priori information during the BLHAZID workflow to facilitate the component-driven side of the analysis.

In BLHAZID methodology, time scale is introduced to provide extra information about the failure propagation rate. A qualitative causal time instance can be attached to each causal pair during the BLHAZID analysis to indicate the speed of the failure propagation and help predict implications with time. Causal time can provide better information to operators for decision making, strategizing and execution.

The outcome of the BLHAZID method provides a powerful, graphical representation of causality pathways, leading to cause-implications diagrams (Németh and Cameron, 2013), shown in Figure 9. It is possible to generate a cause-implication diagram that can trace specific failures through to a potential set of causes, as well as generating possible implications from that failure of interest. It is also possible to attribute causal time to causal pairs, thus providing temporal information within the graph. The cause-implication diagrams can provide further advantages to operators and for other process risk management tasks. Such as the graphs can be used for verifying the PHA results, checking consistency of BLHAZID result, and auditing hazard identification. In operational use it can guide an operator to a possible cause set in the case of a process upset, and can forecast possible implications and consequences, or alternatively it can be used to train operators and make them aware of what could happen and how to respond. In online/offline diagnostics and failure investigations and prediction, the pathways of the causal graphs will facilitate these activities. In the design phase causal graphs will support design decisions. The more powerful ways of reusing the BLHAZID generated knowledge for different purposes during the system lifecycle are highlighted and discussed in Németh and Cameron (2013).

Extensions to people and procedures

The basic concepts that lead to the FSF, such as capabilities, function and failure allow the framework to address a range of performance issues within procedures as well as people. Work done on human factors related to the FSF led to the development of the methodology known as Strategies Analysis for Enhancing Resilience (SAfER): see Hassall, Sanderson and Cameron (2014, 2016). This methodology explores how human performance can be enhanced across a range of tasks to drive increased resilience of systems.

Associated with the FSF is the analysis of procedures, and their potential failure. This approach provides formal analysis of procedures as represented by BLHAZID type outcomes. See Németh et al. (2007).

Thus, the FSF permits a common framework, based on fundamental concepts of capabilities, function and failure to look at system designs and operational issues.

5 Use of identified scenarios in design and in operations

5.1 Causal relationships visualized

The FSF and general system approaches entail the distinction of four hierarchical classifications of causal relationships. Each is encapsulated within the higher hierarchical space. As Cameron et al. (2016) describe, there are 4 key spaces:

- the *Lawful State Space* (LSS): this is the outer one determining what is possible according to the laws of physics, thermodynamics, chemistry, biology, etc.,
- the *Capability State Space* (CSS): within which for the given design, states can be reached due to all the component capability sets. Here, a capability of a component consists of a property (process variable) on which within a certain range an action is exerted, e.g., the three capabilities of a pump are <hold><mass>, <permit><forward flow>, <increase><pressure>, and so on for a valve, a pipe section, and other equipment. An important latent capability is <withstand> in combination with pressure or temperature. A capability can be lost ("fail"), but when intact it creates for a component a function that permits the component to affect the system states,
- the *Functional State Space* (FSS): represents the potential state-space region that results from activation of particular component capabilities that generate all system functions, with the deepest space being,
- the *Operational State Space* (OSS): represents the state space within which the operational normally resides. This is due to 'back-off' from various hard and soft constraints.

Components and process plant can have operational modes, such as a pump being 'on' or 'off'. In both those modes the activated capability <hold><mass> could fail through external leakage or rupture, while <permit><forward flow> can fail because of partial or full blockage. The activated capability <increase> <pressure> can fail in the 'on' mode as it is not pumping sufficiently, fails completely, or its operation is improper, while in the 'off' mode it could still be pumping.

A capability can be visualized by a line interval with constraints depending on the capability's range, while for a specific case a table can contain the numeric values of the ranges. Then, for a line section of a plant one can draw for each property a cross-section or profile over the components in the functional and operational state space. So, if a failure of a component is introduced the profile shows quickly the changes and possible critical situations. A very simplified example of a line segment is shown in Figure 8. For a more extensive, differentiated and interesting version, see Cameron et al. (2016). The effect on pressure of an emergency shut down valve that fails 'closed' is shown. Similar drawings can be generated for flow and mass. Altogether, the visualization shows the effects of failures and therefore will support design decision making. It will also show the role of latent capability in a design and thus will provide insight into the resilience of a design solution.

As previously mentioned in the BLHAZID discussion, visualization can be used to quickly obtain an overview of the situation and the possible causes of a developing mishap. An example of a guard bed capture unit to remove mercury and arsenic hydride from an olefin feed, which at the exit shows an increasing concentration of the contaminants, can be checked for possible causes, as shown in Figure 9. This causal graph visualization is common to a number of developments over the last 25 years.

5.2 Bayesian network modeling and use

Bayesian networks (BNs) are an ideal infrastructure to model cause-effect chains. The chains consisting of nodes representing random variables, connected by arcs (edges) representing causal relation can be branched and intertwined but the chain must be acyclic, as an effect cannot influence its own cause[3]. Hence, fault and event trees and so bowties can be exceptionally well modeled by BNs. A variable (node), e.g., A, can be in different states and can change with a certain probability from one to another state, often simply binary, e.g., from functional to failed, or from normal state to initiating event causing effect event B. State change probability can be expressed as a discrete value, $P(A)$, but current software allows variables to be represented by continuous probability distributions (and also multi-state). Basic failures, the root causes, are unconditioned. All node variables directed by arcs down the chain are conditional on their direct predecessors (parents), hence dependent on the nodes connected with arcs pointing to the node under consideration, yielding: $P(B|A)$, probability of uncertain event B given an instantiated (hence observable, but may be for direct observation hidden) initiating event A. The node at the end of a chain is called leaf node. Calculation is accomplished applying the Bayes Theorem: $P(B|A) = P(A|B)P(B)/P(A)$, deriving the resulting (posterior) probability distribution $P(B|A)$ from the (prior) variable probability $P(B)$, multiplied by the likelihood $P(A|B)$. The product represents the intersection, or co-occurrence of the likelihood with the prior, or new evidence of (observable) event A occurring given the link with B. There will exist general prior (historical) information on, e.g., low pressure occurrence probability of B, sometimes even as a probability distribution, or if not, the prior will be represented by a uniform or flat distribution range, i.e., with all values within the estimated range considered equally probable. The product shall be normalized by the total probability of the variable A, which is $P(A) = P(A|B)P(B) + P(A|notB)P(notB)$. This is to restrict the resulting value of the posterior probability between 0 and 1, which is consistent with the first axiom of probability. Small networks consisting, e.g., of four nodes can in discrete form still be evaluated by hand. But, because the evaluation effort increases exponentially with the number of nodes, BNs attribute their practical application to software developed over the last 15 years, see, e.g., Fenton and Neil (2013). A BN also can be made dynamic by updating (part of) input data at each time step.

In Figure 10 the causal graph of Figure 9 is translated into a BN with mock-up probability values as given in the table next to the network. The possible initiating events are modeled by normal distributions of probabilities per day, the others are reliability figures that are expert estimates and therefore cast into a triangular distribution form. With additional recorded observations the latter could also be normal or fully different distributions to represent skewness and peaks in the data. The output event distribution mean has an occurrence probability of 0.001 per day (std. dev. resulting from the estimated spread in the data according to the BN is 0.00036 per day). Hence the event, assuming constant failure rates and normally distributed errors in the estimation, is expected to occur on average once in 1000 days with a 95% confidence interval ranging from 373 – 1753 days.

To receive early warning that an abnormal situation is expected to develop so that early-on measures can be taken is preferable over a situation in which safety integrity systems are initiated. In the

[3] Thus, a BN cannot model feedback. For that purpose and also for random time delays a Petri Net is suited.

following, two research cases are reviewed in which a combination of HAZOP results and dynamic Bayesian networks generate such early warning alerts. The first is by making use of operator experience to trigger at a certain risk level, and the second is using process historical upset data for that purpose.

5.3 Example of applying operator experience

Naderpour et al. (2015) conducted a study motivated by the CSB investigation (2011) of a run-away pressure vessel explosion in 2008. This concerned treatment of a solvent containing the very toxic residue of the methomyl pesticide production. The main part of the product 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 level.

The residue 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 subsequently cooling water removes reaction heat, as shown in Figure 11, left. The operator monitors 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 derived, but used as probability distributions. It means that at the highest level of the process parameter the probability of alerting the operator is 1 and at the lowest is 0. Next, with the aid of HAZOP results seven abnormal situations were defined, of which the first three are independent and the other four are dependent:

- SVC: situation of vent condenser failure allowing decomposition gases to enter the vapor stream entering the flare. By deposition of solids 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 then cools below 130^{o}C. In such a case the incoming high concentration in the feed is not quickly decomposed, and by accumulation the concentration increases. To avoid runaway when reheating the mixture, the concentration should be measured and the heating adapted.
- SRR: situation of runaway reaction.

The main threat is the runaway, SRR. Equipment component failures capable of causing abnormal situations were determined, so that a Bayesian network could be constructed in which the component failure probabilities are embedded (see Figure 12). In the case of SRR, four consequence reducing measures, called safety barriers, can become active: an air monitor (triggers at concentration >1 ppm), an alarm, an ignition barrier, and several fire extinguishing cannons. The whole system is configured as a Dynamic Bayesian Network (DBN) with the components as the static nodes while the SCADA observable P, T, F, and L -values are updated at each time step with renewed probability values. The net is then evaluated (a BN can also be inferred based on new evidence at a leaf node against the direction of the arcs) and the probability of a consequence event and hence a risk level is calculated.

The risk level follows from the fuzzy product of consequence severity and probability depicted in Figure 11, bottom right. The consequence of an abnormal situation exhibits itself at five levels of severity from negligible to catastrophic, based on damage in units of $\$10^6$ ranging from 0-10^4. Component failure probabilities have been specified. Event probability ranges from 0 to 1 in five classes of very unlikely to very likely. Based on the fuzzy product of probability and consequence the acceptability matrix has been defined (Figure 11, right middle). Tolerable, not acceptable risk (TNA) is reached at risk level 3. When the DBN results in a risk of level 3, the operator is alerted.

Given the definitions reaching the level TNA, a developing abnormal situation is still in an early stage, and when alerted an 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 and component failures follow from affected abnormal situation nodes observed, or of their combinations. A sensitivity analysis on the parameters enabled by the model showed as most hazardous situation a high pressure, and even more so, a high pressure together with a high reactor liquid level. The article presents an example 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 12).

5.4 Example of applying historical process data for enhancing hazard identification

Hu et al. (2015) followed a different approach. These authors worked on a continuous process, a Fluidized Catalytic Cracking Unit (FCCU). Pre-operational HAZOP results were used for revealing and tracking fault propagation paths, possible coinciding of faults and associated consequences. However, for finding causes of abnormal situations, the information from HAZOP results appeared not to be sufficiently comprehensive and reliable. Equipment failures may not be specified by HAZOP, although BLHAZID which incorporates component failure will be less affected from this deficiency. To solve this lacuna, historical data on abnormal situations were used to analyze deviation patterns of observables and associated causes. In the mid-1990s Cooper and Herskovits (1992) developed an algorithm to extract from data the most probable cause-effect structure. This K2-algorithm was developed for the purpose of artificial intelligence and medical diagnostics. Later, Heckerman (March 1995; revised November 1996) reviewed the algorithm and suggested the Bayesian information criterion (BIC) to determine the likelihood of a model structure.

Hu and coworkers applied this algorithm and the criterion on the process data 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 derived. By turning the static Bayesian network into a dynamic one (DBN), the temporal dependencies of failing components can be incorporated. A two-step forwards-backwards algorithm (Murphy, 2002) was applied in order to infer probable fault root causes by failing equipment components which remained hidden to the operator. Given the observed process variables sequence of the operating unit up to and including time t, a forwards inference calculation yields the probability of state transitions of components at time t given the state at $t-1$. Next, a backwards calculation produces 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 with the highest updated probabilities.

Hu et al. (2015) 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

[4] Damage in case of SRR is $\$3.10^6$; in other cases it is $\$10^4$ or below, hence this falls within the first unit of 10^6.

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. Over the course of time while operating the unit, further updating was possible.

The FCCU and a DBN representation are shown in the top of Figure 13, 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. (2015). The starting point of a run is all normal. In the example presented after some time, K, both the 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 it immediately followed that D1_4, the flow of the main air blower, is likely 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.

6 Conclusions

Process hazard identification and possible scenario definition is subject to failure. It is mainly that current methods such as HAZOP and FMEA, given human limitations, are not providing confidence that these will lead to a complete inventory of all significant possibilities. Besides, the methods are labor-intensive. Three questions have been formulated:

- How can we improve the effectiveness of hazard identification and scenario definition?
- How can we enhance the efficiency of the effort?
- Would it be possible to use the hazards analysis findings in the operational stage and be able to correct and augment through operational experience?

Answers to the questions must be sought employing a systems approach and a computer supported/semi-automated methodology. In principle, systems approaches are able to address all possible deviations but the sheer number of possibilities require computerization. Semi-automation using emerging, intelligent tools and a process plant model such as a layered digraph or similar that relates failing equipment and operator functions with process deviations, or the reverse, promises to both improve effectiveness and efficiency. It is further shown that once causation trees are construed, developing abnormal situations during operations can be corrected more effectively and in a timely manner. In addition, scenarios not foreseen in the design or commissioning stage can be added to the system during the operational stage thus enhancing operational safety.

However, it will take considerable effort to obtain a system with sufficient reliability. Cooperation between industry and research is therefore needed. Given a working system, a round robin and a

comparison with results of current practice will help to support a business case for adoption and continued development of a system approach using these methods.

7 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.

Bayesfusion, 2015. http://download.bayesfusion.com/files.html?category=Academia, accessed 12 August 2016.

Bogle, I.D.L. & Cameron, D., 2002. 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), © Elsevier Science b.v., 373-392, ISBN-13: 978-0444549815, ISBN-10: 0444549811.

Cameron, I.T., 1986. "Expert Systems for Hazard and Operability Studies", Proc. Australian Institute of Petroleum Conference. Control and Prevention of Major Hazards, Brisbane, pg. 1-12.

Cameron I.T., Seligmann B, Hangos K. M, Németh E, Lakner R., 2008. A functional systems approach to the development of improved hazard identification for advanced diagnostic systems, *18th European Symposium on Computer Aided Process Engineering – ESCAPE 18*, Lyon, France, on CD (FP_00463), May.

Cameron, I.T., Németh, E., Seligmann, B.J, 2016. New Visualizations in the Development of Function and Failure in Process Design and Operations. Chemical Engineering Transactions 48, 661-666. DOI: 10.3303/CET1648111.

Cooper, G. and Herskovits, E., 1992. A Bayesian method for the induction of probabilistic networks from data. Machine Learning 9, 309-347.

Cui, L., Zhao, J., Qiu, T., & Chen, B., 2008.Layered digraph model for HAZOP analysis of chemical processes. Process Safety Progress 27(4), 293–305.

Cui, L., Zhao, J., and Zhang, R., 2010. The integration of HAZOP expert system and piping and instrumentation diagrams. Process Safety and Environmental Protection 88(5), 327-334.

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

Fenton, N., and Neil, M., 2013. Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press, Taylor & Francis Group, Boca Raton, FL 33487-2742, USA, ISBN 978-1-4398-0910-5.

Hassall, M.E., Sanderson, P. and Cameron, I.T., 2014. The development and testing of SAfER: a resilience-based human factors method. Journal of Cognitive Engineering and Decision Making 8 (2), 162-186. doi:10.1177/1555343414527287

Hassall, M., Sanderson, P. and Cameron, I.T., 2016. Incident analysis: A case study comparison of traditional and SAfER methods. Journal of Cognitive Engineering and Decision Making 10 (2), 197-221. doi:10.1177/1555343416652749

Heino, P., Suokas, J., Karvonen, I., 1988. 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, 225–231.

Heckerman, D., A, March 1995 (Revised November 1996). Tutorial on Learning with Bayesian Networks. Microsoft Research Technical Report MSR-TR-95-06, http://research.microsoft.com/en-us/um/people/heckerman/tutorial.pdf .

Houston, D. E. L, 1971. New Approaches to the Safety Problem, IChemE Symposium Series No.34, 210-216.

Hu, J., Zhang, L., Liang, W., 2012. Opportunistic predictive maintenance for complex multi-component systems based on DBN-HAZOP model. Process Safety and Environmental Protection 90, 376–388.

Hu, J., Zhang, L., and Wang, Y., 2014. 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, paper OS8-4 1061598, Okayama, Japan.

Hu, J., 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.

Johansen I.L., and Rausand M., 2014. Defining complexity for risk assessment of sociotechnical systems: A conceptual framework, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 228 (3), 272-290.

Junger S., 2012. The perfect storm. New York: W.W. Norton & Company; 2000, ISBN 978-0-393-33701-3, in Paté-Cornell E., 2012. "Black Swans" and "Perfect Storms": risk analysis and management when statistics are not enough. Risk Analysis 32 (11): 1823–33.

Kahneman D., 2011. Thinking, Fast and Slow, Farrar, Strauss and Giroux, New York, © Copyright by Daniel Kahneman, ISBN 978-0-374-27563-1.

Khan, F. and S. Abbasi, 1995. HAZEXPT: A comprehensive Knowledge Base system for HAZOP study, in Research report number CPCE/R and D 15/95., Pondicherry University.

Khan, F.I. and S. Abbasi, 1997a. OptHAZOP—an effective and optimum approach for HAZOP study. Journal of Loss Prevention in the Process Industries 10 (3), 191-204.

Khan, F.I., and Abbasi, S.A., 1997b, TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. Journal of Loss Prevention in the Process Industries 10, 333-343.

Khan, F.I., and Abbasi, S.A., 2000. Towards automation of HAZOP with a new tool EXPERTOP. Environmental Modelling & Software 15, 67–77.

Kletz, T.A., 1997. Hazop – Past and future, Reliability Engineering and System Safety 55, 263-266.

Kletz, T.A., 2009. Introduction to Session on HAZOP: Putting HAZOP in Context, IChemE Symposium Series No. 155, Hazards XXI, pg. 118-119.

Lawley, H. G., 1974. Operability Studies and Hazard Analysis, Chemical Engineering Progress 70 (4), 45-56

Leveson, N.G., 2011. Engineering a Safer World, Systems Thinking Applied to Safety. The MIT Press; 608 pp., ISBN-10:0–262-01662-1 ISBN-13:978-0-262-01662-9.

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., 1999**.** 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, 317-326.

McCoy, S. A., Wakeman, S. J., Larkin, M.L., Chung, P. W. H., and Rushton, A. G., 2000. 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), 91–119.

Morbach, J., Yang1, A., Marquardt, W., 2007. OntoCAPE—A large-scale ontology for chemical process engineering. Engineering Applications of Artificial Intelligence 20, 147–161.

Murphy, K.P., Fall 2002. Dynamic Bayesian Networks: Representation, Inference and Learning. Ph.D. Dissertation, University of California Berkeley, http://www.cs.ubc.ca/~murphyk/Thesis/thesis.html

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., Lakner, R., Hangos, K. M. and Cameron, I. T., 2007. Prediction-based diagnosis and loss prevention using qualitative multi-scale models. Information Sciences, 177 (8) 1916-1930. doi:10.1016/j.ins.2006.10.009

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.

Ostrowski, S.W., and Keim, K.K., 2010. Tame Your Transient Operations: Use a special method to identify and address potential hazards. Chemical Processing, June 23, http://www.chemicalprocessing.com/articles/2010/123/?page=full.

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Analysis 32 (8), 1404-1419.

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.

Parmar, J.C., Lees, F.P., 1987. The propagation of faults in process plants: hazard identification (Part I), Reliability Engineering 17, 277–302; The propagation of faults in process plants: hazard identification for a water separator system (Part II). Reliability Engineering 17, 303–314.

Pasman, H. J., 2015. 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., ISBN: 978-0-12-800057-1.

Pasman, H.J., Rogers, W.J., 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

Rahman, Sh., Khan, F., Veitch, B., Amyotte, P., 2009. ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis. Journal of Loss Prevention in the Process Industries 22, 373–380.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem, Safety Science 27 (2/3), 183-213.

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

Rossing, N.L., Lind, M., Jensen, N., Jørgensen, S.B., 2010. A functional HAZOP methodology. Computers and Chemical Engineering 34, 244–253.

Seligmann, B., Németh, E., Hockings, K., McDonald, I., Lee, J., O'Brien C., Hangos, K.M., Cameron, I.T., 2010. A structured, blended hazard identification framework for advanced process diagnosis. *Proceedings of the 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries*, vol. 1, pp. 193-200, ISBN 978-90-76019-291.

Seligmann, B.J., Németh, E., Hangos, K.M., Cameron I.T., 2012. A blended hazard identification methodology to support process diagnosis, Journal of Loss Prevention in the Process Industries 25, 746-759.

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.

Srinivasan, R. and V. Venkatasubramanian, 1998a. Automating HAZOP analysis of batch chemical plants: Part I. The knowledge representation framework. Computers & Chemical Engineering 22 (9) 1345-1355.

Srinivasan, R. and V. Venkatasubramanian, 1998b. Automating HAZOP analysis of batch chemical plants: Part II. Algorithms and application. Computers & Chemical Engineering 22 (9) 1357-1370.

Stanton, N.A, Salmon, P.M., Walker, G.H., Baber, C and D.P. Jenkins, 2005. Human Factors Methods: A practical guide for engineering and design, Ashgate Publishing, ISBN 0-7546-4660-2

Taleb, N.N., 2010. The Black Swan – The Impact of the Highly Improbable, Random House Trade Paperbacks, New York, ISBN 978-0-8129-7381-5.

Taylor, J. R, 2013. Incorporating Human Error Analysis into Process Plant Safety Analysis, Chemical Engineering Transactions 31, 301-306.

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

U.S. Chemical and Hazard Investigation Board, January 2011. Investigation Report, Pesticide Chemical Runaway Reaction, Pressure Vessel Explosion, Bayer Cropscience, LP. Institute, West-Virginia, August 28, 2008, Report No. 2008-08-I-WV.

Vaidhyanathan, R. and Venkatasubramanian, V., 1995. Digraph-based models for automated HAZOP analysis. Reliability Engineering and System Safety 50, 33-49.

Vaidhyanathan, R. and Venkatasubramanian, V., 1996a. A semi-quantitative reasoning methodology for filtering and ranking HAZOP results in HAZOPExpert. Reliability Engineering and System Safety 53, 185-203.

Vaidhyanathan, R. and Venkatasubramanian, V., 1996b. Experience with an Expert System for Automated HAZOP Analysis. Computers and Chemical Engineering 20, 1589-1594.

Venkatasubramanian, V. and R. Vaidhyanathan, 1994. A knowledge‐based framework for automating HAZOP analysis. AIChE Journal, 40(3), 496-505.

Venkatasubramanian, V., Zhao, J., Viswanathan, S., 2000. Intelligent systems for HAZOP analysis of complex process plants. Computers and Chemical Engineering 24, 2291-2302.

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., Venkatasubramanian, V., 2003. Roles of Ontology in Automated Process Safety Analysis. Computer Aided Chemical Engineering 14, 341–346.

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. Implementation and Case Study. Process Safety and Environmental Protection 83 (B6), 533-548.

Zhao, J., Cui, L., Zhao, L., Qiu, T., & Chen, B. 2009. Learning HAZOP expert system by case-based reasoning and ontology. Computers & Chemical Engineering 33 (1), 371–378.

Figure captions:

Figure 1. The progress of semi-automatic HAZOP by Khan et al.

Figure 2. The progress of semi-automatic HAZOP by Venkatasubramanian et al.

Figure 3. The progress of semi-automatic HAZOP by Cui and Zhao et al.

Figure 4. Multi-Flow-Model (MFM) Workbench functional HAZOP assistant developed by Rossing et al. (2010). On the *right*, a MFM sample is shown of the reflux part of an advanced distillation column with component functions (sou = source; tra = transport; sto = storage; bal = balance; sin = sink), flow structure, causal roles, and so-called means-ends. JESS means Java Expert System Shell. *Left below* is an example of a causal tree produced by the system. For a full symbol explanation the reference should be consulted.

Figure 5. Leveson's representation of a socio-technical system and the various communication lines and categories of communication media (Leveson, 2011).

Figure 6. Generic control loop schematic with four control action queries (center) and corresponding failure examples, adapted from Leveson (2011).

Figure 7. Generic process Functional Systems Framework (FSF) for hazard identification by function-driven analysis (e.g., HAZOP) and component-driven analysis (e.g., FMEA), according to Seligmann et al.

Figure 8. *Top*: Small part of a line section, with below capability ranges indicated of the various components (L = pipe; ESDV = emergency shut down valve; V = gate valve; S = line strainer; P = pump; FM = flow meter; c.m = contain mass; p.F = permit flow; s.F = stop flow; rd.Xs = reduce concentration of solids; i.P = increase pressure). *Bottom*: Pressure profiles in FSS and OSS before and after emergency shut down valve fails 'closed'. The figure is a much simplified version of those in Cameron et al. (2016), but it shows the principle.

Figure 9. Cause-implication diagram of a guard bed for removing mercury and arsenic hydride from an olefin feed. The P&ID of the 4 sub-system sections of the guard bed is shown in the top left corner. The concentration of the contaminant in the output reached a 'High'. The diagram provides a quick reference to possible causes, according to Németh and Cameron (2013).

Figure 10. *Left*: Bayesian network representing the Guard bed case of Figure 9. The applied BN software is GeNIe 2.0 developed by Decision Systems Laboratory of the University of Pittsburgh, but licensed to BayesFusion LLC, in 2015. *Right*: Mock-up probability values are shown in the table.

Figure 11. *Left* is shown the reactor. Circled are sensor locations; on *top right* is as example of the fuzzy membership of the observables taken L, reactor liquid level, in the *middle* the decision risk matrix, and at the *bottom* the resulting fuzzy risk level range. Adapted after Naderpour et al. (2015).

Figure 12. Dynamic Bayesian network of possible failing components of a residue treating reactor causing abnormal situations represented by nodes SAR, and/or SHT, SHL, SHC, SVC, SHP, and SRR (see text for these latter acronyms) after Naderpour et al. (2015). Observables L, T, P, and F provide updated evidence for each time step. The operator is alerted when the risk level reaches TNA (see Figure 11, middle right). 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 AM (air monitoring), AL (alarming), FC (fire cannons), and IB (ignition barriers) in parallel.

Figure 13. 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 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.

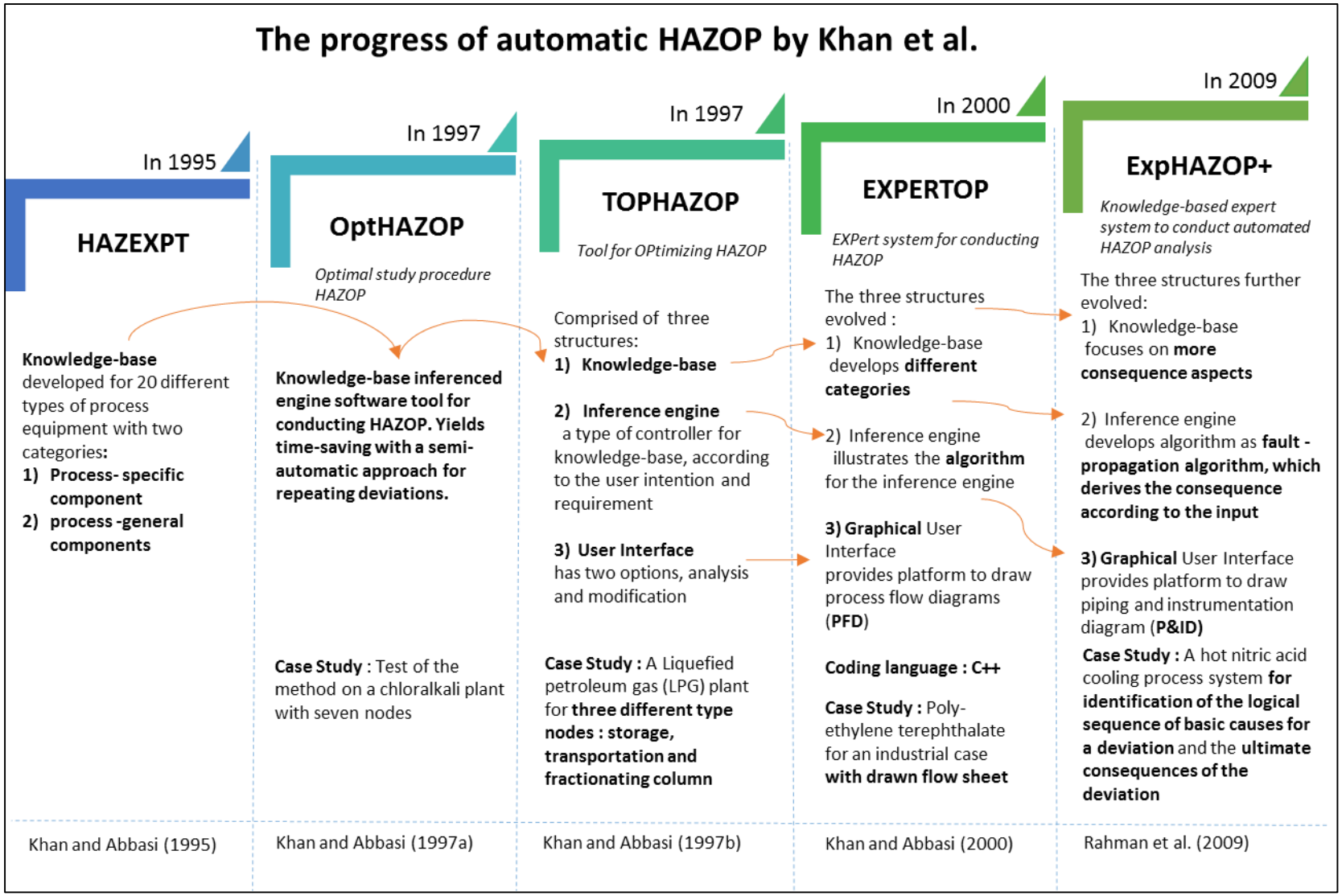


Figure 1

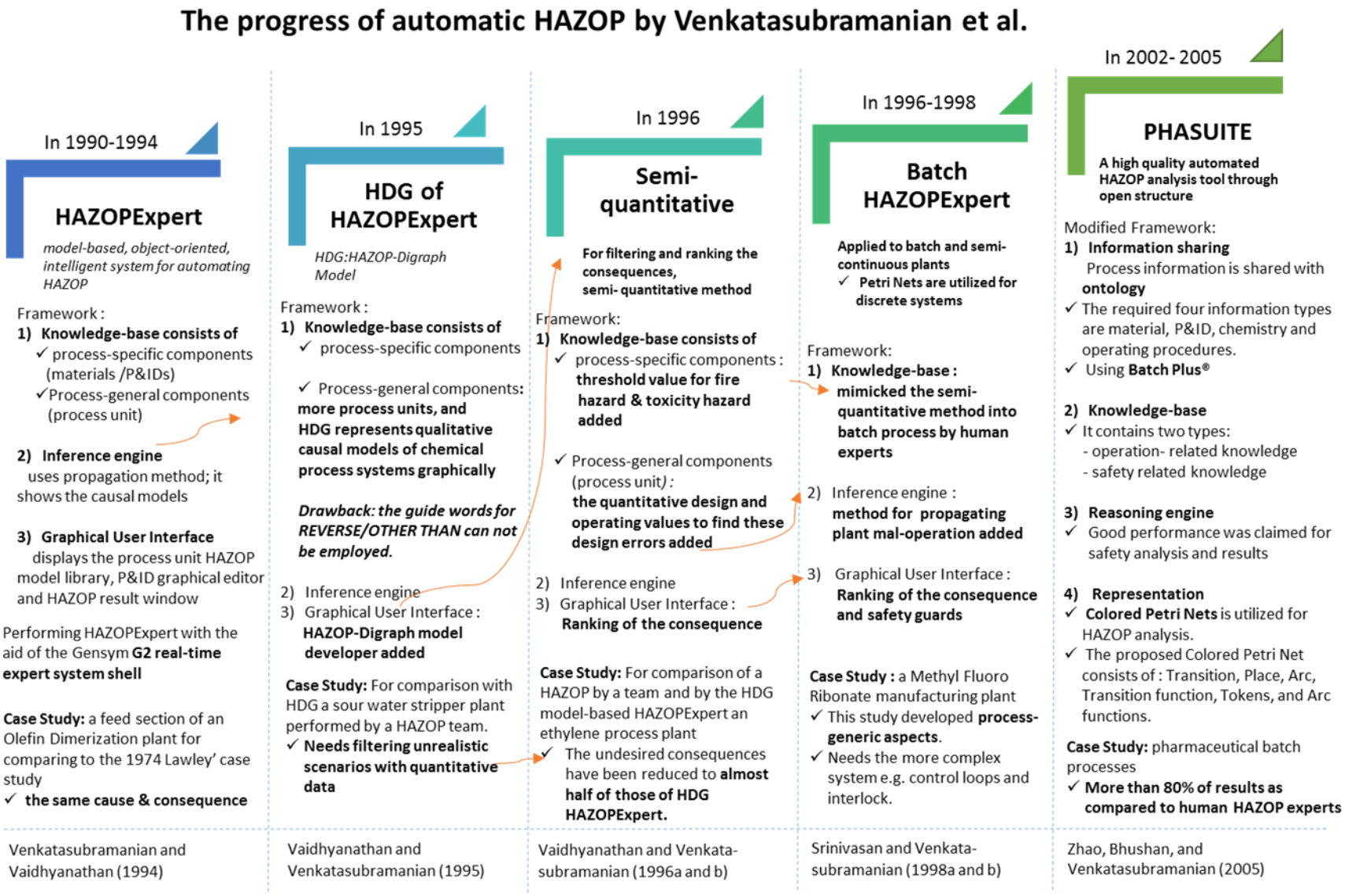


Figure 2

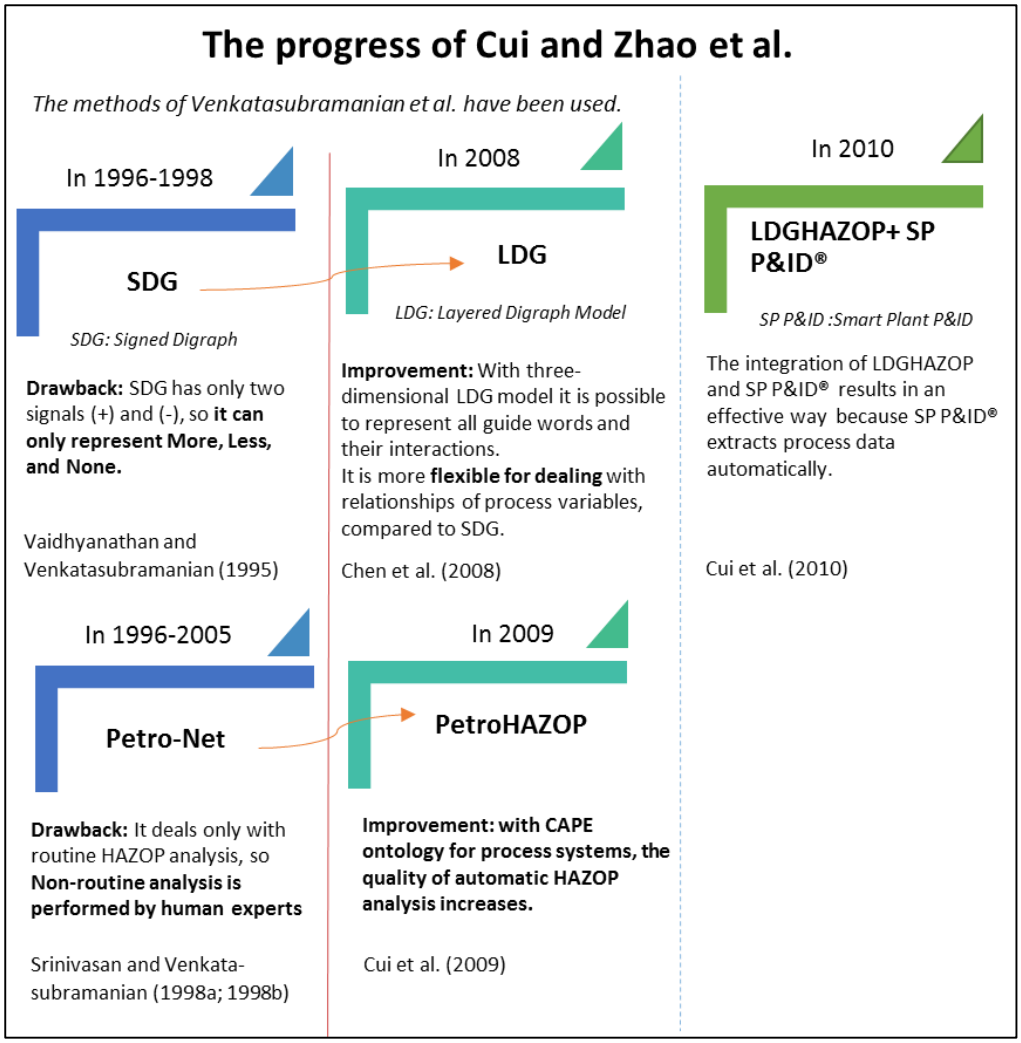


Figure 3

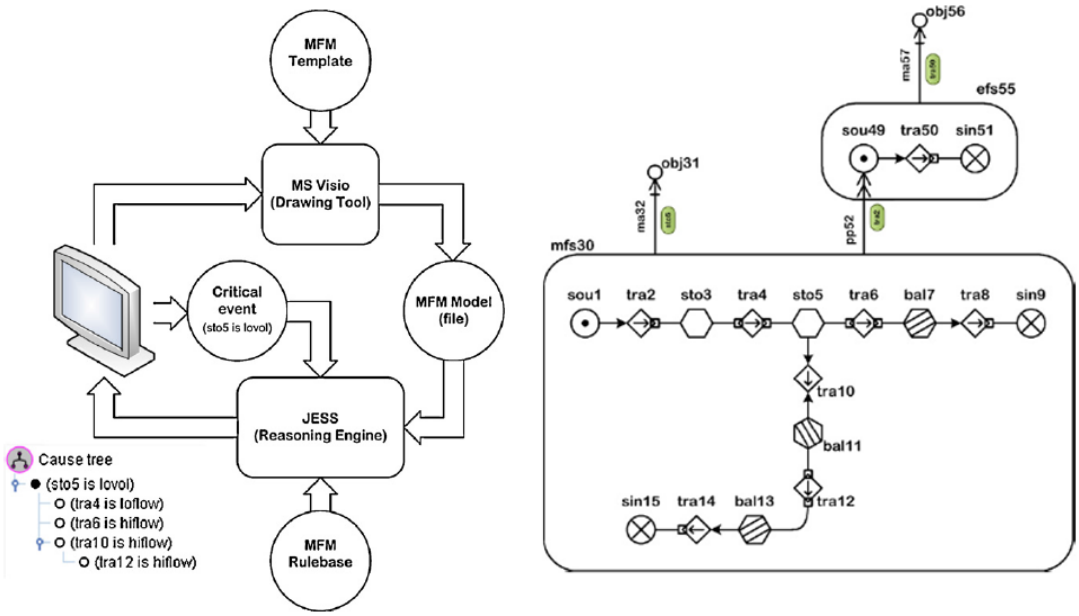


Figure 4

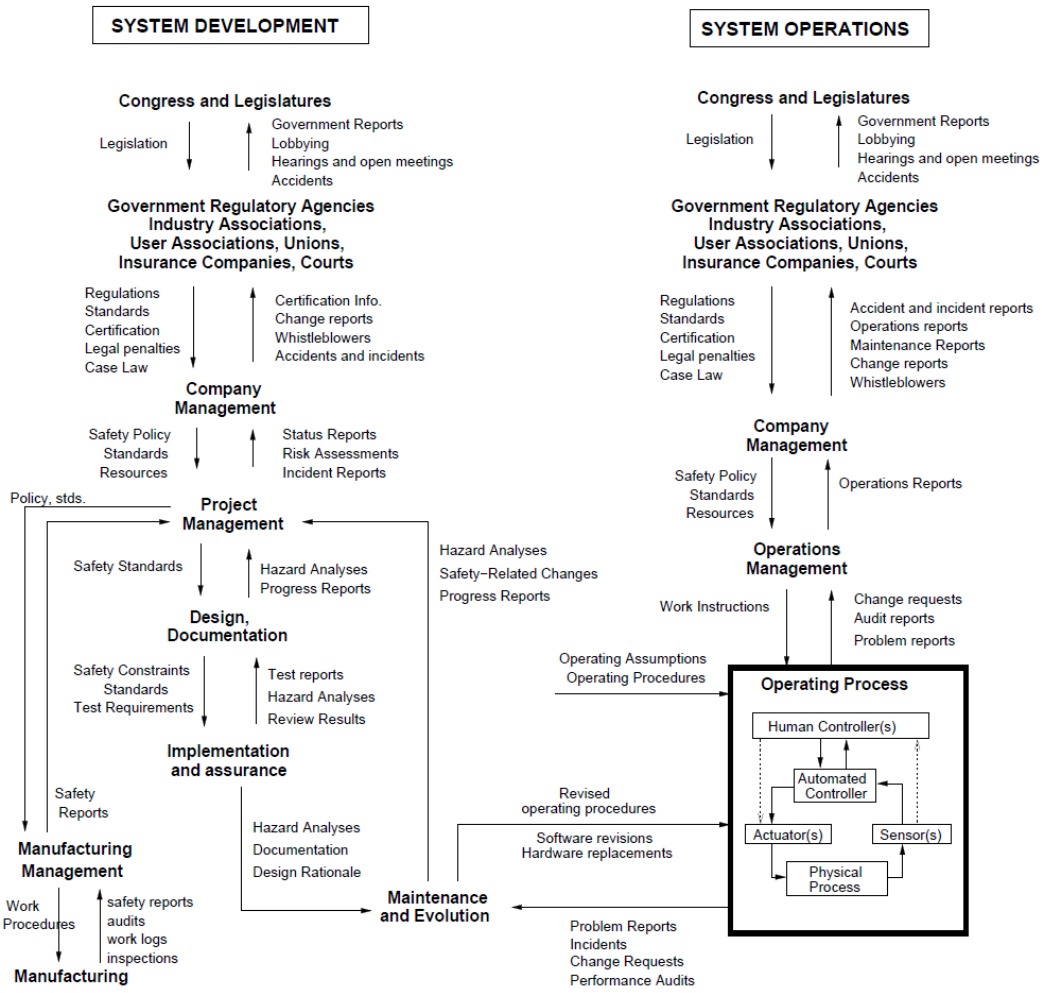


Figure 5

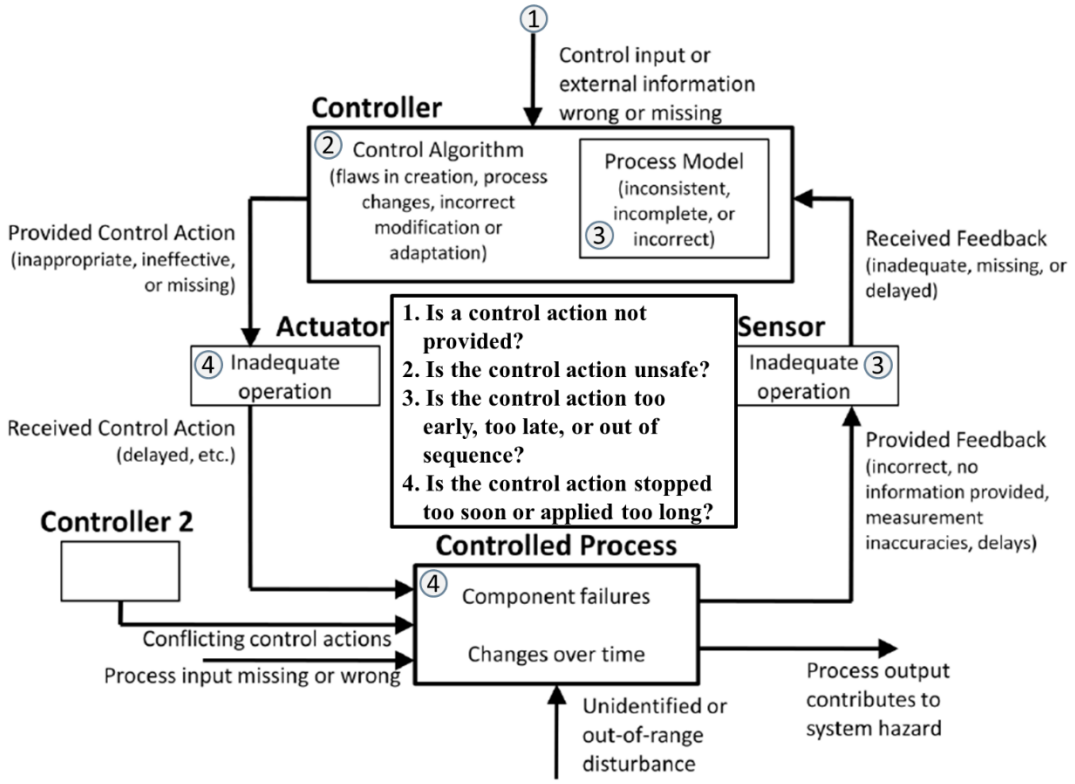


Figure 6

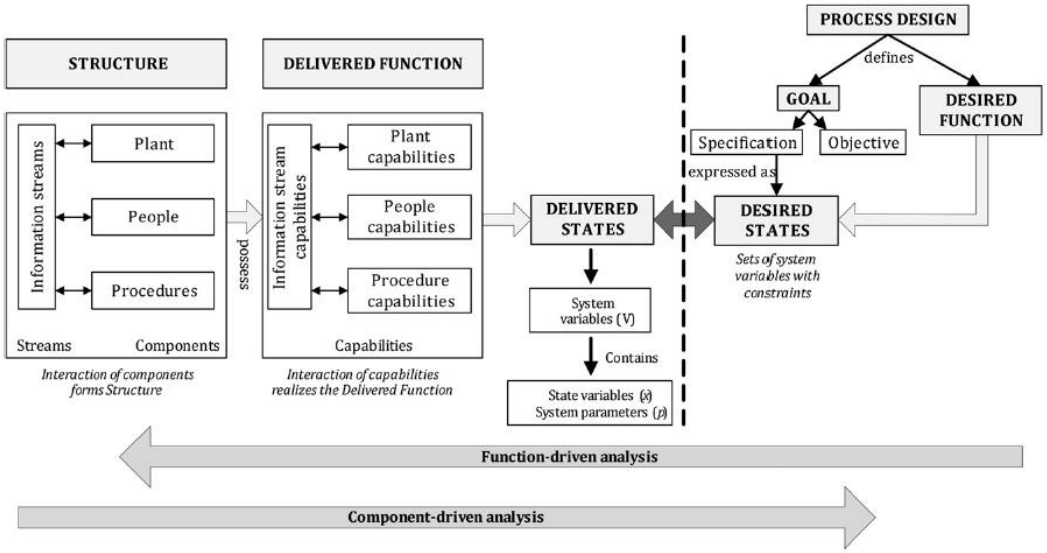


Figure 7

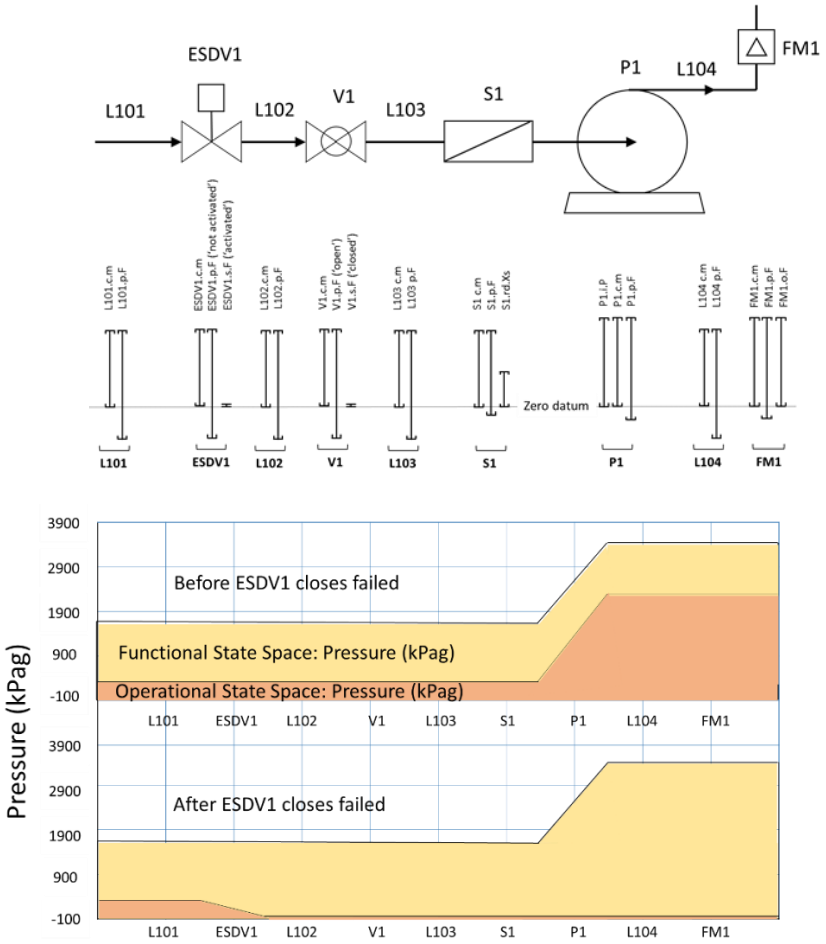


Figure 8

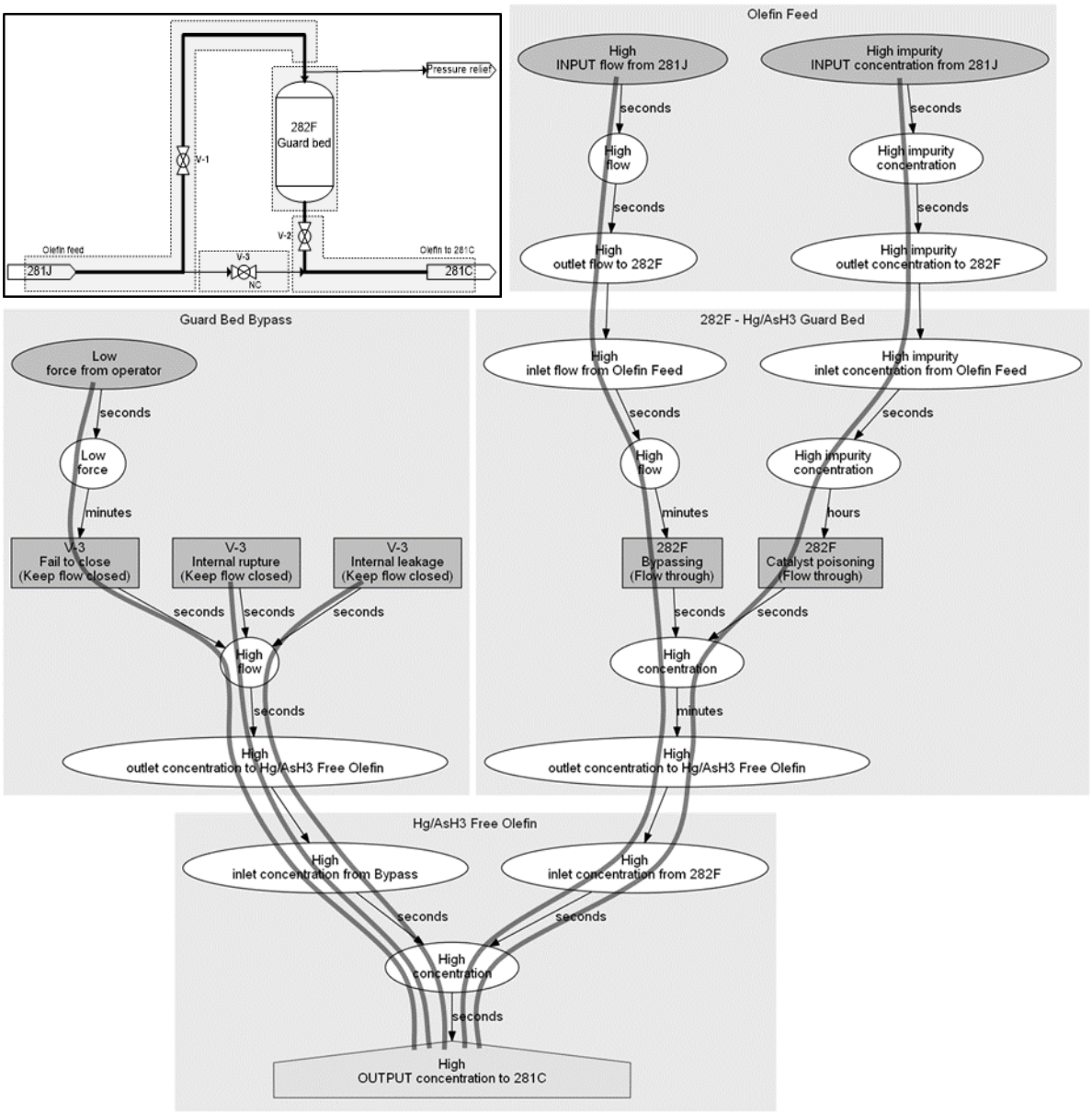
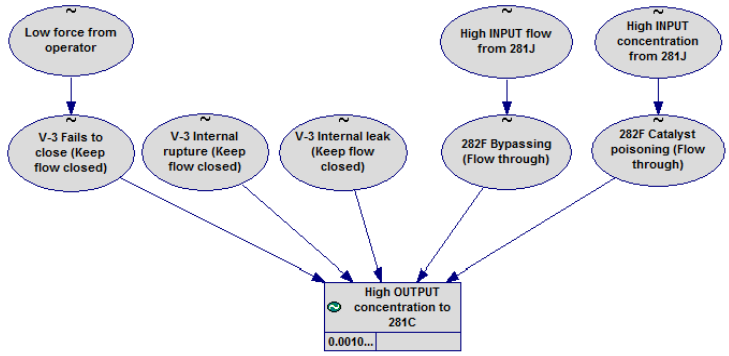


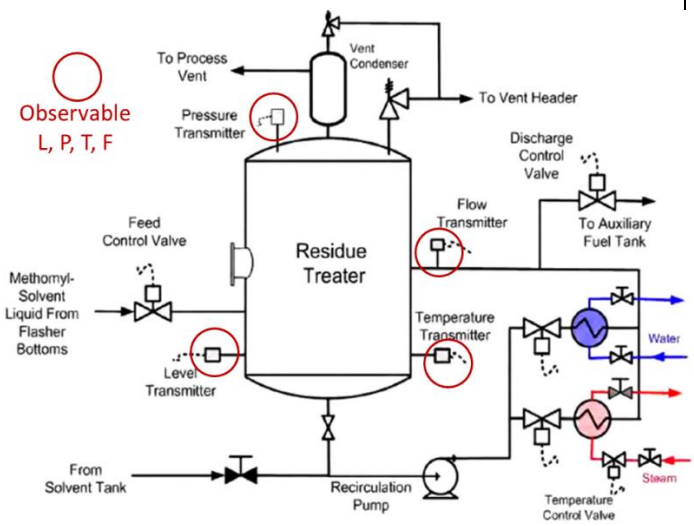
Figure 9

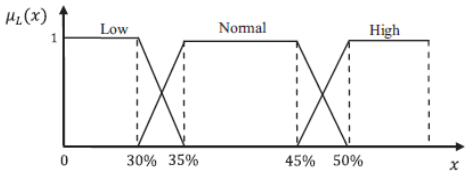


Low Force from operator	N(0.001, 0.0005)	/day
High INPUT flow from 281J	N(0.001, 0.0005)	/day
High INPUT concentration from 281J	N(0.0005, 0.0001)	/day
V_3 keep flow closed	T(0.01,0.015,0.03)	/day
V_3 Internal rupture	T(0.00003,0.00005,0.00007)	/day
V_3 Internal leakage	$T(1.5.10^{-6}, 2.4.10^{-6}, 5.10^{-6})$	/day
282F Bypassing	T(0.5,0.7,0.8)	/day
282F Poisoning catalyst	T(0.3,0.5,0.8)	/day

N = normal distribution (μ, σ); T = triangular distribution (min, mod, max)

Figure 10

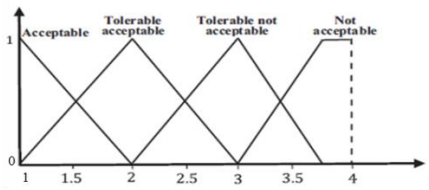




Level membership function example

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 11

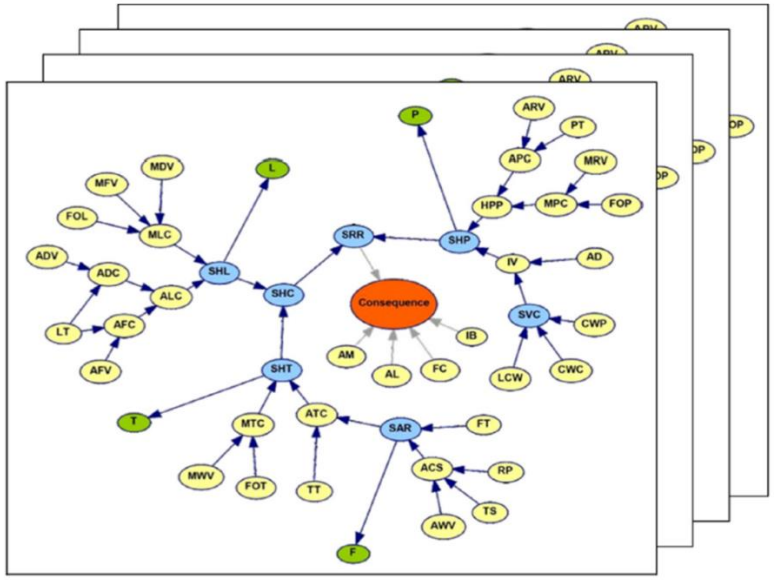
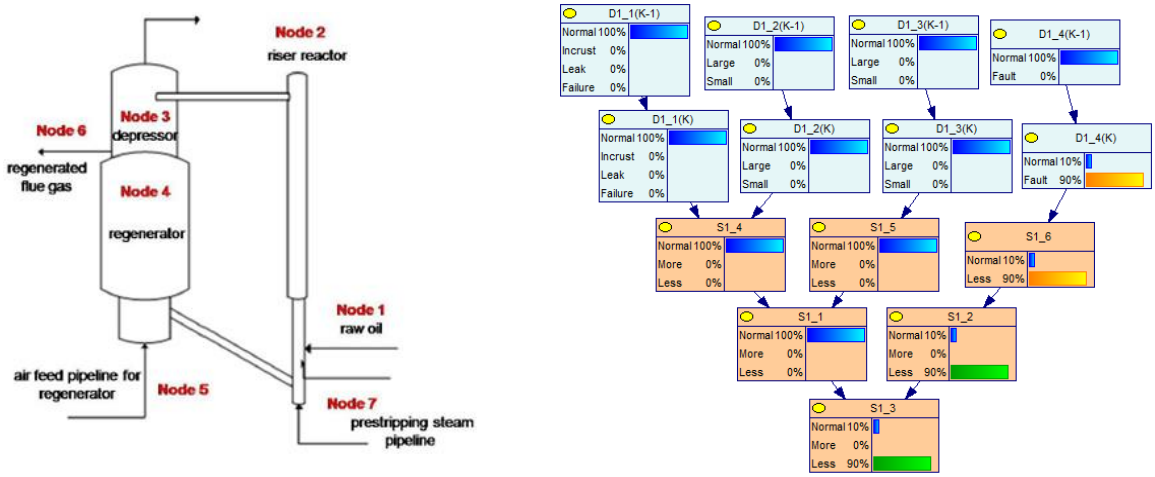


Figure 12



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

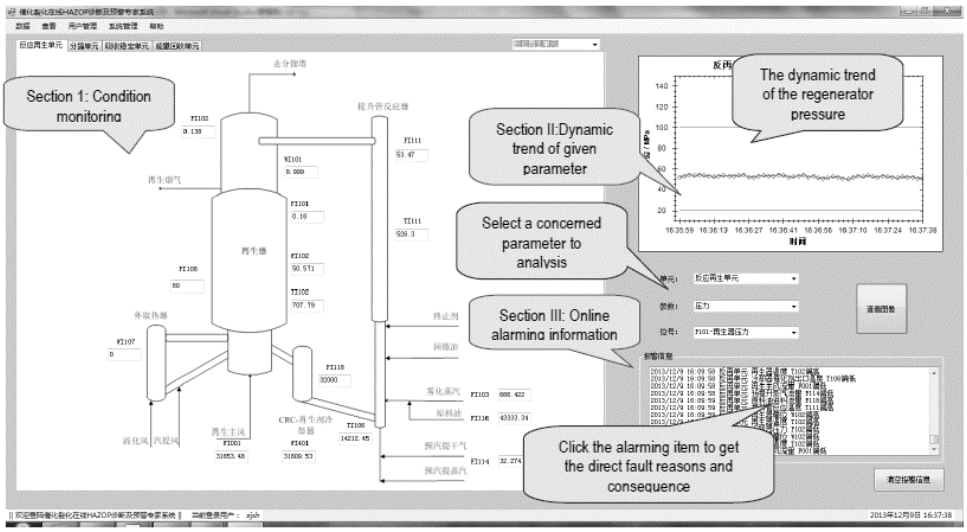


Figure 13