CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331047

What process risks does your plant run today? The safety level monitor

Hans J. Pasman*[a], Bert Knegtering[b]

[a] Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX 88843-3122
[b] Honeywell Safety Solutions, Rietveldenweg 32a, 's Hertogenbosch, The Netherlands
hjpasman@gmail.com

When the question is asked, whether the operation is safe, several sources of information can be tapped to provide information for a reply. But do we really know? Risk assessment is a possibility to obtain a general picture, but it focuses much on stored quantities and technical aspects and is basically static. Management quality, organizational aspects, and human reliability remain out-of-sight as well as temporal risk effects. In this paper, the notion of 'risk factor' will be introduced with effects on the short, middle, and long term. Short term risk factors may be monitored physically by means of the digital control system using fault diagnosis, and if required, additional special purpose sensors. For fault diagnosis, several methods are available, but the method making use of the Blended Hazid approach followed by a reasoning routine looks attractive. For middle and long-term risk factors, it is proposed to use the values of process safety performance indicators as exponents of the safety level. To keep it practical, aggregation of the indicator data may have to be applied first. Because it is expected to have synergy from a holistic approach combining technical and organizational safety information, a universal cause-effect logic infrastructure was sought. Bayesian networks seem to fulfill this demand; they can be instrumental for performance monitoring and therefore can greatly help to improve situational awareness.

1. Introduction and problem analysis

When in the 1960s Loss Prevention as a focus area of the process technology community started, many activities were concerned with looking back, trying to analyze what went wrong, reconstruct causes by clearing up physico-chemical mechanisms that led to unstable process behaviour and loss of control. In the decades following, the reactive way of looking at process safety slowly changed into proactive. From a control point of view one can say, to be reactive is observing signals and correcting process parameters by feed-back. Proactive is then control by feed-forward. The latter is far more difficult; it requires a predictive process model. Hence, although prevention was the ultimate goal, we were often satisfied by installing adequate protective measures. In the 1990s protection obtained a systematic analytical approach named Layers Of Protection Analysis (LOPA) followed by the standard IEC 61511. The latter provided a strong basis for the reliability of the measures as long as the right conditions of testing and maintenance are kept. This has been a major step forward in Loss Prevention, in the sense of avoiding or at least decreasing the frequency of catastrophic consequences when an irreversible process deviation occurs. It is however only partly taking away underlying disruptive causes. Also, as appears in daily, operational life, LOPA and the standard do not avoid mishaps caused by maintenance defects, and in particular, it does not avoid mishaps in abnormal situations such as, e.g., turnarounds and start-ups.
With LOPA and the IEC standard, the probabilistic approach has become more common and risk as the combination of consequence and likelihood of an event accepted as the basis for decision making. In fact, assessment of a safety level of an operation initially, when incidents are abundant, is by learning the hard way, correcting by taking measures and thereby lowering incident frequency. But once matters are relatively under control, the only way to find out about the safety level is to imagine which possible scenarios can develop, hence what risks are looming. So, process safety must become risk-based.

Please cite this article as: Pasman H.J. and Knegtering B., 2013, What process risks does your plant run today? the safety level monitor, Chemical Engineering Transactions, 31, 277-282 DOI: 10.3303/CET1331047

Even more than from improvements in technology, safety of process operations has benefitted from increased management commitment. It has been shown over and over again that when leadership gives safety the right priority, it strongly reduces the frequency of incidents. After the Piper-Alpha disaster in the early 1990s, safety management systems (SMS) have been installed in many companies. This was a first step; caring about the safety culture is another. An SMS requires an extensive set of measures according to the Center for Chemical Process Safety, CCPS (2007) clustered in four areas: commit to process safety, understand hazards and risk, manage risk, and learn from experience. An intrinsic part of the last cluster is audit policy, procedures and operations, and corrective actions.

Over the years it became clear that despite the prescribed feedback through auditing and corrective action, the effectiveness of an SMS must be monitored continually. The mechanism of the Deming cycle for effective management is obvious. To this end from various sides, lagging and leading indicators have been proposed and because safety is in the details, at base level this set of indicators becomes rather extensive. On the other hand, a good overview puts a limit to the number of indicators. Hence, aggregation as, e.g., proposed by Hassan and Khan (2012) will be a prerequisite. Given indicators are established, the question will arise about how we shall assess the situation. As long as there is steady improvement and progress, this question will not be acute, but as soon as the indicator values become stagnant or worse, management will be confronted with the issue of how to interpret the values and to answer the question how safe is safe enough. Once again, this question can be solved only by considering the risks associated with what the indicators are measuring; in other words what does an indicator value mean in terms of risk.

Ultimately, to control safety one would wish the availability of a ‘dashboard’, which will blink when a flaw arises, and with the ability to quickly and reliably locate and diagnose the problem and to correct in time. The latter may sometimes be a matter of seconds but sometimes even months. From the foregoing, we can conclude that making corrections in time implies full control of risks caused by flaws in the technical as well as the organizational system. These flaws can in turn be caused by changes in conditions that can arise suddenly or gradually and that can be of physical nature either internal or external to the process, or, and that may be the largest part, to human work activity. Faulty human action can take many forms: action can be required but not realized, it can be too weak, too strong, too early, or too late, and there can be action not required to damage the operation.

Traditionally, propagation of possible failures of equipment components together forming a system can be schematized in a fault tree and, given the critical release of hazardous material event, the possible sequences of follow-on events causing damage to people, assets and environment in an event tree. The combination is known as a bowtie. Scenarios shown in a bowtie can be quantified both in event probability and consequence, albeit with limited accuracy while they remain static, i.e., input parameters are not a function of time. However, the risk level will be fluctuating and it will be necessary to consider the risk dynamics. Fluctuation can be at the side of the threat level but also at the exposed ‘target’ side if we think of, e.g., the temporary presence of office trailers next to the ISOM unit at BP Texas City. A start in dynamic operational risk analysis has been made by Kalantarnia et al., 2009 (updating frequency using near-miss data) and by Yang and Mannan, 2011 (wear, repairs) but both have been limited in scope.

Knegtering and Pasman (2012) introduced the concept of risk factor to capture temporal effects affecting failure rates. Examples of short term risk factors are welding activity, pipe burst, upcoming stormy weather conditions, alarm over-rides or incidental time pressure. These risk factors can vary from day to day, either in being present or absent, or continually present but fluctuating in strength. Midterm factors to be considered are, e.g., seasonal influences, delayed inspections, maintenance not on schedule, postponed shut-down, or changes in process material composition. These mid-term factors can vary on a weekly or monthly basis. Long term negative factors are corrosion problems, aging of plant, wear-out, degradation of the quality of the SMS such as bad management of change, decrease in competency of people, or deterioration of safety culture, which can vary over years. Full decomposition in all confounding causes of risk will however be ‘nightmarish’ and therefore, to get grip on risk factors, the formation of clusters with averaged properties but preferably keeping track of spread, will be necessary.

In principle, many malfunctions/deviations/disturbances/abnormalities/faults in the process itself with effect on the short term are handled by the Basic Process Control System (BPCS), often named Distributed Control System (DCS), which measures process parameters and through the DCS identifies deviations and corrects. The present-day large variety of available sensors and further development of data processing in the DCS may enable detecting weaker signals, hence making corrections in an earlier stage and taking care of chemical and physical risk factors such as sudden vibrations, larger energy use, smells, and leaky valves. There are, though, numerous problems and limitations specific to process control and automation influencing safety level, and these will be analyzed in more detail in section 2. The complexities of human reliability will be touched upon in section 3. In section 4 Bayesian networks will be proposed as a possible integrating probabilistic infrastructure to describe cause-consequence chains that

can fit indicator results in a plant model. The use of Bayesian networks may lead to the development of a safety level monitor to enable improved situational awareness and plant resilience.

2. Contribution of Basic Process Control System and Safety Instrumented Systems

As Venkatasubramanian and co-workers (2003) noted in various papers, in the 1980s and 1990s, automation of process control brought impressive improvement in achieving high production quality and efficiency in process safety. As a consequence, the operator is now more managing and supervising control of the process rather than directly controlling on a basic level. In addition, in case the BPCS fails, automated Safety Instrumented Systems (SIS) with high safety integrity levels may bring the process back to a safe state (often trip the process) as mentioned before. However, process trips are costly and one would like to correct in advance and keep the process running. For this, there are various factors which demand further insight in order to take the right measures. Processes have become complex, faults are not always easy to trace: so, where is the root cause, in which loop? Is it the sensor (e.g., noise, bias, or other defect), the processor or the actuator (e.g., valve stiction)? Is it only a single fault or are there multiple faults and problems? Faults may propagate: an abnormal signal measured at some location of the installation, may have its cause in a totally different part. The process may also come in a situation that during process design was not foreseen, or it is beyond the competence level of the team to make the right choices or do the right maintenance? This conclusion certainly applies to the life cycle of the SIS components. Just procuring an advanced system does not include a safety guarantee (Knegtering, 2002).
So, next is expanding the development of diagnostics to provide the operator the right (leading) indicators to perform the 'managing' task. In case of a developing (oscillatory) disturbance, the operator needs to detect a fault timely, to classify the fault, and to identify root causes in order to take the right measures. This turns out not to be solved easily, and not only because noise blurs the signal picture. Venkatasubramanian et al., 2003 gave an overview of requirements for a diagnostic system and various possibilities. Detection should be quick (depending on the process safety time), it should discriminate among different types of failures, the system should be robust, it should be able to tell whether a fault is new or already seen before, while preferably the system should make its own error estimate about its identification. It should adapt to process modifications, give sufficient explanation about the root cause, and all that with a minimal effort of modeling and computing. A priori knowledge of possible deviations and their causes and consequences appears to be more important than search strategy. The main categories are model based and process history based control; both can be qualitative and quantitative. All have their positive and negative sides, so hybrids may be the way to go.
Quick to understand are qualitative causal models such as the fault tree and signed directed graphs, both members of the same family of cause-effect chain representations, and in addition 'common sense' physics and decomposition techniques such as HazOp. Quantitative multivariable model based methods try to find causes by determining the difference from normal output and then locate the cause through examining faults. Qualitative process history analysis methods are based on expert system or trend analysis, while quantitative methods make use of neural nets or statistical data processing, which with present day computer power still can be accomplished relatively easy as long as parameter interactions can be assumed linear. However, various cases such as valve stiction behave non-linearly as Shoukat Choudhury et al. (2008) have analyzed in detail and for the solution of which they provided higher-order statistics (bi-spectrum and bi-coherence).
Models are always incomplete, certainly when it comes to details of interest to safety. Resolution in many cases is not sufficient to pick up, e.g., that components generally do not completely fail but keep functioning in a degraded state. So, important safety details may be missed. Jiang et al. (2012) analyzed root causes of two cases of industrial multivariate predictive model control of which performance deteriorated over time, also showing that such analysis is not trivial.
An interesting approach to at least partly automated fault diagnosis is making use of information generated by applying the Blended Hazid (or BLHAZID) method as presented at the 2010 Loss Prevention symposium by Cameron, as described by Seligmann et al. (2010, 2012). Blended Hazid is a combination of HazOp (systematic team exercise to identify effects of process deviations) and FMEA (finding out what effect component and subsystem failures will have). The information gathered is stored in a formal computerized logic structure allowing generation of causal knowledge for a fault finding reasoning procedure on the basis of symptoms by applying the Stanford Protégé Ontology Editor and Knowledge Acquisition System: http://protege.stanford.edu (2008), described in Nemeth et al., 2009. Whether this will also provide an opening to reduce time to event information has yet to be seen.

3. Management, organization and human factor

Inspired by the way in which aviation safety developed, Vinnem et al. (2012), in performing risk analysis of offshore maintenance, distinguished in various work activities the work and the control of it and in both failure of omission and of execution. The latter failure was composed of Reason's main categories of human failure (mistake, slips and lapses, violation) and the whole was modeled as a fault tree with occurrence of a leak as the top event. Failure probabilities are influenced by an underlying layer of risk influencing factors concerning the worker's abilities such as competence, communication, and work load, and in turn, below that a layer of management qualities that influence worker performance. Quantification is through data on incidents occurring in offshore maintenance work collected over the years and weighting of risk influencing factors by expert opinion. Accomplishing this is rather laborious, also because the factors are influencing each other as well.
A possible alternative way proposed in this paper is making use of process safety performance indicator values, both lagging and leading, aggregated to an appropriate level. Indicators contain intrinsically the information mentioned above on human performance and management quality in relation to operational conditions. For aggregation of a large number of indicators to a more manageable set, the importance of each indicator for various groups of activities such as operation, maintenance, and organization (personnel) shall be weighted by experts. Also, the effect an indicator value will have on the overall risk of the operation shall be determined.
Indicators can be considered as exponents of middle and long-term risk factors reflecting reliability of human activity in its many aspects without decomposing it to individual action. If combined with signals from sensors warning for risks on the short term, their influence can be included in bowtie type of cause-consequence scenarios by making use of the Bayesian network infrastructure allowing inclusion of information on aleatory uncertainty of data.

4. Bayesian networks

Members of the Loss Prevention community are familiar with modeling cause-consequence chains using tools such as fault and event tree. Mathematically these are called 'directed acyclic graphs', which consist of nodes representing a stochastic variable and arcs or arrows representing the dependency between the nodes they connect. Base or parent nodes are independent; they can connect to one or more dependent follow-on nodes. In the fault and event trees we are familiar with, the node variable represents a binary change of state (functioning to faulty/failing) due to a change earlier in the chain or an event caused with some probability by a previous event. The acyclic property appears as a dependent node never arcing back (pointing the arrow) to a predecessor, but only to nodes further down the chain. In fact, what is described here is the archetype of a Bayesian network or BN. It is only that the mathematical statistics developed for BNs and the associated software allows much larger flexibility.
BN's usefulness appears by being able to describe discrete multi-mode states, hence various degrees of remaining functionality of a component; it is even possible to handle continuous probability density functions, which allows input of uncertainty estimates of data. By taking triangular distributions (min, mode, max) the same can be done as in a fuzzy set. Some software, e.g., GeNIe of Decision Systems Laboratory, University of Pittsburgh (http://genie.sis.pitt.edu/) also allows for IF..THEN ELSE rules. Cross-connections between branches of a tree can easily be made. The software allows quick insight how the node is defined and modification of it, and its resulting value after a calculation that can be an entire distribution of values complete with mean and standard deviation, which makes it highly transparent. Dynamic BNs allow time functions, in the sense that wear, test intervals, repairs etc. can be modeled in a discrete time slice fashion. The Bayesian character of the networks shows up as the ability to absorb newly observed evidence and updating the net. When the new evidence is in a node near the bottom, the effect it would have on probabilities higher up in the chain is shown allowing easy diagnosis or adapting a model to new observations. This explains BNs current application in medical and psycho-sociological sciences, in economics, and in other fields. BNs are sometimes called Bayesian Belief Nets because nodes can contain subjective information, hence opinions. The non-parametric continuous version of BNs of Cooke and his team, e.g., Morales (2008), is ideally suited to contain expert opinion expressed as the influence of one node variable on the other.

5. Example case

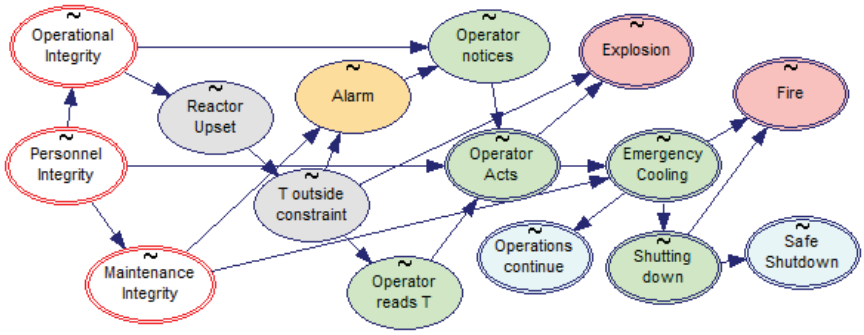

Fig.1. Left: BN describing reactor upset with end states continued operation, safe shutdown, explosion, or fire. Occurrence of upset is once per year expressed in a triangular distribution, because of uncertainty. Applied BN software is GeNIe of DSL, University of Pittsburgh (http://genie.sis.pitt.edu/).

Table 1. Input values to the variables of the nodes shown in the Bayesian network of Figure 1

Node	Variable	Min	Mode	Max	Node	Mean
Reactor Upset, /yr	Triangular distribution	0.23	0.70	2.10	Alarm	0.90
T outside constraint	Triangular distribution	0.07	0.20	0.35	Operator reads T	0.1
Operator notices	Triangular distribution	0.70	0.85	0.95	Emergency Cooling	0.9
Operator acts	Opr_notices OR Opr_reads T				Operations continue	0.85
Fire	0.1*Emer_Cool + 0.2*Shtng_Dwn				Shutting Down	0.15
Explosion	T outside constraint - Op_acts				Safe Shutdown	0.8

Table 2. Results of BN calculations of three levels of integrity indicators

Integrity O,P or M	Reactor Upset /yr	T outside constraint /yr	Operations Continue /yr	Safe Shutdown /yr	Explosion /yr	Fire /yr
1	1	0.21	0.13	0.02	0.04	0.02
0.9	1.13	0.23	0.09	0.01	0.10	0.01
0.75	1.34	0.28	0.06	0.01	0.18	0.01

In Figure 1 a very simple example of a BN of a continuous reactor system is shown of which temperature, T, is controlled. In case of upset, the operator is primarily notified by an alarm. If alarm fails or the operator does not notice it, he may be alerted by routinely reading the temperature indicator. Once notified, the operator can start an emergency cooling, which with some probability restarts the system or brings it into a safe state. Alternatively, if the cooling does not lead to success, the reactor will burst into fire. In case the operator does not act, the likelihood will be high that explosion will occur. Three aggregated top indicators (personnel, operational, and maintenance integrity) as in the study of Hassan and Khan, 2012, influence the success of preventing a mishap. Each indicator influences nodes with which it has a functional relationship. The personnel integrity indicator is assumed to be the determining one, although the weights of all three have been taken equal. In Table 1, inputs to the node variables are shown and in Table 2, the results of calculation of the respective end states, given an average reactor upset frequency triangularly distributed of once per year. If integrity is smaller than unity, explosion probability increases quickly.

6. Conclusions

The way forward in obtaining real-time information on safety level of a process operation will be only by taking into account the effect of risk factors and their time dependence on possible component failures leading to hazardous material release. Technical factors and the effects of management and organization reflecting human reliability in performing tasks correctly shall be merged. Process safety performance indicator values can be instrumental to account for management quality and human performance. Causal chains leading up to release events and their consequences can be modeled by applying Bayesian networks. The method proposed has, however, to prove its usefulness in actual case studies for which the authors invite companies willing to cooperate and to make some investment in time and effort. In case of success, the approach could also serve as a means to make better use of collected indicator values and to facilitate decision making on whether the present state of safety is acceptable or shall be further improved.

Acknowledgement

The constructive comments and editorial guidance by Dr. William Rogers of the Mary Kay O'Connor Process Safety Center are gratefully acknowledged.

References

CCPS (Center for Chemical Process Safety), 2007, Guidelines for Risk Based Process Safety, John Wiley & Sons, Hoboken, NJ, ISBN 978-0-470-16569-0.

Hassan J., Khan F., 2012, Risk based asset integrity indicators, Journal of Loss Prevention in the Process Industries, **25**, 544-554.

Jiang H., Shah, S.L., Huang B., Wilson B., Patwardhan R., Szeto F., 2012, Model analysis and performance analysis of two industrial MPCs, Control Engineering Practice, **20**, 219–235.

Kalantarnia M., Khan F., Hawboldt K., 2009, Dynamic risk assessment using failure assessment and Bayesian theory, Journal of Loss Prevention in the Process Industries **22**, 600–606.

Knegtering B., 2002, Safety Lifecycle Management in the Process Industries, PhD Thesis, Eindhoven University of Technology

Knegtering B. and Pasman H.J., 2012, The Safety Barometer, submitted to Journal of Loss Prevention in the Process Industries.

Morales O., Kurowicka D., and Roelen A., 2008, Eliciting conditional and unconditional rank correlations from conditional probabilities, Reliability Engineering and System Safety, **93**, 699–710.

Németh, E., Lakner, R., Cameron, I.T., Hangos, K.M. 2009, Fault diagnosis based on hazard identification results, In proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS 2009), pp. 1515-1520.

Seligmann B.J., Németh E., Hockings K., McDonald I., Lee J., Hangos K.M., Cameron I.T., 2010, A Structured, Blended Hazard Identification Framework for Advanced Process Diagnosis, G. Suter and E. De Rademaeker eds., Proceedings of the 13th International Symposium, Brugge, Belgium, (193-200). 6-9 June 2010, www.ti.kviv.be

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

Shoukat Choudhury M.A.A., Shah S.L. and Thornhill N., 2008, Diagnosis of Process Nonlinearities and Valve Stiction, Dat Driven Approaches, in Advances in Industrial Control, Springer-Verlag, Berlin-Heidelberg, ISBN 978-3-540-79223-9, e-ISBN 978-3-540-79224-6.

Venkatasubramanian V., Rengaswamy R., Kavuri S.N., Yin K., 2003, A review of process fault detection and diagnosis, Part I: Quantitative model based methods, Computers and Chemical Engineering **27**, 293-311; Part II: Qualitative models and search strategies, Computers and Chemical Engineering **27**, 312-326; Part III: Process history based methods, Computers and Chemical Engineering **27**, 327-346.

Vinnem J.E., Bye R., Gran B.A., Kongsvik T., Nyheim O.M., Okstad E.H., Seljelid J., Vatn J., 2012, Risk modelling of maintenance work on major process equipment on offshore petroleum installations, Journal of Loss Prevention in the Process Industries, **25**, 274-292.

Yang X, and Mannan M.S., 2010, The development and application of dynamic operational risk assessment in oil / gas and chemical process industry, Reliability Engineering and System Safety **95**, 806–815.