Left-hand side BBN model for process safety


Safety Science, Delft University of Technology, Delft, The Netherlands

Dan Ababei
LightTwist Software, The Netherlands

ABSTRACT: This paper describes the blueprint of a model for calculating the left-hand side of the bow-tie for chemical plants is described. The model is based on Non-Parametric Bayesian Belief Nets so that uncertainties are automatically included. Also, the procedure for constructing the elements for the model is described. The aim is to calculate LoC frequencies for entire chemical plants in a single straightforward modeling approach in a single model. It is demonstrated that only four principle design rules are required to construct the blueprint for a model that is flexible and straightforward to work with. It was also found that design process for the components of the model is traceable and reproducible. A structured working procedure was designed to meet those requirements. A numerical validation process will follow in the future.

1 INTRODUCTION

This paper describes part of the continuing development of a QRA model that represents the left-hand side of the bow tie of a chemical processing plant. Earlier steps of this development were described elsewhere (Van Gulijk et al., 2012, Ale et al., 2012, Hanea et al., Lin et al., 2012, Sillem et al. 2012).

The paper focuses on the procedure for the development of modeling parts. This QRA model for the left-hand side is aimed to be more efficient than designing dedicated fault-tree models for each piece of process equipment on a chemical plant. The objective is to capture all process equipment on a plant, including process pipes, pumps, columns and reactors with one and the same modeling technique. The general approach for the model is described in another paper in this conference (Ale et al. 2013).

2 BACKGROUND

The right hand side of the bow tie, where consequences of accidents are modeled, is relatively well developed in QRA for chemical safety. Many years of were spent in the development of consequence models and those models found their way into generic chemical risk analysis techniques on which safety decisions, regulations and sometimes laws are based. In the Netherlands, the Purple Book (Ale & Uitdehaag, 1999) and the associated risk assessment program Safeti-NL play an important role in the issuing of permits for operation of chemical processes. The Purple Book and Safeti-NL supply consequence models for a great number of adverse events following loss-of-containment (LoC) scenarios. The starting frequencies for loss-of-containment events are based on fixed point estimators from literature or historic data collected in chemical corporations. The initiating frequencies represent the left-hand-side of the bow-tie. This work aims at improving the estimates for these left-hand-side frequencies.

According to Dowel (2001) there are three basic categories of modeling for the left-hand-side; full QRA in the form of fault tree analysis; simplified QRA methods such as LOPA; and qualitative analysis. Since constructing a fault tree is a relatively cumbersome activity that is typically reserved for intricate and/or critical process equipment in chemical plants. Many pieces of process equipment are analyzed with LOPA. In this project, however, the objective is to perform a QRA for every part of the plant.

The foundations of the modeling strategies are presented in four steps. They are described in the next paragraph.

3 MODEL STRUCTURE

The model structure is partly described in the paper by Ale (2013); this description focuses on
the underpinning of the basic steps to come to that model.

3.1 Step 1: Model hierarchy

The approach to modeling the left-hand side was originally based on the construction of dedicated fault-trees for process blocks in chemical plants. This, however, turned out to be too cumbersome to model each and every part on a chemical plant that can contain hundreds of pieces of process equipment and thousands of meters of pipes. An alternative method was called for that retained the granularity for the model (model all process equipment) yet facilitates efficient design, use and re-use of modeling blocks.

The approach is inspired by the methodology used in the TECHNICA report (Ale & Whitehouse, 1984). This method has proven its usability in various modeling tools such as Safety-NL. A key element is that standardized parts of chemical process equipment are represented by the same mathematical construct. In this project that construct is the generalized BBN.

In the TECHNICA report, plants are divided in units. Units, in turn, are divided in parts. For parts, standardized failure mechanisms and appropriate consequences are modeled.

For this project, a number of modeling layers are added; they are:

- Region
- Site
- Plant
- Unit
- Equipment (part)
- Excursion Control Path

A more detailed description can be found in the paper by Ale (2013).

3.2 Step 2: LoC models

In order to model all equipment, some harmonization is also necessary in the way that LoC’s are modeled. This harmonization works as follows.

Parameter excursions

Any part of the chemical process plant is designed to contain hazardous chemicals under operational process conditions with a built-in safety margin. These margins are typically subject to rigid design standards. In this work deviations of the process parameters beyond these margins are called parameter excursions. Parameter excursions are quantifiable entities that have probability of occurrence [year⁻¹].

Barriers

Ordinarily, there is at least one safety barrier that controls parameter excursions. Barriers have a probability of failure per activation [activation⁻¹] or [−]. The failure probabilities are the input parameters for a barrier.

Excursion control path

For process parameter excursions (like temperature or pressure) there may be up to three or more consecutive, independent barrier systems to prevent loss-of-control. In that respect this work follows the LOPA method (Dowell, 2001). This methodology leads to a chain of barriers that may be activated when a parameter excursion takes place. The parameter excursion, including the initiating parameter excursion and the activation of the chain of barriers is termed an excursion control path. The combination of starting frequencies and the frequency of failure of the barriers leads to an annual frequency of occurrence for LoC’s.

LoC

A Loss of Containment or LoC of process equipment follows when all barriers fail. The uncontrolled deviations from normal process conditions and operations that are so extreme that leaks, cracks and/or ruptures cause the uncontrolled transport of materials from inside process equipment to the outside.

Combination of LoC’s in equipment

For a given piece of equipment, a number of excursion controls combine; for instance corrosion, wrong installation, and overpressure combine (amongst others) into a vessel equipment model. It is important to remember that an excursion control path links a single type of a parameter excursion (say, corrosion) to an LoC. The combined LoC’s model the LoC frequency of the equipment.

3.3 Step 3: Barrier block

The technical details of a barrier are not expanded into fault trees. This has a specific advantage because there can be hundreds or more technical and human barrier systems, each of which would require a fault tree structure. Alternatively, the fault tree is expanded into the basic function of a barrier or the barrier validity rules. These rules are given the LOPA handbook.

Figure 1 elucidates the concept. When a component is technical, the model for the BBN is not extended. If it incorporates a human activity (say, operator action) two human performance models can be inserted: the Shell Human factor model and the Contractor Human Performance model. They are treated elsewhere (Sillem et al., 2012).
Note that the barrier blocks are the actual BBN’s. Depending on the number of human models, the BBN can be as small as four nodes up to forty nodes.

### 3.4 Step 4: Types of Excursions

The number of causes for excursions is limited in the current working version of the model. Four types of parameter excursions are considered. The parameter excursions are fundamentally different in each of those processes. These processes are:

- **Process parameter excursions**: the most important excursions being pressure excursions, temperature excursions and (liquid) level excursions.
- **Slow degradation excursions**: the most important processes being corrosion and erosion.
- **Mechanical degradation excursions**: the most important processes being direct mechanical impact and wind and water shear, and overloading.
- **Installation excursions**: these excursions do not originate during operation but are engraved into the system because of faulty installation or faulty construction; the most important excursions being faulty installation, poor welds and use of the wrong materials.

This classification was derived from the twelve categories of direct cause in the STATAS methodology (Mannan, 2005): corrosion; erosion; external load; impact; overpressure; vibration; temperature (high/low); wrong equipment; defective equipment; human error; other; unknown.

### 4 CONSTRUCTING AN EQUIPMENT MODEL

Equipment LoC models form the backbone of the risk analysis for the left-hand side of the bow-ite. The excursion control paths have to contribute to the risk in an equipment LoC. Excursion control paths have to be credible and non-negligible. In other words, they have to contribute to the risks associated with the equipment. However, it is not so easy to decide which excursion control paths should be taken up in the model and which not: double counting and addressing diminutive risks are a constant concern.

A straightforward procedure was developed to provide a systematic selection procedure. The basis of this procedure is the risk management cycle by Ale (2009). The risk management cycle shows procedure for risk decision making. It provides a template for the selection and development of excursion control paths. Figure 2 illustrates the risk management cycle as blueprint for the process of excursion control path selection. Each step is treated briefly.
The first step of the procedure is to identify LoC threats in a piece of equipment using a HAZOP scheme (HSE, 1995). The HAZOP guides the selection of the type of excursions and the threat scenario’s associated with them. More importantly, it makes it hard to overlook relevant excursion control paths.

Once excursion control paths are identified, it is important to verify whether the threats lead to an accident or incident scenarios. In this stage two methods are used to judge whether a LoC can cause problems. If there is enough industry data available a straightforward Risk Assessment Matrix (RAM) is used. When given excursion control paths turn out to have a very low risk contribution, they are eliminated from the equipment LoC model.

When the threat poses a less tractable risk the UKOOA risk decision framework is used to guide the qualitative discussion (Hartford, 2007). However, it was found that this is rarely called for.

The identification of risk by HAZOP and the analysis by RAM and UKOOA yield a decision to further develop an excursion control path. The decisions have to be registered for future reference.

The fourth step is the actual development of the excursion control path and the last step is a verification step where the entire equipment LoC is tested against historical data.

Following this procedure, at least eleven equipment LoC base models are under development. They are:

1. vessels HC only V-HC
2. vessels L-L separator V-LL
3. reactors R-GEN
4. pipework PW
5. centrifugal pump P-C
6. reciprocating pump P-R
7. furnace F-GEN
8. fin-fan coolers E-FF
9. tubular heat exchanger E-TS
10. centrifugal compressor C-C
11. reciprocating compressor C-R

5 DATA GATHERING

The successful use of the model in the software depends on the quality of data. Most of the data that is used in the project is either available through the open literature or through company data. This para graph describes how technical failure frequency data is translated into a BBN distribution in the case that such distributions are not available.

Failure data is usually present as point estimators (e.g. the failure frequency in [year⁻¹]). As an alternative a predetermined distribution is assigned in the BBN. In this stage of development a triangular shape has been chosen as a general model for distributed error rates. The central estimate (from literature or otherwise) is the middle of the triangle, say value x. As a first estimate the left edge of the triangle is 0.9x the right edge of the triangle is 1.1x. The top of the triangle is on the position of x with a height of 10/x because the area under a probability frequency distribution has to be 1. Figure 2 illustrates this.
Note that the data for the human models was derived from dedicated expert elicitation exercises (Sillem et al. 2012) a distribution is available for all human error models.

In some cases, the data that is available influences the structure of the BBN of the barrier block. Since a barrier block only contains the parameters related to the presence of the barrier and the validity rules for barriers only five barrier factors are modeled as BBN blocks: the initiating frequency; the detector function, the logic function, the actuator function, and the node recording how often the barrier is installed. Note that the detector, logic and actuator are sometimes integrated in a single piece of equipment with a single failure rate (e.g. a pressure relief valve). And as already mentioned before; when one of the functions (detector, logic or actuator) is performed by a human a human performance BBN is attached to that BBN node.

6 EXAMPLE OF MODEL BUILDING

The next step in modeling an entire chemical plant is very much a bookkeeping exercise. Say a unit consists of the following parts: 21 units of pipework, 2 vessels and 1 specialized pump. The LoC frequency of that unit is calculated as follows. First, the standardized equipment LoC for pipes is engaged. It consists of six excursion control paths: one for corrosion, two for mechanical impact, one for faulty installation, one for over-pressurization and one for vibrations. Without detailed further information about the pipework, standard input parameters are used. These six control paths, composed of BBN’s are calculated using the program. The overall LoC for pipework is calculated and multiplied by 21. A similar exercise takes place for the vessels that have seven standardized excursion control paths. The pump is a special case, here two exceptional excursion control paths have to be added to the standard five excursion control paths: cavitation and vibration. They need to be specified through the process described above (including the number of barriers, the linkage with human models, excursion frequencies and barrier efficiencies). Since the same humans operate all equipment in this unit, the input parameters for the human influences are the same in the calculation, the same holds for management influences.

Now, the following calculation is performed:

- 5 excursion control path calculations for the pipework equipment LoC. The result (a risk distribution) is multiplied by 21;
- 7 excursion control path calculations for the HC-vessel excursion control paths multiplied by 2;
- 7 excursion control path calculations for the reciprocating pump, five standard and two exceptional excursion control paths.
- One addition of the three groups of equipment LoC to calculate the LOC of the unit.

After the design of a user interface and assigning meaningful labels to the data, interpreting the results will be relatively easy. Note that it would not be difficult to design alternative input parameters to accommodate dedicated changes in human factors; e.g. when personnel was recently trained in pump maintenance, the inputs for the pump excursion control paths can be changed. It all becomes part of a bookkeeping exercise: making sure that the right input parameters are calculated in the correct calculation loop of the program.

7 DISCUSSION

The paragraphs above describe the blueprint for the generic modeling approach. What this does not show is that the risk analysis method is very flexible. Consider the following examples. The first example is when not all excursion control paths are needed in the calculation of an equipment LoC, say, for a length of pipe. This is easily accommodated. Say that parts of pipework are free from mechanical impact risks, based on a judgment based on local information of the plant. Then only four excursion control paths are necessary in the equipment LoC. This is easily accommodated. Say that parts of pipework are free from mechanical impact risks, based on a judgment based on local information of the plant. Then only four excursion control paths are necessary in the equipment LoC. The excursion control paths for those equipment LoC’s can be deleted.

The second example is if only one physical barrier is present in an excursion control path where there normally are two. BBN blocks that represent a single barrier can be rendered inoperative in the
BBN structure. This is technically possible either by setting the failure rates to zero or giving the connecting arches to specific values so that the next barrier steps do not contribute in the top node.

The third example is when a specific human contribution in a barrier is replaced by a technical system. In that case the influences by human factors can be rendered inoperative or simply deleted from the BBN. These examples demonstrate that the basic BBN structure is very flexible in its use.

Flexibility is also introduced by the fact that each part, say, a length of pipe, has its own characteristic input parameters for parameter excursions, barrier effectiveness, human factors and management factors. These parameters are different for vessels, pumps, bends and other parts. So by introducing different input parameters, the LoC frequencies of different excursion control paths can be modeled without changing the basic structure of a barrier BBN. In theory, it is possible to try to find input parameters for each individual excursion control path but in practice many parts will have the same input parameters: e.g. for each 100 m of 1” pipes the input parameters are very alike, even if there is 10 km of it in the plant. When detailed information is available for specialized parts (e.g. a specialized chemical reactor) the input parameters can be introduced easily.

Two important challenges remain to be solved. Firstly, what if one part influences the excursion of another part? In a single, excessively large BBN it would be possible to just create a link and see what happens. In this case, the BBN’s are decoupled between excursion control paths and the interference cannot be dealt with in that way. Alternatively, the effect that one part has on another has to be quantified so that initiating frequencies and barrier failure modes change. From that point on it becomes a book-keeping exercise once again.

Secondly, how can we account for changes in human models and management influences? Firstly, the calculation structure as is proposed here accommodates the use of two human models: shell and contractor. If the human support of a barrier changes from shell personnel to contractors or vice versa, it is simply a matter of switching on the influence of the one human model and switching the other off in the BBN. Secondly, if detailed information is available about specific sites the input parameters for the human models can be adjusted to the local conditions. Also, specific management actions can be modeled: if management decides to increase contractor training for the maintenance of vessels, only vessels would be affected. Again it boils down to an input-output problem of the calculation.

8 CONCLUSION

The full quantitative analysis of the entire chemical plant in a single model, based on BBN’s, is within reach. Some important steps had to be taken to structure the model in a practical way and a design process for the model components had to be developed but that problem was solved. The working method makes the development of huge dedicated fault trees obsolete thereby greatly simplifying the break down of a chemical plant into manageable.

A fairly small BBN structure can be used to estimate the frequency of loss of control events in chemical plants of any types. The major problems are twofold. Firstly, the generic BBN has to be as generic as possible so that it can accommodate all possible variations of excursion control paths yet be flexible to use for all parts. Secondly, the program that is the shell around the BBN has to be able to handle input and output parameters meticulously; no crossover of data is tolerated and all data has to be coupled to meaningful descriptors.

A future possibility is that a smart input-output shell could simply read existing equipment lists and derive the number of excursion control paths so that they can be calculated with preset, or manually altered values to generate LoC frequencies even before a plant is even built. The third distinct possibility is that the effects of specific management decisions, and changes in personnel can immediately be calculated, provided that they are related to barriers and a valid quantification of those effects can be made.

In the near future, validation of the method will take place with historical accident data to evaluate the predictions that the model makes.

ACKNOWLEDGEMENT

This work reported above was fully funded by Royal Dutch Shell plc.

REFERENCES