Automating HAZOP studies using D-higraphs

Manuel Rodríguez, José Luis de la Mata

ABSTRACT

In this paper, we present the use of D-higraphs to perform HAZOP studies. D-higraphs is a formalism that includes in a single model the functional as well as the structural (ontological) components of any given system. A tool to perform a semi-automatic guided HAZOP study on a process plant is presented. The diagnostic system uses an expert system to predict the behavior modeled using D-higraphs. This work is applied to the study of an industrial case and its results are compared with other similar approaches proposed in previous studies. The analysis shows that the proposed methodology fits its purpose enabling causal reasoning that explains causes and consequences derived from deviations, it also fills some of the gaps and drawbacks existing in previous reported HAZOP assistant tools.

1. Introduction

Throughout the history of the Process Industry there have been a lot of accidents of different consideration, from mild to catastrophic. The gravity of an accident can be analysed in terms of economical, human or environmental losses. Kletz (1999b, 2001) has performed a deep review of several accidents, analysing the causes and proposing modifications that could have avoided them. From the information gathered of the accidents new safety procedures, process modifications and working methods have been implemented, however, prevention should have come first.

> *"It is better to see the hazards afterwards than not see them at all, as we may pass the same way again, but it is better still to see them when they still lie ahead".* (Kletz, 2001)

In economic terms, operating a process plant in a safe way—lack of accidents—reduces the losses associated to shut-downs, reparations, compensations and fines. But, at the same time, the incomes increase because productivity does. As a consequence of costs decrease and incomes increase, profits grow. Of course, there are other aspects, such as environmental impact, pollution or operators occupational health that also benefit from a safe operation.

Apart from economical issues, tighter regulations, public concern on industrial incidents and a greater presence of chemical industry accidents in the media are making accident prevention a major task in process industry. It involves the analysis of the process itself, the control system, the additional safety systems, the backup systems, the operation procedures and so on. They are analysed during the design stage and during the operation of the plant. In these papers we will focus in the former, the design stage.

Process Hazard Analyses (PHA) are carried out to identify the potential safety problems but also to propose possible solutions such as process changes, new control strategies or the use of safety instrumentation. To perform PHA there is a wide range of techniques: What-If, Checklist, Hazard and Operability (HAZOP), Failure Modes and Effects Analysis and Fault Tree Analysis. However, HAZOP studies gather the two following features (Zhao, Bhushan, & Venkatasubramanian, 2005a): (1) it is a tool easy to learn and use and (2) it is reusable and adaptable for almost all industrial processes.

Hence, HAZOP is widely accepted as the method for conducting the PHA analysis. It was first developed in the late 1960s at Imperial Chemical Industries (ICI), nowadays taken over by AkzoNobel. HAZOP studies provide a systematic methodology to identify and reduce the potential risks or process hazards (Swann & Preston, 1995). This tool will be discussed further in the present article.

Although HAZOP studies are easy to learn, reusable and systematic, it is a procedures that consumes a lot of time and effort which can be translated to money. During the last two decades, there have been developed different tools that automate the HAZOP studies, some of them are:

- HAZOPExpert, a model-based intelligent system for HAZOP of continuous processes (Venkatasubramanian, Zhao, & Viswanathan, 2000).
- PHASuite, an automated HAZOP analysis tool for chemical processes (Zhao, Bhushan, & Venkatasubramanian, 2005b; Zhao et al., 2005a).

- Functional HAZOP assistant, a functional modeling based methodology (Rossing, Lind, Jensen, & Jørgensen, 2010a, 2010b).
- Layered Digraph Model (Cui, Zhao, Qiu, & Chen, 2008)
- PetroHAZOP (Zhao, Cui, Zhao, Qiu, & Chen, 2009)

The main objective of this paper is to present the use of D-higraphs to perform HAZOP studies. The key idea of a D-higraph is to capture the functional as well as the structural aspects of process plants. In other words, the aim of a D-higraph model is to gather activity and ontological features of the system modeled in an integrated model (Rodríguez & Sanz, 2009).

D-higraphs, as a functional modeling technique, can be used in the same way than Multilevel Flow Modeling (Lind, 1994, 2005) is used to develop the 'Functional HAZOP assistant' proposed by Rossing et al. (2010a, 2010b). D-higraphs provide almost the same functional knowledge than MFM but as they integrate structural information, the correlation with the real system is much more direct and easier. However, using the extensions presented in Lind (2010), MFM also integrates structural information. At this point it should be noticed that a D-higraph is not a hypergraph, thus abstraction is not facilitated, in contrast to MFM.

The proposed methodology is compared with the above mentioned tools and also with conventional HAZOPs. To that end, we have developed the D-higraph of the Indirect Vapor Recompression Distillation pilot Plant (IVaRDiP) at the Department of Chemical and Biochemical Engineering at Technical University of Denmark (Danmarks Tekniske Universitet, DTU) and we have also performed a HAZOP analysis using the D-higraphs framework. Rossing et al. (2010a, 2010b) used this case study, so a direct comparison can be made.

The paper is structured as follows. Next section introduces an overview of HAZOP studies. The following section briefly describes the D-higraphs technique. The D-higraphs HAZOP assistant is presented in the succeeding section. Then, the methodology is applied to the IVaRDiP system. Next, the methodology is compared to other tools. Finally, the 'assistant' is analysed, the conclusions are drawn and further work is proposed.

2. Five brief questions (and answers) on HAZOP studies

2.1. What is a HAZOP?

According to Kletz (1999a) a HAZOP is "*the method recommended for identifying hazards and problems which prevent efficient operation*". Once the hazards and problems are identified, possible solutions and modifications can be proposed to avoid and get rid of these hazards and problems, that is, HAZOP is a prevention tool.

2.2. Who carries out the study?

A Hazop is accomplished by a multidisciplinary team so each of the members of the group can provide his experience and knowledge about the project under study (Skelton, 1997). For a plant under design the team should consist of the following members: Project or design engineer, process engineer, commissioning manager, control system design engineer, research chemist and independent team manager.

If the study involves an existing plant the HAZOP team should be formed by these members: Plant manager, process foreman, plant engineer, control engineer, process investigation manager and independent team manager. In case of an existing plant being modified, rearranged or extended, the team should include a combination of both teams (Kletz, 1999a).

Table 1
Deviations generated by each guide word.

Guide word	Deviations
NONE	No forward flow when there should be.
MORE OF	More of any relevant physical property than there should be.
LESS OF	Less of any relevant physical property than there should be.
PART OF	Composition of system different from what it should be.
MORE THAN	More components present in the system than there should be.
OTHER THAN	What else can happen apart from normal operation.
REVERSE	The opposite of the design intent occurs.

An inappropriate team 'setup' can undercut the advantages of the HAZOP study and it can even cost several times the expenses of gathering a proper team (Swann & Preston, 1995).

2.3. When is it performed and how long does it take?

During the design of a new process plant, the study should be carried out as soon as possible. The beginning of the study takes place once the Process Flow Diagram (PFD) and the Piping and Instrumentation Diagram (P&ID) are ready and it should be performed before the detailed design starts. If the plant under study is an existing plan, the study starts once the line diagrams are up to date (Kletz, 1999a).

The analysis of each main item of the plant takes from 1.5 to 3 h. 1.5 h if it is an already known item and 3 h if it is a brand new device. Meetings should last no more than 3 h, 2–3 days per week. Meetings of short duration manage to keep the team centered and focused during the entire study. For a big project it may take months to complete the HAZOP study, costing between $ 13,000 and $ 25,000 per week (Freeman, Lee, & McNamara, 1992; Nolan, 1994).

Stated the huge amounts of time and effort—which means money—involved in carrying out HAZOP studies, there is significant interest and considerable incentives to implement systems for automating them (Kletz, 1999a; Rossing et al., 2010a; Swann & Preston, 1995; Venkatasubramanian et al., 2000; Zhao et al., 2005a).

2.4. Why is it necessary?

The conclusions of many of the accidents described by Kletz (1999b, 2001) show the need for critical examination of the design by hazard and operability studies or similar techniques. In the majority of these cases, a thorough HAZOP study could have prevented the accident. *Prevention* is the key word.

2.5. How is it done?

The P&ID is divided into sections or nodes and then each section is studied applying an algorithm (see Fig. 1). Usually nodes are equipment items, however, if nodes are too small, certain hazards may be missed. Therefore various devices are joined in a single node but if nodes are too large they became confusing and hard to handle.

Once a node is chosen, each line of the node is analysed applying certain deviations. These deviations result from the combination of a 'guide word' with a 'property' of the line (Hyatt, 2003):

$$GuideWord + Property = Deviation$$

Guide words are gathered in Table 1 while line properties or parameters are flow, temperature, composition, etc.

The study consists of the following steps:

1. Define objectives and scope of the HAZOP study.
2. Prepare for the study: Gather process information, such as PFDs and P&IDs.

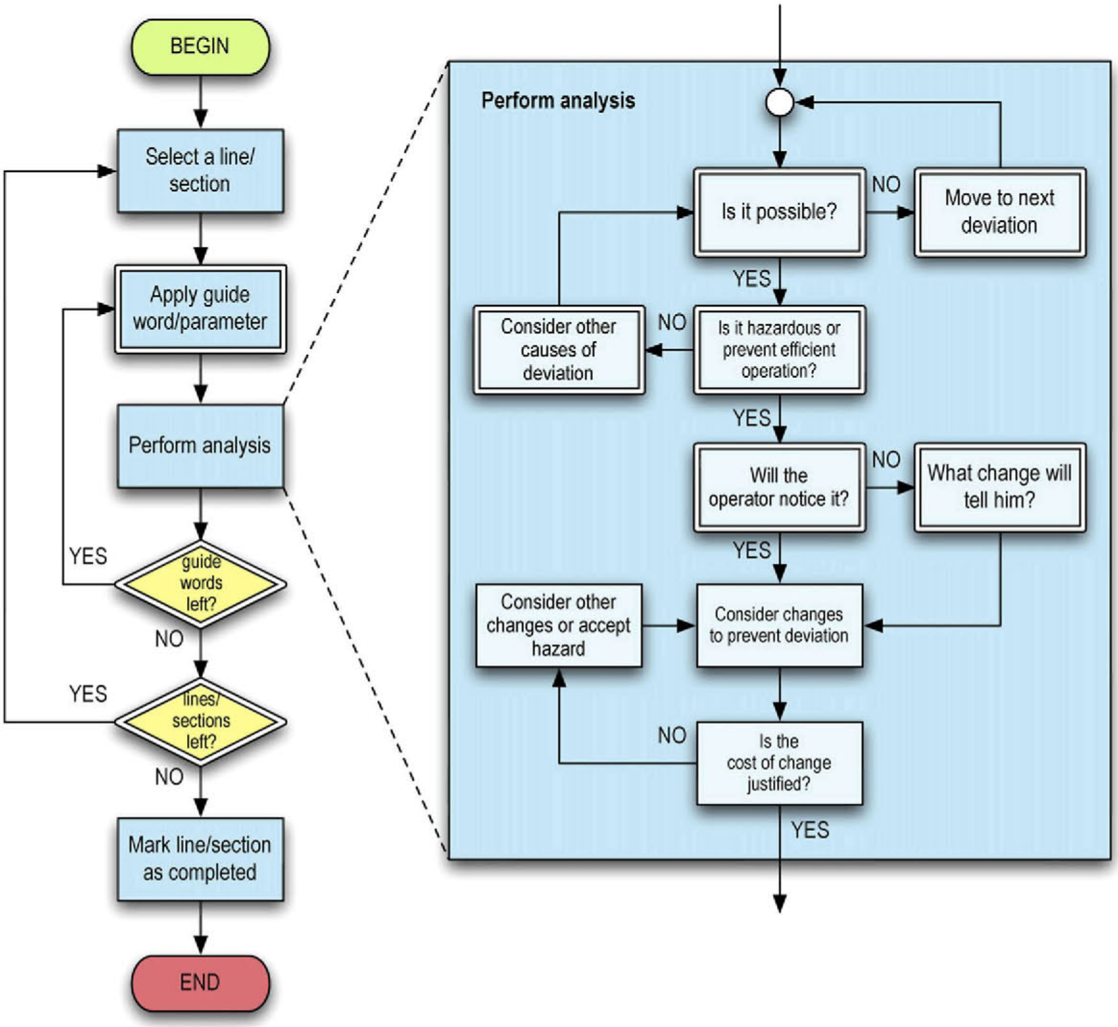
BEGIN
Select a line/ section
Apply guide word/parameter
Perform analysis
YES
guide words left?
NO
YES
lines/ sections left?
NO
Mark line/section as completed
END
Perform analysis
Is it possible?
NO
Move to next deviation
YES
Consider other causes of deviation
NO
Is it hazardous or prevent efficient operation?
YES
Will the operator notice it?
NO
What change will tell him?
YES
Consider other changes or accept hazard
Consider changes to prevent deviation
NO
Is the cost of change justified?
YES

Fig. 1. HAZOP procedure.

3. Carry out the study. First review the methodology, remember de objective of the study and brief description of the process. Then, each section is studied applying the procedure shown in Fig. 1.
4. Record the results.
5. Follow up action items.

Note that some of the boxes in Fig. 1 have a double-line boundary. The procedures or actions that they represent can be automated using the *D-higraph HAZOP Assistant* that will be presented later in this paper.

3. D-higraphs

3.1. Higraphs, the antecedent

Harel (1987, 1988) originally presented higraphs as a general kind of diagramming objects. They are well suited—and were designed for—for the behavioral specification of complex concurrent systems. They constitute a visual formalism of topological nature that can represent set enclosure, exclusion and intersection, and the Cartesian product (orthogonality). They can be considered as an extension and combination of conventional graphs and Venn diagrams.

In conventional graphs the relative position of vertices has no significance but in higraphs the relative position of blobs provides valuable information about the relations between them, such as enclosure exclusion or intersection, like Euler/Venn diagrams. Higraphs extend the notion of graphs with the provision of depth (or hierarchy) and orthogonality, so they can be defined as (Grossman & Harel, 1997):

$$higraphs = graphs + depth + orthogonality$$

Higraphs consist of two main elements: blobs and edges. Blobs are represented as rounded-corner rectangular shapes. They represent mutual exclusive sets, they may intersect and be arranged in an inclusion hierarchy. Edges are represented by arrowed lines and connect blobs at any depth (Grossman & Harel, 1997).

Orthogonality is represented by a dashed line inside a blob, meaning an OR relation. One fundamental interpretation of higraphs, where blobs are interpreted as states and edges are interpreted as transitions between states, led to the language of statecharts. Statecharts are used for the description of discrete-event systems.

Fig. 2 illustrates higraphs components and features. It represents the state of a watch (Harel, 1988). The `stopwatch` blob (state) has two states, the `zero` state and the `disp/run` state. These states are OR components. The `disp/run` state has a `disp` state and a `run` state, these are AND states, so both happen at the same time. The `run` state has the `on` and `off` states (which, again, are OR states). Transitions between states are labeled (`b`,`d`) and they can contain

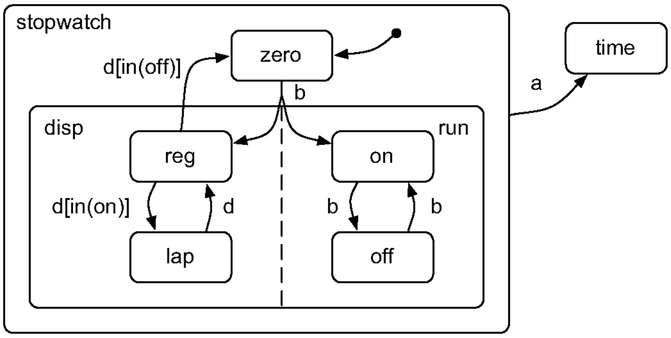

Fig. 2. Statechart diagram representing the stop-watch state of a watch.

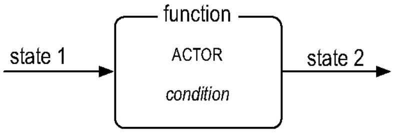

Fig. 3. Basic blob.

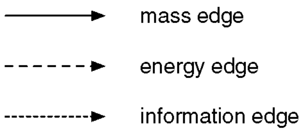

Fig. 4. Types of edges.

a condition (`in (on)`). The transition from `reg` to `lap` happens in the event of `d`, and when the condition is true.

3.2. *Dualization of higraphs*

Rodríguez and Sanz (2009) first presented D-higraphs as a modeling technique that merges functional and structural information of the system modeled. D-higraphs have the same appearance than higraphs. Both consist of blobs and edges, they are represented using blob inclusion, exclusion and the Cartesian Product and blobs are connected by edges. However, in D-higraphs the meaning of these properties changes.

In higraphs, disjoint blobs mean that there is an OR relation between them, while the AND relation is represented by orthogonal blobs. On the other hand, in D-higraphs we interpret them the other way around, i.e., disjoint blobs imply an AND relation while orthogonal blobs represent an OR relation. We are using higraphs properties in a dual way, that is why we call this new visual formalism dual higraphs or D-higraphs.

When we apply higraphs to behavioral specification and design of complex concurrent systems we get the statecharts. In this application, blobs represent states and edges the transitions between states. These statecharts are not useful to specify functional models of process systems because they provide depth in states.

When describing the functional relations of these kind of systems, depth is required in functions so functional dependency and hierarchy can be captured in the model. Also in these models we need to show the states that enable the functions. Therefore, in order to use higraphs for process systems they will have to be used in a dual way as they are used in statecharts. Blobs will represent now transitions and edges will represent states (Rodríguez & Sanz, 2009).

Note that the term *dualization* used along this text has a different meaning from the term used in conventional dual graphs. A D-higraph is not produced by changing blobs by edges and edges by blobs in a higraph, as we would do to develop a dual graph. We change the interpretation of blobs properties, in fact, we use them in a dual way. Another thing that changes is the application to process systems where the assignment of states and functions to blobs and edges is also done in a dual way.

3.3. *Blobs*

Blobs represent functions and they are depicted as shown in Fig. 3. The name of the function appears in the border of the blob, and the actor—usually an equipment or device—that performs or allows that function will be indicated inside the blob. This figure means that the function is performed by the actor if the `state 1` is enabled and if the condition inside the blob is true. The performance of the function makes that `state 2` is achieved.

A blob has the following elements:

- *function*. It describes the function of the overall system that the blob is representing. For example: remove heat, produce or store.
- ACTOR. It is the device, equipment or system that performs the function. For example: heat exchanger, reactor or vessel.
- *condition*. It is a boolean variable of the blob which is necessary for the function to be carried out. For example: reactor temperature must be over 500 K. All the blobs need a function and an actor, but the condition is an optional feature of the blob.

We are going to distinguish between different kinds of blobs and between different hierarchies (or levels of inclusion). Control blobs are colored in orange while process blobs are painted in green. There is an additional situation, called blend, in which we have both types of blobs included. In such case the blob is colored in blue. Using different colors can differentiate between different types of blobs, however, we also want to point out the hierarchy of these blobs. To that end, we use the same color for the same kind of blobs but with different saturation. The ancestor blob is painted using a less saturated color than its descendant, which, therefore, is coloured using a more saturated color (Note: this is by the sake of clarity, it is not necessary for the algorithms that analyze the D-higraphs).

3.4. *Edges*

Firing the function causes new states, represented by the edges coming out from the blob, so edges represent states of the modeled system. As we are working with process systems, edges represent flows of mass, energy or information, for example product flowing, heat transfer or state measured. These three kinds of flows are responsible of all of the interactions that could arise in a process plant. The type of flow does not affect the behavior of the model but in order to provide more information to whom is looking at the D-higraph, we will depict the edges in different ways. We will represent mass flows with a solid line, energy flows with a dashed line and information flows with a dotted line (see Fig. 4).

Note that if the function is fired we have new states, but if the function is not triggered, the states are not produced. In this point we can say that the function is a necessary condition for the state produced. Another thing that should be noticed is that, under certain conditions, there can be two blobs linked by two edges with opposite senses. In this particular case, we can simplify the D-higraph by substituting these two edges by a double-sense edge.

3.5. *Properties*

3.5.1. *Blob connection*

An edge always links two blobs: its tail and its head. This means that the blob at the tail performs a certain function that produces a state that is necessary for the blob at the head of the edge. There is always a blob at the tail and a blob at the head of a given edge. It is not possible to have an edge without head or tail because, by definition, an edge links two blobs. However, under certain conditions, the blob at the tail or at the head of the edge is not represented in the D-higraph, but it exists. It is called an elliptical blob. This situation typically happens with the inputs and outputs of the process but not in the middle of the D-higraph. They usually represent devices that are not depicted in the flowsheet of the process such as downstream or upstream equipments.

3.5.2. Blob inclusion

Blobs can be included inside of other blobs. The outer blob is the ancestor of the included blob which is called the descendant of the outer blob. The inclusion of a blob inside of another blob means that the function performed by the subblob is necessary for the superblob to perform its function. Moreover, the actor performing the subblob function is an element of the actor of the superblob. Here appears the integration of functional–structural features of the system in a single model which is one of the main aims of this methodology. If a blob has no subblobs or descendants it is called an atomic blob. A blob can enclose various blobs. A blob can be included in a blob which has been already included in other blob.

3.5.3. Partitioning blobs

A blob can be partitioned into orthogonal components which are separated using a dashed line. Each orthogonal component must contain at least one blob which establishes an OR condition for the partitioned blob. From another point of view, the partition of a blob only represents the separation of its subblobs into orthogonal components.

3.6. Causal reasoning

D-higraphs allow us to develop functional–structural models of process systems, gathering information about the relations between goals, functions and devices. However, this methodology has been developed not only to represent these knowledge but to use it to perform certain analyses.

De la Mata and Rodríguez (2010a, 2010b) provide a series of causal rules that relate two events, one as cause and the other as its effect. The rules have been set according to Mackie (1974), which also provides the notation used. Once an event is triggered these rules let us follow its propagation through the system in the sense of causes and in the consequences. These rules enable the possibility of analysing the chain of causation of a given failure upstream and downstream.

However, the above mentioned causation rules 'only' allow us to perform analyses using terms such as *faults* or *failures*. The term *failure* is pretty clear but the term *fault* does not provide any information about the sense of the deviation. For example, the level of a tank tagged as fault represents two possible situations: low and high level; which are indistinguishable in these kind of analyses.

3.7. Qualitative simulation

To solve the *Deviation Sense Problem* in D-higraphs, Qualitative Physics are taken into account. Let us remember that Qualitative Physics predicts and explains the behavior of mechanisms or systems in qualitative terms. The main goal of Qualitative Physics is to be far simpler than the Classical Physics and retain all the important distinctions without invoking the mathematics of continuously varying quantities and differential equations (DeKleer & Brown, 1984). Moreover, Qualitative Physics produces causal accounts of physical mechanisms that are easy to understand.

The description of the system is made in three different layers (Kuipers, 1984):

Table 2
Relation between HAZOP guide words and D-higraph deviations.

Guide word	Variable value	Variables
NONE	Failure	All
MORE OF	*inc*	All
LESS OF	*dec*	All
PART OF	*dec*	Comp. (x)
MORE THAN	*inc*	Comp. (x)
OTHER THAN	–	–
REVERSE	–	–

1. *Structural description*: variables that characterize the system.
2. *Behavioral description*: potential behaviors of the system as a network.
3. *Functional description*: purpose of a structural component of connections.

The first and the second layers—structural and behavioral descriptions—are described below. The third layer, the functional description, which represents the purposes, goals and objectives of the system, is gathered in the D-higraph of the system.

3.7.1. Structural description: blobs and edges variables

If we consider a process plant, the most common variables—with their symbols—related to the elements that represent them are:

- Edges:
  - Mass: Flow (F), temperature (T), composition (x) and pressure (P).
  - Energy: Energy (E), occasionally it may be interesting to specifically refer heat (Q) and voltage (U).
  - Information: Current (I).
- Blobs:
  - Inventory: Level (L), pressure (P) and composition (x).
  - Others: Valve opening, pump speed, etc.

These variables can take three values: (1) *std* if it is at its design or expected value; (2) *inc* if it is above its design or expected value; and (3) *dec* if it is below its design or expected value. If there is not registered value of a variable, the event is considered as a failure. Table 2 gathers the relations between HAZOP guide words and the D-higraphs deviations. Note that there are only two guide words that do not have any treatment in this paper: "OTHER THAN" and "REVERSE", which correspond to situations apart from normal operation.

3.7.2. Behavioral description: monotonic function constraint

Once the variables and their values have been settled, we can move on to the next step, the behavioral description of the system. In this step we need to connect the different variables among them. This connection tells us what happens to a variable when other changes. We will rely on Qualitative Physics to provide this feature.

According to Kuipers (1986) M^+ is a two-place predicate on reasonable functions $f, g : [a, b] \rightarrow \mathbb{R}^*$. $M^+(f, g)$ is true iff $f(t) = H[g(t)]$ for all $t \in [a, b]$, where H is a function with domain $g([a, b])$ and range $f([a, b])$, differentiable and with $H'(x) > 0$ for all x in the interior of the domain. M^- is defined similarly, except that $H'(x) < 0$.

If we consider two variables *Var*1 and *Var*2, where $M^+(Var1, Var2)$, then:

$$Var1 = inc \Rightarrow Var2 = inc \tag{1}$$

$$Var1 = std \Rightarrow Var2 = std \tag{2}$$

$$Var1 = dec \Rightarrow Var2 = dec \tag{3}$$

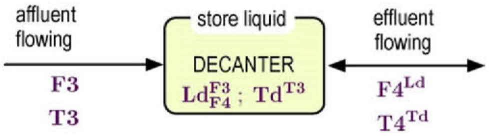

Fig. 5. Three layer D-hiagraph.

if the constraint is M^-, then:

$$Var1 = inc \Rightarrow Var2 = dec \tag{4}$$

$$Var1 = std \Rightarrow Var2 = std \tag{5}$$

$$Var1 = dec \Rightarrow Var2 = inc \tag{6}$$

Note that in the definition provided by Kuipers (1986) the relation between variables was an "iff" ($\Leftrightarrow$) and here we are using an implication ($\Rightarrow$). That is so because the relation between variables presented in the D-higraph are simplifications of the real behavior implying more than a single couple of variables.

Given a certain system, let us consider a single variable Z. It is related with other variables by M^+ and M^- constraints in the following way

$$\begin{cases} M^+(X_1, Z) & M^+(X_2, Z) & \ldots & M^+(X_n, Z) \\ M^-(Y_1, Z) & M^-(Y_2, Z) & \ldots & M^-(Y_m, Z) \end{cases} \tag{7}$$

where n is the number of M^+ constraints and m the number of M^-. Therefore, variable Z is influenced by $m+n$ variables, which are represented by $m+n$ constraints.

This representation of all of the constraints can be compressed in one single expression:

$$Z^{X_1,X_2,\ldots,X_n}_{Y_1,Y_2,\ldots,Y_m} \tag{8}$$

where Z is the variable under consideration; $X_1, X_2, \ldots, X_n$ is the set of variables related with Z by M^+; and $Y_1, Y_2, \ldots, Y_m$ is the set of variables related with Z by M^-. This notation is compact, easy to understand and keeps all the information about the constraints. Therefore, it can be included in the graphical representation provided by the D-higraph.

3.7.3. *Functional description: representation of the three layers*

At this point, we have a set of variables which are related using certain constraints (M^+ and M^-) and we need to represent them together with the functional description of the system. In Fig. 5 a simple D-higraphs is shown. It has the main features of a D-higraph in which the three layers of representation are present.

There is one device called "DECANTER" and its function is to "`store liquid`". It has two variables *Ld* and *Td* which represent its level (inventory) and its temperature. There are two edges called `affluent flowing` and `effluent flowing` that are characterized by a flow and a temperature variable each.

Note, for example, that variable *Ld* is presented as Ld^{F3}_{F4}, therefore

$$M^+(F3, Ld) \quad ; \quad M^-(F4, Ld) \tag{9}$$

which means that if *F3* increases *Ld* will also increase and if *F4* increases *Ld* will decrease. This behavior is consistent with the real behavior of the system, if the flow rate of the incoming stream to a tank increases, the level of the tank also increases. And if the flow rate of the effluent increases the level of the tank will decrease.

4. D-higraphs HAZOP assistant

Fig. 6 shows the environment where D-higraphs are developed. It also shows the reasoning system used. D-higraphs are built using a tool implemented with Microsoft Visual Basic which not only produces the visual part of the model but the internal relations between blobs and edges (Álvarez, 2010). The reasoning system is implemented using CLIPS (acronym for *C Language Integrated Production System*) which is a free software tool for building expert systems (CLIPS, 2011).

The reasoning engine uses the model generated with the model builder. The D-higraph rule database is carried out as a CLIPS rule database and it allows the reasoning engine to produce causal and consequence trees for deviations. The events that can be analyzed using this environment are failures (NONE) and deviations (MORE OF , LESS OF, PART OF and MORE THAN).

Once the model has been built, to perform the HAZOP analysis the procedure shown in Fig. 1 is followed. However, the processes represented using a double-line boundary are carried out using the D-higraph reasoning engine. Rossing et al. (2010a) provide a more detailed description of this procedure.

5. Application to a distillation pilot plant

Let us consider an industrial case: the Indirect Vapor Recompression Distillation pilot Plant (IVaRDiP), at the Department of Chemical and Biochemical Engineering at the Technical University of Denmark (DTU). The process carried out in this pilot plant is described by Li, Andersen, Gani, and Jørgensen (2006), Li, Gani, and Jørgensen (2003) and the functional decomposition of the system is provided by Rossing et al. (2010a, 2010b).

5.1. *Process description*

A simplified P&ID of IVaRDiP is shown in Fig. 7. The process consists of the following elements: column (0.45 m diameter, 19 sieve trays with 8 mm holes), condenser (total), reboiler (thermosiphoon) and a decanter or reflux drum. The reboiler and the condenser are energy-integrated through a heat pump in order to minimize energy utilization.

The heat pump fluid is routed through a throttle valve—in fact, an expansion valve—to reduce the pressure from the high pressure (P_H) to the low pressure (P_L) section. At this pressure, the fluid evaporates in the condenser and then is superheated before entering the compressors. The compressors rise up the pressure to the high pressure. At this pressure the fluid partially condenses in the reboiler and then condenses again in the secondary condenser. Note that from the heat pump fluid side the condenser works as a boiler and the reboiler as a condenser. The condensed fluid is then routed through the receiver and the superheater before getting again to the throttle valve. The secondary condenser is refrigerated by a cooling water circuit which dissipates the excess heat to the environment by a set of air coolers.

The P&ID in Fig. 7 also shows the basic control loops: condenser level, decanter level, reboiler level, high pressure and low pressure. There are additional control loops that are not shown in this paper, for more information about them the reader is encouraged to read (Li et al., 2006). There is also an internal control to maintain the heat pump fluid level in the condenser (Andersen, 1996).

The main objective of the overall system is to separate the feed stream into two pure products—distillate (D) and bottom (B)—while minimizing the energy used. In order to achieve this objective the main system can be divided in the following subsystems (with their own subgoals):

- *Column section.* Facilitate gas–liquid contact.
- *Reflux section.* Provide a reflux stream to the column and remove excess liquid as distillate (D).
- *Reboiler section.* Provide a gas stream to the column and remove excess liquid as bottom (B).

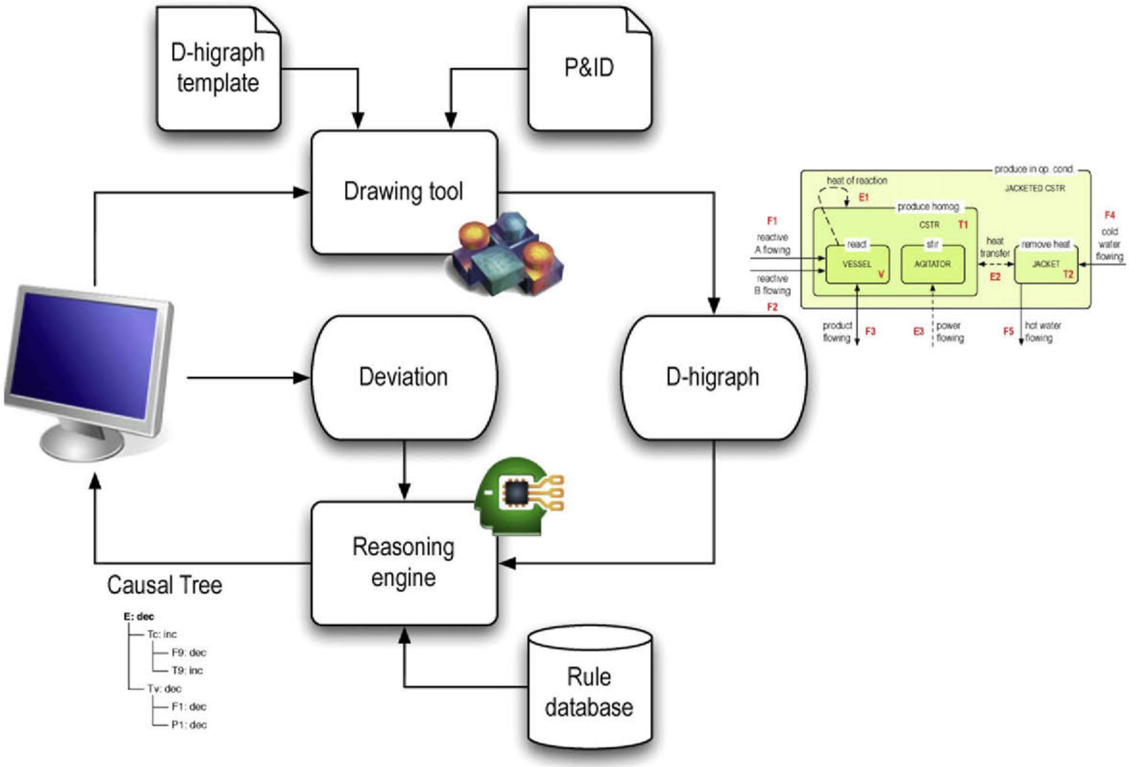

Fig. 6. D-higraphs environment.

- *Low pressure heat pump section.* Transport energy from condenser to compressors.
- *High pressure heat pump section.* Provide energy to the column.
- *Excess heat removal section.* Transport heat pump fluid excess energy to the environment.

5.2. D-higraph of the process

According to the decomposition above described and the structure of the process, the D-higraph of the system can be developed. Note that the D-higraph has been splitted into two parts (Figs. 8 and 9) in order to fit the size of the paper, however, it is a single D-higraph of the overall process.

This D-higraph presents not only the functionality of the system with its goals and subgoals, but also the relation existing between these functions/goals and the devices that perform/achieve them. The hierarchy of functions/goals is presented in terms of blobs inclusion and the dependences between them in terms of edges connecting the blobs. The D-higraph models the process elements of the system such as column, condenser, reboiler and so on but it also includes the control system elements such as control loops with their components.

It has to be remembered that the condenser works as a condenser from the column side and as a boiler from the heat pump side and that the reboiler works as a reboiler from the column side and as condenser from the heat pump side.

5.3. HAZOP studies of the IVaRDip reflux section

The overall IVaRDiP process has been divided into six parts which, for the HAZOP study, represent each of the nodes of the analysis. In this paper we are going to focus on the *reflux section* of IVaRDiP. Fig. 10 shows the D-higraph of this node, extracted from the overall D-higraph gathered in Figs. 8 and 9. Note that for this partial D-higraph we have added the variables and the relations among them. The following notation has been used: *F* flow, *T* temperature, *L* level, *P* pressure, *A* valve opening, *E* heat-energy transfer, *S* pump speed, and *I* intensity.

Taking a similar approach to that presented in Rossing et al. (2010a, 2010b) we are going to consider only two deviations: (1) the level of the decanter and (2) the energy transfer in the condenser. The variables associated to each deviations are *Ld* and *E*, respectively.

5.3.1. Low level in the decanter

If we consider low level in the decanter, i.e., $Ld = dec$, the possible causes are gathered in the causal tree in Fig. 11. These causes, directly related to their physical components, are:

- $F4 = inc$: High flow in the effluent of the decanter. Caused by:
  - $S = inc$: High speed in the pump.
- $F3 = dec$: Low flow in the affluent to the decanter. Caused by:
  - $A1 = dec$: Opening of the valve less than it should be. Caused by:
    - $I12 = dec$: Low control signal to the valve. Caused by a low measured level in the shell of the condenser ($I11 = dec$), caused by low level seen in the shell of the condenser ($I10 = dec$), caused by a low level in the shell of the condenser ($Lv = dec$), caused by distillate low flow ($F1 = dec$).
  - $F2 = dec$: Low distillate flow.
    - $Ls = dec$: Low level in the shell of the condenser.

The identified causes are directly related to physical components and devices. The conclusions obtained from this analysis are the same than a conventional HAZOP study would have drawn. This tree shows all the possible causes of this deviation—low level in the decanter—constrained to the reflux section of IVaRDiP, however, it is possible to extend the analysis to the overall process if needed.

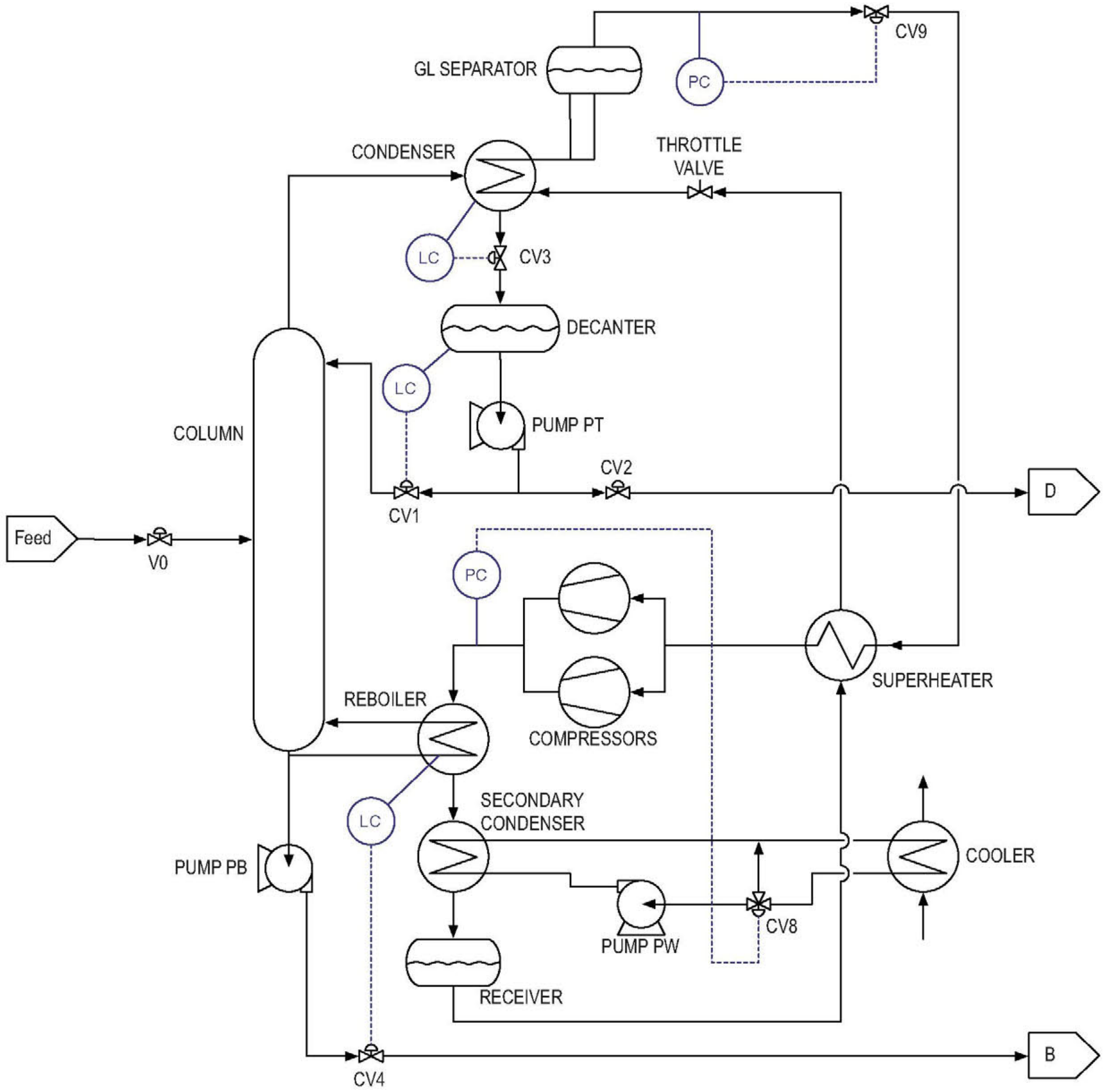

Fig. 7. Simplified P&ID of the column part and heat pump part of IVaRDiP at DTU.

5.3.2. Low energy transfer in the condenser

Another deviation considered is a low energy transfer in the condenser, that is to say, $E = dec$. The causal tree for this deviation is shown in Fig. 12. This tree, in more detail, says that the possible causes for this deviation are:

- $Tt = inc$: High temperature in the tubes of the condenser. Caused by:
  - $F9 = dec$: Cooling fluid low flow.
  - $T9 = inc$: Cooling fluid high temperature.
- $Ts = dec$: Low temperature in the shell of the condenser. Caused by:
  - $F1 = dec$: Distillate low flow.
  - $P1 = dec$: Distillate low pressure.

Again, the information provided is the same than a conventional HAZOP study would do. Of course, de depth of the analysis can be extended using the overall model of the process. This would lead to deeper and further causes for the deviation under consideration.

Note that in both deviations—low level in the decanter and low energy transfer—the causal trees obtained are quite self explanatory if they are related to the D-higraph. They do not need additional explanations because there is a direct relation between the D-higraph and the structure of the system analyzed.

6. Comparison with other methodologies

6.1. Conventional HAZOP studies

HAZOP studies are a systematic and logical approach to PHA but 70% of time and effort is devoted to the analysis of routine process deviations (Venkatasubramanian et al., 2000). Automating the process saves time, effort and therefore money. Moreover, its automation eliminates routine aspects and allows the team to focus on the failures and on their causes and consequences, which are the important aspects of the study.

The results obtained with the D-higraph HAZOP Assistant are pretty similar to a conventional HAZOP study since the D-higraphs methodology is a functional–structural approach. Every item in a D-higraph has a direct relation with an item of the process being studied.

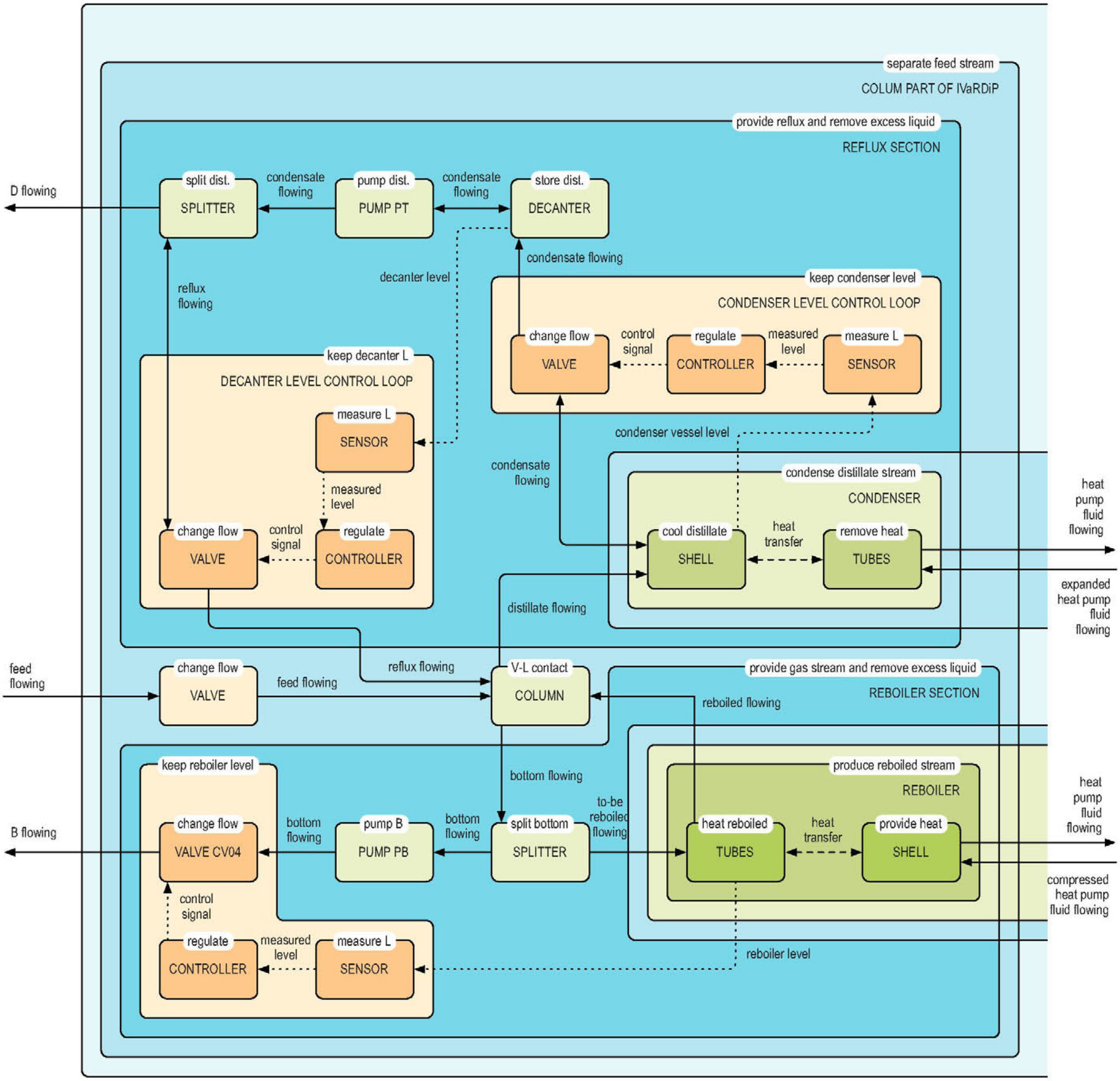

Fig. 8. D-higraph of the column part of IVaRDiP.

During the HAZOP analysis using D-higraphs, deviations are propagated in an automatic and systematic way, i.e., each node is fully explored and no branches are left unexplored. The causes and consequences trees can be extended even beyond the node itself. With all of these features the quality of the analyses is improved while reducing the time involved, if compared with conventional HAZOP studies.

6.2. *Expert systems*

6.2.1. *HAZOPExpert*

HAZOPExpert (HE) is a model-based, object-oriented, intelligent system consisting of two different knowledge base: process specific and process general knowledge (Venkatasubramanian et al., 2000). The process specific knowledge changes from plant to plant and must be updated for each process. On the other hand, the D-higraph HAZOP assistant rule base does not change. To analyze different processes the only thing that changes is the D-higraph, which is the functional–structural model of the process.

It should be noticed that in the D-higraphs approach, the D-higraph represents specific knowledge about the plant while the rule base for the causal reasoning is the general knowledge, which is common for all the analyses. However, it should be noticed that the effort that has to be put in the development of the D-higraph is significantly lower when compared with the implementation of the rule base of an expert system gathering the specific knowledge of the process.

The accuracy of the analysis using HE depends on the degree of expertise of the team developing the knowledge base. However it has been tested on a number of actual industrial processes and

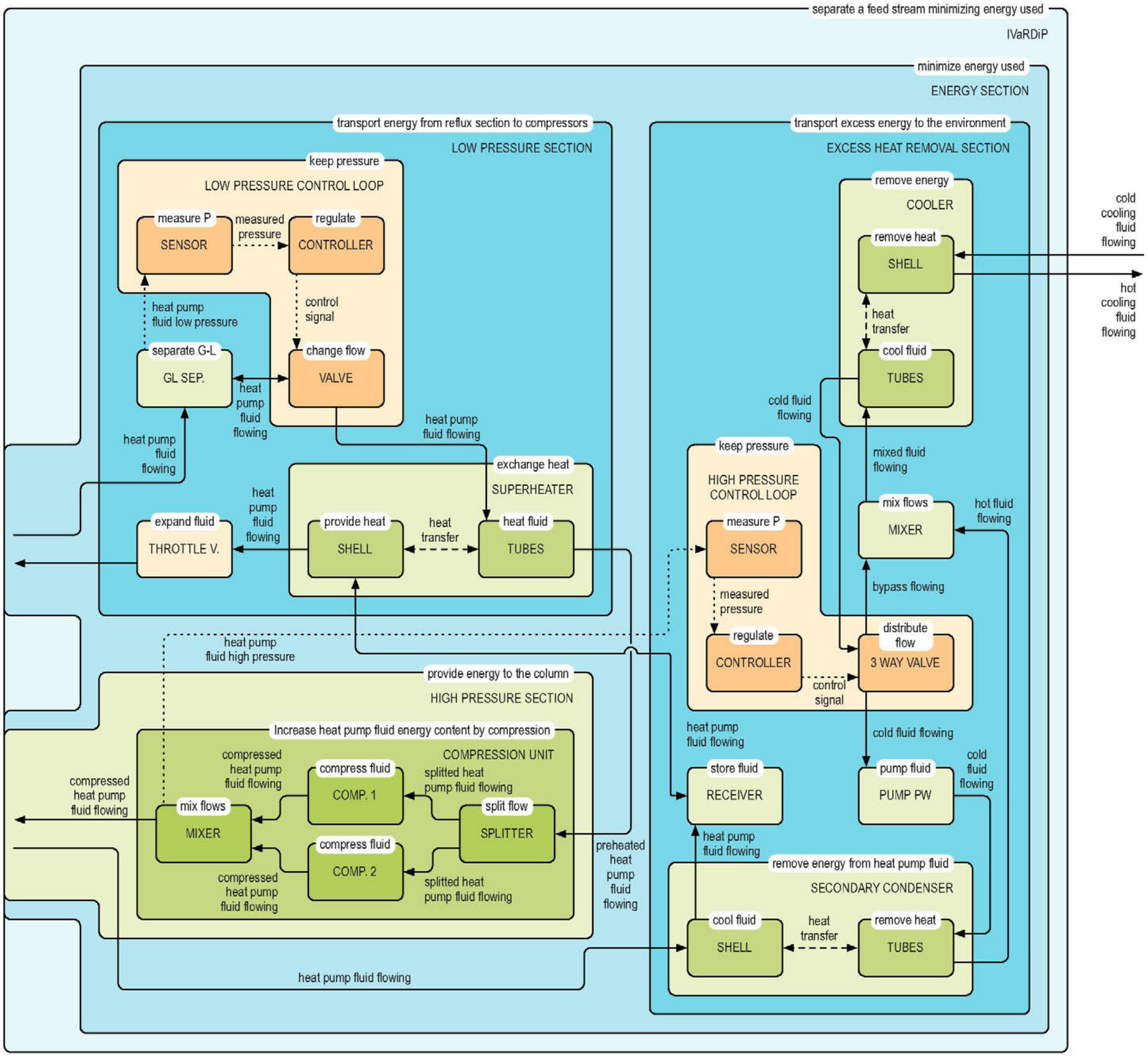

Fig. 9. D-higraph of the heat pump part of IVaRDiP.

there is also available a Batch HAZOPExpert (BHE) tool, which is based on HE and developed for batch processes.

HE and D-higraphs HAZOP assistant are similar approaches to the PHA problem—model-based, object oriented, intelligent systems—but the methodology presented in this paper incorporates an additional feature that HE does not: functional information. This functional aspects are integrated with the structure of the process under consideration; the goals and objectives of each part of the system, their hierarchy and relations are explicitly included in the model and they are linked to the HAZOP study.

6.2.2. PetroHAZOP

Zhao et al. (2009) presents a learning HAZOP expert system, called PetroHAZOP, that integrates case-based reasoning (CBR). The most important aspect of this approach is that it can “map past experiences to the new cases.” It has been applied to several cases showing that it provides valuable information.

However, it has the same problem as HAZOPExpert when compared to D-higraphs: they do not include any information about functional aspects of the plant. They are based only on structural models, where functions and goals are left behind.

6.3. Multilevel functional modeling

Rossing et al. (2010a, 2010b) present a functional HAZOP methodology based upon Multilevel Flow Models (MFM). MFM is used to represent the knowledge of the process combining means-end and whole-part dimensions (Lind, 1994). The methodology here presented is quite similar to this Functional HAZOP assistant; both use a functional modeling paradigm integrated in a workbench that allows causal reasoning.

The main difference lies in the modeling technique itself. D-higraphs integrate functional and structural information so the conclusions of the study can be directly related to the devices and

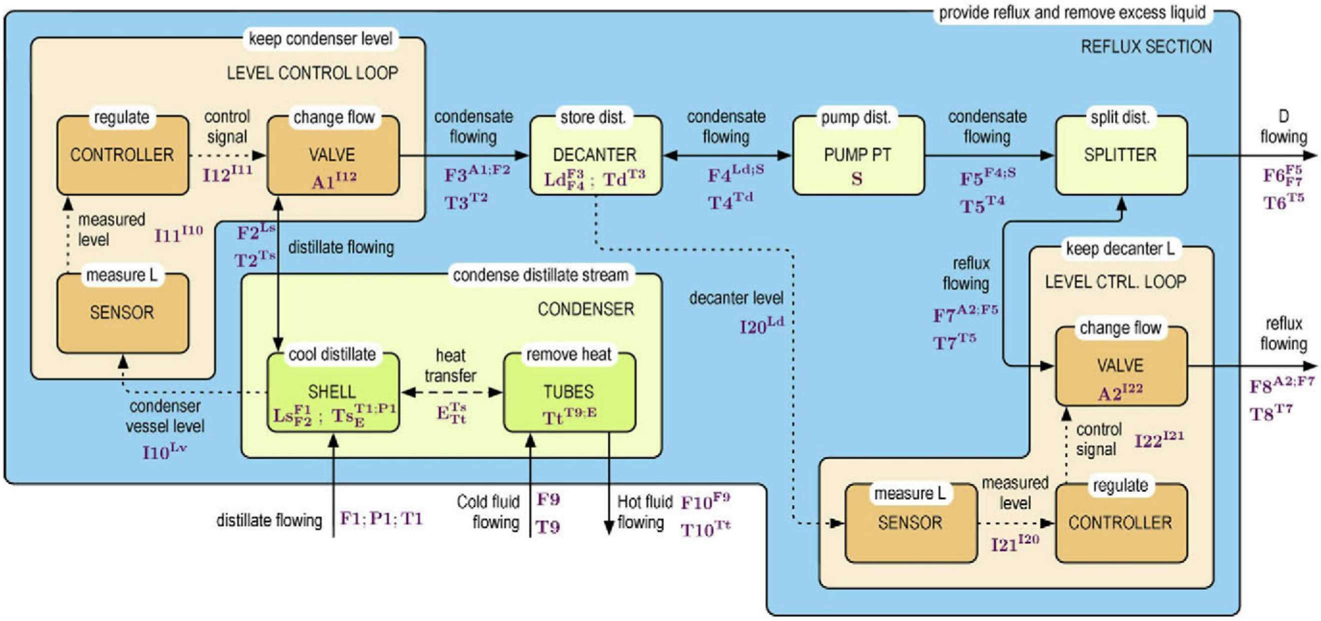

Fig. 10. D-higraph of the IVaRDiP reflux section.

equipments of the process. When using MFM an exact comparison is not possible, moreover, "*the effective use of MFM models to facilitate HAZOP meetings requires further development of the integrated computer aided design environment for MFM modeling to allow the causal trees to be mapped to the P&ID's familiar to process engineers, and rules of the reasoning engine to be extended to facilitate identification of possible consequences*" (Rossing et al., 2010a).

D-higraphs assistant conclusions are directly related to the devices and equipments that already appear in the P&ID, so this translation to "*Process Engineers Language*" is completely direct and clear.

The MFM HAZOP Assistant needs a MFM model for each node which is developed according to the node main objective. Using the D-higraph methodology, only an overall model is needed. To perform the analysis we only need to indicate the desired deep in terms of causality propagation. This issue saves even more time and enables the disturbances and deviations to propagate through the whole system (if desired). However, the other side of the story is that in MFM the modeling effort may be lower when investigating specific events or reviewing an existing HAZOP, as shown in the example in Rossing et al. (2010a).

6.4. Layered digraph model

A layered digraph model (LDM) can be seen as an extension of the HAZOP-Digraph model (Vidhyanathan & Venkatasubramanian, 1995). LDM were first presented (in English) in Cui et al. (2008) and it consists of several workspaces associated with the HAZOP guide-words. This workspaces are layered vertically and they contain nodes interconnected by unsigned directed arcs. Nodes represent process variables and a node within a workspace represent a unique deviation of the represented variable. Two nodes liked by an arc represent that one deviation can cause the other one. The links between nodes are not constrained to a single workspace, there can be arcs connecting nodes in different workspaces.

The LDG representation does not provide information about the relationships between the deviations and the functions or goals of the system while MFM or D-higraphs do. Moreover, LDG are HAZOP specific, i.e., they are only developed to perform HAZOP studies, as shown in the dependence between workspaces and the HAZOP guide-words. Other approaches, such as D-higraphs, use the model for different purposes, like fault detection or alarm managing (De la Mata & Rodríguez 2010a, 2010b).

However, in contrast to the D-higraph HAZOP assistant, the use of LDM covers all of the possible guide-words of the HAZOP study. To add a new guide-word, only a new layer has to be added and all the dependences have to be filled out. At this point it should be noticed that the D-higraph HAZOP assistant is only a tool to help the HAZOP team to perform the analysis providing the chains of causes and consequences of the deviations.

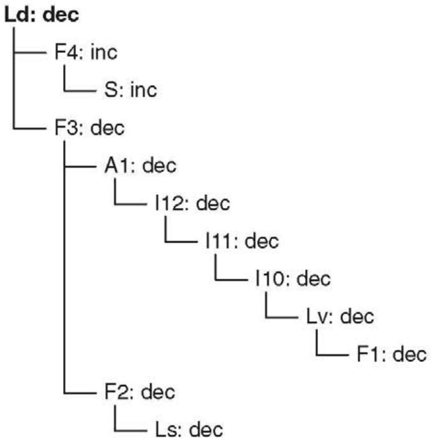

Fig. 11. Causal tree of deviation *Ld* : *dec*.

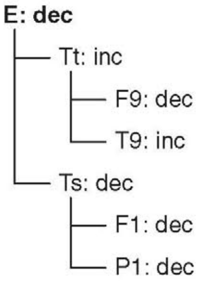

Fig. 12. Causal tree of deviation *E* : *dec*.

6.4.1. Integration with P&I diagrams

HAZOP studies should form part of the design stage of any plant. As pointed out before, the study should take place as soon as the PFD and the P&ID are ready but also before the detailed design starts (Kletz, 1999a). To facilitate this analysis the integration of the system performing the HAZOP and the tool used to implement the P&ID would be advantageous. It would save time and will always use the most recent and updated diagrams.

Cui, Zhao, and Zhang (2010) show the integration between the commercial process design package Smart Plant P&ID (SPPID) with their expert system named LDGHAZOP, which uses a layered digraph model of the process. Although this approach has the great advantage of the integration with the PFD and P&ID diagrams, has the same kind of drawbacks (and advantages) than the LDM approach, discussed previously.

The authors of the present work are currently working in the integration of the D-higraph HAZOP assistant with the simulation environment Aspen Plus. The available P&I representation of the process is translated to an Aspen Plus model. Then, this steady state model is converted to a dynamic model (Aspen Dynamics or Aspen Custom Modeler) which is the structural representation of the process (Rodríguez, De la Mata, & Alvarez, 2012).

The steady state model is automatically translated to D-higraphs model, additional information regarding the functionality of the different units is provided to the API to perform the creation of the model (Rodríguez et al., 2012). Álvarez (2010) presents a tool that allows a visual representation of the goals of the process.

7. Conclusions and further work

This study has proposed a systematic methodology to perform guided HAZOP analysis using the D-higraphs formalism. The applicability of this procedure has been demonstrated through its application to an industrial process. The realization of a guided (semi-automatic) HAZOP study implies a reduction in costs and reduces the probability of errors or unconsidered events.

The presented work has been compared with other existing approaches to this problem resulting in a more complete analysis (it considers in a natural way the control system and not only the process system) and with the advantage of integrating the functional model into the structural one (i.e. grounding functions to existing devices in the same model-diagram). A compact notation has been established which allows to understand easily looking at a single diagram not only the system functions and the components that perform them but the impact of deviations on the depicted functionality.

Further steps include the use of this very same formalism to perform online fault diagnosis and identification and the use of quantitative models to verify and disambiguate non unique possibilities of the causes-consequences explanation.

References

Álvarez, M. E. (2010). *Diagnosis de fallos en procesos químicos mediante modelos D-higraph. Final Project*. Departamento de Ingeniería Química Industrial y Medio Ambiente, Universidad Politécnica de Madrid.

Andersen, T. R. (1996). *Distillation multiplicities and product composition estimation*. M.Sc. Thesis, Department of Chemical Engineering, Technical University of Denmark.

CLIPS A tool for building expert systems (13.03.11). http://clipsrules.sourceforge.net/.

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., & Zhang, R. (2010). The integration of HAZOP expert system and piping and instrumentation diagrams. *Process Safety and Environmental Protection*, *88*(5), 327–334.

DeKleer, J., & Brown, J. S. (1984). A qualitative physics based on confluences. *Artificial Intelligence*, *24*, 7–83.

De la Mata, J. L., & Rodríguez, M. (2010). Abnormal situation diagnosis using D-higraphs. In S. Pierucci, & G. Buzzi Ferraris (Eds.), *Computer aided chemical engineering, vol. 28. 20th European symposium on computer aided process engineering* (pp. 1477–1482). Ischia, Naples (Italy): Elsevier.

De la Mata, J. L., Rodríguez, M. (2010b). D-higraphs. ASLab report, Madrid. http://www.aslab.org.

Freeman, R. A., Lee, R., & McNamara, T. P. (1992). Plan HAZOP studies with an expert system. *Chemical Engineering Progress*, *88*(8), 28–32.

Grossman, O., & Harel, D. (1997). *On the algorithms of higraphs*. Weizmann Science Press.

Harel, D. (1987). Statecharts: a visual formalism for complex systems. *Science of Computer Programming*, *8*(3), 231–274.

Harel, D. (1988). On visual formalisms. *Communications of the Association for Computing Machinery*, *3*, 514–530.

Hyatt, N. (2003). *Guidelines for Process Hazards Analysis, Hazards Identification & Risk Analysis*. Richmond Hill, Ontario: Dyadem Press.

Kletz, T. (1999a). *HAZOP and HAZAN: Identifying and assessing process industry hazards* (4th ed.). Rugby, Warwickshire: IChemE.

Kletz, T. (1999b). *What went wrong? Case histories of process plant disasters* (4th ed). Houston, TX: Elsevier Gulf Proffesional Publishing.

Kletz, T. (2001). *Learning from Accidents* (3rd ed). Oxford, Boston: Gulf Professional Publishing.

Kuipers, B. (1984). Commonsense reasoning about causality. *Artificial Intelligence*, *24*, 169–203.

Kuipers, B. (1986). Qualitative simulation. *Artificial Intelligence*, *29*, 289–338.

Li, H., Gani, R., & Jørgensen, S. B. (2003). Integration design and control for energy integrated distillation. In Andrzej Kraslawski, & Ilkka Turunen (Eds.), *Proc. of the 13th European symposium on computer aided process engineering (ESCAPE 13). Computer aided chemical engineering, vol. 14* (pp. 449–454). Elsevier B. V.

Li, H. W., Andersen, T. R., Gani, R., & Jørgensen, S. B. (2006). Operating pressure sensitivity of distillation-control structure consequences. *Industrial & Engineering Chemistry Research*, *45*(25), 8310–8318.

Lind, M. (1994). Modeling goals and functions of complex industrial plant. *Applied Artificial Intelligence*, *8*(2), 259–283.

Lind, M. (2005). Modeling goals and functions of control and safety systems—Theoretical foundations and extensions of MFM. In *Electronic report. Nordic nuclear safety research (NKS)*

Lind, M. (2010). Knowledge representation for integrated plant operation and maintenance. In *Seventh American nuclear society international topical meeting on nuclear plant instrumentation, control and human–machine interface technologies NPIC & HMIT 2010* Las Vegas, Nevada, USA.

Mackie, J. L. (1974). *The Cement of the Universe: A Study of Causation*. Oxford University Press.

Nolan, D. P. (1994). *Application of HAZOP and What-If safety reviews to the petroleum, petrochemical and chemical industries*. Park Ridge, NJ: Noyes Publications.

Rodríguez, M., & Sanz, R. (2009). Development of integrated functional–structural models. In E. N. Pistikopoulos, M. C. Georgiadis, & A. C. Kokossis (Eds.), *Computer aided chemical engineering 27. 10th international symposium on process systems engineering* (pp. 573–578). Salvador, Bahia (Brazil): Elsevier.

Rodríguez, M., De la Mata, J. L., & Alvarez, M. E. (2012). Information integration: Generating functional models from structural ones. In I. D. L. Bogle, & M. Fairweather (Eds.), *Computer aided chemical engineering 30. 22nd european symposium on computer aided process engineering* (pp. 1138–1142). London (UK): Elsevier.

Rossing, N. L., Lind, M., Jensen, N., & Jørgensen, S. B. (2010a). A functional HAZOP methodology. *Computers & Chemical Engineering*, *34*(2), 244–253.

Rossing, N. L., Lind, M., Jensen, N., & Jørgensen, S. B. (2010b). A goal based methodology for HAZOP analysis. *Nuclear Safety and Simulation*, *1*(2), 134–142.

Skelton, B. (1997). *Process safety analysis - An introduction*. UK: IChemE.

Swann, C. D., & Preston, M. L. (1995). Twenty-five years of HAZOPs. *Journal of Loss Prevention in the Process Industries*, *8*(6), 349–353.

Venkatasubramanian, V., Zhao, J., & Viswanathan, S. (2000). Intelligent systems for HAZOP analysis of complex process plants. *Computers & Chemical Engineering*, *24*(9-10), 2291–2302.

Vidhyanathan, R., & Venkatasubramanian, V. (1995). Digraph-based models for automated HAZOP analysis. *Reliability Engineering and Systems Safety*, *50*, 33–49.

Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005a). PHASuite: An automated HAZOP analysis tool for chemical processes. Part I. Knowledge engineering framework. *Process Safety and Environmental Protection*, *83*(6), 509–532.

Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005b). PHASuite: An automated hazop analysis tool for chemical processes. Part II. Implementation and case study. *Process Safety and Environmental Protection*, *83*(6), 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.