A Behaviour Model for Risk Assessment of Complex Systems Based on HAZOP and Coloured Petri Nets

Damiano Nunzio Arena[1](✉), Dimitris Kiritsis[1], and Natalia Trapani[2]

[1] École Politechnique Fédérale de Lausanne,
STI-IGM-LICP ME, Station 9, CH-1015 Lausanne, Switzerland
{damiano.arena, dimitris.kiritsis}@epfl.ch

[2] Dipartimento di Ingegneria Industriale (D.I.I.), University of Catania,
Viale Andrea Doria 6, 95125 Catania, Italy
ntrapani@dii.unict.it

Abstract. To support the knowledge of specialists during a HAZOP brainstorming session, a support system, which is able to automatically generate a preliminary HAZOP report was developed. The support system, which is based on Coloured Petri Nets (CPNs), simulates the behaviour of the system when different abnormal scenarios occur. The research demonstrates that integration of CPNs and HAZOP is very effective to obtain a smart tool for risk assessment of complex systems, improving the HAZOP analysis procedures.

Keywords: Major hazard identification · HAZOP · Coloured petri nets

1 Introduction

Today more than ever, safety in process industries represents an extremely important issue, which requires development and adoption of procedures helpful for carrying out a formal identification of hazard and risk assessment generated by the system complexity both in design phase and during operations. HAZOP (Hazard and Operability) analysis is a structured technique used to execute a systematic examination of process risks in major hazard plants. Although it is really time-consuming and requires significant human and economic resources, it is still most dependent tool for risk identification in chemical and petrochemical plants.

A brief literature review of these studies is discussed in order to set the state-of-the-art of a potential HAZOP automation.

2 Literature Review

A method, called HAZID, was the forerunner for the computer aided hazard identification [1]. McCoy set out to develop a tool for hazard identification based on fault propagation, but did not aim that this tool would necessary emulate HAZOP. McCoy obtained a more efficient tool by the creation of a computer program for hazard identification, which is a HAZOP emulator. The general approach appears similar to

S. Umeda et al. (Eds.): APMS 2015, Part I, IFIP AICT 459, pp. 573–581, 2015.
DOI: 10.1007/978-3-319-22756-6_70

HAZOPExpert [2], a system based on a strong graphical interface which allows the user to easily specify piping and instrument diagrams but it is not meant to replace the HAZOP team. Its objective is to automate the routine aspects of the analysis as much as possible, thereby allowing the team to focus on more complex aspects of the analysis that cannot be automated. An evolution of HAZOPExpert for Batch processes (BHE) was first developed by Srinivasan and Venkatasubramanian, and later improved by other researchers [3]. Thereafter, the same authors developed an automated HAZOP analysis tool for chemical processes called PHASUITE and based on Petri Nets [4].

In the past few years, researchers have concentrated on combining HAZOP with dynamic simulation [5], with Signed Directed Graph [6] or with techniques able to catch the structural aspects of process plants, such as Digraphs [7], D-higraphs [8], Case-Based Reasoning, [9], and Cause-Implication Diagrams [10, 11]. Most recent studies, on HAZOP methodology and its automation, was done by Lotero-Herranz and Galàn [12]. The use of Petri Nets, as a modelling language for batch or continuous processes, has proven to be efficient and powerful, but there is a lack in literature about the use of CPNs [13] for hazard.

3 HAZOP Methodology

Hazard and Operability (HAZOP) study is a well-known methodology for hazard identification, useful in design phase as well as in operational phase, for analysing chemical process hazards. In order to identify causes and consequences of deviations in complex systems, a multidisciplinary team of experts applies a set of guidewords to the process sections, during structured brainstorming sessions. The analysis of problems within a HAZOP study is qualitative, but integration with quantitative risk assessment methodology is well documented [14].

Although this method is very liable for hazard identification in complex systems and to support risk drive engineering in manufacturing [15], also useful for, however, the limitations of HAZOP study have been widely discussed [14], motivating academic and industrial researchers in seeking technological solutions for obtaining a more efficient application of this methodology.

Hence, the aim of this paper is to propose an HAZOP study carried out by analysing the propagation of several faults through different connected models that are based on Coloured Petri Nets (CPNs), taking advantage of the enhanced characteristics that will be discussed in the following section.

4 Coloured Petri Net Language and CPN-Based Model

Coloured Petri Nets (CPNs) is a discrete-event graphical modelling language for constructing models of concurrent systems and analysing their properties. CPNs combine the modelling advantages of Petri Nets and compactness of the high level functional programming language Standard ML. The CPN modelling language is a general-purpose modelling language, i.e., it is not aimed at modelling a specific class of systems, but is aimed towards a very broad class of systems that can be characterized as concurrent systems.

A CPN model of a system is both state and action oriented. It describes the states of the system and the events (transitions) that can cause the system to change state. By performing simulations of the CPN model, it is possible to investigate different scenarios and explore the behaviour of the system, using customizable tokens, places, transitions and functions. The formal definition of CPNs a coloured Petri net model is a nine-tuple:

$$\mathrm{CPN}\,\{\Sigma, \mathrm{P}, \mathrm{T}, \mathrm{A}, \mathrm{N}, \mathrm{C}, \mathrm{G}, \mathrm{E}, \mathrm{IN}\}$$

where Σ is a finite set of non-empty types, called colour sets, P is a finite set of places, T is a finite set of transitions, A is a finite set of arcs, N is a node function, C is a colour function, G is a guard function, E is an arc function, IN is an initialization function. Further details on CPN can be found in [12].

The potential integration between HAZOP and CPN is studied in order to extract a behavioural model of e.g. process plant the related HAZOP analysis. The paper presents an on-going research, which shows the potential of CPN and HAZOP integration to obtain a support system for HAZOP studies. In fact, a library of component and behaviour model of typical chemical plant equipment is being developed, each component will be able to be connected with others in order to easily reproduce the P&ID (Piping and Instrumentation Diagram) of the plant, like so the system processes and information flow.

The first step for system modelling is the drawing up of a list of relevant process parameters concerning each equipment type: i.e. Flow In and Out, Level (for vessels and tanks, Pressure, Temperature, Reaction (only for reactors).Then, the mental process, through which logical connection between causes of a failure and its consequences, typical of HAZOP study, needs not only a complete knowledge of all the components failure modes but a full understanding of the so-called propagation of a failure inside and outside the component. Failure is intended as a deviation from the "normal behaviour", e.g. high level within the vessel, low flow and so on. The concept of "normal behaviour" is related to the functioning of the system, and then it is not a static condition because it evolves together with the system.

Therefore, two further steps must be performed:

- The collection of all the typical causes of failure concerning each one of the modelled components;
- The creation of CPN-based mechanism, which emulate the propagation of failures.

The first of these steps can be tackled by leveraging CPN colour sets. Data related to typical accidents together with their impact on the involved process variables will be collected and represented through their proper colour sets. Then, the second one is the most challenging. The automation of the so-called "failures propagation" is crucial in order to detect causes and consequences related to all the possible failures that can occur in the system. Causes and Consequences of the process variable deviations, which are related to analysed node/section/plant, constitute the main elements of a HAZOP analysis. Therefore, in this context, we define:

- Internal Cause: An occurring fault within the component that causes a deviation on the component parameter (e.g., accidental event).
- External Cause: The propagation of a deviation from an upstream component might be the cause of a failure within the analysed one.
- Internal Consequence: Deviating process variable within a component might produce one or more internal faults.
- External Consequence: An internal deviation might propagate through downstream components. It might potentially be the external cause of a downstream deviation.

Finally, HAZOP methodology uses a set of guidewords and parameters from which it is possible to define the above-mentioned deviations by their combination (e.g. No/Less/More Flow, Less/More Pressure, Less/More Temperature, etc.). Hence, successive issues in terms of creating models that emulate the propagation of failures through an industrial plant as well as reproducing the information flow in detail is summarized in Fig. 1.

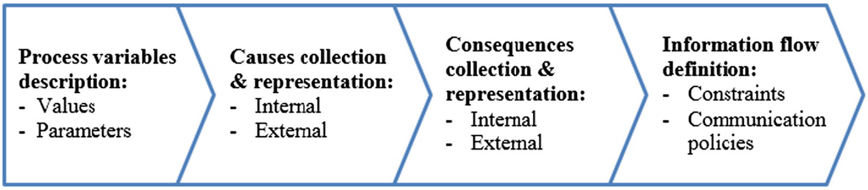

Process variables description:
- Values
- Parameters
Causes collection & representation:
- Internal
- External
Consequences collection & representation:
- Internal
- External
Information flow definition:
- Constraints
- Communication policies

Fig. 1. Sequence of issues in modelling process

4.1 Declarations

'CPN Tools' [16] constitute the modelling framework, which has been adopted in order to create behavioural models of industrial components such as a tank, a pump, a valve, etc. 'CPN Tools' is used for editing, simulating, state space and performance analysis of CPN models. Moreover, it supports untimed and timed hierarchical CPN models.

Figure 1 shows the types of data that are consumed within the model. In this context, coloured tokens and their properties seem particularly suitable to represent either Process variables or Causes, Consequences and Information Flow policies.

Thus, according to both the given definition of a Coloured Petri Net (Sect. 3) and editing framework rules, a CPN model of a component requires:

- A colour set for each kind of:
  - Process variable (VAL: Z | VL | L | N | H | VH);
  - Internal and external cause or consequence (STRING);
- A set of places that may store/contain all those information modelled by colour sets.
- A set of transitions, arcs and functions, which run and control the correct information flow.

"VAL" colour set represents all the "qualitative" values that can be reached by a process variable in the CPN model. It has been defined to represent the qualitative value that can be reached from any process variable, for instance, “Z” = Zero, “VL” = Very Low, L = Low, N = Normal, H = High, VH = Very High.

4.2 Components

The entire analysed section of the plant comprises of 4 elements such as, 2 valves, 1 vessel, and 1 pump. Each of the CPN models is made up of these primitive elements:

- Places, depicted as circles and necessary for storing information about the process variables;
- Transitions, used for running the above mentioned information;
- Arcs, connect places and transitions by driving the information flow.

Those components are consuming the above-mentioned data such as, process variable values modelled by tokens, flow policies defined by SML functions etc.

Thus, starting from previous definitions together with many available information concerning the analysed node, further issues in terms of specificity of the modelling component have been tackled during its translation into CPN model.

Figure 2 shows a snippet of the vessel model, which is made up of 5 places and 10 transitions. These are able to consume information concerning the vessel’s process variables such as, temperature, pressure, level, flow-in, and flow-out, and satisfy its working policies through guards, arc and other functions.

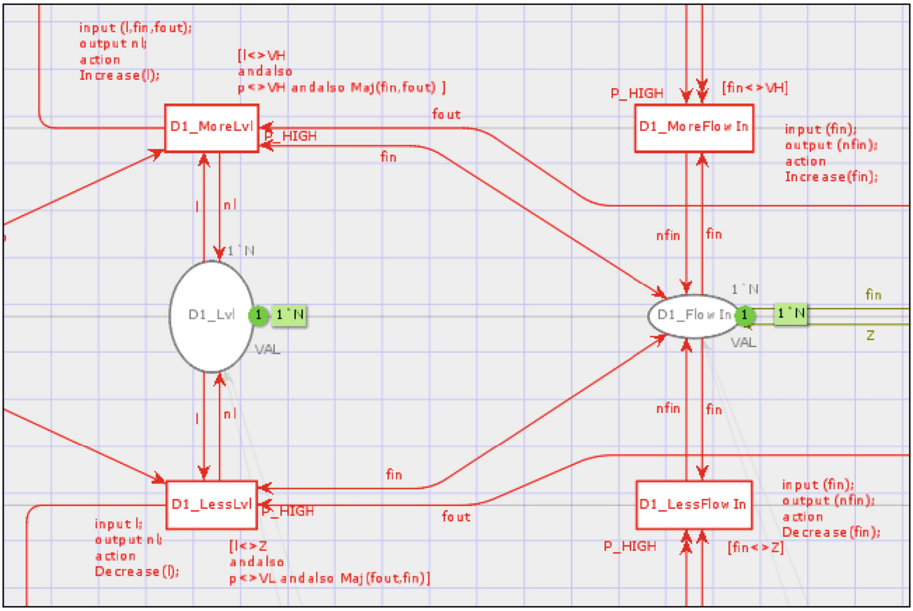
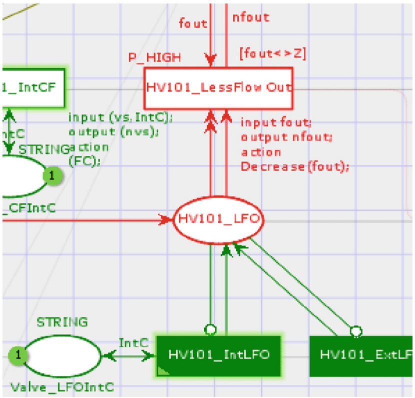


Fig. 2. CPN model – vessel (D1)

4.3 Causes and Consequences

Each grey place (see Fig. 2), which models a specific process variables, may be connected with green depicted places and transitions, which are used in order to use data related to internal and external causes (see Fig. 3). Each of those causes acts on one or more specific process variables, thus, it acts on the qualitative information modelled by a token that is stored within the relative place. During a simulation of the CPN model, the occurrence (or firing) of a green transition triggers a ripple effect, which may change the state of the involved components, according to predefined communication policies. Much of the same applies to the consequences (purple places and transitions, Fig. 4).

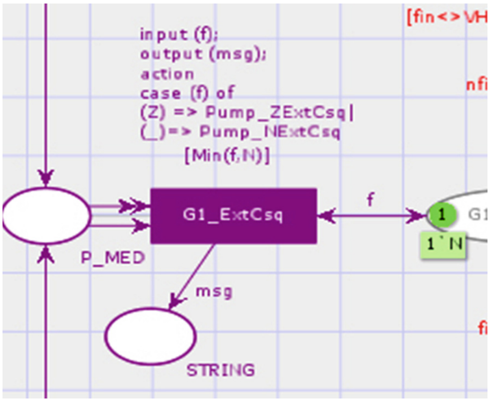
A purple transition is enabled when specific conditions are reached by the system, which leads a component to fail in a specific way. As previously mentioned, a ripple effect is triggered when the system state changes, hence, the new state that is reached from each involved component may represent the disruption cause of a linked component. More details are given in the next section.



```
input (vs, IntC);
output (nvs);
action
(FC);
```

```
input fout;
output nfout;
action
Decrease(fout);
```

Fig. 3. CPN model – valve causes



```
input (f);
output (msg);
action
case (f) of
(Z) => Pump_ZExtCsq|
(_)=> Pump_NExtCsq
    [Min(f,N)]
```

Fig. 4. CPN model – pump consequences

4.4 Information Flow

Guards, inscriptions, priority levels and other customized SML functions have been defined in order to drive the information flow within the CPN model according to policies that reflect the real behaviour of the modelled system. These elements represent the model's core, in particular, guards are necessary to set bounding conditions on transitions firing, meanwhile priority levels are there to rule the execution order. This priority level definition is made according to the following typical failure evolution mechanism I → P→T (Initiation, Propagation, and Termination). In particular, only green transitions (Sect. 4.3) may occur at the beginning because they are the only enabled ones (Initiation of the fault). Then, the propagation of a fault is due to component's features and communication policies. This stops when a final state has been reached.

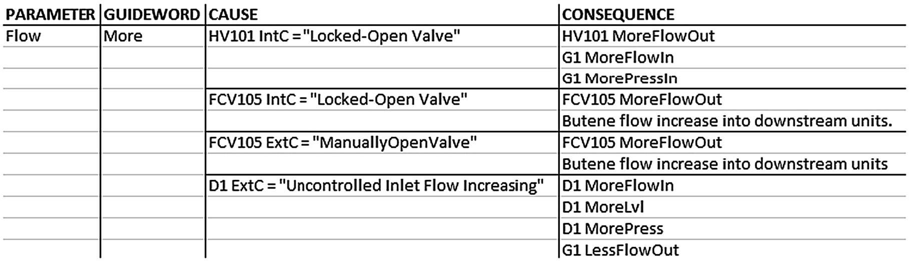
Therefore, it is possible to obtain a “behaviour forecast report” from the CPN-based system by randomly firing initiating causes and tracking the system behaviour.

5 From CPN Model to HAZOP

Once the CPN model has been developed, it is possible to extract data that will guide the HAZOP study executed by experts. Simulation of propagation of failures through the modelled system reveals interesting data about its response to those typical component failures. The term “controlled” means, it is always possible to get meaningful outputs from each firing (stop criteria have been set out not to reach meaningless states).

Therefore, CPN Tools simulation produces a “.txt” file, which exactly reports a list of all the binding elements involved during the so-called token game.

Report data should be collected even by monitoring functions or mined by external tools such as ProM [16] or CPNaaS (on-going project). However, data collected from simulation have been translated into a HAZOP like form through an Excel VBA macro ad hoc designed to manage those data. The HAZOP report is still in a raw format (Fig. 5), which includes only guidewords, causes and consequences, but further developments may include important information such as automatic control systems and safeguards.



PARAMETER	GUIDEWORD	CAUSE	CONSEQUENCE
Flow	More	HV101 IntC = "Locked-Open Valve"	HV101 MoreFlowOut
			G1 MoreFlowIn
			G1 MorePressIn
		FCV105 IntC = "Locked-Open Valve"	FCV105 MoreFlowOut
			Butene flow increase into downstream units.
		FCV105 ExtC = "ManuallyOpenValve"	FCV105 MoreFlowOut
			Butene flow increase into downstream units
		D1 ExtC = "Uncontrolled Inlet Flow Increasing"	D1 MoreFlowIn
			D1 MoreLvl
			D1 MorePress
			G1 LessFlowOut

Fig. 5. HAZOP report – “more flow” deviation

6 Discussion and Conclusions

The markings of a CPN represent the states of the modelled system. Once the analysed system has been modelled, the most linear procedure seems to be exploring all the possible states that system may be achieved (by performing a reachability analysis) and then analysing each path. However, this is a complex process in terms of time and computational effort. This could be at odds with proposed goals concerning time saving and process simplification for a HAZOP study.

Therefore, simulating a CPN model and by reading values from the generated report, it is possible to extract all the information needed to perform a HAZOP analysis of the modelled system. For the time being the simulation has been run on a small model just to analyse both feasibility and effectiveness of the results. The under development "CPN component library" may help in expanding the model easily and quickly. Lastly, the solution obtained by translating CPN Tools report data through Excel does not represent a final product but just the quickest way to get a readable one as above mentioned. However, comparing it with an "old style" HAZOP report, the "automated" HAZOP report shows almost all the risk cases together with representing an environmentally friendly and time saving way of working. This is why the use of CPNs, in order to model the behaviour of the plant through which we can obtain a HAZOP analysis, represent a possible integration between those two methodologies, moreover, it provides a very useful and smart tool both for hazard identification process and to assess operational matters which affect production dependability and resilience.

References

1. McCoy, S.A.: HAZID, a computer aid for hazard identification 1. Trans. IChemE Part B Process Saf. Environ. Prot. **77**(B6), 317–327 (1999)
2. Vaidhyanathan, R., Venkatasubramanian, V.: HAZOPExpert: an expert system for automating HAZOP analysis. Reliab. Eng. Syst. Saf. **53**(2), 185–203 (1996)
3. Venkatasubramanian, V., Zhao, J., Viswanathan, S.: Intelligent systems for HAZOP analysis of complex process plants. Comput. Chem. Eng. **24**(9–10), 2291–2302 (2000)
4. Zhao, C., Bhushan, M., Venkatasubramanian, V.: PHASUITE an automated HAZOP analysis tool for chemical processes, part I: knowledge engineering framework. Process Saf. Environ. Prot. **83**(6), 533–548 (2005)
5. Wu, J., Zhang, L., Liang, W., Hu, J.: A novel failure model for gathering system based on multilevel flow modelling and HAZOP. Process Saf. Environ. Prot. **91**(1–2), 54–60 (2013)
6. Isshiki, K., Munesawa, Y., Nakai, A., Suzuki, K.: HAZOP analysis system compliant with equipment models based on SDG. In: Ali, Moonis, Bosse, T., Hindriks, K.V., Hoogendoorn, M., Jonker, C.M., Treur, J. (eds.) IEA/AIE 2013. LNCS, vol. 7906, pp. 460–469. Springer, Heidelberg (2013)
7. Boonthum, N., Mulalee, U., Srinophakun, T.: A systematic formulation for HAZOP analysis based on structural model. Reliab. Eng. Syst. Saf. **121**, 152–163 (2014)
8. Rodriguez, M., De la Mata, J.S.: Automating HAZOP studies using D-higraphs. Comput. Chem. Eng. **45**, 102–113 (2012)
9. Cui, L., Shu, Y., Wang, Z., Zhao, J., Qiu, T., Sun, W., Wei, Z.: HASILT: an intelligent software platform for HAZOP, LOPA, SRS and SIL verification. Reliab. Eng. Syst. Saf. **108**, 56–64 (2012)
10. Nemeth, E., Cameron, I.T.: Cause-implication diagrams for process systems. their generation, utility and importance. Chem. Eng. Trans. **31**, 193–198 (2013)
11. Toth, A., Hangos, K.M., Werner-Stark, A.: A structural decomposition-based diagnosis method for dynamic process systems using HAZID information. J. Loss Prev. Process Ind. **31**, 97–104 (2014)
12. Lotero-Herranz, I., Galàn, S.: Automated HAZOP using hybrid discrete/continuous process models. Comput. Aided Chem. Eng. **32**, 991–996 (2013)
13. Jensen, K., Kristensen, L.M., Wells, L.: Coloured petri nets and CPN tools for modelling and validation of concurrent systems. Int. J. Softw. Tools Technol. Transf. **9**(3–4), 213–254 (2007)

14. Rausand, M.: Risk Assessment: Theory, Methods, and Applications. Wiley, New York (2013)
15. Trapani, N., Macchi, M., Fumagalli, L.: Risk driven engineering of prognostics and health management systems in manufacturing. In: 15th IFAC, Ottawa, 11–13 May 2015
16. CPN Tools Homepage. http://cpntools.org