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

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331033

Cause-Implication Diagrams for Process Systems: Their Generation, Utility and Importance

Erzsébet Németh, Ian T. Cameron*

School of Chemical Engineering, The University of Queensland, Queensland, Australia 4072
i.cameron@uq.edu.au

This paper presents a powerful visualization of structured process knowledge generated semi-automatically from the blended hazard identification (BLHAZID) methodology. The knowledge visualization is in the form of causal diagrams that show linked cause-failure-implication sequences generated from the structured language outcomes of the BLHAZID methodology. Causal diagrams give deep insights into what potential equipment and operational failures can occur, the failure propagation pathways and the probable timescales of propagation, as well as the extent of propagation across the system. These causal diagrams generated from the BLHAZID methodology can be used for a range of important design related and operations focused applications, and can also be used to give insights into enhancements in process systems resilience. An industrial case study shows the important ideas and outcomes.

1. Introduction

Major industrial failures still occur despite the significant innovation and investment in risk management practices over many years. Much has been done to address issues around plant, human and organizational failures. A significant challenge is the capture and reuse of process and related knowledge captured in conceptual and detailed design that can then be deployed in meaningful ways across the product and process lifecycle. A specific challenge has been the generation and reuse of knowledge in the area of hazard identification. Numerous software tools are available to document hazard identification sessions around, for example HAZOP studies as developed by IHS (2013) and Zhao et al. (2005). However, few systems allow easy reuse of the captured knowledge in a manner that can aid a range of lifecycle activities, such as real-time diagnosis, operator training systems or regulatory compliance.
The issue of knowledge generation, capture and reuse was a key focus of recent work by Seligmann et al. (2012) who developed a new blended methodology for hazard identification and causality representation. This structured, semi-automated method provided detailed causal information in a structured, reusable form for different stages of the system life-cycle. One application is a powerful, graphical representation of causality pathways, leading to cause-implications diagrams (Németh et al., 2011). These can provide further advantages to operators and for other process risk management tasks.

This paper briefly describes the BLHAZID methodology based on a functional systems framework (FSF) as developed by Seligmann et al. (2012). The concept of cause-implication diagrams with their generation from BLHAZID analysis of process systems is discussed and illustrated using a simple industrial case study.

2. Semi-automated blended hazard identification

2.1 Functional system framework

The functional systems framework (FSF) developed by Cameron et al. (2008) is a formalism that represents the way function is generated in complex processes through the interaction of plant, people and procedural components. The FSF is used as a modelling framework to describe the structure-function-goal relationships of complex systems.

Please cite this article as: Nemeth E. and Cameron I., 2013, Cause-implication diagrams for process systems: their generation, utility and importance., Chemical Engineering Transactions, 31, 193-198 DOI: 10.3303/CET1331033

The FSF has been the basis for considering hazard identification methods. The function-driven analysis investigates how the intended function of the system is lost or degraded, while the component-driven analysis considers failures in the structure, that is, the components, and seeks to ascertain the effects of these failures on the system function.

2.2 Semi-automated blended hazard identification method

The FSF has been the basis, and provides the development of the Blended Hazard Identification (BLHAZID) methodology (Seligmann et al., 2012) that uses both a component driven analysis and a function driven analysis. The BLHAZID methodology takes advantage of the blending of two fundamental approaches to hazard identification: in this case, the function-driven Hazard and Operability Study (HAZOP) is used, together with the component-driven Failure Mode and Effects Analysis (FMEA). In blending these methods, the weaknesses in the individual approaches are minimized whilst the strengths are highlighted and utilized. The workflow has 3 main steps:

i) System decomposition*:* the overall system is decomposed into subsystems, the analysis is done at the subsystem level.
ii) Functional failure analysis*:* looks for deviations from intended functions, their causes and implications.
iii) Component failure analysis*:* identifies failures in each component of a subsystem and elicits the causes and effects of these failures on the function of the system.

The knowledge associated with the BLHAZID methodology is captured and expressed in a structured language using a computer based BLHAZID tool. This knowledge can then be reused.

The original BLHAZID workflow presented by Seligmann et al. (2012) provides a systematic and highly structured step-by-step manual analysis. Based on deploying BLHAZID workflow in industrial case studies, a semi-automated version of the BLHAZID workflow was developed. A generic knowledge database is formed to store a priori knowledge, which serves as a knowledge store for static and generic information about process variable types. This includes process variables and applicable guide words, component properties, like capabilities, operation and failure modes, failure mode causes and implications. During the semi-automated BLHAZID the applicable information from the generic knowledge is presented to the analysis team for consideration. Based on the nature of the generic knowledge, available component information is static, and so from the original workflow the order of the two main steps was swapped. Now the component analysis comes before the functional analysis, and provides more coverage of component related causality information.

2.3 Extending causality information with time scale

The aim of introducing time scales in BLHAZID methodology is to provide extra information about the failure propagation rate. Qualitative time instances are defined and used to distinguish the causal time between a failure and its implication. To do this, the following qualitative time instances are defined: seconds, minutes, hours, days, months, years. This list can be extended or refined depending on the process system under analysis.

Attaching a causal time instance for each causal pair (precondition, implication) during the BLHAZID analysis gives detailed knowledge about the speed of the failure propagation. The significance of available causal time instances for each causal pair helps predict implications/consequences with time. It gives the possibility to highlight or focus on more serious events in the near future above those events of months or years duration. Causal time can provide better information to operators for decision making, strategizing and execution. It can also determine the necessity of automated systems where other forms of action are inappropriate.

3. Case study process system

As an industrial example, a mercury and arsenic hydride guard bed of a hydro-isomerisation unit in a refinery was considered. This unit is responsible for removing mercury and arsenic hydrate from an olefin feed to prevent poisoning or degradation of the downstream reactor catalyst. A BLHAZID analysis was performed according the workflow presented in Seligmann et al. (2012). The simplified P&ID of the guard bed unit with the resultant highlighted subsystem decomposition is shown Figure 1.

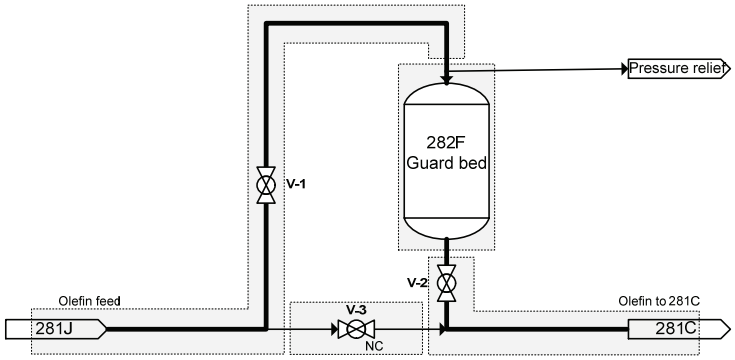

Figure 1: Simplified P&ID of the Guard bed unit with decomposition into 4 subsystems

4. Generation of cause-implication diagram

The adopted structured language facilitates capturing causal relationships during the BLHAZID workflow. As a graphical representation of the causality information, the cause-implication graph was introduced by Németh et al. (2011) to visualize it. Causal pathways can be easily generated and visualized in graph form. This has proven a particularly powerful form for process operators.

The nodes of the graph are either component or functional failures. Each edge represents a causal relationship between nodes. The edges are directed, in that the source node of an edge is one of the causes of the target node. The cause-implication diagram contains more sub-diagrams or sub-graphs, if the graph is built over multiple subsystems.

The generation of a cause-implication graph starts with a 'question' about displaying the possible root causes or alternatively, implications of a deviation in the system. In answering these sorts of questions, we start from the selected deviation and build the graph using backward reasoning for causes and forward reasoning for implications, through the appropriately stored causal triplets in the BLHAZID result. This finds the causal pathways in and through sub-systems.

In the case of causal time information determined during BLHAZID workflow, causal time data can be added as an edge weight to represent the quantitative causal time between the two failures connected by the edge. Colour and shape coding of the nodes helps highlight the important nodes requiring further consideration. House or inverted house shaped nodes correspond to the failure being questioned; internal ellipse shaped nodes are the functional failures; rectangle nodes are the component failures; diamond nodes are missing connections between subsystems or they are unfolded due to limitations around the questioning. Such a display limits sub-systems or causal time extents. Across subsystem boundaries there are ellipse shaped port connection nodes, as well as nodes representing system inputs or outputs.

4.1 Example for cause-implication diagrams

Figure 2 shows a cause-implication diagram for the possible causes of failure 'High OUTPUT concentration to 281C' in the subsystem Hg/AsH3 Free Olefin, which is denoted by the house-shape at the base of the figure. There are 4 subsystems involved, with the set of possible cause nodes having a grey fill. The arc labels indicate qualitative causal times between two failures. The graph shows 2 main ways to get a high output concentration from the system:

- Having a flow via the bypass line due to some component failure of the valve V-3, such as internal leakage, internal rupture or an operator accidently having opened/left opened or failed to close the valve.
- Getting high concentration from the guard bed, because of the component failure of the bed itself, either via by-passing or catalyst poisoning. Each failure can be traced back to functional deviation, high flow rate for the by-passing, and high impurity concentration for the catalyst poisoning which can be traced further backward until the system inputs are reached.

In this case there are 5 identifiable pathways within the system for the nominated event.

It is important to note that the failure mode causes (also called 'failure mechanism') are failures happening at the part level, such as corrosion, a welding problem or blockage of a moving part. The failure mechanism that caused a failure mode can be of many different kinds, and multiple failures need to take place at the same time to cause a system failure. It is rare that a single failure mechanism creates a hazard. In many cases, the real cause can be attributed to forms of human error during component design/specification, component production, system design, component installation, operations,

maintenance and the like. This links plant with people and procedures in the FSF. Connecting cause-implication graphs with live plant data giving the actual system state, and comparing it with the causal data helps to determine more specific possible causes via causal pathways as done in Németh et al. (2009).

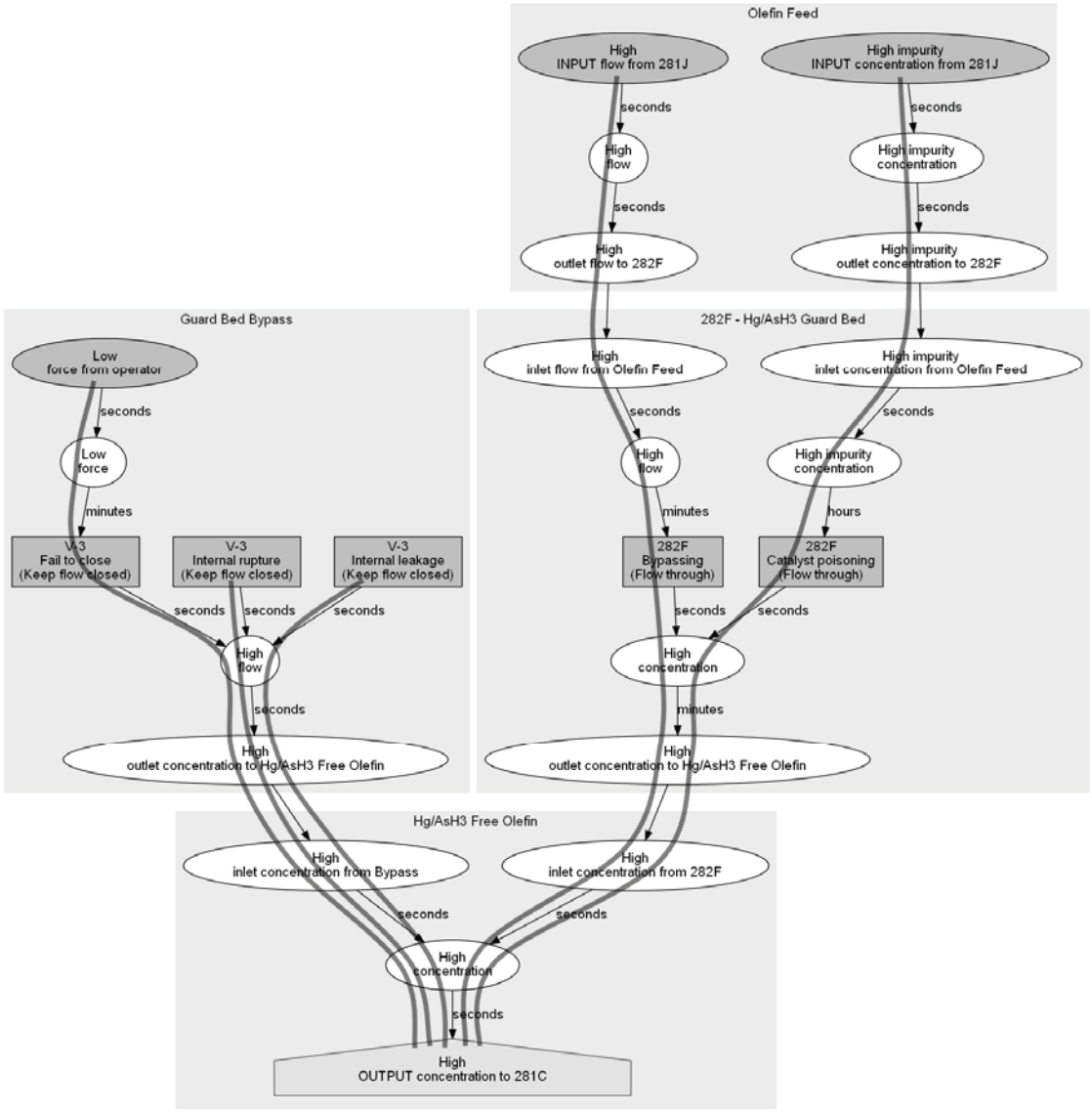

Figure 2: Cause-implication diagram for possible causes of failure "High output concentration to 281C" in subsystem Hg/AsH3 Free Olefin

A cause-implication diagram can be seen in Figure 3, where possible implications and consequences are searched from a valve component failure 'V-2 partial blockage' in the subsystem 'Hg/AsH3 Free Olefin', represented by an inverted house-shape node at the top of the figure. There are 3 subsystems present in this scenario. The significant implications, called consequences are marked during the BLHAZID analysis and highlighted. In this case, valve partial blockage creates low output flow from the system, and a high pressure situation in the guard bed and the feed line. The causal time indicates the order of magnitude of the failure propagation.

5. Utility and significance of cause-implication diagrams

There is significant application of the BLHAZID outcomes in the form of causal pathways, owing to the nature of the underlying structured language. There are many ways to reuse the result other than simply storing outcomes in spreadsheets and document folders. We summarize a number of application benefits in using the cause-implication diagrams in process system operations.

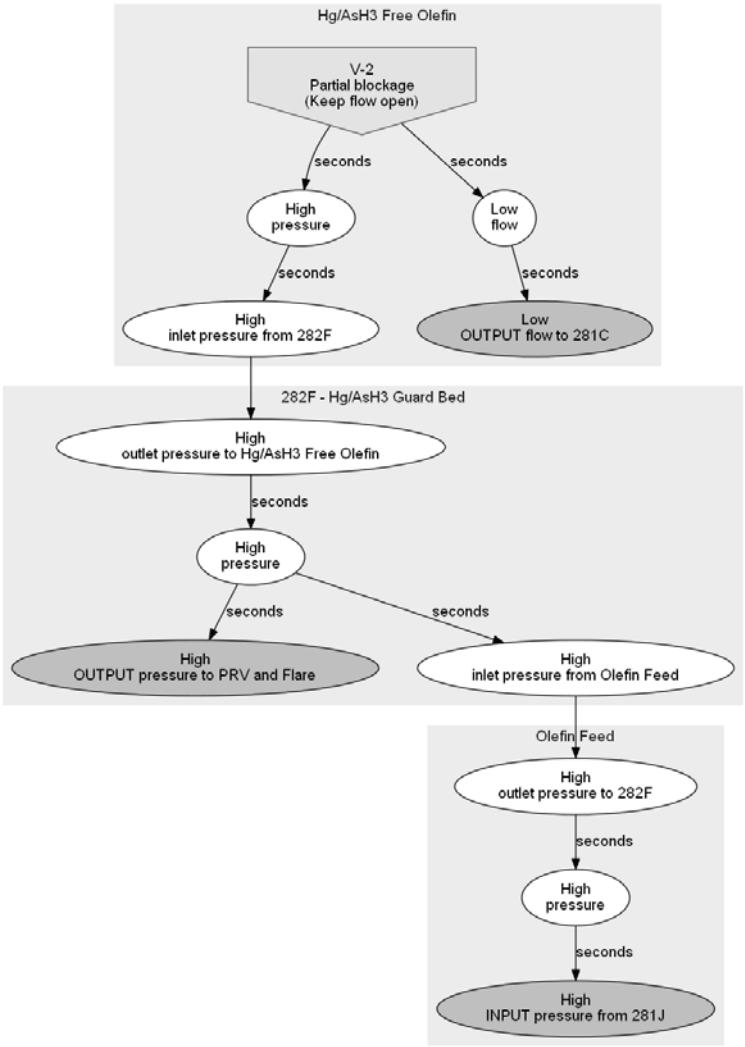

Figure 3: Cause-implication diagram for possible implications of failure "V-2 partial blockage" in subsystem Hg/AsH3 Free Olefin

Doing hazard analysis during the system life cycle is important, but is a labour-intensive task. Supporting engineers with reusable HAZID results can be seen as a great benefit.
Options for using or reusing BLHAZID generated causal data and cause-implications graphs are:

- **Consistency checking of BLHAZID result:** Applicable graph algorithms can be used to check consistency issues during or after the BLHAZID analysis, such as missing causality relationships, orphaned failures or un-analyzed failures and sub-graphs.
- **Auditing hazard identification:** Other graph results provide formal means of auditing hazard identification across the lifecycle, helping meet auditing requirements under major hazard facility regulations.
- **Supporting design decisions:** In the process design phase there are many possible realizations of the final system. Evaluating the BLHAZID analysis result of each of the possible architectures or realizations can help to make decisions about the selection or modification of the design for reliability and improvements for enhanced safety, reliability and/or resilience.
- **Operator training:** During operator training, different fault scenarios can be examined, operators can be trained using the cause-implication graphs to learn and become familiar with abnormal system conditions. The graphs provide a much deeper insight into the system behavior than simply observing input-output traces, thus building a greater fundamental understanding of the process and contributing to enhanced operational resilience.

By providing live measurement data connected to the BLHAZID causality information, this generates the following opportunities:

- **Operator decision support:** Connecting the BLHAZID result with the SCADA system, graphs can receive measurement data and provide a range of feedback to the operators about possible causes and potential near future implications, warning of potential consequences so as to inform operator decision making.
- **Online diagnostics:** Knowing the actual system state and comparing it with the causal data helps to determine the possible causes via causal pathways. More on this topic is given in Németh et al. (2009).
- **Prediction:** Having knowledge about the system behaviour merged with the BLHAZID causality result helps forecast future possible implications and could help to advise operators of actions to mitigate failures thus preventing escalation and serious hazardous events.

When historical measurement data are available, the usage of the causality data could be in the areas of:

- **Operator training:** Using historical data, operators can be trained to recognize fault situations earlier and act upon that information.
- **Offline diagnostics/failure investigation:** Accident investigation in the process industries is a crucial activity as highlighted by Kidam et al. (2010). Causal graphs can be a starting point for unravelling many of the accident sequences.

6. Conclusions

This work highlights the more powerful ways of reusing the HAZID knowledge for different purposes during the system lifecycle. Utilizing the structured language of a Blended HAZID tool it is possible to now generate a range of cause-implication diagrams that can trace specific failures through to a potential set of causes, as well as generating possible implications from that failure of interest. It is also possible to attribute causal time to causal pairs, thus providing temporal information within the graph. The questioning function can thus provide an output representation in a form that is easily interpretable by operators, engineers and managers. The cause-implication diagrams have a very wide range of applications and benefits, from design through to operations and their utility in these areas has been discussed and illustrated through a simple case study. More complex case studies have been undertaken.

Acknowledgement

The authors acknowledge support from the Australian Research Council under Linkage Grant LP0776636. We acknowledge the financial support of BlueScope Steel (BSL), Australia and BP Refinery (Bulwer Island), Australia.

References

Cameron I.T., Seligmann B.J., Hangos K.M., Németh E., Lakner R., 2008, A functional systems approach to the development of improved hazard identification for advanced diagnostic systems, In 18th European Symposium on Computer Aided Process Engineering (ESCAPE-18), on CD, paper ID FP-00463

IHS, 2013, PHA-Pro Process Hazard Analysis desktop software tool, <www.ihs.com/info/ehss/dyadem-stature-pha-pro.aspx>, accessed January 15, 2013

Kidam, K., Hurme, M., Hassim, M.H., 2010, Technical Analysis of Accident in Chemical Process Industry and Lessons Learnt, Chemical Engineering Transactions, 19, 451-456, DOI: 10.3303/CET 1019074.

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

Németh E., Seligmann B.J., Hockings K., Oakley J., O'Brien C., Hangos K.M., Cameron I.T., 2011, Generating cause-implication graphs for process systems via blended hazard identification methods, Computer Aided Chemical Engineering, 29, 1070-1074, DOI: 10.1016/B978-0-444-53711-9.50214-5

Seligmann, B.J., Németh, E., Hangos K.M., Cameron I.T., 2012, A blended hazard identification methodology to support process diagnosis, Journal of Loss Prevention in the Process Industries, 25(4), 746-759, DOI: 10.1016/j.jlp.2012.04.012

Zhao C, Bhushan M, Venkatasubramanian V., 2005, PHASuite: An automated HAZOP analysis tool for chemical processes: Part I: Knowledge engineering framework, Process Safety and Environmental Protection, 83(6), 509-532, DOI: 10.1205/psep.04055