Identifying Causality from Alarm Observations

Kirchhübel, Denis; Zhang, Xinxin; Lind, Morten; Ravn, Ole

Publication date:
2017

Document Version
Peer reviewed version

Citation (APA):
Kirchhübel, D., Zhang, X., Lind, M., & Ravn, O. (2017). *Identifying Causality from Alarm Observations*. Paper presented at International Symposium on Future Instrumentation & Control for Nuclear Power Plants, Gyeongju, Korea, Republic of.

Identifying causality from alarm observations

Denis KIRCHHÜBEL[1], Xinxin ZHANG[2], Morten LIND[3], and Ole RAVN[4]

1. Department of Electrical Engineering, Technical University of Denmark, Elektrovej, Building 326, Kgs. Lyngby, 2800, Denmark (dekir@elektro.dtu.dk)
2. Department of Electrical Engineering, Technical University of Denmark, Elektrovej, Building 326, Kgs. Lyngby, 2800, Denmark (xinz@elektro.dtu.dk)
3. Department of Electrical Engineering, Technical University of Denmark, Elektrovej, Building 326, Kgs. Lyngby, 2800, Denmark (mli@elektro.dtu.dk)
4. Department of Electrical Engineering, Technical University of Denmark, Elektrovej, Building 326, Kgs. Lyngby, 2800, Denmark (or@elektro.dtu.dk)

Abstract: The complexity of modern industrial plants poses significant challenges for the design of effective alarm systems. Rigorous alarm management is recommended to ensure that the operators get useful information from the alarm system, rather than being overloaded with irrelevant state information. Alarm management practices have been shown to significantly reduce the frequency of alarms in industrial process plants. These practices help focusing the operators' attention on actually critical situations. However, they cannot resolve the cascades of critical situations frequently occurring during emergency situations.

Multilevel flow modelling (MFM) has been proposed as a way of representing knowledge about the industrial process and infer causes and consequences of deviations throughout the system. The method enables the identification of causes and consequences of alarm situations based on an abstracted model of the mass and energy flows in the system.

The application of MFM for root cause analysis based alarm grouping has been demonstrated and can be extended to reason about the direction of causality considering the entirety of the alarms present in the system for more comprehensive decision support.

This contribution presents the foundation for combining the cause and consequence propagation of multiple observations from the system based on an MFM model. The proposed logical reasoning matches actually observed alarms to the propagation analysis in MFM to distinguish plausible causes and consequences. This extended analysis results in causal paths from likely root causes to tentative consequences, providing the operator with a comprehensive tool to not only identify but also rank the criticality of a large number of concurrent alarms in the system.

Keywords: decision support, causality, multilevel flow modelling

1 Introduction

Modern industrial plants contain a large number of interacting control loops and concurrent processes affecting the productivity and safety of the system.

While control practices for individual components and constrained processes are widely adapted in industry, plant-wide control often faces too many uncertainties from the environment and the interconnected processes to be economically feasible [1]. Human operators who rely on alarm systems to supervise the plant operation thus control the vast majority of plants in the energy, petrochemical and chemical industries. Due to the large risks for humans as well as the environment in case of failures, rigorous alarm management is recommended for these industries to avoid overloading the operators [2].

Alarm management practices have been shown to significantly reduce the amount of irrelevant alarms presented to the operator by thoroughly scrutinizing the necessity and importance of the most frequent alarms and where possible combining and removing redundant alarms [3].

A well maintained alarm system can avoid operator overload during normal operation. However, emergencies frequently generate cascades of true critical situations throughout the plant that overwhelm the operator with so called alarm floods. To cope with such situations the relation of those alarms needs to be examined and compiled into concise information to aid the operator in identifying the most relevant and immediate threats. [4]

To identify relevant information during alarm floods the causality relation of the occurring alarms is a key information. While the analysis of historian data on the alarms gives insight in common correlation between alarm occurrences, inference of causality requires incorporating process knowledge. [5]

Multilevel Flow Modelling (MFM) provides an abstract representation of an industrial process as a decomposition of connected mass and energy flows [6]. MFM methodology has been proposed as a versatile process representation to analyze causal patterns in a plant [7]. Inoue et al. [8] propose to use MFM for counter action planning in unknown emergency situations. Larsson and DeBor [9] and more recently Wang et al. [10] have demonstrated the application of MFM for root cause identification and alarm reduction based on identified root causes. The combination of dynamic alarm reduction and a system to propose feasible counter-actions would enable operators to react efficiently to any situation in the plant.

As a starting point toward this comprehensive operator support system the extension of the method for root cause identification is described here. The identification of root causes as well as propagation paths based on the causality between observed alarms is discussed in this contribution.

The following sections introduce the MFM methodology and the propagation reasoning based on MFM models. Based on that the proposed method for combination is outlined and conclusions for future work are drawn.

2 Multilevel Flow Modelling

Multilevel Flow Modelling (MFM) represents the goals and functions of a system by decomposing the mass and energy flows as means and ends of operating the system.

Each flow component along the means-end dimension is described by basic flow functions. By the combination of means-end decomposition of the overall operation and part-whole perspective of individual flows the function of the system is analyzed and can be represented as a graphical model using the MFM concepts shown in Fig. 1. As example the MFM model of a watermill is considered, adapted from Lind [11] and shown in Fig. 2.

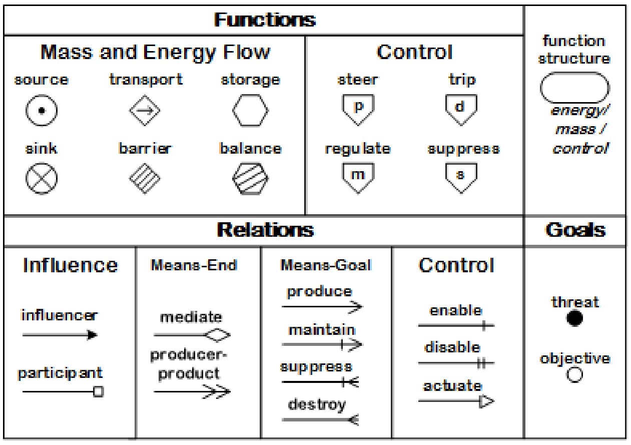

Fig. 1 MFM concepts used for modelling.

The model shows the main objective of grinding grain as *obj1*, which is achieved by the mass flow of grain in *mfs1*. The grains fed into the mill are converted to flour and split-up bran. Energy flow *efs1* reflects the conversion of the energy from the water by the gears and mill stone to energy used for grinding and energy losses not used in the system. This energy in turn is supported by the mass flow of water into the flume across the water wheel represented by *mfs2*. In this way the interacting functions throughout the system are described for the nominal operation.

Industrial plants, however, often have a multitude of different operational situations by design. Each of these operational modes is defined by different nominal functions in the system and thus requires an adaptation of the model [12]. As described by Inoue et al. [8] adapting the model also facilitates the investigation of alternative behaviors of the plant.

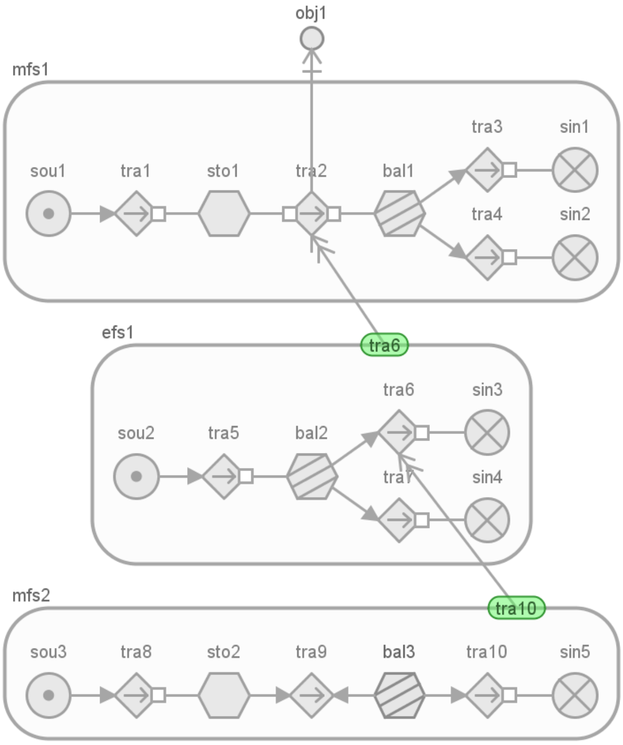

Fig. 3 MFM model of a watermill as described by Lind [11]

3 Prognostic and Diagnostic Reasoning

Based on the MFM modelling primitives the propagation of failures through the system can be analyzed. Combinations of propagated states and patterns in the model describe the failure propagation in the system. Zhang [13] describes the most recent version of these propagation rules.

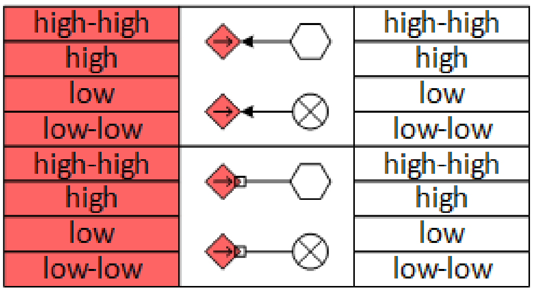

Fig. 2 Downstream consequence propagation of faults on a transport function [13]

The rules are defined for both, plausible causes and consequences of an observed state. The example in Fig. 3 shows how a failure associated with a transport function has consequences on connected functions downstream of that transport. Applying all propagation rules to an observed failure, a fault tree of failures in the model can be generated. The resulting tree generally reflects alternative propagation paths at the same level. The alternative paths are not necessarily but frequently mutually exclusive.

In conjunction with a set of truth-maintenance rules the possible propagation paths of each observation present in the system can be dynamically generated. This way changes to the observations as well as the considered configuration of the plant are taken into account at any given moment. The resulting causal paths are limited to plausible scenarios connected to specific observations, whereas a generic fault model as used by Wang et al. [10] comprises a comprehensive causal representation of all possible states. While the computational burden of this dynamic approach is higher than a precompiled causal graph, it yields more flexibility to accommodate changes of the system behavior.

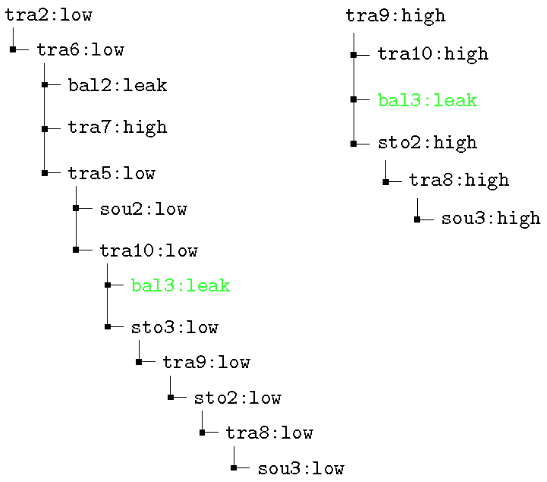

Fig. 4 Cause analysis of two faults in the water mill, common cause *bal3:leak* is highlighted

The propagation analysis for causes of two different faults is illustrated in Fig. 4. Each subordinate level in the tree structure reflects plausible causes for the immediate parent.

The fault *tra2:low* equals to a low processing throughput of the mill, meaning that no grain is being milled. The other fault *tra9:high* corresponds to a too high flow of water from the flume over the waterwheel. The comparison of the two consequence trees reveals, that neither of the two observed alarms can be the cause for the other. In fact, if the low throughput were caused by a fault of the water flow it would be the opposite – low flow instead of a high flow as observed.

In addition, a later observation of the flume level being high – *sto2:high* – is considered (Fig. 5). This observation may well be a direct cause for the high flow

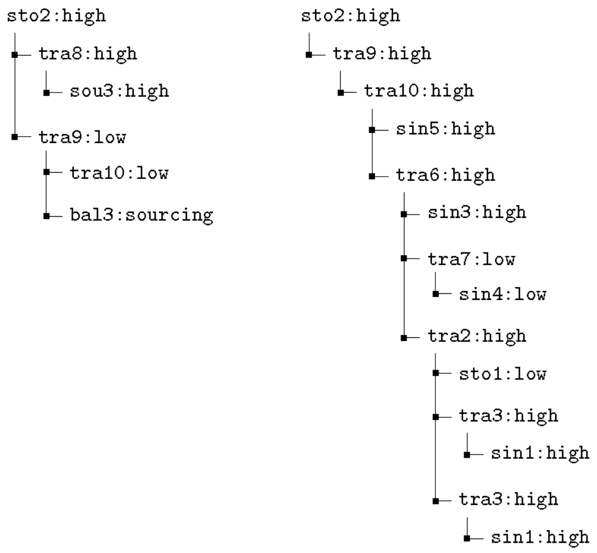

Fig. 6 Cause and consequence analysis for observation of high flume level

of water from the flume. If it were the only fault in the system, however, it could not explain why the production of the water mill is low in the considered situation. Hence, a combined analysis of the possible causes and consequences is necessary.

4 Combining Multiple Alarms

By comparing the cause tree representation for the first two considered failures in Fig. 4 the common cause *bal3:leak* can be manually inferred. For a more complex system and a larger number of simultaneous observations, however, the proper inference becomes significantly more complex. This raises the need for a general and structured solution for reliable identification of the best explanation.

Considering the combination of all suggested causes and consequences as a directed causal graph grants a better overview of the whole situation. Furthermore, a directed graph can be systematically analyzed by applying graph theory.

The example of *tra2:low* and *tra9:high* results in the graph shown in Fig. 6. All edges are directed from cause to consequence. The green nodes represent the states that are supported by observations. The results generated from *tra2:low* are shown in blue and the results based on the observation *tra9:high* are shown in black.

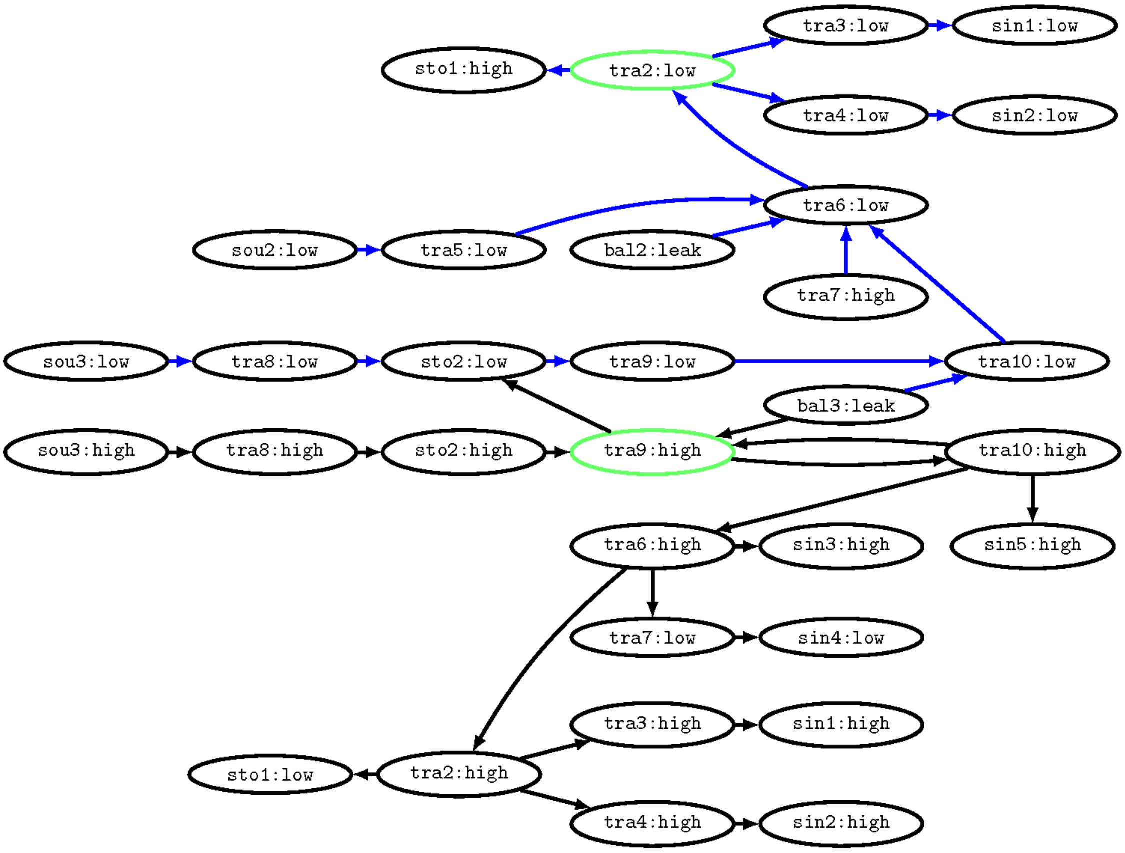

Fig. 5 Graph combining the causes and consequences suggested for two faults in the water mill. The graph is directed from cause to consequence.

tra2:low and *tra2:high* both cause that the main objective of the water mill would fail, i.e. *obj1:false*. This relation is ommited here for readability.

Finding the root cause in this graph is a matter of finding a minimal tree, which includes as many of the observations as possible while obeying the directivity of the graph.

The tree rooted in *bal3:leak* thus yields the best explanation for the given observations. In terms of the physical system this can be interpreted as the water spilling over the water wheel instead of being transported by the buckets of the water wheel. This could for instance be caused by the water wheel being broken or bypassed.

Each causal tree that can be identified by this analysis can be extended to also cover the consequence scenarios for the current situation. Considering a tree *T* whose leaves are the observations *o(T)*, the tree can be extended by the consequences of each of these observations, so long as a consequence does not refer to a function that is already considered by any vertex in *T* or any observation from the system.

Applying this method to the example results in the tree shown in Fig. 6. The states in grey are the relevant consequences beyond the observed states.

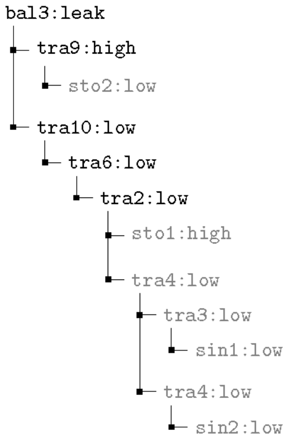

Fig. 7 Consequence tree derived from the first observed scenario

The combined graph can be efficiently updated with new connected observations. Considering *sto2:high*, the complete cause and consequence analysis is already present in the graph and no new inference is necessary. As there exists no causal tree that also includes the new observation, the high flume level has to be an independent contribution to the high flow from the flume.

The diagnosed causes would hence be a high inflow to the flume (*sou3:high* or *tra8:high)* as well as the spill of water represented by *bal3:leak.* The consequences will no longer include a low level in the flume (*sto2:low*) as the flume level has been identified as a likely cause for the situation. This shows, that the combined analysis of fault propagation from the observations yields a clear distinction of the causality between connected functions in the system.

5 Conclusion

This contribution outlined a generic method for situation analysis and distinction of causality based on MFM reasoning and graph interpretation.

In the context of alarm management for a complex plant the underlying framework as well as the models have to be adaptive for many different configurations in the plant.

The method proposed here takes in dynamic reasoning results based on an MFM model and has the potential to reliably distinguish the direction of causality as well as identifying the most plausible root causes and tentative consequences of any given scenario.

This method is currently being implemented in a real-time environment of a pilot-scale oil and gas production plant. Further investigation will be dedicated to the efficiency of the method and the integration of selective advanced signal processing for prognostic analysis of scenarios and fast distinction of situations.

Acknowledgement

The authors would like to acknowledge the support of the Danish Hydrocarbon Research and Technology Center (DHRTC) at the Technical University of Denmark as well as the fruitful cooperation with Eldor Technology, Norway.

References

[1] G. P. Rangaiah and V. Kariwala, *Plantwide Control : Recent Developments and Applications*. Wiley, 2012.

[2] Engineering Equipment Materials Users' Association, "Alarm systems – A guide to design, management and procurement," London, 2013.

[3] D. H. Rothenberg, *Alarm Management for Process Control: A Best-practice Guide for Design*. New York: Momentum Press, 2009.

[4] D. Beebe, S. Ferrer, and D. Logerot, "The

Connection of peak alarm rates to plant incidents and what you can do to minimize," *Process Saf. Prog.*, vol. 32, no. 1, pp. 72–77, Mar. 2013.

[5] J. Wang, F. Yang, T. Chen, and S. L. Shah, "An Overview of Industrial Alarm Systems: Main Causes for Alarm Overloading, Research Status, and Open Problems," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 2, pp. 1045–1061, Apr. 2016.

[6] M. Lind, "An overview of multilevel flow modeling," *Nucl. Saf. Simul.*, vol. 4, no. 3, pp. 186–191, Sep. 2013.

[7] T. Us, J. Niels, L. Morten, and J. Sten Bay, "Fundamental Principles of Alarm Design," *Int. J. Nucl. Saf. Simul. Nucl. Saf. Simul.*, vol. 2, no. 1, pp. 44–51, 2011.

[8] T. Inoue and A. Gofuku, "A technique to prioritize plausible counter operation procedures in an accidental situation of plants," *Nucl. Saf. Simul.*, vol. 7, no. 2, 2016.

[9] J. E. Larsson and J. DeBor, "Real-time root cause analysis for complex technical systems," *2007 IEEE 8th Hum. Factors Power Plants HPRCT 13th Annu. Meet.*, pp. 156–163, 2007.

[10] W. Wang, M. Yang, and H. Seong, "Development of a rule-based diagnostic platform on an object-oriented expert system shell," *Ann. Nucl. Energy*, vol. 88, pp. 252–264, 2016.

[11] M. Lind, "An Introduction to multilevel flow modeling," *Nucl. Saf. Simul.*, vol. 2, no. 1, pp. 22–32, 2011.

[12] D. Kirchhübel, M. Lind, and O. Ravn, "Representing Operational Modes for Situation Awareness," *J. Phys. Conf. Ser.*, vol. 783, no. 1, 2017.

[13] X. Zhang, "Assessing Operational Situations," Technical University of Denmark, 2015.