Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P537-cd

From Fault Trees to Piping and Instrumentation Diagrams

Wouter Bos, Matthias Volk, Mariëlle Stoelinga
University of Twente, The Netherlands. E-mail: m.volk@utwente.nl

Marc Bouissou
Électricité de France, France

Pavel Krčál
RiskSpectrum AB, Sweden

Piping and Instrumentation Diagrams (P&IDs) are a graphical representation of the design of industrial plants. While images of P&IDs for a given system exist, a formal representation of a P&ID containing safety-relevant information is often missing. Such a formal P&ID model (1) provides a high-level representation of the system including its safety and reliability properties which is easier to understand for non-experts, and (2) enables automatic generation of fault trees by tools like RISKSPECTRUM MODELBUILDER, which allows for systematic updates of the safety model after system modifications.
In this work, we aim to automatically infer a formal representation of (the safety-relevant part of) a P&ID from a given a set of fault trees. Fault trees (FTs) are manually created from P&IDs and capture the safety-relevant part of the system. We present an automatic translation from FTs to P&IDs. The transformation starts by creating the P&ID components from the labels of basic events in the FTs. In a second step, the topology of the P&ID – including the pipe connections – is inferred from the structure of the FTs and their minimal cut sets.

Keywords: Piping and Instrumentation Diagrams, Fault Trees, Automatic translation, Safety analysis, Formalisation

1. Introduction

Piping and Instrumentation Diagrams (P&IDs) are a graphical representation of the design of industrial plants Toghraei (2019), for instance nuclear power plants. P&IDs describe, among other things, the mechanical components, the process control instrumentation and the process piping. For a safety assessment of a plant, P&IDs serve as one of the inputs and a starting point.

When performing a probabilistic safety assessment (PSA), P&IDs are often translated into fault trees. *Fault trees (FTs)* are a graphical model that provides a comprehensive understanding of risks and mitigation strategies in the modelled system Ruijters and Stoelinga (2015). Typically, reliability experts create and update FTs manually. The link between the system description and the safety model stays in the expertise of safety analysts. Interpreting reliability results or updating FTs after a design change depends fully on their knowledge.

An alternative to this manual process is the automatic generation of FTs from a formal representation of a P&ID Renault et al. (1999), as supported by tools such as RISKSPECTRUM MODELBUILDER or KB3 Bouissou (2005). This approach maintains the connection between the system description and the safety analysis.

However, in most cases, a formal P&ID model does not exist because FTs were created manually. In these cases, we still want to obtain a *formal P&ID model*, because (1) it is easier to communicate results of the safety assessment to non-specialists, and (2) automatic generation of FTs from possibly updated formal P&ID models helps to keep FTs consistent with the system description after modifications.

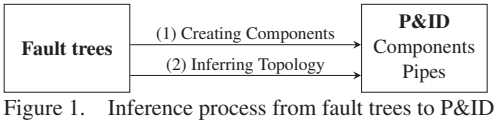

Figure 1. Inference process from fault trees to P&ID

We present a method (see Fig. 1) to infer the safety-relevant part of P&IDs from manually built FTs, given definitions of P&ID components with their reliability information in a Knowledge Base in RISKSPECTRUM MODELBUILDER. While existing approaches commonly use image recognition to infer formal P&ID models from existing P&ID images Arroyo et al. (2016), these pictures do not contain all safety-relevant information – whereas the FTs we use as input do.

2. Fault tree to P&ID

Formalising P&IDs We formalise P&IDs based on Bayer and Sinha (2020) as a graph $D{=}(C, P)$. The vertices C represent P&ID *components* associated with a label and type. The edges P represent *pipes* (with an optional label) connecting two components. The example P&ID in Fig. 3 depicts parts of a Residual Heat Removal System (RHS).

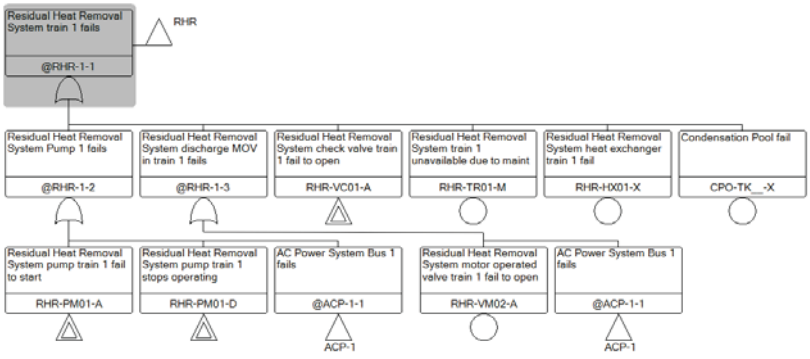

Figure 2. FT modelling RHS train 1 failure

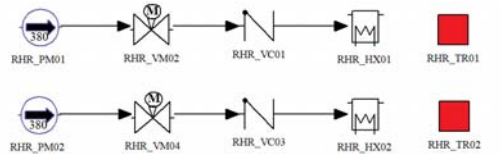

Figure 3. P&ID of a Residual Heat Remove System (RHS). Each redundant part consists of a pump, an RHS-specific valve, a check valve, a heat exchanger and an event representing a failure due to maintenance.

Approach We infer P&IDs from FTs as outlined in Fig. 1. The approach takes as input FTs in .rsa files from RISKSPECTRUM PSA. We create a P&ID from these FTs by (1) creating the P&ID components from the basic events in the FTs, and (2) inferring the pipe connections from the FT structures. The resulting P&ID is exported into .kbi files for import by RISKSPECTRUM MODELBUILDER. We show the translation by example of the RHS, using the FT in Fig. 2 as input.

Creating P&ID components From the FTs, we first create the P&ID components, i.e., vertices C in the graph. As basic events in the FT represent failures in system components, we can deduce the component names (and their types) from the labels of the basic events. Here, we exploit a systematic naming schema in the FTs present in large studies – especially in nuclear power plant PSAs.

From the basic event labels in the FT in Fig. 2, we identify five component labels RHR-PM01, RHR-VM02, RHR-VC01, RHR-HX01, RHR-TR01. We obtain the type of component from the labels based on the two characters after the dash.

Inferring P&ID topology We infer the topology of the P&ID – particularly the pipe connections P – based on the structure of the FTs and their minimal cut sets. For instance, basic events in the same cut set indicate that the corresponding components belong to trains in parallel. Note that the FTs alone might not suffice to fully infer the P&ID topology, e.g., the order of components in series. Post-processing can be employed using domain-specific knowledge or manual expert intervention.

Continuing the example, the pipe connections between the P&ID components are inferred, resulting in the P&ID in Fig. 3. Components within one train of RHS are connected by an OR-gate. Failure of any of them will fail the whole train. Thus, these components are in series. Their order in the P&ID can follow the order of the basic events in the FT, it can be determined by additional domain knowledge, or is manually edited by an expert. The two trains of RHS are connected by an AND-gate. Thus, both trains are in parallel.

3. Conclusion

We presented an automatic translation from FTs to formal P&ID models. The approach is implemented in a prototypical Python tool and creates P&IDs for import in RISKSPECTRUM MODELBUILDER. We will validate our approach on several P&IDs from industrial case studies.

Acknowledgement

This work has been partially funded by the NWO grant NWA.1160.18.238 (PrimaVera), the ERC Consolidator Grant 864075 (*CAESAR*) and by EU Horizon 2020 project MISSION, number 101008233.

References

Arroyo, E., M. Hoernicke, P. R. Carrion, and A. Fay (2016). Automatic derivation of qualitative plant simulation models from legacy piping and instrumentation diagrams. *Comput. Chem. Eng. 92*, 112–132.

Bayer, J. and A. Sinha (2020). Graph-based manipulation rules for piping and instrumentation diagrams.

Bouissou, M. (2005). Automated dependability analysis of complex systems with the KB3 workbench: the experience of EDF R&D. In *Proc. of ICEE*.

Renault, I., M. Pilliere, N. Villatte, and P. Mouttapa (1999). KB3: computer program for automatic generation of fault trees. In *RAMS*, pp. 389–395.

Ruijters, E. and M. Stoelinga (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Comput. Sci. Rev. 15*, 29–62.

Toghraei, M. (2019). *Piping and Instrumentation Diagram Development*. John Wiley & Sons.