



Concept for Alarm Flood Reduction with Bayesian Networks by Identifying the Root Cause

Paul Wunderlich and Oliver Niggemann

Ostwestfalen-Lippe University of Applied Sciences, Institute Industrial IT,
Langenbruch 6, 32657 Lemgo, Germany
{paul.wunderlich,oliver.niggemann}@hs-owl.de
<http://www.init-owl.de>

Abstract. In view of the increasing amount of information in the form of alarms, messages or also acoustic signals, the operators of systems are exposed to more workload and stress than ever before. We develop a concept for the reduction of alarm floods in industrial plants, in order to prevent the operators from being overwhelmed by this flood of information. The concept is based on two phases. On the one hand, a learning phase in which a causal model is learned and on the other hand an operating phase in which, with the help of the causal model, the root cause of the alarm sequence is diagnosed. For the causal model, a Bayesian network is used which maps the interrelations between the alarms. Based on this causal model the root cause of an alarm flood can be determined using inference. This not only helps the operator at work, but also increases the safety and speed of the repair. Additionally it saves money and reduces outage time. We implement, describe and evaluate the approach using a demonstrator of a manufacturing plant in the SmartFactoryOWL.

1 Introduction

The next industrial revolution (digital transformation) not only affects society but also the working world. In the future, a few plant operators will have to operate highly automated and complex plants. Especially, the vision of complete networking of all components and parts of a plant (IoT) leads to overloaded operators due to the enormous load of information. This is particularly critical in the area of the alarm management of plants and machines, since none, too late or incorrect intervention can result in high material damage or even personal injury. As a result of the increasing automation, additional sensors are increasingly installed because of their allegedly very good ratio of security per cost. However, this results in an enormous number of warnings and alarms, which overexert the operator [15]. Such situations are called alarm floods. As an effect of this, the operator is only able to acknowledge most of the alarms, but cannot process the information that they provide. This may cause dramatic effects especially at high hazard facilities like in the process industry and reduces the overall value of an alarm system (see Example: Refinery Explosion).

The Author(s) 2018

O. Niggemann and P. Schüller (Eds.), *IMPROVE – Innovative Modelling Approaches for Production Systems to Raise Validatable Efficiency*, Technologien für die intelligente Automation 8, https://doi.org/10.1007/978-3-662-57805-6_7

An alarm flood corresponds to a time interval in which the number of alarms is higher than the reactivity of an operator. There exist different reasons for an alarm flood. Most common is a badly designed alarm management system. Based on [21, 24, 28] typical distinctive features of an inefficiently designed alarm management are: missing alarm philosophy, irrelevant alarms, chattering or nuisance alarms, incorrectly configured alarm variables, alarm design isolated from related variables, permanent alarms in normal state, alarms and warnings at the same time, missing option to remove remedied alarms and too many priorities.

Therefore an effective alarm management for factories is of huge interest and current research topic. Regardless of very good alarm management, the weaknesses of humans are that they are not able to perform 100 percent consistently well all the time. For example, if operators are tired, sick, distracted or stressed, their performance might be degraded. Therefore, even with well managed alarm systems, it is recommended to limit the credit given to alarms [13]. However, despite an effective alarm system design and configuration efforts, the occurrence of alarm flooding cannot be eliminated completely [5]. The spread of alarms has become one of the biggest problems for plant operators in modern times. Therefore, it is essential to protect the operator from unnecessary information and to help him focus on his task. One way to accomplish it, is to reduce the amount of alarms in an alarm flood. In particular, sequences of alarms, which are connected in a causal context, are very suitable because they cannot be excluded despite a good alarm management. This alarm sequence is reduced so that only the alarm which points to the cause is displayed. For this purpose the root cause of the alarm flood must be identified. The root cause is an initiating cause of a causal chain which leads to an alarm flood. To achieve this, we developed a concept based on a causal model of the interrelations of the alarms. This is discussed in more detail in Section 4. We use Bayesian networks, which were developed by J. Pearl et al. [22] as a causal model. With the causal model we determine the potential root causes followed by an inference of the root cause of the current alarm flood. After the inference of the root cause, the alarm flood can be reduced to one alarm that caused the other alarms. This alarm is also the closest to the actual cause of the fault. However, this applies to a single alarm sequence. If multiple alarm sequences occur, there are also several root causes that are displayed, minimum one per alarm sequence.

In the following, a meaningful example is depicted to illustrate the effects of alarm floods. It also shows the importance to address this aspect in the field of research.

Example: Refinery Explosion

On the 24th July in 1994 an incident of the Pemproke Cracking Company Plant at the Texaco Refinery in Milford Haven happened. An explosion was followed by a number of fires caused by failures in management, equipment and control systems. These failures led to the release of 20 tonnes of flammable hydrocarbons from the outlet pipe of the flare knock-out drum of the fluidised catalytic cracking unit. These hydrocarbons caused subsequently the explosion. The failures started after plant disturbances appeared caused by a severe electrical storm.

The incident was investigated and analysed by the Health and Safety Executive (HSE) [11]. In total, there appeared 2040 alarms for the whole incident. 87% of these alarms were categorized in high priority. In the last 10.7 minutes before the explosion two operators had to handle 275 alarms. The alarm for the flare drum was activated approximately 25 minutes before the explosion but was not recognized by the operators. As a result, 26 persons were heavily wounded and the total cost of the economical damage was ca. €70 million. In a perfect scenario, where they would have found the crucial alarm immediately, the operators would have had 25 minutes to shut down the plant or at least minimize the possible damage caused by an explosion. This was impossible because of the flood of alarms so the operators could not handle the situation in an appropriate way.

Based on incidents like this, especially the chemical and oil industry expedited the topic of alarm management in industrial plants. One result is the guideline EEMUA 191 "Alarm Systems- A Guide to Design, Management and Procurement" by the non-profit organization Engineering Equipment & Materials Users' Association (EEMUA) [8]. The quasi-standard EEMUA 191 for alarm management recommends to have only one alarm per 10 minutes. The huge difference between this number and the 275 alarms from the example demonstrates the high potential for improvement. This is supported by the study of Bransby and Jenkinson [4]. They investigated 15 plants including oil refineries, chemical plants, pharmaceutical plants, gas terminal, and power stations. The average alarm rate per 10 minutes under normal operation ranged from 2 to 33 and the peak alarm rate per 10 minutes in plant upsets varied from 72 to 625.

Based on the guideline EEMUA 191, the International Society of Automation (ISA) developed a new standard called ANSI/ISA-18.2-2009 "Management of Alarm Systems for the Process Industries" in 2009 [17]. In 2014, another standard based on ISA 18.2 was developed by the International Electrotechnical Commission (IEC) the IEC62682:2014 [16]. The increasing focus of organizations and industry on the topic of alarm management shows the importance of reducing the amount of alarms in the future. In this challenge, the alarm flood reduction is one of the main tasks.

This is not only a beneficial effect for the safety of people, especially the employees, but also the plant itself. Moreover, the company can save a lot of money due to increased production and improved quality because the operator is able to focus better on the failures. This will also reduce the time to correct the failures and prevent unnecessary shut downs of parts of the plant.

In this work, we present an entire novel concept for alarm flood reduction in industrial plants. We depict the current status of alarm management in industrial plants and the state of the art in the field of alarm flood reduction (Section 2). For our approach a causal model, which represents the relations between the alarms in the plant is fundamental. Therefore, we discuss in Section 3 what knowledge is required for an accurate representation in the causal model. In our approach a Bayesian network is used as a causal model. In case of an alarm flood we are able to apply inference to identify the root cause and reduce the alarm flood to only the root cause. The whole approach is described in detail in Section 4. For the evaluation

we applied our approach to a manufacturing plant in the SmartFactoryOWL. In the conclusion we give an outlook for further research which needs to be done to utilize the concept in real industrial plants.

2 State of the Art of Alarm Management

The basic intention of alarm management is to assist the operator in detecting, diagnosing and correcting the fault. Due to the advancing technology and automation, an increasingly number of alarms occur in plants, which requires a great amount of effort in the detection of faults. In addition, the risk of committing mistakes and unnecessarily exchanging parts increases. In the next paragraphs the current status of treating alarm floods in industrial plants is depicted and subsequently, relevant work in the field of alarm flood reduction is presented.

Current Status

The traditional practice for operators is using a chronologically sorted list-based alarm summary display [3]. During an alarm flood this alarm list reveals multiple weak points. In many cases the alarms occur faster than the human being is able to read them. The most common ways to handle alarm floods can be roughly grouped in one of the following approaches [5, 7, 26]:

- alarm shelving,
- alarm hiding/suppressing,
- alarm grouping,
- usage of priorities.

With alarm shelving the operator is able to postpone alarm problems till he has time to focus on the problem. This creates the opportunity to solve the problems subsequently. Alarm hiding means that some alarms are suppressed completely for special occasions like the starting procedure. Consequently, alarms that are expected, but irrelevant for this special situation, do not disturb the operator. Alarm grouping is used to create an alarm list which is clearer for the operator. Instead of many alarms, there will be only one alarm for one group. The technique of prioritizing enables the operator to identify immediately the most important alarms to prevent critical effects.

Most of these techniques just disguise the real problem. To reduce the amount of alarms in an alarm flood it is necessary to identify the real root cause or the alarm, which points out the real root cause. So that the operator is still provided with the required information to correct the faulty behaviour of the plant. In the next subsection some approaches for reducing the amount of alarms in an alarm flood are presented.

Related Work

There exist several concepts addressing the topic of alarm flood reduction. Wang et al. [28] give a comprehensive overview over the diverse ideas. For an overview of methodologies with probabilistic graphical models please refer to our previous work [29]. In this paragraph we will only focus on the most recent approaches in science. Most of them are related to the topic of pattern matching. Folmer et al. [9] developed an automatic alarm data analyzer (AADA) in order to identify the most frequent alarms and those causal alarms which allow to consolidate the alarm sequence. Ahmed et al. [2] use similarity analysis to investigate similar alarm floods in historical dataset. Based on the results they group patterns of alarms. A similar strategy is pursued by Fullen et al. [10]. They developed a case-based reasoning method on similar alarm floods. Cheng et al. [6] use a modified Smith-Waterman algorithm to calculate a similarity index of alarm floods by considering the time stamp information. Karoly and Abonyi [19] propose a multi-temporal sequence mining concept to extract patterns and formulate rules for alarm suppression. Xu et al. [30] introduce a data driven method for alarm flood pattern matching. With a modified BLAST algorithm using the Levenshtein distance they discover similar alarm floods. Rodrigo et al. [23] do a multiple steps causal analysis of alarm floods to reduce them. After removing chattering alarms and identifying alarm floods, they cluster similar alarm floods. Following this they try to isolate the causal alarm of an alarm flood. We want to focus on reducing alarm floods by identifying the root cause of it. Therefore we need a causal model which represents the dependencies of the alarms. Probabilistic graphical models, such as Bayesian nets, fault trees, or Petri nets are particularly suitable for this purpose. They have been already used in the field of alarm flood reduction. Especially Bayesian networks show great potential for this task.

Abele et al. [1] propose to combine modelling knowledge and machine learning knowledge to identify alarm root causes. They use a constrained-based method to learn the causal model of a plant represented by a Bayesian network. This enables faster modelling and accurate parametrization of alarm dependencies but expert knowledge is still required. Wang et al. [27] apply an online root-cause analysis of alarms in discrete Bayesian networks. They restrict the Bayesian network to have only one child node. The method is evaluated on a numerical example of a tank-level system. Wunderlich and Niggemann [29] investigate and evaluate different structure learning algorithms for Bayesian network in the field of alarm flood reduction. It turned out, that Bayesian networks are feasible and the state of the art structure learning algorithms are able to learn the causal relationships of alarms from industrial plants.

Based on the findings in our previous work, we developed a concept for the reduction of alarms. The foundation for this concept is the Bayesian network as a causal model. It is essential to learn a very accurate causal model in order to identify the causal chain and to determine the root cause. Therefore, it is important to know how a causal model can be learned in an unsupervised way and what information about the plant or process is necessary to be included.

3 Knowledge Representation

The research on alarm floods is still in an early stage and has a high potential of improvement. Therefore we want to find out, which knowledge is necessary and required to improve the situation. In general, once the amount of alarms is too high to be handled, the new arriving alarms will be ignored by the operator. This means the amount of alarms is randomly reduced which has a high potential of causing a disaster. Therefore, to improve the handling it is necessary to use all available knowledge to reduce the alarm flood in an intelligent way. Best case scenario would be if only the alarms which hint to the real causes, would be displayed. Therefore, it is a demanding task to identify all required causal relations between alarms [14]. To be able to achieve this, it is necessary to construct a causal model. Probabilistic graphical models are suitable for this use case. They represent in an easy-to-understand way the relationships and their probabilities. All these models are composed of nodes n and edges e . In our use case a node is equal to one alarm. The relations of two alarms (nodes) are represented by edges. For the causal model it is beneficial to include as much knowledge about the system as possible to be close to the reality. There are two extreme ways to achieve a representation of the real world such as phenomenological and first principle representation. The first approach is to learn the statistical relations of the alarms based on the alarm logs. However, it does not include every aspect of the plant. For example, as shown in Fig. 1, only the symptoms (alarms) are presented. But the alarms themselves may

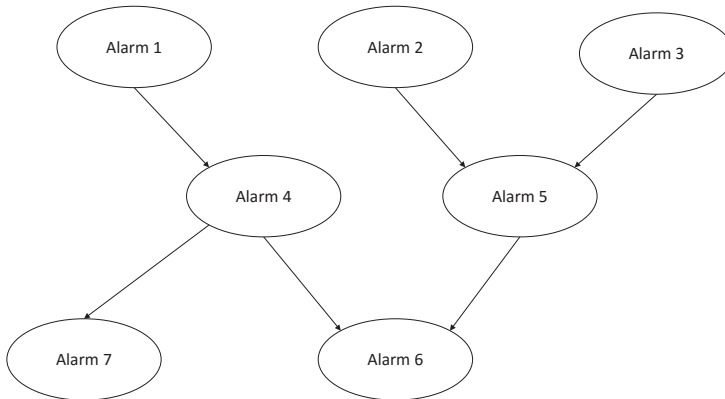


Fig. 1. Phenomenological representation

not be depended directly on each other. It's more viable to believe, that based on location or process flow the alarms are propagating and have effect on each other. The representation only depicts correlations and not causal relationships.

This leads to the second approach. Here, a first principle model of the system is built to create an exact image of the system. Not only the symptoms (alarms) are included, but also all aspects such as sensor values see Fig. 2. This has an advantage

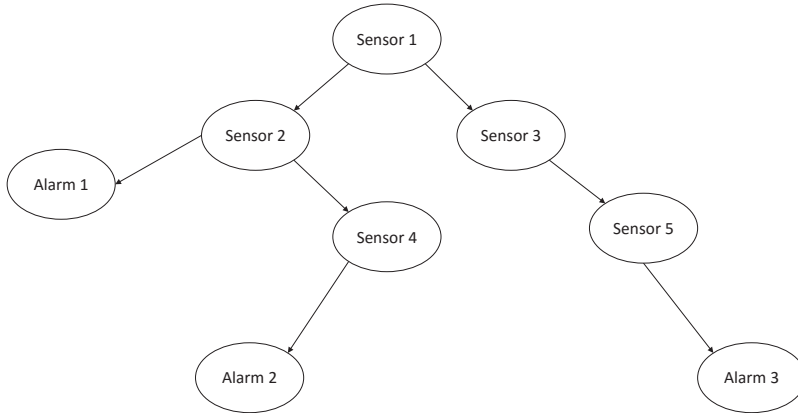


Fig. 2. First principle representation

of representing a deeper knowledge about the relations between the alarms and how the dependencies are. However, in most cases this is not possible due to missing information about some parts of the plant such as process flow. Also the creation of a model needs an expert and is very time-consuming. Hence, a combination of both is the most favourable solution. The model should include as much knowledge about the plant (process flow, environment etc.) as possible without being too time consuming. Finding a good balance is one of the challenges for researchers. In a best case scenario, the advantages of fast learning from historical data approach can be combined with the valuable expert knowledge about the plant and process.

We use a Bayesian network as a data-driven approach and try to fill it with as much information about the plant as possible.

4 Concept for Alarm Flood Reduction

Based on the findings, we design a concept for reducing alarm floods. To represent the causal relationships, we use Bayesian networks. An overview of the overall concept is shown in Fig. 3.

The concept consists of two different phases. First, the learning phase which is outlined in red and second, the operating phase which is outlined in green. In the learning phase, all historical data about the machine or system are used to learn a causal model of the alarms and their probabilities. This is done offline and usually takes several minutes to hours to calculate. The causal model contains information

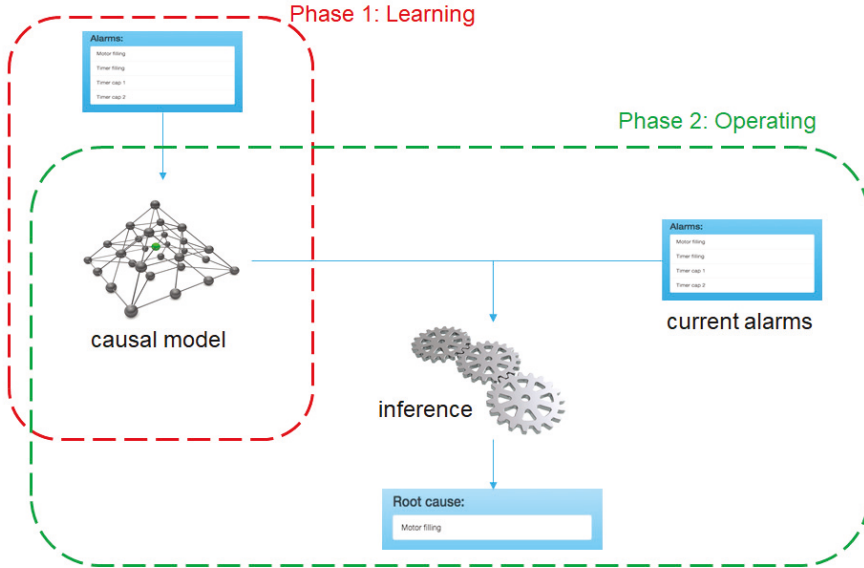


Fig. 3. Overview Concept Alarm Flood Reduction

about relations and dependencies of all alarms. However, the learning of the causal model is necessary only in the case of major changes of the system (for example, the production of a new product).

Once the learning of the causal model has been completed, the second phase, the so-called operating phase, can begin. The current alarms are used together with the causal model. With the aid of the causal model, it is possible to conclude the root cause of the current alarm sequence. This inference allows the number of alarms to be reduced to these root causes and thus to only display these root causes to the operator. Thus, the operator can correct the fault quickly and purposefully.

Demonstrator For the evaluation of this alarm flood reduction concept, we implemented two simple scenarios of alarm floods in the Versatile Production System (VPS), which is located in the SmartFactoryOWL¹. This scenarios serve as use cases to identify the root cause. The VPS is a manufacturing plant in a laboratory scale where sensors, actuators, bus systems, automation components, and software from different manufacturers are considered. The VPS is a hybrid technical process considering both continuous and discrete process elements with a focus on the information processes and communication technologies from the plant level down to the sensor level. It thus provides an ideal multi vendor platform for testing and validation of innovative technologies and products.

¹ <https://www.smartfactory-owl.de>

The use cases are implemented in the "bottle filling module" of the VPS. The bottles can be filled either with water or with grain. The two use cases represent two possible root causes for an alarm flood. We want to identify these root causes with correctly learnt dependencies of alarms. In Fig. 4 an overview of the "bottle filling module" is depicted. The module consists of a conveyor belt and a rotary

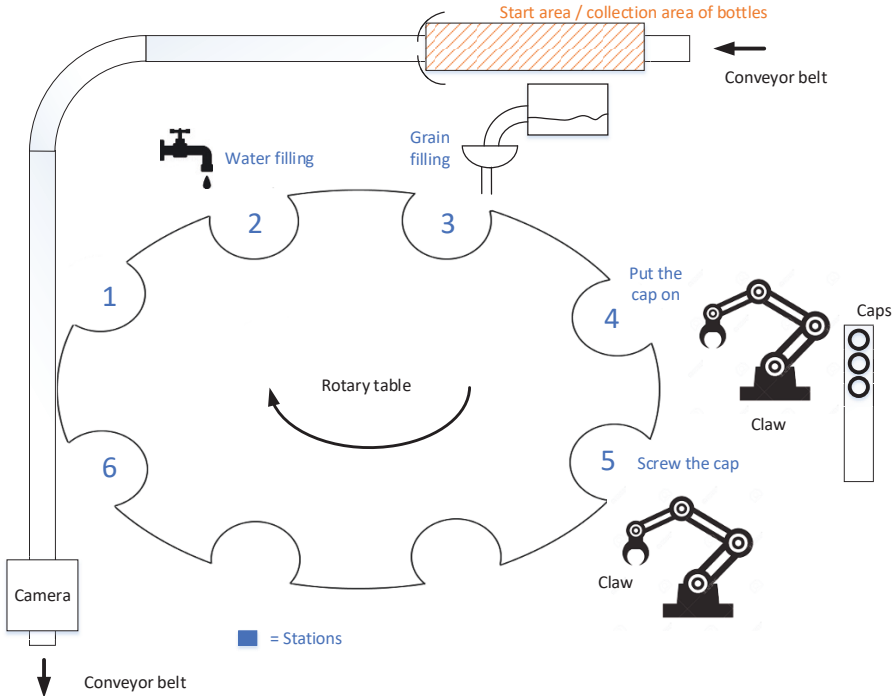


Fig. 4. Overview bottle filling module

table with six stations. At the first station the bottle is handed over by the conveyor belt to the rotary table. It's possible to fill the bottle either with water at station two or to fill it with grain at station three. The next two stations are there for putting the cap on. At the first step, the cap is placed on top of the bottle and in the second step, the cap is fastened. In the last station the bottle is handed over back to the conveyor belt passing a camera check, whether the bottle is filled.

In total the following alarms are implemented: bottle rotary table entrance (BRE), timer water tank (TW), drive filling (DF), timer filling (TF), timer cap 1 (TC1), timer cap 2 (TC2), bottle not filled (BNF). The real dependencies between the alarms are depicted in Fig. 5. This structure shows the real causality within the plant. The two root causes for an alarm flood are bottle rotary table entrance

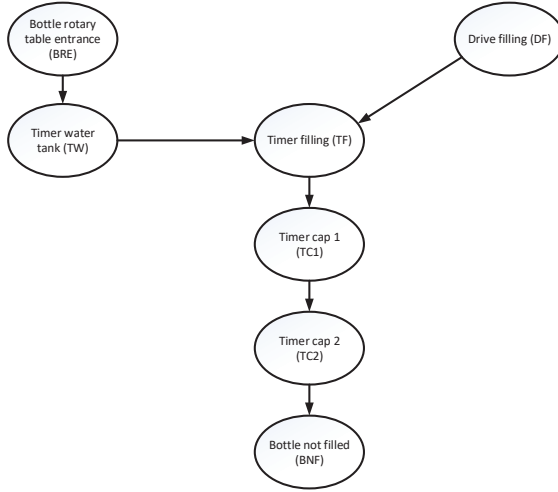


Fig. 5. Real causality structure

(BRE) and drive filling (DF). If a bottle is missing the alarm BRE triggers. This alarm causes the subsequent alarms TW, TF, TC1, TC2, and BNF. In the other root cause of a blocked drive the alarm DF causes the subsequent alarms TF, TC1, TC2, and BNF.

4.1 Learning Phase

Bayesian networks are a class of graphical models which allow an intuitive representation of multivariate data. A Bayesian network is a directed acyclic graph, denoted as $B = (N, E)$, with a set of variables $\mathbf{X} = \{X_1, X_2, \dots, X_p\}$. Each node $n \in N$ is associated with one variable X_i . The edges $e \in E$, which connect the nodes, represent direct probabilistic dependencies.

Abele et al. [1] and Wang et al. [27] have already tried to use Bayesian networks for detection of a root-cause in an alarm flood. Abele et al. learned a Bayesian network, which is consequently the basis for root-cause analysis of a pressure tank system. The structure of the Bayesian network was learned with a constrained-based method and needed some expert knowledge to achieve the correct model of the pressure tank system. Therefore, they concluded that expert knowledge and machine learning should be combined for better results. Wang et al. applied a special kind of Bayesian networks. They restrict themselves to only one-child nodes. This is a huge restriction and it cuts off many possible failure cases, because in a modern and complex industrial plant the interconnectivity is increasing dramatically. This means that the alarms are also more connected and dependent on each other.

Structure Learning

Therefore, we want to pursue the idea of Abele et al. and use the Bayesian network as a model to represent the causality of the alarms. But other than Abele et al. we do not limit ourselves to constraint-based learning methods. All in all these learning algorithms can be differentiated into the following three groups of methods:

- constrained-based,
- score-based,
- hybrid.

In a constrained-based method the Bayesian network is a representation of independencies. The data is tested for conditional dependencies and independencies to identify a structure, which explains the dependencies and independencies of the data the best. Constrained-based methods are susceptible to failures in individual independence tests. Just one wrong answered independence test misleads to a wrong structure.

Score-based methods view Bayesian network as specifying a statistical model. Therefore, it is more like a model selection problem. In the first step, a hypothesis space of potential network structures is defined. In the second step, the potential structures are measured with a scoring function. The scoring function shows how good a potential structure fits the observed data. Following this, the computational task is to identify the highest-scoring structure. This task consists of a superexponential number of potential structures $2^{O(n^2)}$. Therefore, it is unsure if the highest-scoring structure can be found, so the algorithms use heuristic search techniques. Because the score-based methods consider the whole structure at once, they are less susceptible to individual failures and better at making compromises between the extent to which variables are dependent in the data and the cost of adding the edge [20].

Hybrid methods combine aspects of both constraint-based and score-based methods. They use conditional independence tests to reduce the search space and network scores to find the optimal network in the reduced space at the same time. In a previous work [29], we have already investigated different structural algorithms for reducing alarm flood. It turned out that a hybrid approach is the most promising due to the greater accuracy.

Algorithm

In the following, an hybrid method algorithm is presented and evaluated on the use cases. The Max-Min Hill-Climbing (MMHC) from Tsamardinos et al. [25] performed the best in previous tests and is chosen for the evaluation of the concept. MMHC is a hybrid of a constrained-based and score-based approach. In the first step, the search space for children and parents nodes is reduced by using a constrained-based approach, namely Max-Min Parents and Children (MMPC) algorithm. In the second step, the Hill-Climbing algorithm is applied to find the best fitting structure from the reduced search space.

For a better understanding of the associated pseudo code, we need a few definitions. The dataset D consists of a set of variables ϑ . In the variable PC_x the candidates of parents and children for the node X are stored. This set of candidates is calculated with MMPC algorithm. The variable Y is a node of the set PC_x . The pseudo code of MMHC looks as follows:

Algorithm 1 MMHC Algorithm

```

1: procedure MMHC( $D$ )
2:   Input: data  $D$ 
3:   Output: a DAG on the variables in  $D$ 
4:   % Restrict
5:   for every variable  $X \in \vartheta$  do
6:      $PC_X = \text{MMPC}(X, D)$ 
7:   end for
8:   % Search
9:   Starting from an empty graph perform Greedy Hill-Climbing with operators add-edge, delete-edge, reverse-edge.  $Y \rightarrow X$  if  $Y \in PC_X$ 
10:  Return the highest scoring DAG found
11: end procedure

```

The algorithm first identifies the parents and children set of each variable, then performs a greedy Hill-Climbing search in the reduced space of Bayesian network. The search begins with an empty graph. The edge addition, removal, or reversing which leads to the largest increase in the score is taken and the search continues in a similar way recursively. The difference from standard Hill-Climbing is that the search is constrained to only consider edges which were discovered by MMPC in the first phase. The MMPC algorithm calculates the correlation between the nodes. Based on a training dataset the MMHC algorithm gives the structure which is depicted in Fig. 6. The training data set was recorded at the VPS and consists of 525 observations of the seven alarms. The states of the alarms are binary coded with 0 for inactive and 1 for active.

The result is very close to the true causal model in Fig. 5. Both, the use-case with the missing bottle ($BRE \rightarrow TW \rightarrow TF \rightarrow TC1 \rightarrow TC2 \rightarrow FNB$) and the use-case with the blocked drive ($DF \rightarrow TF \rightarrow TC1 \rightarrow TC2 \rightarrow FNB$) are shown correctly. Only the connection between DF and BRE is not present in reality.

In a graph with n nodes, there exist $n \cdot (n - 1)$ possible connections. For the evaluation we define the following terms. A true positive connection (TP) is an edge which is in the original and in the learned Bayesian network. A false positive connection (FP) is an edge which is not in the original but in the learned Bayesian network. A false negative connection (FN) is an edge which is in the original but not in the learned Bayesian network. A true negative (TN) connection is an edge which is not in the original and not in the learned Bayesian network. The results of the evaluation for the MMHC algorithm is depicted in detail in Table 1.

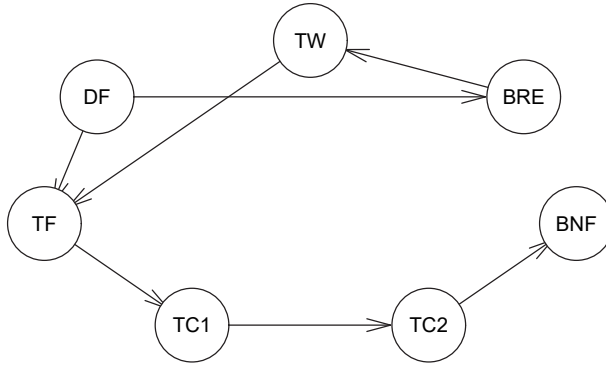


Fig. 6. BN Max-Min Hill-Climbing

Table 1. Results of evaluation

| | MMHC |
|---------------------|-------|
| True Positive (TP) | 6 |
| False Positive (FP) | 1 |
| False Negative (FN) | 0 |
| True Negative (TN) | 35 |
| Accuracy [%] | 97.62 |
| F1-Score | 0.92 |
| Mean runtime [ms] | 9.82 |

The MMHC learned all six edges from the original Bayesian network with the correct orientation. With only one misaligned edge (FP) and zero unwanted edges (FN) MMHC shows its strength. The accuracy is with 97.62% very good and underlined with an F1-score of 0.92. One slight disadvantage is the runtime. Based on the mean of 1000 runs the MMHC algorithm needs 9.82 ms which is quite long compared to other methods. However, it has to be considered, that in today’s world the bottleneck is not the calculation power. The accuracy of the structure is more important. All in all, the hybrid method with the MMHC algorithm is best suited for learning a causal model from alarms. This was proven by Wunderlich and Niggemann [29], who evaluated different structure learning algorithms.

Parameter Learning

Once the structure of the causal model has been learned, it is still necessary to calculate or estimate the probabilities for the dependencies. Only in the combination of structure and parameters (probabilities) the inference of the root cause can be done in the operation phase. To learn the parameters, the classical method

maximum likelihood estimation (MLE), which was developed by R.A. Fischer, is used. Here, a parameter p is estimated to maximize the probability of obtaining the observation under the condition of the parameter p . In other words, the MLE provides the most plausible parameter p as an estimate with respect to the observation. If the parameter p is a probability in the Bayesian network and the historical data D represents the observations, the likelihood function is composed as follows:

$$L(D|p) = \prod_{i=1}^n f(D_i|p) \tag{1}$$

The probability density function of D under the condition p is $f(D|p)$. In Figure 7 the causal model with the learned probabilities is shown. It is noteworthy that the

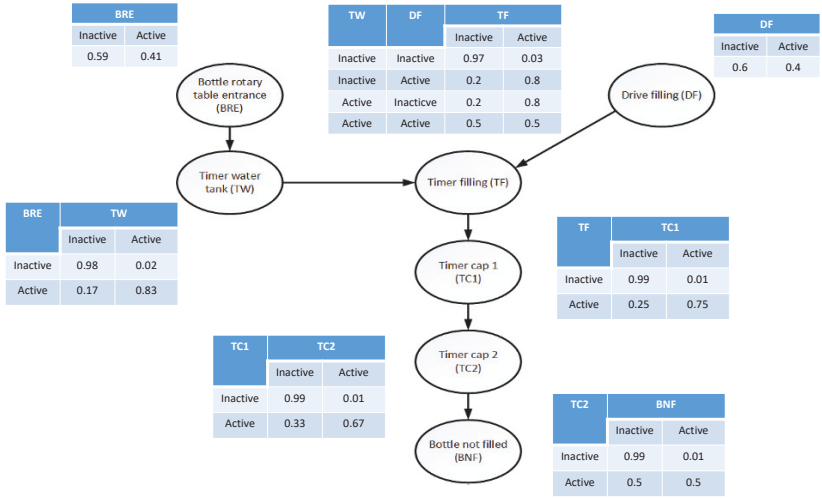


Fig. 7. Bayesian net with Probabilities

variant with active alarms TW and DF never occurs so there are no probabilities in this regard. With the learned structure and the probabilities, the inference can begin.

4.2 Operation Phase

There are two different variants for the inference, namely the exact inference and the approximate inference. For the exact inference, the probabilities are calculated specifically for the query. One famous method of exact inference is the variable elimination (VE). In doing so, variables irrelevant to the query are eliminated from

the probability distribution. This is computationally very complex and expensive. Therefore, such a method is only feasible for very small Bayesian networks.

An alternative and more frequently used are the approximate inference methods. Here the model, which is represented by the Bayesian network, is randomly simulated. This process is called sampling. This makes it possible to approximate the probability of the query. For example, it can be determined how high the probability is that a particular node assumes a specific state. The cases in which this is occurred are counted and set in proportion to the total sample size. A disadvantage of this method is that under certain circumstances, a large number of samples are required in order to provide a reliable result and thus significantly increase the calculation time.

To evaluate our concept, we opted for the simple and fast logic sampling (LS) algorithm. The LS algorithm is a very simple procedure developed by Max Henrion in 1986 [12]. In this case, a state is arbitrarily assumed per sample for the root nodes according to their probability table. Thus, a certain number of samples, which are determined, are carried out. Subsequently, the probability that e.g. a node X assumes the state True as follows:

$$P(X = True) = \frac{\text{No. of cases with X=True}}{\text{No. of all samples}} \quad (2)$$

This process always converges to the correct solution, but in very rare cases the number of samples required can become exorbitant [18].

Inference

In this subsection we apply and evaluate the inference with the LS algorithm on the VPS demonstrator. In the previous subsection it was shown, that a decent structure could be learned. Combined with time-limited expert knowledge we achieved an accurate causal model. Based on this causal model and the learned probabilities the inference of the root causes is enabled. For the inference of an alarm flood in the demonstrator we use as possible root causes the two alarms BRE and DF. This is given by the learned structure of the Bayesian network. For the evaluation we investigate the use case of a missing bottle. Therefore we have as evidence E the alarms (TW, TF, TC1, TC2, BNF) and formulate the following two queries.

$$P(BRE = active|E = active) = \frac{\text{No. of cases with BRE=active given E=active}}{\text{No. of all samples}} \quad (3)$$

$$P(DF = active|E = active) = \frac{\text{No. of cases with DF=active given E=active}}{\text{No. of all samples}} \quad (4)$$

The two queries calculate the probability of BRE or DF to be active given that all alarms of evidence are active. In our use case, the estimation shows a probability of 97 % for BRE to be active and a probability of 40 % for DF to be active. This results in the conclusion, that the alarm BRE is the root cause for the current alarm flood.

A comparison of the concept for the use case of a missing bottle in the VPS is shown in Table 2.

Table 2. Alarm Flood Reduction

| Without | With |
|------------------------------|------------------------------|
| Timer Filing | Bottle Rotary Table Entrance |
| Timer Cap 1 | |
| Timer Cap 2 | |
| Bottle Not Filled | |
| Bottle Rotary Table Entrance | |
| Timer Water Tank | |

If a bottle is missing, the six alarms (Timer Filing, Timer Cap 1, Timer Cap 2, Bottle Not Filled, Bottle Rotary Table Entrance and Timer Water Tank) will appear. The operator is not immediately able to identify the cause of this alarm sequence. It changes when our concept is applied in this scenario. The amount of alarms can be reduced from six to only one alarm. This one alarm BRE is also the cause of the alarm flood. This result allows the operator to quickly and efficiently identify the cause and take the necessary steps to remedy the problem. A similar result is also obtained for the other use case of a blocked drive for grain filling.

5 Conclusion

We presented the increasing problem of overwhelming alarm floods in industrial plants. One way to solve this problem is to reduce the alarm floods, especially sequences of alarms caused by one alarm. Therefore, we propose a concept to identify the real root cause of an alarm flood using Bayesian networks. The Bayesian network serves as a causal model and enables inference about the root cause. Instead of all alarms, only the root cause is depicted to the operator. This supports the operator to take better care of the plant. The concept is evaluated on real use cases of a demonstrator in the SmartFactoryOWL. For the use cases the concept shows a promising result identifying the real root cause. Obviously, the demonstrator is still quite small and not complex compared to real industrial plants. Therefore, it is necessary to evaluate how this approach scales on real industrial plants, where also additional challenges appear. This not only means the increasing complexity, but also the occurrence of disturbances or missing or incorrect historical data records.

Nevertheless, we think that Bayesian networks are a good foundation to learn a causal model of the dependencies of alarms in a plant. Bayesian networks are robust against uncertainty such as incomplete or defective data. Because it's a data-driven approach it reduces the amount of time in which an expert is needed for constructing the causal model. The expert knowledge is still necessary, but the approach with Bayesian network can be improved by including time behaviour or dynamic process like a product change in the plant. Also the algorithms for learning the structure can be improved by using methods like Transfer Entropy for a better edge orientation.

Acknowledgment

This work was supported by the German Federal Ministry of Education and Research (BMBF) under the project ADIMA (grant number: 13FH019PX5) and by the European Union's Horizon 2020 research and innovation programme under the project IMPROVE (grant agreement No. 678867).

References

1. Abele, L., Anic, M., Gutmann, T., Folmer, J., Kleinstaubler, M., Vogel-Heuser, B.: Combining knowledge modeling and machine learning for alarm root cause analysis. *IFAC Proceedings Volumes* 46(9), 1843 – 1848 (2013)
2. Ahmed, K., Izadi, I., Chen, T., Joe, D., Burton, T.: Similarity analysis of industrial alarm flood data. *IEEE Transactions on Automation Science and Engineering* 10(2), 452–457 (April 2013)
3. Bransby, M.: Design of alarm systems. *IEE CONTROL ENGINEERING SERIES* pp. 207–221 (2001)
4. Bransby, M., Jenkinson, J.: The management of alarm systems: a review of best practice in the procurement, design and management of alarm systems in the chemical and power industries. Technical Report CRR 166, Health and Safety Executive (1998)
5. Bullemer, P.T., Tolsma, M., Reising, D., Laberge, J.: Towards improving operator alarm flood responses: Alternative alarm presentation techniques. *Abnormal Situation Management Consortium* (2011)
6. Cheng, Y., Izadi, I., Chen, T.: Pattern matching of alarm flood sequences by a modified smithwaterman algorithm. *Chemical Engineering Research and Design* 91(6), 1085 – 1094 (2013)
7. Directorate, Norwegian Petroleum: Principles for alarm system design. YA-711, Feb (2001)
8. Engineering Equipment and Materials Users' Association: Alarm Systems: A Guide to Design, Management and Procurement. EEMUA publication, EEMUA (Engineering Equipment & Materials Users Association) (2007)
9. Folmer, J., Vogel-Heuser, B.: Computing dependent industrial alarms for alarm flood reduction. *Transactions on Systems, Signals and Devices (TSSD) PP* (2013)
10. Fullen, M., Schüller, P., Niggemann, O.: Semi-supervised case-based reasoning approach to alarm flood analysis. In: 3rd Conference on Machine Learning for Cyber Physical Systems and Industry 4.0 (ML4CPS) (10 2017)

11. Health and Safety Executive: The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994: A Report of the Investigation by the Health and Safety Executive Into the Explosion and Fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 July 1994. Incident Report Series, HSE Books (1997)
12. Henrion, M.: Propagating uncertainty in Bayesian networks by probabilistic logic sampling. In: Uncertainty in Artificial Intelligence 2 Annual Conference on Uncertainty in Artificial Intelligence (UAI-86). pp. 149–163. Elsevier Science, Amsterdam, NL (1986)
13. Hollender, M., Skovholt, T.C., Evans, J.: Holistic alarm management throughout the plant lifecycle. In: 2016 Petroleum and Chemical Industry Conference Europe (PCIC Europe). pp. 1–6 (June 2016)
14. Hollender, M., Beuthel, C.: Intelligent alarming. ABB review 1, 20–23 (2007)
15. Hollifield, B., Habibi, E., Pinto, J.: The Alarm Management Handbook: A Comprehensive Guide. PAS (2010)
16. International Electrotechnical Commission: EN-IEC 62682:2014 Management of alarm systems for the process industries. Tech. rep., International Electrotechnical Commission
17. International Society of Automation and American National Standards Institute: ANSI/ISA-18.2-2009, Management of Alarm Systems for the Process Industries. ISA (2009)
18. Kanal, L., Lemmer, J.: Uncertainty in Artificial Intelligence 2. Machine Intelligence and Pattern Recognition, Elsevier Science (2014)
19. Karoly, R., Abonyi, J.: Multi-temporal sequential pattern mining based improvement of alarm management systems. In: Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on. pp. 003870–003875. IEEE (2016)
20. Koller, D., Friedman, N.: Probabilistic Graphical Models: Principles and Techniques - Adaptive Computation and Machine Learning. The MIT Press (2009)
21. Larsson, J.E., Öhman, B., Calzada, A., DeBor, J.: New solutions for alarm problems. In: Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Interface Technology, Albuquerque, New Mexico (2006)
22. Pearl, J., Bacchus, F., Spirtes, P., Glymour, C., Scheines, R.: Probabilistic reasoning in intelligent systems: Networks of plausible inference. *Synthese* 104(1), 161–176 (1995)
23. Rodrigo, V., Chioua, M., Hägglund, T., Hollender, M.: Causal analysis for alarm flood reduction. In: 11th IFAC Symposium on Dynamics and Control of Process Systems Including Biosystems. IFAC (2016)
24. Rothenberg, D.: Alarm Management for Process Control: A Best-practice Guide for Design, Implementation, and Use of Industrial Alarm Systems. Momentum Press (2009)
25. Tsamardinos, I., Brown, L.E., Aliferis, C.F.: The max-min hill-climbing Bayesian network structure learning algorithm. *Machine Learning* 65(1), 31–78 (2006)
26. Urban, P., Landryov, L.: Identification and evaluation of alarm logs from the alarm management system. In: 2016 17th International Carpathian Control Conference (ICCC). pp. 769–774 (May 2016)
27. Wang, J., Xu, J., Zhu, D.: Online root-cause analysis of alarms in discrete bayesian networks with known structures. In: Proceeding of the 11th World Congress on Intelligent Control and Automation. pp. 467–472 (June 2014)
28. Wang, J., Yang, F., Chen, T., Shah, S.L.: An overview of industrial alarm systems: Main causes for alarm overloading, research status, and open problems. *IEEE Transactions on Automation Science and Engineering* 13(2), 1045–1061 (April 2016)

29. Wunderlich, P., Niggemann, O.: Structure learning methods for Bayesian networks to reduce alarm floods by identifying the root cause. In: 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2017). Limassol, Cyprus (Sep 2017)
30. Xu, Y., Tan, W., Li, T.: An alarm flood pattern matching algorithm based on modified BLAST with Leveshtein distance. In: Control, Automation, Robotics and Vision (ICARCV), 2016 14th International Conference on. pp. 1–6. IEEE (2016)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

