Integration of Failure Assessments into the Diagnostic Process

Roxane Koitz[1] and Franz Wotawa[2]

[1,2] *Institute for Software Technology, Graz, Styria, 8010, Austria*
rkoitz@ist.tugraz.at
wotawa@ist.tugraz.at

Abstract

The complexity of technical systems requires increasingly advanced fault diagnosis methods to improve safety and reliability. Particularly in domains where maintenance poses an extensive part of the entire operation cost, accurate identification of failure sources has a large economic impact. Model-based diagnosis, as a subfield of Artificial Intelligence, allows to determine root causes based on observed anomalies and has already been applied to a variety of domains. Abductive model-based diagnosis considers information on failures and how they affect detectable system measurements. Thus, this type of fault localization procedure depends on systematic and analytic knowledge on components, their possible malfunctions, and the subsequent effects. In this paper, we examine various common failure assessments such as Failure Mode Effect Analysis, in regard to serving as a basis for abductive diagnosis. In particular, we analyze the methods concerning their advantages and limitations as sources of failure information within our diagnosis process.

1. Introduction

Accurate failure localization in technical systems is a topic of interest from an industrial as well as research point of view due to their increasing complexity and magnitude. An intensive body of research has concerned itself with this subject ranging from fields such as Control Engineering to Artificial Intelligence. Within the former and the latter model-based approaches have been suggested. These methods exploit a formalization of the system behavior to identify causes of observed anomalies (Cordier et al., 2004). In the Artificial Intelligence community two main techniques have emerged: consistency-based and abductive diagnosis. The first requires a model of the correct operation to determine inconsistencies stemming from failure effects on the system (Reiter, 1987). In contrast abductive model-based diagnosis reasons on knowledge of the system performance in case of a defect (Console, Dupre, & Torasso, 1991).

Even though these model-based approaches build on solid theories, have been applied to various domains, and continuous research improves their methods, a widespread adoption is yet to be observed. Certainly, the initial creation of the system descriptions suitable for diagnosis poses an obstacle (Console & Dressler, 1999). Further, as noted by Milde, Guckenbiehl, Malik, Neumann, and Struss (2000), the current industrial work processes have to be known in order to integrate model-based diagnosis successfully. To account for the complexity of systems, the models have to be developed in relation to existing knowledge on products, such as design, construction, and failure information.

An essential benefit promoted by the community has been the reuse of knowledge inherent to the model-based techniques. To emphasize this potential and provide an economic additional benefit besides diagnosis, research has focused on further tasks which can be performed with the initially generated diagnosis models. Struss, Malik, and Sachenbacher (1996) describe an automated approach integrating diagnosis and the creation of Failure Mode Effect Analysis (FMEA) as well as repair manuals based on compositional qualitative models of the intended part behavior. Similar goals have been pursued by Hawkins and Woollons (1998a), Price and Taylor (2002) or Milde et al. (2000). While the former two proposed methods for FMEA, the latter automatically generates fault trees from device knowledge by predicting the correct and erroneous behavior based on qualitative models.

In contrast, we propose a different approach to reuse knowledge: As certain reliability assessments, such as FMEA or Fault Tree Analysis (FTA) are common practice and even mandatory in certain industries (Rausand & Høyland, 2004), the information captured can be exploited for diagnostic reasoning. In particular, these types of analyses describe the relation of failures and their consequences on the system, thus, can form the basis for abductive diagnosis.

The remaining paper is structured as follows. First, we present the theoretical background of abductive model-based diagnosis and subsequently recap a previously shown process of incorporating it in an industrial setting. Second, we analyze different assessments which can be used to automatically infer abductive models. In particular, we focus on FMEA, FTA and an approach incorporating Physics of Failure (PoF). For each type of failure analysis a modeling methodology is introduced generating a system formalization suitable for abductive reasoning. Further, we give a short overview of advantages and disadvantages of each assessment in regard to the resulting model and its capabilities within the entire diagnosis process. Lastly, we present general limitations of our approach and conclude the paper.

2. PRELIMINARIES

Abductive model-based diagnosis reasons about explanations for a given set observations via entailment, i.e. the observations are logical consequences of the explanations (Poole, Goebel, & Aleliunas, 1987). Formally we write this relation as $\psi \models \phi$, where ψ denotes the explanations or causes and ϕ represents the observations. Thus, in order to employ abductive reasoning, this type of model-based approach depends on a formalization of failures and their discoverable effects to infer diagnoses from observed symptoms.

Abduction belongs to the intractable problems, meaning that in general it requires exponential time (Nordh & Zanuttini, 2008). Therefore, we focus within our research on subsets of logic, which allow computing explanations rather efficiently. We consider the propositional Horn clause abduction problem (*PHCAP*) (Friedrich, Gottlob, & Nejdl, 1990). Before formulating the *PHCAP*, we define a knowledge base *KB* as a set of Horn clause sentences over a finite set of propositional variables. A subset of these propositional variables constitute the hypotheses or abducibles, i.e. the variables which can pose as part of an explanation or a diagnosis. Later when considering the model generation based on failure assessments these hypotheses refer to faults. The Horn clause theory characterizes the relations between the causes and their effects.

Definition 1 *A knowledge base (KB) is a tuple (A,Hyp,Th) where A denotes the set of propositional variables, Hyp $\subseteq$ A the set of hypotheses, and Th $\subseteq$ HC the set of Horn clause sentences over A.*

As abduction derives explanations for given symptoms, a set of observables has to be considered in addition to the *KB* to form a *PHCAP*.

Definition 2 *Given a knowledge base (A,Hyp,Th) and a set of observations Obs $\subseteq$ A then the tuple (A,Hyp,Th,Obs) forms a propositional Horn clause abduction problem (PHCAP).*

Definition 3 *Given a PHCAP (A,Hyp,Th,Obs). A set $\Delta \subseteq$ Hyp is a solution if and only if $\Delta \cup$ Th $\models$ Obs and $\Delta \cup$ Th $\not\models \perp$. A solution Δ is parsimonious or minimal if and only if no set $\Delta' \subset \Delta$ is a solution.*

As we are considering abduction, the solution to the *PHCAP* comprises the hypotheses which together with the background theory logically entail the set of observables. If not specified otherwise, we refer to minimal diagnoses simply as diagnoses. The restriction to subset minimal solutions is due the fact that in most practical applications only parsimonious results are of interest. There are several approaches capable of computing abductive explanations such as abductive logic programming (Kakas, Kowalski, & Toni, 1992), prooftree completion (McIlraith, 1998), or consequence finding (Marquis, 2000).

2.1. Observation Discrimination

Abductive diagnosis is exponential in the number of possible explanations, that is in the worst case $2^{|Hyp|}$ solutions are determined. As mentioned before, yet, from a practical point of view a single diagnosis is preferred. Thus, probing has been proposed as a means to decrease the solution space. Wotawa (2011) suggests computing all explanations and subsequently adding new symptoms which allow discrimination of diagnoses.

Definition 4 *Given a PHCAP (A,Hyp,Th,Obs) and two diagnoses Δ_1 and Δ_2. A new observation $o \in A \setminus Obs$ discriminates two diagnoses if and only if Δ_1 is a diagnosis for (A,Hyp,Th,Obs $\cup \{o\}$) but Δ_2 is not.*

Entropy is the informations gain, thus, the probing point, with the highest entropy $H(o)$ (Eq. (1)) determines the measurement with the greatest discrimination capabilities (de Kleer & Williams, 1987).

$$H(o) = -p(o) \cdot \log_2 p(o) - (1 - p(o)) \cdot \log_2(1 - p(o)) \quad (1)$$

In Equation (2) the probability $p(o)$ of observation o is defined, where Δ-Set is the set of diagnoses obtained as a solution to the *PHCAP*.

$$p(o) = \frac{|\{\Delta \mid \Delta \in \Delta\text{-Set}, \Delta \cup Th \models \{o\}\}|}{|\Delta\text{-Set}|} \quad (2)$$

Once the next best probing points have been selected on basis of the entropy value, additional measurements are taken and passed on to the diagnosis engine as observations. The fault identification process is then restarted. Within the *PHCAP* a diagnosis Δ is discriminated in case we observe a complementary observation, i.e. $\neg o \subseteq Obs : \Delta \cup Th \models \{o\}$.

2.2. Diagnosis Ranking

According to Bayes rule the conditional probability of an explanation can be computed as shown in Eq. (3):

$$p(\Delta \mid o) = \frac{p(o \mid \Delta)p(\Delta)}{p(o)} \quad (3)$$

Since we aim at determining the probability of a diagnosis given the *PHCAP*, we only consider effects actually observed. Let us further assume that there is no uncertainty in the measurement, hence the data has not be subjected to errors or noise. For any $o \in Obs$, we can infer that $p(o) = 1$. As the explanation logically implies the observation we can assign $p(o \mid \Delta) = 1$. Hence, $p(\Delta \mid o) = p(\Delta)$. Assuming independence amongst faults, the probability of each diagnosis Δ can be computed based on the a-priori probability $p(h)$ of each hypothesis h represented within the diagnosis, as shown in Eq. (4).

$$p(\Delta) = \prod_{h \in \Delta} p(h) \prod_{h \notin \Delta} (1 - p(h)) \tag{4}$$

Given a *PHCAP* we compute $p(\Delta)$ for all diagnoses in Δ-Set and subsequently assign ranks accordingly.

3. PROCESS

Even though abductive model-based diagnosis is based on solid theoretical background, its adoption in practice is hindered by two main obstacles: (1) the initial domain modeling effort necessary and (2) the computational complexity. In this paper, we focus on the former and describe various failure assessments used in practice and their capabilities to function as a basis for abductive diagnosis. We previously defined a process for applying abductive model-based diagnosis to real-world applications, which relies on an automated model creation (Koitz & Wotawa, 2015b). In this section we give a short introduction into the process, which is divided into three main steps, as can be seen in Figure 1:

1. Model Development. Abductive model-based diagnosis utilizes a formal description of how failures manifest themselves within the system. In order to diminish the modeling effort, we propose an automated technique exploiting failure analyses common in practice. An essential requirement for these assessments to function as the basis of abductive diagnoses is to contain knowledge of failures and their symptoms to enable a mapping to a *KB* as discussed in the previous section. Depended on the underlying fault analysis, the generated logical theory presents different characteristics.

2. Fault Detection. The diagnosis process is triggered once a symptom is observed for which a cause is to be computed. Thus, there has to be a mechanism to detect the presence of a fault, such as a condition monitoring system.

3. Fault Identification. Once an anomaly has been discovered, the diagnosis process is started, i.e. a solution to the *PHCAP* is computed. Various approaches are capable of computing abductive explanations (Koitz & Wotawa, 2015a). Depending on the information embedded in the failure assessment additional refinements to the initial diagnosis results can be made.

Our focus in the upcoming section is on how different failure assessments can form the input to a model creation procedure and which improvements to the initial fault identification can be made based on the information contained in the assessment.

4. MODEL-BASED DIAGNOSIS WITH FAILURE ASSESSMENTS

The initial construction of the system description related to model-based diagnosis constitutes a disadvantage. To automate this task, we propose a mapping function associating entries from failure assessments to propositional clauses to form an abductive *KB* (Wotawa, 2014). Risk analysis tools provide a systematic and comprehensive identification, review, and evaluation of possible threats or hazards. Usually, the assessment comprises the risk sources, consequences, magnitude, and likelihood (Ayyub, 2014). While there is a distinction between failure and fault mode, we use these terms synonymously throughout the paper.

In previous work we have focused on the modeling process based on FMEA (Wotawa, 2014; Koitz & Wotawa, 2015b), while in this research we further discuss FMEA in comparison to other failure assessments common in practice, namely FTA and a PoF approach and show how these can be used for model generation. In particular, the upcoming subsections describe the methods, how the knowledge can be translated into a propositional Horn theory as well as the advantages and disadvantages of each failure assessment in regard to constituting the basis of an abductive knowledge base.

4.1. Failure Mode Effect Analysis

FMEA is an established standardized reliability tool in which components are systematically assessed in regard to their possible failure modes. These rigorous and comprehensive reliability and safety design evaluations are usually required by industry standards or government policies (Vogl, Weiss, & Donmez, 2014). Generally, the objectives of an FMEA include the identification and prevention of failures and safety hazards, minimization of performance loss, development of preventive maintenance plans, and the usage for diagnostic techniques (Carlson, 2014). The reasoning is performed in an inductive bottom-up manner, where the general theories are derived from detailed examples on various levels of depth. Besides determining component-based single faults, each failure mode is examined in regard to its causes, detection mechanisms, and consequences. Further, the assessment encompasses fault probabilities and severity ratings. As detailed knowledge about the system structure, the requirements, the behavior of the components as well as their oper-

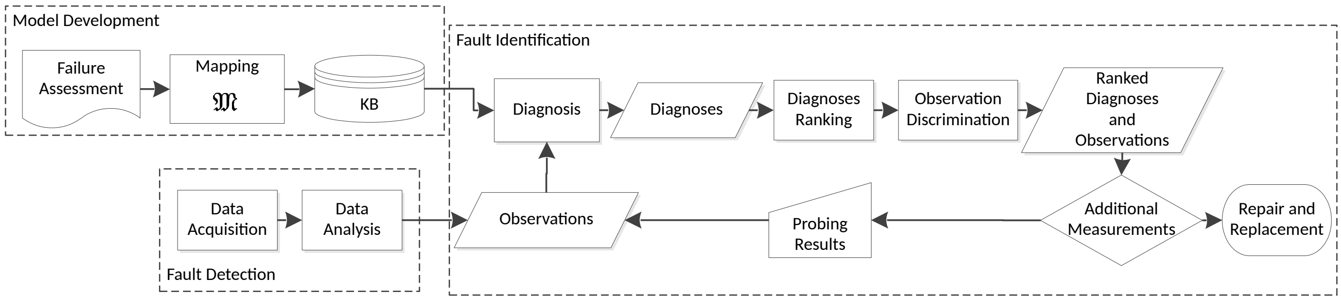

Figure 1. Process for incorporating abductive model-based diagnosis in an industrial setting.

ational relationship is necessary, such a review is conducted by a team of specialists (Rausand & Høyland, 2004).

In case the criticality of each failure mode is identified the technique is referred to as Failure Mode, Effects, and Criticality Analysis (FMECA). The criticality of a failure encompasses how hazardous or serious the caused interference is and is determined by the occurrence likelihood and the severity of the fault. Even though there are slight differences between the various FMEA/FMECA standards (Mode, 2002; Vogl et al., 2014), both analyses result in a detailed document with a tabulation of components and their single point failures as well as consequences. Frequently, the results can be utilized qualitatively as a hazard analysis method or quantitatively considering the various ratings (Liu, 2016).

The parts of an FMEA differ depending on the followed standard or guideline. However, certain parts are usually incorporated (Carlson, 2014):

- Component/Item: The component or item determines the artifact being analyzed.
- Failure Mode: The potential failure mode encompasses the manner in which the component potentially fails to deliver its intended function with the desired performance at various levels of depth within the system.
- Failure Cause: A failure cause describes the internal and external influences as well as their interaction which may lead up to the failure mode such as wear, aging, defective material, or damage.
- Failure Effect: Effects are failure consequences and have to be considered at various levels such as local effects or impacts on the overall system and operation.
- Detection Method and Rating: Often a particular detection mechanism is recorded, such as automated warnings as well as alarms or the discovery by a human operator. Additionally, a rating is applied to account for the detectability of a failure, i.e. the likelihood of discovery. Evident failures are detected instantly when they occur, while hidden failures can usually only be confirmed through testing.
- Severity: To quantify the analysis a severity rating is included, based on the most serious failure consequences.
- Occurrence: The occurrence rating associates a failure with the likelihood of its presence.
- Risk Priority Number (RPN): The RPN is the arithmetic product of severity, occurrence and detection ratings.
- Actions: The actions are recommended efforts to reduce or eliminate the risk associated with the cause of a failure.

Table 1 depicts an excerpt of an exemplary FMEA for the yaw drive of a wind turbine. As can be seen, not all columns described previously are present within the analysis. Yet, the most important information for the mapping, i.e. component, failure mode and effects, are included.

4.1.1. Model Development

Formally, we create an abductive knowledge base. As the failures recorded in the FMEA represent the connections between single faults and a conjunction of effects, we can create a theory consisting of definite propositional Horn clauses (Wotawa, 2014). This limitation of the expressiveness of the logical model leads to an avoidance of some of the computational inefficiencies inherent to abduction in general (Nordh & Zanuttini, 2008).

We previously presented this modeling methodology, thus, the following definitions are equivalent to the ones proposed in Wotawa (2014). For model creation we simplify the FMEA to three essential columns, namely the one featuring the set of components *COMP*, their potential failure modes *MODES*, and the set of failure effects forming a subset of the set of propositional variables *PROPS*.

Definition 5 *An FMEA is a set of tuples* (C, M, E) *where* $C \in$ *COMP is a component,* $M \in$ *MODES is a failure mode, and* $E \subseteq$ *PROPS is a set of effects.*

Table 1. *Example 1:* FMEA excerpt (adapted from Rademakers et al. (1993)).

Component	Failure Mode	Failure Effect	Failure Cause	Likelihood	Severity	Detection Method
Yaw Drive	Fails to rotate	No yaw, failure of safety system, decrease of efficiency	Motor not electrically powered, Motor burned after emergency stop, Yaw drive disconnected from frame, mechanical damage, fatigue fracture, capacitors burned during emergency stop	$2.2\mathrm{E}-5$	3	Visual inspection
Yaw Drive	Yaw shaft blocked	No yaw, decrease of efficiency	Motor not electrically powered, Motor burned after emergency stop, Yaw drive disconnected from frame, mechanical damage, fatigue fracture, capacitors burned during emergency stop	$1.3\mathrm{E}-5$	3	Visual inspection

As abductive reasoning relies on a formalization of failures and their symptoms, the conversion of an FMEA to a propositional *KB(A,Hyp,Th)* is straightforward. First, we create the set of hypotheses. In the FMEA each component-failure mode pair represents a possible cause. Each pair is mapped to a propositional variable *mode(C,M)*, where *C* is the component and *M* is the failure mode. This propositional variable is then added to the set *Hyp*. Equation (5) defines *Hyp* in this modeling context.

$$Hyp =_{def} \bigcup_{(C,M,E)\in \mathit{FMEA}} \{\mathit{mode}(C,M)\} \tag{5}$$

Second, the set *A* then is simply the union over all hypotheses as well as propositional variables representing effects as shown in Eq. (6).

$$A =_{def} \bigcup_{(C,M,E)\in \mathit{FMEA}} E \cup \{\mathit{mode}(C,M)\} \tag{6}$$

Example 1 (cont.): Considering the FMEA in Table 1, there are two component-failure mode pairs forming the set *Hyp*:

$$Hyp = \left\{ \begin{array}{c} \textit{mode(Yaw\_Drive, Fails\_to\_rotate)}, \\ \textit{mode(Yaw\_Drive, Shaft\_blocked)} \end{array} \right\}$$

The set of all propositional variables then contains the hypotheses as well as all propositional variables constituting effects.

$$A = \left\{ \begin{array}{c} \textit{mode(Yaw\_Drive, Fails\_to\_rotate)}, \\ \textit{mode(Yaw\_Drive, Shaft\_blocked)}, \\ \textit{no\_yaw, failure\_safety\_system}, \\ \textit{decrease\_of\_efficiency} \end{array} \right\}$$

Lastly, the propositional theory is determined by the relation between defects and their manifestations as depicted in the FMEA. For each record of the FMEA the mapping function $\mathfrak{M} : 2^{\mathit{FMEA}} \mapsto HC$ generates a Horn clause as a subset of the set of Horn clauses HC.

Definition 6 *Given an FMEA, the function $\mathfrak{M}$ is defined as follows:*

$$\mathfrak{M}(\mathit{FMEA}) =_{def} \bigcup_{t\in \mathit{FMEA}} \mathfrak{M}(t) \tag{7}$$

where

$$\mathfrak{M}(C, M, E) =_{def} \{\mathit{mode}(C, M) \rightarrow e \,|e \in E\} \tag{8}$$

Example 1 (cont.): The theory then simply comprises Horn clauses where a single hypothesis implies one of its effects.

$$Th = \left\{ \begin{array}{c} \textit{mode(Yaw\_Drive, Fails\_to\_rotate)} \rightarrow \textit{no\_yaw}, \\ \textit{mode(Yaw\_Drive, Fails\_to\_rotate)} \\ \rightarrow \textit{failure\_safety\_system}, \\ \dots \end{array} \right\}$$

4.1.2. Advantages and Limitations

The application areas of FMEA are widespread as it can be applied to complex systems. Its representation can form a comprehensive knowledge base for failures in each part of the system, explaining their effects on subcomponents that are dependent on them and the entire system (Hawkins & Woollons, 1998b). Thus, the mapping to an abductive model can be automated in a simple manner. Due to the structure of the FMEA, the resulting system descriptions are acyclic and contain solely bijunctive clauses, i.e implications always lead from one hypothesis to a single effect variable. These types of models require polynomial time when used for computing abductive diagnoses (Koitz & Wotawa, 2015c). In addition as FMEA usually considers single faults, the resulting diagnostic system holds the single fault assumption.

Furthermore, the analysis holds additional information which can be incorporated in the diagnosis process such as data on failure occurrence likelihood or severity. Those can be integrated into the diagnosis ranking procedure to prioritize probable or severe defects. However, these ratings are often subjective, thus, they should merely be considered as a means to focus on a subset of diagnoses and not as a discrimination criteria.

Since abductive diagnosis depends on the premise of model completeness, we assume that all significant fault modes for each contributing part of the system are being considered in the analysis. Furthermore, our mapping approach expects consistent effect descriptions, i.e. a symptom is represented in a uniform way throughout the FMEA. Of course, in order to count as an observation within the diagnostic process, each effect mentioned in the analysis has to be detectable in nature.

FMEA does not take into account the potential interdependencies between various failure modes and effects. While the absence of interconnections between failures may apply to some systems or subsystems, a generalization is not correct (Lee, 2001; Medina-Oliva, Iung, Barberá, Viveros, & Ruin, 2012). Thus, depending on the underlying assessment artifact, the analysis might not depict the causal relations in its entirety. Furthermore, as the set of effects corresponding to a failure is represented by a conjunction, the contrary measure of any of these manifestations results in a discrimination of the failure mode. Assume for *Example 1* that even though there is no yaw and a decrease in efficiency, the safety system does not fail. Then the Δ-Set would contain *mode(Yaw_Drive, Shaft_blocked)* but not *mode(Yaw_Drive, Fails_to_rotate)* as the Horn theory requires in case of the yaw drive failing to rotate that the safety systems fails.

4.2. Fault Tree Analysis

Fault trees provide a systematic sequence of events leading to an incident of interest, i.e. the top event. By employing a top-down approach the analysis reasons from effects to causes. Starting at the root the chain of events prompting the undesired event at the top is determined in a deductive manner. Besides basic events forming the leafs of the fault tree, intermediate incidents leading up to the top event are considered (Rausand & Høyland, 2004). Logic gates describe the relations between these events. Each gate has a set of basic or intermediate failures as input and the output is defined by a single event. Thus, the tree represents logical paths of cause-effect relationships (Vesely, Goldberg, Roberts, & Haasl, 1981).

Based on information on event likelihood, the tree can be quantified. To compute the frequency of the top event, the probabilities of each output event are determined by the gates and the input events' probabilities in a bottom-up manner. Thus, it is apparent that for the basic events the probabilities have to be know (Rausand & Høyland, 2004).

Figure 2 shows an exemplary systematic chain of events leading to insufficient lubrication of a gearbox in a wind turbine. The depicted fault tree has a top event (*Insufficient lubrication*), three basic events (*Oil filter failure*, *Leakage/Cracks of cooler* and *Rusty cooling fins of radiator*) and one intermediate event (*Poor cooling*). These incidents are connected by an OR as well as an AND gate. The former states that either the

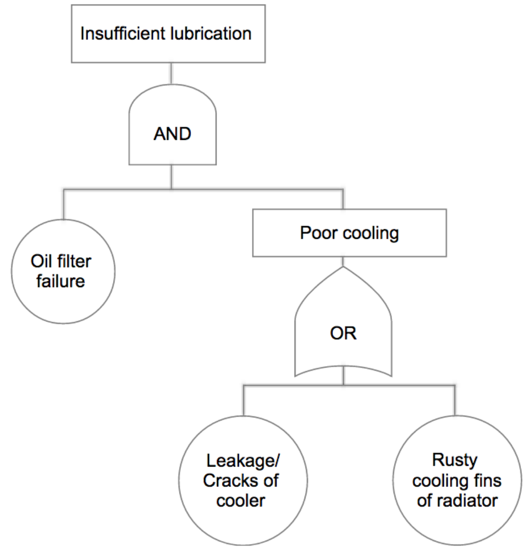

Figure 2. *Example 2:* Fault Tree (adapted from Márquez et al. (2012); Botsaris et al. (2012)).

Leakage/Cracks of cooler or *Rusty cooling fins of radiator* or both must occur, to cause *Poor cooling*, while the latter states that for *Insufficient lubrication* to arise both *Poor cooling* and *Oil filter failure* are necessary to appear.

4.2.1. Model Development

While there are several logic gates and symbols available in fault trees, we focus in our analysis on a simple fault tree representation with three types of events (basic, intermediate, top) and the two most common gates, i.e. AND and OR. We assume that each system is described by a set of fault trees *T*. Each fault tree describes the event combinations leading to a top event which represents a certain effect of interest.

Definition 7 *A fault tree FT is a pair $(G, \mathcal{E})$ where G is a set of logic gates and $\mathcal{E}$ a set of events. $\mathcal{BE} \subset \mathcal{E}$ is the set of basic events, while $\epsilon \in \mathcal{E}$ is the top event. $\Omega(I, \omega) \subseteq G$ denotes the set of OR gates and $\mathcal{A}(I, \omega) \subseteq G$ the set of AND gates, where $I \subseteq \{\mathcal{E} \setminus \epsilon\}$ is the set of input events and $\omega \in \{\mathcal{E} \setminus \mathcal{BE}\}$ the output event.*

As a fault tree is a pictorial representation of a Boolean formula depicting how the top event is caused by other events, we can simply transform the tree into a set of clauses by determining the Boolean expression for each gate. Each event corresponds to a propositional variable in *A*. In our case, we assume that the basic events represent the initial root causes, thus, we limit the set of hypotheses to only comprise propositional variables corresponding to these primary events. The relevant sets *A* and *Hyp* are defined the following way:

$$A =_{def} \bigcup_{e \in \mathcal{E}} \{e\} \tag{9}$$

$$Hyp =_{def} \bigcup_{\beta \in \mathcal{BE}} \{\beta\} \tag{10}$$

In case intermediate events depict failures which should be diagnosable, we would define the set *Hyp* as $\{\mathcal{E} \setminus \epsilon\}$.

Example 2 (cont.): For the fault tree in Figure 2 we can record the following set of propositional variables and hypotheses:

$$A = \left\{ \begin{array}{c} \textit{Insufficient\_lubrication}, \textit{Oil\_filter\_failure}, \\ \textit{Poor\_cooling}, \textit{Leakage\_cracks\_of\_cooler}, \\ \textit{Rusty\_cooling\_fins\_of\_radiator} \end{array} \right\}$$

$$Hyp = \left\{ \begin{array}{c} \textit{Oil\_filter\_failure}, \textit{Leakage\_cracks\_of\_cooler}, \\ \textit{Rusty\_cooling\_fins\_of\_radiator} \end{array} \right\}$$

We have a mapping function $\mathfrak{M}_{FTA} : 2^{FT} \mapsto HC$, creating for each fault tree a set of Horn clauses based on the gates comprising the tree.

$$\mathfrak{M}_{FTA}(FT) =_{def} \bigcup_{g \in G} \mathfrak{M}(g) \tag{11}$$

where

$$\mathfrak{M}_{FTA}(g) = \begin{cases} \bigcup_{i \in I} \{i \rightarrow \omega\}, & g \in \Omega(I, \omega) \\ \bigwedge_{i \in I} i \rightarrow \omega, & g \in \mathcal{A}(I, \omega) \end{cases} \tag{12}$$

In case of an OR gate, for each input event a Horn clause is created where the input implies the gate's output. As the AND gate represents the relation that all inputs have to be present in order for the output event to occur, a single implication is added, such that a conjunction of the variables representing the inputs leads to the output event. The theory of the abductive *KB* then is the union over all Horn clauses generated over the gates of the fault tree.

Example 2 (cont.): Thus, considering the gates of *Example 2* the resulting theory of the fault tree is as follows:

$$Th = \left\{ \begin{array}{c} \textit{Oil\_filter\_failure} \land \textit{Poor\_cooling} \\ \rightarrow \textit{Insufficient\_lubrication}, \\ \textit{Leakage\_cracks\_of\_cooler} \rightarrow \textit{Poor\_cooling}, \\ \textit{Rusty\_cooling\_fins\_of\_radiator} \rightarrow \textit{Poor\_cooling} \end{array} \right\}$$

Note that the resulting *KB*, however, encompasses solely the information of a single tree. Thus, to create an entire system model the knowledge bases resulting from each tree in the system have to be combined into a single *KB*.

4.2.2. Advantages and Limitations

Fault trees provide a clear and logical representation of cause-effect relations between combinations of events. In order to produce a meaningful abductive theory which can be utilized in diagnosis, each basic event has to represent a failure or cause. Further, for each diagnosable effect there has to be a fault tree where the top event represents the symptom. As with the FMEA a coherent description of the failures throughout the fault trees of the systems has to be guaranteed for an automatic model creation. Additionally, since it is a top-down approach, the analysis has to ensure that all contributors, i.e. failures, for a particular effect have been considered within the assessment to secure completeness.

Since we assume that the fault trees contain only AND as well as OR gates, the created theories can feature a disjunction and conjunction of hypotheses. Thus, the models are Horn, however, in contrast to the FMEA models they do not feature a bijunctive form. It is apparent that due to the knowledge encompassed within the fault tree, the resulting models are more expressive than the ones generated on top of an FMEA, i.e. the information stored in a fault tree can depict more relations than an FMEA due to the different logical connections that can be represented. In case of a quantitative analysis of the fault tree, the prior probability of the basic events are to be known. Thus, this knowledge can be utilized in the diagnostic context to compute diagnosis probabilities as described in Section 2.

The relation between FTA and abductive reasoning is worth mentioning. A (subset) minimal cut set (MCS) encompasses a possible combination of basic events that lead to the top event (Rausand & Høyland, 2004). As a MCS is the prime implicant of the top event, it is equivalent to an abductive diagnosis for the observation of the top event (Bobbio, Montani, & Portinale, 2002).

Example 2 (cont.): Given the fault tree, the MCSs are $\{$*Oil_filter_failure, Leakage_cracks_of_cooler*$\}$ and $\{$*Oil_filter_failure, Rusty_cooling_fins_of_radiator*$\}$, which in fact are the diagnoses given the *KB* and *Obs* $=$ $\{$*Insufficient_lubrication*$\}$.

4.3. Physics of Failure

The PoF approach to reliability analyzes root causes of failures and utilizes theoretical models capturing the relation between operational and environmental loads as well as damage accumulation rates (Pascoe, 2011). Thus, these mathematical models have to represent the physics inherent to the damage process. Based on the knowledge on failure mechanisms and potential degradation in addition to life cycle stress information, estimates can be made in regard to the probability of certain failures for a component or product under investigation (Pecht & Dasgupta, 1995; Oh et al., 2010).

Table 2. *Example 3:* Failure Mode Assessment (FMA) of the Converter.

Fault Mode	**Component**	**Damage Promoting Operating Mode**	**Aggravating Boundary Conditions**	**State Indicators/Part Inspection**
Electrical chemical aging	Buck Boost - Electrolyte Capacitor	Partial load	High ambient temperature	(T_power_cabinet *OR* P_turbine) *AND* Equivalent series resistance higher
Corrosion	Fan - Pin	Full load	Saline environment, high temperature environment	T_cabinet *OR* P_turbine
Thermo-mechanical fatigue (TMF)	Fan - Bearing Running Surface	Start Up/ Shut Down, Transient current/voltage events	Light winds (frequent start up and shot down), changing wind direction (yaw adjustment)	T_cabinet *AND* P_turbine
High-cycle fatigue (HCF)	IGBT - Wire Bonding	Start Up/ Shut Down, Transient current/voltage events	Low ambient temperature	T_inverter_cabinet *OR* T_nacelle *OR* P_turbine

C. Gray, Langmayr, Haselgruber, and Watson (2011) describe a failure mode assessment (FMA) combining diagnostic and prognostic techniques. Their method relies on a structured evaluation of faults, in particular, physical and chemical failure mechanisms, and their manifestations. In order to create a comprehensive assessment of a system, it is decomposed into its subcomponents. Each part is then analyzed in regard to its potential failure modes as well as the damage driving physics. To ensure a complete depiction of the system, top-down and bottom-up reasoning are incorporated to determine failure relevant operational and environmental boundary conditions. For each combination of failure mode and component, a mathematical model is used to calculate the rate at which damage accumulates in response to the operating environment. The approach is similar to Failure Modes, Mechanisms and Effects Analysis (FMMEA) (Ganesan, Eveloy, Das, & Pecht, 2005) as it emphasizes the evaluation of damage driving conditions. The FMA method differentiates between automatically retrieved state indicators such as Supervisory Control and Data Acquisition (SCADA) results and measurements from inspections (C. S. Gray & Watson, 2010). In contrast to FMEA or FMMEA, the evaluation considers a more detailed view on the relationships between failure effects. By incorporating logical connections, namely AND as well as OR, the description of effects is a Boolean expression representing which consequences are observed in case of a fault and how these are linked.

Table 2 shows parts of an FMA produced by an expert group during a system analysis for the converter of an industrial wind turbine. As can be seen the analysis encompasses the failure mechanism, i.e. fault mode, the component, the operation and environmental conditions promoting the damage as well as the effects which are on the one hand state indicators automatically retrieved from a condition monitoring system as well as manual part inspections.

4.3.1. Model Development

As we are creating propositional Horn clauses to form a *PHCAP*, some adjustments to the information stored in the FMA have to made. Again we can use three sources of information for modeling: the set of components *COMP*, their potential fault modes *MODES*, and the Boolean formulas *FORM* describing the connection between the state indicators and part inspections.

Definition 8 *An FMA is a set of tuples (C, M, ϕ) where $C \in$ COMP is a component, $M \in$ MODES is a fault mode, and $\phi \in$ FORM is the Boolean expression relating effects to one another.*

Example 3 (cont.): The first entry of the FMA in Table 2 results in the following tuple:

(Buck_Boost, Electrical_chemical_aging,
(T_power_cabinet $\vee$ P_turbine) $\wedge$
Equivalent_series_resistance_higher)

Since the effects can be connected by disjunctions, a simple mapping to Horn clauses as with the FMEA is not possible. As a disjunction of effects implies that at least one of these manifestations is present in case of the failure, a mapping to conjunctions, as Horn clauses would require, is inadequate. Thus, the underlying information has to be preprocessed in a new FMA which we denote FMA$_p$. The first step is to ensure that each Boolean expression in the effect description is in disjunctive normal form (DNF), i.e. each formula is a disjunction of conjunctions. This can be simply achieved by applying the laws of Boolean algebra. Let us assume that there is a function *DNF* converting a Boolean expression ϕ into its DNF form:

$$\forall \phi \in \mathit{FORM} : \phi' = \mathit{DNF}(\phi) \tag{13}$$

Thus, each tuple $(C, M, \phi') \in \mathit{FMA}_p$ now contains the DNF formula ϕ' of ϕ.

Example 3 (cont.): For the first entry, we can record ϕ' as

$$\textit{(T\_power\_cabinet} \wedge \textit{Equivalent\_series\_resistance\_higher)} \vee$$
$$\textit{(P\_turbine} \wedge \textit{Equivalent\_series\_resistance\_higher)}$$

In the second step we create for each record, where ϕ' consists of a disjunction, a new fault mode M_c for each conjunction $c \in \phi'$. Each resulting tuple (C, M_c, c) is added to FMA$_p$. It is apparent that each original tuple (C, M, ϕ') has to be removed subsequently from FMA$_p$.

Example 3 (cont.): The Boolean expression in DNF of the first entry comprises a disjunction with two conjunctions, i.e. *(T_power_cabinet ∧ Equivalent_series_resistance_higher)* and *(P_turbine ∧ Equivalent_series_resistance_higher)*. Thus, for each of the conjunctions a new fault mode M_c is generated and the resulting tuples of the form (C, M_c, c) are:

$$\textit{(Buck\_Boost, Electrical\_chemical\_aging\_1,}$$
$$\textit{T\_power\_cabinet} \wedge \textit{Equivalent\_series\_resistance\_higher)}$$

and

$$\textit{(Buck\_Boost, Electrical\_chemical\_aging\_2,}$$
$$\textit{P\_turbine} \wedge \textit{Equivalent\_series\_resistance\_higher)}$$

It is apparent that the number of records within the FMA$_p$ is increased in regard to the primary FMA, as each DNF formula can be exponentially larger than its original. Table 3 shows the processed FMA$_p$ of *Example 3*. Then, the mapping $\mathfrak{M}_{FMA} : 2^{FMA_p} \mapsto HC$ is similar to $\mathfrak{M}$ and the composition of *Hyp* (Eq. (16)) and *A* (Eq. (17)) is analog to the FMEA modeling.

Definition 9 *Given an FMA$_p$, the function $\mathfrak{M}_{FMA}$ is defined as follows:*

$$\mathfrak{M}_{FMA}(FMA_p) =_{def} \bigcup_{t \in FMA_p} \mathfrak{M}(t) \tag{14}$$

where

$$\mathfrak{M}_{FMA}(C, M_c, c) =_{def} \{mode(C, M_c) \rightarrow v \,|v \in c\} \tag{15}$$

$$Hyp =_{def} \bigcup_{(C,M_c,c) \in FMA_p} \{mode(C, M_c)\} \tag{16}$$

$$A =_{def} \bigcup_{(C,M_c,c) \in FMA_p} \{mode(C, M_c)\} \cup \bigcup_{v \in c} v \tag{17}$$

Example 3 (cont.): Applying Eq. (16), Eq. (17) and $\mathfrak{M}_{FMA}$ to the FMA$_p$ in Table 3 results in the following *KB*:

$$Hyp = \left\{ \begin{array}{c} \textit{mode(Buck\_Boost, Electrical\_chemical\_aging\_1)}, \\ \textit{mode(Buck\_Boost, Electrical\_chemical\_aging\_2)}, \\ \textit{mode(Fan\_Pin,Corrosion\_1)}, \ldots \end{array} \right\}$$

$$A = \left\{ \begin{array}{c} \textit{mode(Fan\_Pin,Corrosion\_1)}, \\ \textit{T\_power\_cabinet, P\_turbine}, \ldots \end{array} \right\}$$

$$Th = \left\{ \begin{array}{c} \textit{mode(Buck\_Boost, Electrical\_chemical\_aging\_1)} \\ \rightarrow \textit{T\_power\_cabinet}, \\ \textit{mode(Buck\_Boost, Electrical\_chemical\_aging\_1)} \\ \rightarrow \textit{Equivalent\_series\_resistance\_higher}, \\ \textit{mode(Buck\_Boost, Electrical\_chemical\_aging\_2)} \\ \rightarrow \textit{P\_turbine}, \\ \ldots \end{array} \right\}$$

It is apparent that in case the diagnoses are computed, these do not contain the original fault modes, but the additionally created ones of the second transformation step. Thus, these have to be mapped back once the explanations have been computed. Note here, that due to the creation of the auxiliary hypotheses the abductive solutions when converted back to the original fault modes might not be minimal and subsequently supersets have to be removed.

4.3.2. Advantages and Limitations

Due to describing the logical relations between effects, a more detailed representation of the real physical interconnections within a system is possible. Further, the FMA takes into account the gradual degradation of components over their lifetime and thus allows in the succeeding refinements of the initial diagnosis result to consider historic data of the life cycle stress of a part in addition to the damage model. Hence, a combination of the diagnosis and prognosis process is possible, such that the current component condition can identify failures more probable.

As the *PHCAP* requires a Horn theory, some conversions are necessary which may involve an exponential explosion of the formula and a growing number of hypotheses. Besides the computational effort increasing, the solutions generated based on the theory might not be minimal once transformed back to the original hypotheses space. Therefore, additional superset checks are required at the end to ensure parsimonious diagnoses. Furthermore, due to the inclusion of disjunctions between effects, the discrimination capability of probing is limited to a certain extend.

5. DISCUSSION

Depending on the utilized assessment, the resulting models differ in their structure and expressiveness. The Horn theory constructed from the information stored within an FMEA is the most straightforward and simple, as each clause represents a causal relation between a single failure and a single effect. Due to the consequences of a cause being related by conjunctions, the produced models are rather strict in the sense that in case the opposite of one manifestation out of the effect set is perceived, the corresponding cause is no longer a viable part of a diagnosis. Thus, the associated hypothe-

Table 3. *Example 3 (cont.):* Processed Failure Mode Assessment (FMA$_p$) of the Converter.

Fault Mode	**Component**	**Damage Promoting Operating Mode**	**Aggravating Boundary Conditions**	**State Indicators/Part Inspection**
Electrical chemical aging 1	Buck Boost - Electrolyte Capacitor	Partial load	High ambient temperature	T_power_cabinet *AND* Equivalent series resistance higher
Electrical chemical aging 2	Buck Boost - Electrolyte Capacitor	Partial load	High ambient temperature	P_turbine *AND* Equivalent series resistance higher
Corrosion 1	Fan - Pin	Full load	Saline environment, high temperature environment	T_cabinet
Corrosion 2	Fan - Pin	Full load	Saline environment, high temperature environment	P_turbine
Thermo-mechanical fatigue (TMF)	Fan - Bearing Running Surface	Start Up/ Shut Down, Transient current/voltage events	Light winds (frequent start up and shot down), changing wind direction (yaw adjustment)	T_cabinet *AND* P_turbine
High-cycle fatigue (HCF) 1	IGBT - Wire Bonding	Start Up/ Shut Down, Transient current/voltage events	Low ambient temperature	T_inverter_cabinet
High-cycle fatigue (HCF) 2	IGBT - Wire Bonding	Start Up/ Shut Down, Transient current/voltage events	Low ambient temperature	T_nacelle
High-cycle fatigue (HCF) 3	IGBT - Wire Bonding	Start Up/ Shut Down, Transient current/voltage events	Low ambient temperature	P_turbine

ses have to be removed from all solutions. In practice this signifies that observation data have to be preprocessed to remove noise or account for inaccurate measurements to ensure that feasible fault modes are not discriminated prematurely. As the FMEA comprises certain information on occurrence likelihood and severity or criticality, additional improvements to the diagnosis results are possible. Ideally, a-priori failure probabilities are known from manufacturers or historic data. However, even ratings, as are very commonly used in FMEA, can indicate a prioritization. Particularly severity or criticality can signify failures most paramount in regard to safety or economic considerations.

In comparison to the FMEA-based models, fault trees can express a wider range of situations by allowing to represent the combination of events. To create a *KB* for an entire system, the modeling requires a fault tree for each possible observation and subsequently the knowledge bases have to be joined in a comprehensive system description. In case the FTA is quantitative, the probabilities of the basic events corresponding to hypotheses can be incorporated to determine cause likelihoods. Interesting enough to create abductive diagnoses a mapping to a *KB* is not necessary, as we could exploit the notion of MCS. Assume a *PHCAP* with $Obs = \{o_1, \ldots, o_n\}$ and for each $o_i \in Obs$ there is a fault tree $ft_i \in \mathcal{T}$ with ϵ corresponding to o_i. To obtain an MCS equivalent to the abductive explanations for the given problem, the fault trees need to be joined. A combined fault tree with a new top event ex is introduced with a gate $\alpha \in \mathcal{A}(I, \omega)$ such that $\omega = \{ex\}$ and $I = \bigcup_{ft_i \in \mathcal{T}} \epsilon$. The MCSs of ex then constitute the prime implicants or minimal abductive diagnoses of the *PHCAP*.

The last approach combines prognosis and diagnosis by determining damage models for recorded fault modes. As FMA allows to express the combination of effects with disjunctions a simple mapping to a Horn theory is not possible. Thus, a conversion prior to model creation is necessary. The disadvantage is that the resulting processed model might be exponentially larger than the original assessment due to the transformation, that the resulting diagnoses have to be mapped back to the initial causes and that finally subset checks have to be performed to ensure minimal explanations. Note that there are other abduction frameworks, which do not restrict their underlying models to feature a Horn structure and thus not require a conversion for this type of knowledge. The main benefit of the FMA is the prognosis capabilities based on the knowledge of failure mechanisms and life cycle stress. In comparison to the other methods, the incorporation of information of time to failure, allows a more accurate ranking of diagnoses.

Essentially, the advantages and disadvantages of the underlying assessments are not only inherent in the type of relation they are capable of expressing, but also in the incorporated additional information they hold. In particular, any ranking information can be viable to determine probable or critical diagnoses. It is apparent that the quality of the model automatically generated is largely depended on the underlying failure assessment. Failure modes or effects not considered in the analysis, are absent in the abductive model and thus diagnoses involving those cannot be uncovered. Model completeness is a primary requirement, thus, an essential aspect is a systematic and comprehensive review of the system to achieve a high coverage of faults and their consequences (Milde et al., 2000). Certain assumptions are fundamental to our approach, e.g. to ensure the feasibility of an automatic creation of the model, manifestations and failures have to be coherently reported throughout the assessment and consequences have to be detectable in order to be useful in a diagnostic context.

6. CONCLUSION

Model-based diagnosis requires a description of the system under consideration to determine causes for symptoms observed. Although applications have been developed for various domains, the need to construct a suitable model remains a hindering factor in the adoption of these approaches. Therefore, we propose to exploit failure assessments already available in practice to generate the formalizations which are necessary for abductive model-based diagnosis.

We discuss three different analysis methods, namely FMEA, FTA and an approach based on PoF, in regard to their capabilities to form the basis of an abductive diagnosis process. Depending on the assessment, the resulting models feature different characteristics as well as expressiveness and further the additional information included can be utilized in successive refinements of the initial diagnosis.

To analyze the suitability of the modeling methodology and the diagnosis refinements, evaluations on practical failure assessments are planned. In particular, an investigation of the combination of the Pof approach and our diagnosis process within the domain of industrial wind turbine should reveal the practicability of the integration of failure assessments in the diagnosis process as well as the incorporation of model-based diagnosis into an industrial setting.

ACKNOWLEDGMENT

The work presented in this paper has been supported by the FFG project Applied Model Based Reasoning (AMOR) under grant 842407. We would further like to express our gratitude to our industrial partner, Uptime Engineering GmbH.

REFERENCES

Ayyub, B. M. (2014). *Risk analysis in engineering and economics*. CRC Press.

Bobbio, A., Montani, S., & Portinale, L. (2002). Parametric dependability analysis through probabilistic horn abduction. In *Proceedings of the Nineteenth conference on Uncertainty in Artificial Intelligence* (pp. 65–72).

Botsaris, P. N., Konstantinidis, E., & Pitsa, D. (2012). Systemic assessment and analysis of factors affect the reliability of a wind turbine. *Journal of Applied Engineering Science (Istrazivanja i projektovanja za privredu)*, *10*(2).

Carlson, C. S. (2014). Understanding and applying the fundamentals of FMEAs. In *Proceedings of the 2014 Annual Reliability and Maintainability Symposium.*

Console, L., & Dressler, O. (1999). Model-based diagnosis in the real world: lessons learned and challenges remaining. In *Proceedings* 16^{th} *International Joint Conf. on Artificial Intelligence* (pp. 1393–1400).

Console, L., Dupre, D. T., & Torasso, P. (1991). On the Relationship Between Abduction and Deduction. *Journal of Logic and Computation*, *1*(5), 661–690. doi: 10.1093/logcom/1.5.661

Cordier, M.-O., Dague, P., Lévy, F., Montmain, J., Staroswiecki, M., & Travé-Massuyès, L. (2004). Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, *34*(5), 2163–2177.

de Kleer, J., & Williams, B. C. (1987). Diagnosing multiple faults. *Artificial Intelligence*, *32*(1), 97–130.

Friedrich, G., Gottlob, G., & Nejdl, W. (1990, September). Hypothesis classification, abductive diagnosis and therapy. In *Proceedings of the International Workshop on Expert Systems in Engineering.* Vienna: Springer Verlag, Lecture Notes in Artificial Intelligence, Vo. 462.

Ganesan, S., Eveloy, V., Das, D., & Pecht, M. (2005). Identification and utilization of failure mechanisms to enhance FMEA and FMECA. In *Proceedings of the IEEE workshop on accelerated stress testing & reliability (ASTR), austin, texas.*

Gray, C., Langmayr, F., Haselgruber, N., & Watson, S. J. (2011). A practical approach to the use of scada data for optimized wind turbine condition based maintenance. *EWEA Offshore Wind Amsterdam.*

Gray, C. S., & Watson, S. J. (2010). Physics of failure approach to wind turbine condition based maintenance. *Wind Energy*, *13*(5), 395–405.

Hawkins, P. G., & Woollons, D. J. (1998a). Failure modes and effects analysis of complex engineering systems using functional models. *Artificial Intelligence in Engineering*, *12*, 375–397.

Hawkins, P. G., & Woollons, D. J. (1998b). Failure modes and effects analysis of complex engineering systems using functional models. *Artificial Intelligence in Engineering*, *12*(4), 375–397.

Kakas, A. C., Kowalski, R. A., & Toni, F. (1992). Abductive logic programming. *Journal of logic and computation*, *2*(6), 719–770.

Koitz, R., & Wotawa, F. (2015a). Finding explanations: an empirical evaluation of abductive diagnosis algorithms. In *Proceedings of the international workshop on defeasible and ampliative reasoning (DARe-15).*

Koitz, R., & Wotawa, F. (2015b). From theory to practice: Model-based diagnosis in industrial applications. In *Proceedings of the annual conference of the prognostics and health management society 2015.*

Koitz, R., & Wotawa, F. (2015c). On the feasibility of abductive diagnosis for practical applications. In *9th IFAC symposium on fault detection, supervision and safety of technical processes.*

Lee, B. H. (2001). Using bayes belief networks in industrial fmea modeling and analysis. In *Reliability and maintainability symposium, 2001. proceedings. annual* (pp. 7–15).

Liu, D. (2016). *Systems engineering design principles and models*. CRC Press.

Márquez, F. P. G., Tobias, A. M., Pérez, J. M. P., & Papaelias, M. (2012). Condition monitoring of wind turbines: Techniques and methods. *Renewable Energy*, *46*, 169–178.

Marquis, P. (2000). Consequence finding algorithms. In *Handbook of defeasible reasoning and uncertainty management systems* (pp. 41–145). Springer.

McIlraith, S. A. (1998). Logic-based abductive inference. *Knowledge Systems Laboratory, Technical Report KSL-98-19*.

Medina-Oliva, G., Iung, B., Barberá, L., Viveros, P., & Ruin, T. (2012). Root cause analysis to identify physical causes. In *11th international probabilistic safety assessment and management conference and the annual european safety and reliability conference, PSAM11-ESREL 2012* (p. CDROM).

Milde, H., Guckenbiehl, T., Malik, A., Neumann, B., & Struss, P. (2000). Integrating model-based diagnosis techniques into current work processes–three case studies from the india project. *AI Communications*, *13*(2), 99–123.

Mode, P. F. (2002). Effects analysis in design (design FMEA) and potential failure mode and effects analysis in manufacturing and assembly processes (process fmea) reference manual. *Society of Automotive Engineers, Surface Vehicle Recommended Practice J*, *1739*.

Nordh, G., & Zanuttini, B. (2008). What makes propositional abduction tractable. *Artificial Intelligence*, *172*, 1245–1284.

Oh, H., Azarian, M. H., Pecht, M., White, C. H., Sohaney, R. C., & Rhem, E. (2010). Physics-of-failure approach for fan phm in electronics applications. In *Prognostics and health management conference, 2010. PHM'10.* (pp. 1–6).

Pascoe, N. (2011). *Reliability technology: Principles and practice of failure prevention in electronic systems*. John Wiley & Sons.

Pecht, M., & Dasgupta, A. (1995). Physics-of-failure: an approach to reliable product development. *Journal of the IES*, *38*(5), 30–34.

Poole, D., Goebel, R., & Aleliunas, R. (1987). *Theorist: A logical reasoning system for defaults and diagnosis*. Springer.

Price, C. J., & Taylor, N. S. (2002). Automated multiple failure fmea. *Reliability Engineering & System Safety*, *76*(1), 1–10.

Rademakers, L., Seebregts, A., & van Den Horn, B. (1993). *Reliability analysis in wind engineering*. Netherlands Energy Research Foundation ECN.

Rausand, M., & Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications* (Vol. 396). John Wiley & Sons.

Reiter, R. (1987). A theory of diagnosis from first principles. *Artificial Intelligence*, *32*(1), 57–95.

Struss, P., Malik, A., & Sachenbacher, M. (1996). Case studies in model-based diagnosis and fault analysis of car-subsystems. In *Proc. 1st int'l workshop model-based systems and qualitative reasoning* (pp. 17–25).

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault tree handbook* (Tech. Rep.). DTIC Document.

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014). Standards for prognostics and health management (phm) techniques within manufacturing operations. In *Annual conference of the prognostics and health management society, september.*

Wotawa, F. (2011). On the use of abduction as an alternative to decision trees in environmental decision support systems. *International journal of agricultural and environmental information systems*, *2*(1), 63–82.

Wotawa, F. (2014). Failure mode and effect analysis for abductive diagnosis. In *Proceedings of the international workshop on defeasible and ampliative reasoning (DARe-14)* (Vol. 1212). CEUR Workshop Proceedings.