Qualitative Modeling is the Key

A Successful Feasibility Study in Automated Generation of Diagnosis Guidelines and Failure Mode and Effects Analysis for Mechatronic Car Subsystems

P. Struss, A. Malik, M. Sachenbacher
Technical University of Munich
Orleansstr. 34, 81667 München, Germany
{struss, malik, sachenba}@informatik.tu-muenchen.de

Abstract

The paper presents objectives and results of a case study in computer support for failure mode and effects analysis and for the creation of repair manuals in the domain of automotive systems. Model-based prediction and diagnosis reflect the requirements of these tasks. More specifically, qualitative models of system components are necessary for both capturing the available knowledge and achieving the desired coverage and granularity of the analysis results. We describe models for parts of the anti-lock braking system (ABS) and the electronic diesel control (EDC), focusing on a qualitative approach to compositional modeling of the involved electrical circuits. The summarized results of the case study demonstrate the necessity and utility of qualitative models for the successful application of automated diagnosis to industrial problems.

1 Introduction

Cars are a classical example for a class of technical systems that comprises a large set of variants assembled from a repository of basic components. Knowledge-based systems that support tasks such as design, analysis, and diagnosis in this domain are worthless if they cannot solve this “variants’ dilemma”. In order to cover all variants of a certain subsystem, such systems have to be model-based. More specifically, they have to be based on

- a **compositional model**.

This means that a device model is obtained by assembling independent, context-free behavior models of components just like the device itself is assembled from a set of components - an aspect that is often ignored in academic work on model-based diagnosis. Furthermore, safety requirements demand for high standards in coverage and completeness of any automated analysis of causes and effects of faults, thus ruling out solutions that are based on purely empirical knowledge.

Failure mode and effects analysis (FMEA) aims at assessing the potential impact and origin of malfunctions for a **designed** artifact. Completeness and reliability of this step (which is often mandatory by law or a customer’s requirement) is obviously crucial under the aspects of safety, environment, and cost. Diagnosis as it happens in a garage is dealing with similar problems and requirements, but related to an existing **physical** artifact.

Since FMEA faces a blueprint (or at most a prototype) rather than a physical system that has been experienced before, experience-based expert systems cannot provide a solution for principled reasons. In fact, the same holds for the diagnostic task in the garage. Although experience can be gained over time and exploited, effective and fast diagnosis of new models and variants has to be assured, as well. Obviously, it cannot be (and is not) based on gaining experience as a result of trial and error. This applies even more to an important step in establishing an effective diagnostic practice in the field: the generation of diagnosis guidelines (sometimes called “repair manuals”) which are distributed to the mechanics in the garages.

In collaboration with Robert Bosch GmbH in Stuttgart, we carried out a case study to explore the feasibility of model-based support for the tasks of FMEA and generation of diagnosis guidelines. As subjects of the case study, the anti-lock braking system (ABS) and the electronic diesel control system (EDC), respectively subsets of them, were chosen.

The clear-cut success criteria for the feasibility study were

- the automated model-based **generation** of significant parts of
- an **FMEA** protocol for an **EDC subsystem** and
- the **diagnosis guideline** for an **ABS subsystem** and
- their **comparison** with the existing **respective documents**.

As a side-effect, the case study was expected to shed a light on the relation between the kinds of knowledge underlying the two tasks. Their very nature imposes additional requirements on the kind of models. This is because they have to make statements about **classes** of faults and symptoms rather than specific, individual ones. A study of respective documents confirms this principled consideration. Rather than starting diagnosis of a particular instance from a set of precisely measured variables (“signal for rotational speed of left front wheel equals 12.5 s^{-1}”), a diagnosis guideline for an ABS may list potential causes for “signal for rotational speed of left front wheel is too high” (represented by an errorcode stored in the control unit) or an even more qualitative symptom observed by the driver such as “vehicle drifts to the left when brakes are in operation”. Similarly, an FMEA for the EDC would link failure modes such as “pedal position sensor voltage too large, idle detection switch o.k." with failure causes like "potentiometer detuned towards upper bound" (without necessarily specifying the exact pedal position sensor voltage).

As a result, we had to develop

- **qualitative models**

in order to capture the available knowledge and to generate appropriate results, an aspect that is often ignored in work on model-based diagnosis in industrial environments.

This paper does not present new sophisticated theories or techniques for model-based prediction and automated diagnosis. On the contrary, one of the main insights we would like to convey is that for the tasks tackled here, fairly standard techniques described elsewhere completely suffice. This motivates focusing on modeling as the crucial precondition for successful applications - the second insight. How to find the "right models", is the question we want to shed a light on in the context of our case studies. Although we will briefly present a somewhat novel way of circuit modeling, we did not have to invent new qualitative modeling methods for the examples treated. (This may be the case, though, for other subsystems we have started work on).

In the following presentation, we focus mainly on electrical subsystems of the ABS and the EDC. Section 2 briefly describes the electric circuit of a basic ABS, illustrates contents of a respective diagnosis guidelines (2.1), and shows examples from an FMEA of the pedal position sensor of the EDC system (2.2).

Qualitative models for components of subsystems are presented in section 3, in particular an approach to modeling of electrical circuits based on local propagation of structural aspects, namely connectivity to sources and sink (3.1). Finally, we summarize the overall results of the feasibility study and discuss lessons learned.

2 Two Scenarios from the Case Study

In our work, as usual, we had to learn a lot about how the respective devices are designed and perform their function. An important principle was to carry out this knowledge aquisition **in the context of the respective tasks**, and for this purpose, the existing documents (FMEA protocols and diagnosis guidelines) were used as manifestations of requirements and knowledge and carefully analyzed. We present typical examples in the following subsections.

2.1 Diagnosis Guidelines for ABS

The purpose of the ABS is to prevent the wheels of the vehicle from locking up in order to enable the driver to steer the car while using the brakes. This is achieved by a control unit that reduces and increases pressure on the brake cylinders based on the measured rotational speeds of the wheels through appropriate actions of valves and pumps. Besides the hydraulic system, it comprises a subsystem for sensing the wheel speeds and transmitting the respective signals to the control unit. Although this has been an important part of our case study (since a similar technology is used for measuring the rotational speed of the motor in the EDC system, this allowed us to explore the reusability of models), we omit details here and concentrate on the actuation part.

Figure 1 shows the electrical topology of an ABS. Wire 30 (the one at the top) is battery, wire 15 (below) is ignition and wire 31 (at the bottom) is ground. Whenever the ECU (A1) accesses one of the three magnetic valves (VL, VR and HA) in the valve block (Y2) by connecting the respective wire to ground (via pin 3 of plug X2), the magnetic valve is activated, providing that the valve relay (K1) is closed, thus establishing a connection to the battery.

The section of the ABS repair manual shown in Table 1 lists the successive test steps to be performed by a

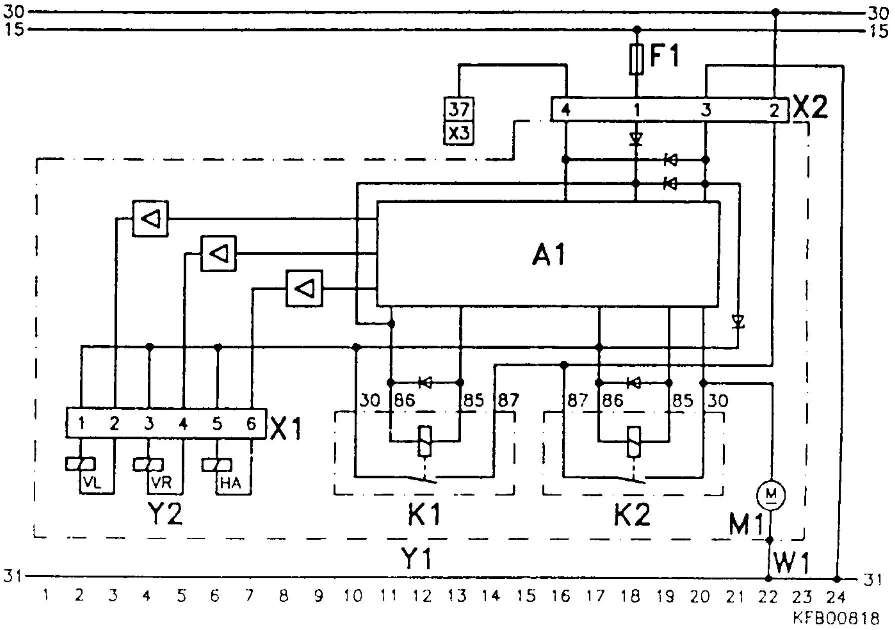


Figure 1 A simple electrical circuit for the ABS

mechanic if the error code "magnetic valve VL defective" is present in the system's control unit. The term "check" more precisely means testing the wires for shorts to battery or ground as well as for breaks. Essentially, the measurements amount to verifying the valve's connectivity both to sink and source direction; else the valve relay, the ECU or the magnetic valve itself are suspicious.

Error Code No. 2 - "magnetic valve VL defective"
• check wires: from plug X1 pin 1 to valve relay pin 30, from valve relay pin 87 to plug X2 pin 2 and further on to battery.
• check the magnetic valve's resistance: specific value is 0.7 to 1.7 ohm
• check wire to ground, ECU ground pin and wire 31's ground connection
• valve relay or ECU faulty

Table 1 Entry of a typical repair manual

2.2 FMEA for the Pedal Position Sensor of an EDC

Figure 2 depicts a subsystem of an EDC, a pedal position sensor, which transforms the position of the speed-pedal into two signals, v_{PPS} and v_{IDS}. A mechanical connection (consisting of bowden-wire, springs, etc.) passes the angle of the speed pedal (reflecting the speed desired by the driver) on to the electrical components potentiometer and switch. Whilst the potentiometer transforms the angle into a voltage by a continuous transfer-function, the idle detection switch, acting as a backup, only distinguishes between idle and drive position and has an input angle interval of uncertainty, in which it may be in either position. The potentiometer voltage corresponding to this switch-over interval is a relevant system-parameter and specified during design.

Further components included in the pedal position sensor are a power supply as well as electrical wires and nodes connecting potentiometer and switch to an evaluation unit and to the power supply.

A basic step in FMEA is to relate **failure modes** of a (sub-)system and **faults of its components** that could possibly cause them. For the subsystem discussed here, a typical FMEA considers the **failure modes** listed in Table 2.

As origins for these failure modes, the FMEA mentions the **failure causes** of Table 3.

The lists suggest a number fo distinctions that appear to be relevant for the analysis. For instance, the range of the potentiometer output voltage, v_{PPS}, is partitioned into five intervals:

- below idle (only present under faulty behavior)
- idle (voltage when the pedal is in a position before switch-over)
- switch over (voltage specified for the switch-over interval)
- drive (voltage in a position past the switch-over interval)
- above drive (again, only for faulty behavior)

This induces corresponding (classes of) failure modes of the potentiometer ("slider beyond upper/lower bound"). In addition, the "vocabulary" includes statements about deviations from expected values ("too high/low") and the occurrence of values and deviations ("always" not only refers to time, but implies "for all angles").

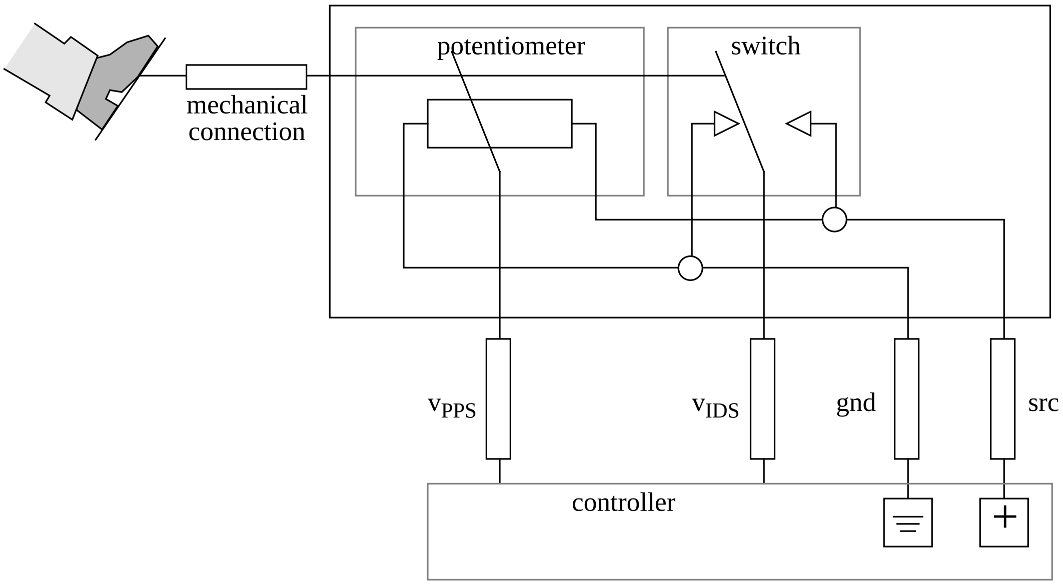


Figure 2 The Pedal Position Sensor Subsystem of an EDC

Failure modes of the pedal position sensor
• v_{PPS} out of lower bound (there is a minimal voltage below which a signal is assumed distorted)
• v_{PPS} out of upper bound
• v_{PPS} too low (detuned), v_{IDS} o.k.
• v_{PPS} too high (detuned), v_{IDS} o.k.
• v_{PPS} constant (inert) in idle interval
• v_{PPS} constant (inert) in switch over interval
• v_{PPS} constant (inert) in drive interval
• v_{IDS} always off, v_{PPS} = idle
• v_{IDS} always on, v_{PPS} constant
• Like 1, but intermittent
• Like 2, but intermittent
• pedal position sensor signal distorted
• v_{IDS} always off, v_{PPS} o.k.
• v_{IDS} always on, v_{PPS} o.k.
• v_{IDS} intermittent in idle, v_{PPS} o.k.
• v_{IDS} intermittent everywhere, v_{PPS} o.k.
• v_{IDS} detuned switch over, v_{PPS} o.k.

Table 2 Failure modes in an FMEA protocol

Component faults in the pedal position sensor
• **Wires:** broken/disconnected, shorted to ground, shorted to source, loose contact/transition resistance/signal disturbance
• **Switch:** internal fault (stuck at rest contact, stuck at make contact), worn-out contact (early switch over, late switch over)
• **Power supply:** empty, low, overcharged
• **Mechanical connection:** stuck at idle position, stuck at drive position
• **Potentiometer:** internal fault (slider stuck in idle position, - switch over position, - drive position, slider beyond lower bound, slider beyond upper bound, detuned towards lower bound, detuned towards upper bound)

Table 3 Failure causes mentioned in an FMEA protocol

3 Qualitative Models

The analysis of the FMEA documents as well as the diagnosis guidelines emphasize the need for qualitative models by the nature of the available information as well as the qualitative distinctions between classes of behavior models. The diagnosis guidelines and the FMEA documents refer to open and short circuits, low battery, etc. as opposed to exact figures on a wrong resistance, for instance.

This section presents some important aspects of the models for solving the tasks described above.

3.1 Qualitative Modeling of Electrical Circuits Based on Propagation of Connectivity

Compositionality of the models reflects the necessity to “assemble” the model from elements of a library. While this implies that the component models have to be purely local descriptions of their behavior, independent of a particular context (“no-function-in-structure principle” cf. [de Kleer-Brown 84]), there is a related stronger requirement on the **use** of these models stemming from the diagnostic technique. Consistency-based diagnosis determines suspect components from inconsistencies among model-based predictions and actual observations. Obviously, this works best when the set of models that contribute to an inconsistency is determined as precisely as possible. This prevents the application of techniques that simply determine global solutions to the system of constraints or equations aggregated from the local models. Instead, a common practice is to **locally propagate** computed values along the connections between component models thereby keeping track of the models the various predicted values depend on.

For analog circuits this method does not apply unless we add global structural information, since the local flow of current through a component depends on the existence of a closed circuit containing this component. For instance, for the circuit shown in Figure 3, a local scheme cannot achieve more than propagating voltage=ground across node N_2 to terminals t_5 and t_6. Since R_1 receives only voltage=source at terminal t_1, each resistor model fails to determine more variables. Of course, a glance at the structure tells us immediately that R_2 and R_3 are connected to the source via t_3 and t_4, respectively, that, hence, there is current flow through R_2 and R_3, hence at t_2, etc.

The problem is then to add and exploit as much of the global structural information as possible without sacrificing the local nature of the models and of the prop-

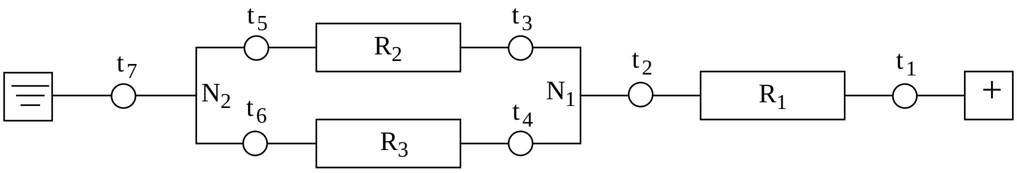


Figure 3 An Example for Connectivity in a Circuit with Sink, Nodes, Resistors, and Source

agation algorithm. It turns out that there is a partial solution to this problem. The crucial information is whether or not a circuit component is connected to source(s) and sink(s) of the circuit and if so, in which direction(s) and kinds (directly or only via finite resistance). The simple observations underlying the solution are, firstly

- that such connectivity information actually **can be propagated** to neighboring components

(the fact that resistor R_1 in Figure 3 is directly connected to “source” via terminal $\mathbf{t_1}$ implies that node N_1 is connected to “source” across a finite resistance), and secondly,

- that this information is initially available at the source(s) and sink(s) which determines the starting point of the propagation

(this is t_1 in the example and also t_7). Hence, in our models component terminals contain, besides voltage and current, four variables capturing the connectivity to source and sink, respectively, for either direction (in, out). For instance, **con-source-in** characterizes whether a connection to source exists across a respective component (and what kind), while **con-sink-out** tells about a connection of the component to sink from outside.

The domain for all four connectivity variables is

- 0 (for a direct connection)
- pos (if there exist only connections via finite resistance), and
- inf (for “no connection” or “via infinite resistance”).

The values are ordered,

$$0 < \text{pos} < \text{inf},$$

and a qualitative addition, ⊕, is defined as shown in Table 4.

⊕	0	pos	inf
0	0	pos	inf
pos	pos	pos	inf
inf	inf	inf	inf

Table 4 Qualitative Sum of Connectivities

Voltage has the obvious, ordered qualitative values

ground < between < source,

with between - between = ?

and ground - ground = source - source = 0,

and **current** represents only non-existence (0) or direction w.r.t. the component ([+],[-]) with the usual sign addition, ⊕, needed to state the appropriate abstraction of Kirchhoff’s Law.

As the connectivity variables represent something like “accumulated resistance” towards source and sink, our model could probably be regarded as a qualitative variant of the one used in [Lee-Ormsby 92] and [Hunt-Price-Lee 93] for FMEA, which basically counts the resistors on a path, assuming that their resistances are in the same order of magnitude. However, a detailed comparison remains to be done.

Table 5 shows the application of the simplest version of this modeling approach to the basic components. The relevant simplifying assumptions are that only one source (one battery) exists and that it is not directly shorted to ground. Since connectivity to source and sink are handled in the same way, the respective constraints are stated for con-x-in and con-x-out, where x is either “source” or “sink”. Symmetry w.r.t. terminals is exploited by a notation involving Ti, Tj, and Tk, where i,j(,k) varies over permutations of (1,2) ((1,2,3), respectively).

To illustrate that this extension helps, we go back to Figure 3. While propagation of voltage stops, connectivity information spreads. Since R_2 and R_3 are directly connected to ground, t_3 and t_4 have con-sink-in=pos (w.r.t. R_2 and R_3, respectively), and so do t_2 (w.r.t. N_1) and, finally, t_1 (w.r.t. R_1). This triggers the battery model, determines current through R_1, voltage=between at N_1, hence the current for R_2, R_3.

Apparently, other components of the circuit can be viewed as combined from these basic components, e.g.

- **diode** = wire with direction
- **switch** = wire with status:
  status = closed ⇔ like a wire
  status = open ⇔ like a broken wire,

etc.

Also, faulty behaviors can be described in straightforward manner. For instance, the model of a broken wire states, besides Ti.current=0, that there is no connectivity across the component:

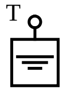
Ti.con-x-in = inf

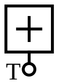
3.2 Limitations of the Model

Although the simple model presented above actually handles not only the example from Figure 3 but also the scenarios encountered in the case study without violating locality of the models and the propagation scheme, it has obvious limitations. Some of them are easy to overcome, others require a new approach.

- If we modify the example circuit in Figure 3 by inserting another resistor between node N_2 and sink, the model would fail, because at both nodes, voltage has the same qualitative value “between”. A richer domain for voltage is a possible cure.
- The assumption that there exists no direct connection between source and sink makes sense in the application considered here, since this would not correspond to an observed state (fuses would burn etc.). Covering this case, as well, requires only small changes in the source model.
- At a first glance, also the second assumption (“Only one source in the circuit”) seems reasonable in our domain. After all, there is only one battery. But there is a caveat: since shorts to source have to be considered, the respective fault models must be represented as a structural change in the circuit (e.g. by replacing a wire by a node which is attached to source).

component	symbol	constraints involving...	
		connectivity	current, voltage

sink		T.con-sink = 0
		T.con-source-in = inf
			T.voltage = ground

source		T.con-sink-in = inf
		T.con-source-in = 0
			T.voltage = source

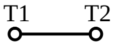
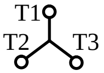
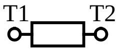
		T.con-sink-out = pos ⇒ T.current = out	
wire		Ti.con-x-in = Tj.con-x-out	T1.current ⊕ T2.current = 0 T1.voltage = T2.voltage
node		Ti.con-x-in = min(Tj.con-x-out, Tk.con-x-out)	T1.current * T2.current * T3.current = 0 T1.voltage = T2.voltage = T3.voltage
resistor		Ti.con-x-in = Tj.con-x-out ⊕ pos	T1.current ⊕ T2.current = 0 Ti.current = Ti.voltage – Tj.voltage
		Ti.current = in ∧ • Ti.voltage > ground ∧ Tj.con-sink-out = pos ⇒ Tj.voltage = between • Tj.voltage < source ∧ Ti.con-source-out = pos ⇒ Ti.voltage = between	

Table 5 Models of Basic Components

A more elegant solution is to model a wire shorted to source by stating

Ti.con-source-in = 0

Ti.con-sink-in = inf

for both terminals. Howeveer, since this amounts to treating it as a source with two terminals, the model fails in soem situations. In fact, in our case study, we used a model that handles multiple sources, provided their voltages are equal.

- The major limitation has its origins in the effects of loops which, basically, eleiminate information about the direction of connectivity. For instance, the fact that t_2 is connected to source via R_1 (i.e. t_2.con-source-in=pos w.r.t. R_1), propagates along the loop N_1-R_2-N_2-R_3-N_1 and arrives again at t_2 as t_2.con-source-out=pos w.r.t. R_1! The fact that connectivity in this direction is irrelevant because it is established via a path that includes the one in the opposite direction, is lost in the simple value “pos”. The cure is to elaborate connectivity to reflect the shortest paths, either w.r.t. magnitude of resistances (similar to [Lee-Ormsby 92]) or w.r.t. subsumtion of paths.

3.3 Models with Qualitative Deviations

A large group of fault classes and symptoms are characterized in the documents by stating a qualitative deviation of a parameter or variable from a value that would be expected under normal conditions (for instance “v_{PPS} too low (detuned)”).

This led to a another class of models in which values of parameters and variables are represented as a pair (act, Δ) of the actual value and its deviation from the correct one, where the domain for both could be signs only. Again, no new qualitative reasoning scheme was necessary for implementing such models.

4 Results of the Feasibility Study

The models presented above and the ones for other system components were used to generate information relevant to FMEA and the diagnosis guidelines, respectively. For producing diagnosis guidelines, the error codes that are provided by the control unit and used as entry points in the guidelines were stated as the set of (qualitative) observations that trigger the error code and in this form used as an input to the model. From this, the standard general diagnosis engine (GDE, [de Kleer-Williams 86]), based on models of correct behavior only, generated a set of diagnosis candidates under a single fault focus (see [Dressler-Farquhar 90]) in accordance with the single fault assumption underlying the diagnosis guidelines. Hence, the result was a set of suspect components to be checked in the repair shop. For the 11 considered errorcodes for the ABS (which make about 60% of the entire set, some of which are symmetric for the different wheels),

- the set of components occurring in the actual diagnosis guidelines was **completely covered** by the automatically generated diagnoses.

GDE generated additional diagnoses which were obviously ignored in the diagnosis guidelines as unlikely or implicitly subsumed by the checks (e.g. plugs by the adjacent wires). The former case could be handled by adding failure probabilities (even in a rough, binary way), which we did not.

- The **runtime** required (in the order of 1 minute per errorcode on a SPARC20) is acceptable if the task of computer-supported generation of the guidelines is considered.

A further step involved generation of multiple-fault candidates. Although in our example only very unlikely ones were found, this is an option for critical symptoms or for a second stage of fault localization if no single fault can be localized.

Finally, fault models were used by the extended diagnosis engine, GDE+ ([Struss-Dressler 89]) to rule out failures of suspect components that are inconsistent with the observations. This resulted in a refinement of the existing diagnosis guideline, which, for instance, always proposes to check a wire for short to ground and battery and open circuit, no matter whether all faults could possibly account for the error code. This does not result from mistakes or ignorance during the production of the guidelines, but is simply due to the fact that obviously standard text blocks were copied in order to reduce the production time. However, even this sheds a light on the fact that model-based systems for support of this task bear the potential for both saving precious time and improving the results. Furthermore, the error codes often summarize different symptoms, e.g. by “wrong signal”. The plausibility check involved is actually more specific, for instance triggered by “signal too high”. If this information would be available in future control units, the results of the automated diagnosis could exploit this information without any change or extension of the models and the algorithm and generate even more specific candidates.

In another experiment, a “diagnosis guideline” was generated for an ABS that exists only as a blueprint, designed for a future car. Thus, we demonstrated that such guidelines can be produced early in the design phase and that the models and the diagnostic approach really solve the “variants’ dilemma”. Whilst the analysis of the domain and the development of the model library took us several months, entering the structural description of the new ABS (by hand!) and generating the diagnoses was a matter of one afternoon.

As for the FMEA, the task was to generate two columns of the respective document for the pedal position sensor: namely the appropriately linked entries under “failure mode” and “failure cause” (see section 2.2). There are two possible directions for deriving these links. Starting with a given failure mode and determining the potential failure causes for it corresponds to GDE+ diagnosis as described for diagnosis guidelines generation. In our case study, the system operated in the reverse direction: for a given component fault (single fault as in the FMEA document) the potential effects on the crucial output variables (v_{PPS} and v_{IDS}) are predicted. For this task, we do not even need a diagnostic engine, but only the model-based predictor. In a loop, all single component faults are “inserted” and the respective values of the outputs are predicted by this model of the faulted subsystem.

The section of the FMEA that dealt with the pedal position sensor listed 26 relationships between fault modes and causes (covering six A4 pages out of approximately 60 for the entire EDC), disregarding the always applying possibility of a broken control unit and effects of intermittent faults which have not yet been included in our models.

- 23 out of these 26 links were found by the automated system.
- One additional cause was detected for one of the fault modes.

The cases not covered were related to bridge faults in the circuit. Our model as presented in section 3 could not handle this properly, because the distinctions between voltages “ground”, “between”, and “source” do not suffice; for this purpose, the value “between” has to be refined or ordinal information about voltages exploited.

- Runtime for generation of the entire list was about 20 minutes.

As a side remark, we mention that the use of an ATMS contributed to the efficiency (which also is in an acceptable order of magnitude for the given task): it caches results of inferences and, hence, helps to avoid re-computation of results for sub-structures shared by the various variants of the (faulty) device models. Furthermore, the generated results were more specific in many cases in mentioning the specific (classes of) faults, rather than summarizing them by terms such as “internal errors”.

5 Lessons learned

What are the major lessons learned from this case study?

- **It works! - But, what is it that works?**

  It was demonstrated that the available techniques for model-based prediction and consistency-based diagnosis were a sufficient basis for tackling the described tasks without simplifying them down to the usual academic toy scenarios. Yet we are aware that one has to be careful when generalizing the results. We demonstrated that the two selected tasks can be solved for the types of systems we studied. And more: that the same models could be used for the different tasks. We state some preconditions and limitations below.

- **Compositional, context-free models are necessary**

  The positive result of the feasibility study would be worthless if it were not based on a library of **local component models** that can be **composed** to create models of a whole class of devices, as demonstrated by our ABS-variant example. For this reason, component models have to be stated independently of a particular context. Obeying this **“no-function-in-structure principle”** ([de Kleer-Brown 84]) for the kind of tasks to be performed is a practical demand, and academic discussions of the infeasibility of this goal in the ideal sense are a waste of time.

  However, there is a subtle problem here, because a local, context-free component model is not guaranteed to make all distinctions required in a particular context. In the pedal position sensor, for instance, the “switch-over” interval for the angle is not intrinsic to the behavior of the potentiometer. Rather, it is the reflexion of a distinction that has to be made for a different component, the idle detection switch. If the potentiometer model is used in a different environment, this distinction may be irrelevant. Inducing such local distinctions from the context of the task and the entire device seems to be an interesting task for automated modeling, and we are not aware of work that addresses it in a general and systematic way.

- **Qualitative modeling is the key**

  By their very nature, the tasks considered here demand for **qualitative** techniques, since they require statements about classes of symptoms and faults. Numerical methods could not satisfy the requirements. Moreover, a solution based on **first principles** is required, since new systems have to be handled, sometimes only existing as a blueprint. Associational or case-based methods would not help. But does not previous experience contribute to the solutions? Yes, but it is only useful if it is cast in models or in strategies for selecting and applying the models. Qualitative models are also an important precondition for compositional modeling. Because they capture the essential distinctions only, they ensure re-usability of models and help to keep the size of the model library small. The components in the ABS-variant may have different parameters and subtle peculiarities, but these do not matter for the task considered, and this is reflected by the qualitative models.

- **Tackling real problems is essential for further progress**

  It is essential because it forces to address the central problem: modeling. And it is essential for solving this problem. Finding models that make the essential distinctions is the key issue, and only real diagnostic tasks provide criteria and a context for determining what is essential. For instance, the model of the mechanical connection could be arbitrarily complex; only the restrictions of the tasks (represented by the existing documents) determined the appropriate level of abstraction. But does this not contradict the “no-function-in-structure principle”? It certainly does, but if we continue to escape to OR-gates and inverters instead of going through this step of modeling for real world problems, we will not make further progress in modeling and, hence, not in model-based diagnosis.

  The existing documents suggest that, although the systems considered are dynamic, most, if not all, of the required analysis can be done at a high level of qualitative and temporal abstraction without sophisticated temporal reasoning or qualitative simulation. We are investigating this working hypothesis in our current work on more complex dynamic subsystems and feed-back control loops. Another direction is describing, at a very high level, the interaction of the various subsystems of a car and the overall behavior of a car (for being able to establish links to symptoms at this global level as they are experienced by the driver which most of the time initiate the diagnosis, anyway).

Acknowledgments

We thankfully acknowledge support as well as information and help provided by Robert Bosch GmbH, Stuttgart. Discussions with Oskar Dressler, Anton Beschta, Ulrich Heller and Michael Montag helped to promote this work. Thanks also to the reviewers for their valuable comments.

References

[de Kleer-Brown 84] J. de Kleer and J. S. Brown, “A Qualitative Physics Based on Confluences”, AI Journal 1984.

[de Kleer-Williams 87] J. de Kleer and B. Williams, “Diagnosing Multiple Faults”, AI Journal 1987.

[Dressler-Farquhar 90] O. Dressler, A. Farquhar, “Putting the Problem Solver Back in the Driver’s Seat: Contextual Control over the ATMS”, Springer LNAI 515.

[Hunt-Price-Lee 93] J. E. Hunt, C. J. Price, M. H. Lee, “Automating the FMEA Process”. In: Intelligent Systems Engineering, Summer 1993

[Lee-Ormsby 92] M. H. Lee, A. R. T. Ormsby, “Qualitative Modeling of Electrical Circuits”. In: “Proceedings of the QR 92”, 6th International Workshop on Qualitative Reasoning about Physical Systems, Heriot-Watt University, Edinburgh, 1992

[Struss-Dressler 89] O. Dressler, P. Struss, “Physical Negation: Integrating Fault Models into the General Diagnostic Engine”, Proceedings of the 11th International Joint Conference on Artificial Intelligence (IJCAI), 1989