QUALITATIVE MODELING IS THE KEY TO AUTOMATED DIAGNOSIS

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.

Keywords: Qualitative simulation, Modeling, Computer-aided diagnosis, Artificial Intelligence, Failure detection/isolation, Reasoning, (Intelligent) Knowledge-based systems, Quality control. Diagnostic Inference

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. Furthermore, safety requirements demand for high standards in coverage and completeness of any automated analysis of causes and effects of faults, thus ruling out the application of traditional expert systems which 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.

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, numerical models and methods are useless, and we had to develop

- **qualitative models**

in order to capture the available knowledge and to generate appropriate results. Theories and techniques for qualitative modeling have been developed in a subfield of Artificial Intelligence (see Faltings-Struss 92, Weld-de Kleer 90)

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 (3.1). Finally, we summarize the overall results of the feasibility study.

2 TWO SCENARIOS FROM THE CASE STUDY

In order to obtain appropriate models, 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 re-usability of models), we omit details here and concentrate on the actuation part.

Figure 1 shows the electrical topology of an ABS. Wire 30

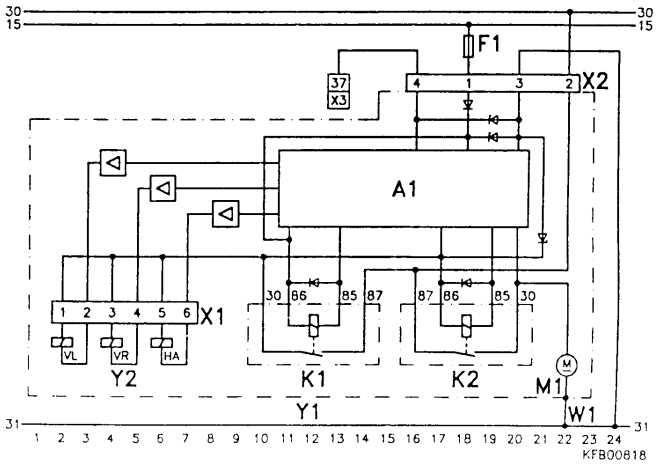


Fig. 1. A simple electrical circuit for the ABS

(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 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.

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

Table 1 Entry of a typical repair manual

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

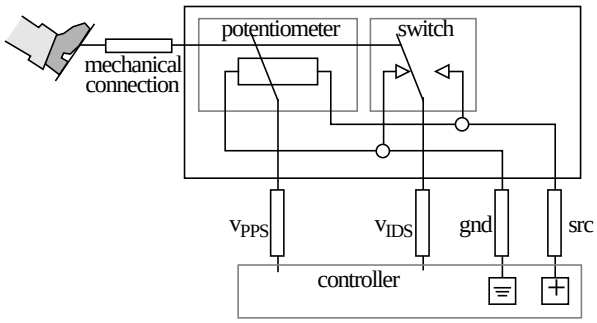


Fig. 2. The Pedal Position Sensor Subsystem of an EDC

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 in the pedal position sensor are a power supply, 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:

Table 2 Failure modes in an FMEA protocol

- v_{PPS} out of lower bound (there is a minimal voltage below which a signal is assumed distorted)
- Likewise, but intermittent
- v_{PPS} out of upper bound
- Likewise, but intermittent
- 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
- 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.
- 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”).

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 compo-

Table 3 Failure causes mentioned in an FMEA protcol

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)

nents 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 propagation 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 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)

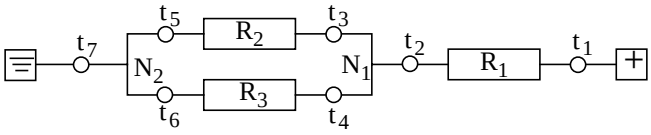


Fig. 3. An Example for Connectivity in a Circuit with Sink, Nodes, Resistors, and Source

- 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, $\oplus$, is defined as shown in Table 4.

Voltage has the obvious, ordered qualitative values

$$\text{ground} < \text{between} < \text{source},$$

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, $\oplus$, 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.

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 $\Leftrightarrow$ like a wire
  status = open $\Leftrightarrow$ 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:

$$\text{Ti.con-x-in} = \text{inf}.$$

Table 4 Qualitative Sum of Connectivities

$\oplus$	0	pos	inf
0	0	pos	inf
pos	pos	pos	inf
inf	inf	inf	inf

We emphasize that this model has a number of limitations, due to the underlying assumptions and the three-valued representation (see Struss et al. 95). They can be overcome by more sophisticated, but still qualitative, models exploiting the connectivity aspect.

3.2 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),

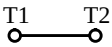
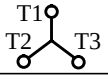
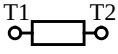
- the set of components occurring in the actual diagnosis guidelines was **completely covered** by the automatically generated diagnoses.

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

Table 5 Models of Basic Components.
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).

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	

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.

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.

In many cases the generated results were more specific in mentioning the specific (classes of) faults, rather than summarizing them by terms such as "internal errors".

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.

The case study domonstrates the utility of qualitative models in situations where numerical models are not available or inappropriate due to the nature of the task and/or given information. They provide a means for expressing and exploiting seemingly informal knowledge, for instance about qualitative deviations of behavior, on a firm theoretical ground in formal models. Since qualitative models make explicit the essential distinctions only, they cover types or classes of components rather than individual ones, thus facilitating rather small model libraries.

In our current work we extend the application of qualitative modeling and model-based diagnosis to treating feedback and dynamic aspects in car subsystems and employ them in interactive problem solving tools, e.g. for generation of repair manuals.

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. This work has been supported by the German Ministry for Education and Research (# 01 IN 509 41).

REFERENCES

de Kleer, J. and Brown, J. S. (1984) A Qualitative Physics Based on Confluences, *AI Journal*.

de Kleer, J. and Williams, B. (1987), Diagnosing Multiple Faults, *AI Journal*.

Dressler, O. and Farquhar, A. (1990), *Putting the Problem Solver Back in the Driver's Seat: Contextual Control over the ATMS*, Springer LNAI 515.

Faltings, B. and Struss, P., editors (1992), *Recent Advances in Qualitative Physics*, MIT Press

Hunt, J. E. , Price, C. J. and Lee, M. H. (1993), Automating the FMEA Process. In: *Intelligent Systems Engineering*, Summer 1993

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

Dressler, O. and Struss, P. (1989) Physical Negation: Integrating Fault Models into the General Diagnostic Engine, In: *Proceedings of the 11th International Joint Conference on Artificial Intelligence* (IJCAI'89)

Struss, P., Malik, A. and Sachenbacher, M., (1995) Qualitative Reasoning is the Key, *Proceedings of the 6th International Workshop on Principles of Diagnosis* (DX-95), Goslar, October

Weld, D. S. and de Kleer, J., editors (1990), *Readings in Qualitative Reasoning about Physical Systems*. San Mateo.