Diagnosing a Dynamic System with (almost) no Observations

A case study in off-board diagnosis of the hydraulic circuit of an anti-lock braking system

Peter Struss[1], Martin Sachenbacher[2], Florian Dummert[1]
{struss, sachenba, dummert}@informatik.tu-muenchen.de
http://wwwradig.informatik.tu-muenchen.de/research/qreason/

[1]Technical University of Munich
Department of Computer Science
Orleansstr. 34
D-81667 Munich
Germany

[2]Robert Bosch GmbH
Dept. FV/SLN1
Robert-Bosch-Str. 2
D-70442 Stuttgart
Germany

Abstract

We present requirements and results of a case study in model-based (off-board-)diagnosis of the hydraulic circuit of an anti-lock braking system. The primary problems to be addressed quite fundamental: it is impossible to predict the behavior of the system and, additionally, there are no measurements of the actual behavior available. Both might be considered fatal for model-based diagnosis. We tackle these problems by applying models that capture qualitative deviations of variables and parameters from nominal behavior. They allow to exploit vaguely described symptoms such as "brake pedal too soft". The models are used in a state-based diagnosis framework, i.e. only the observed states are checked for consistency with the model, and no simulation of the dynamic behavior is required. The crucial step in making the approach work is to exploit basic constraints on continuity and for complementing the directly obtained observations by information about derivatives. Experimental results are compared to expert knowledge represented in existing failure mode and effects analysis (FMEA) documents and prove to be adequate.

1 Introduction

Commonly, the principle of consistency-based diagnosis of a device is described as follows:

- Take measurements of the actual device behavior.
- Predict the expected behavior of the device based on its model.
- Infer potential diagnoses from discrepancies derived from predictions and measurements.

But what do you do if

- you are **not able to predict** the device behavior?!

And, on top of it, if

- you have **no measurements?!**

We describe a case study that demonstrates how and to what extent (consistency-based) diagnosis can be performed even under these conditions. The problem was encountered in our work on (off-board) diagnosis of anti-lock braking systems (ABS). For a complete treatment of this car subsystem, we had to model and diagnose its hydraulic circuit, in addition to the electrical circuit and the speed sensor which were covered by previous work ([Struss et al. 95]).

Behavior prediction for the hydraulic circuit is a problem for two reasons:

- It is a **controlled** dynamic system. Model-based prediction would require to include a model of the complex behavior of the electronic control unit (ECU) of the ABS.
- Crucial **contextual influences**, such as road conditions, are **not measurable**, and, hence there is no sufficient input to prediction.

This leads to the second problem, measurability:

- There are **no sensors** in the hydraulic circuit.
- The only **observations** available are related to the behavior of the **wheels** and the **pedal**, and they are inherently **vague and qualitative** ('The pedal feels soft when pushed', 'The left front wheel tends to lock up'), in particular when reported by the driver.
- The occurrence of such symptoms is not temporally specified.

A description of the system and the diagnosis scenario is given in section 2 of this paper. Section 3 describes how the model addresses the problems:

- A **qualitative model** is required to enable the exploitation of the qualitative observations.
- The relative nature of the observations ('pedal too soft') and the lack of behavior predictions in absolute terms, lead us to the use of **deviational models** which capture how deviations in system parameters relate to deviations from some reference behavior, independently of a specification of this reference behavior.

The features of the utilization of this model by the diagnostic algorithm are discussed in section 4:

- We apply **state-based diagnosis** which checks consistency of observed and modeled (qualitative) states only, taking into account that there is hardly

any information about the dynamics in the observations and that predicting it is also infeasible.
- General (device-independent) constraints are exploited to **infer derivatives** of variables which turns out to be crucial for having state descriptions that are strong enough for state consistency checking.

We summarize results of an experiment in which the approach described above was applied to several fault scenarios extracted from a failure mode effects analysis document which represented available expertise and was used to provide success criteria. The results were basically positive, but depend on a number of assumptions and decisions. These assumptions can be considered reasonable in this application, but are far from being generally met preconditions which is why we discuss them at the end.

2 Application Domain

2.1 Anti-lock Braking System Hydraulics

The purpose of the anti-lock braking system (ABS) [Bosch 96] is to prevent the wheels from locking up and, thus, to maintain the steerability and stability of the car while braking. The ABS consists of an
- electronic control unit (ECU),
- wheel-speed sensors and
- pressure-modulation valves.

The rotational speed of the wheels is measured and serves as an input to the control unit, which governs the valves and pump elements inside a hydraulic unit to reduce or increase the pressure exerted on the wheel brake cylinders.

The vehicle speed is estimated based on the wheel speeds of two diagonally opposite wheels. From this reference speed and the individual wheel speeds the ECU calculates the brake slip for each wheel, and, by combining this value with the (de-)acceleration of the wheel, it determines whether a wheel has a tendency to lock up. If this is the case, the control unit energizes the magnets of the pressure-modulation valves which control the brake pressure in the respective brake cylinders.

A typical ABS consists of two subsystems, each one operating on a pair of diagonally opposite wheels. As shown in Figure 1, the hydraulic circuit of each diagonal comprises
- four valves,
- two brake cylinders,
- a return pump element,
- an accumulator,
- a damper with throttle.

The pump elements of the two diagonals share one common drive motor. The hydraulic circuit is connected to the master cylinder that transforms a force acting on the brake pedal into increased pressure. To ensure that the pressure in the brake cylinders is never higher than the actual pressure in the master cylinder, inlet valves have built-in non-return valves. If the ABS is inactive, the braking system acts in the regular manner, maintaining the pressure on the brake

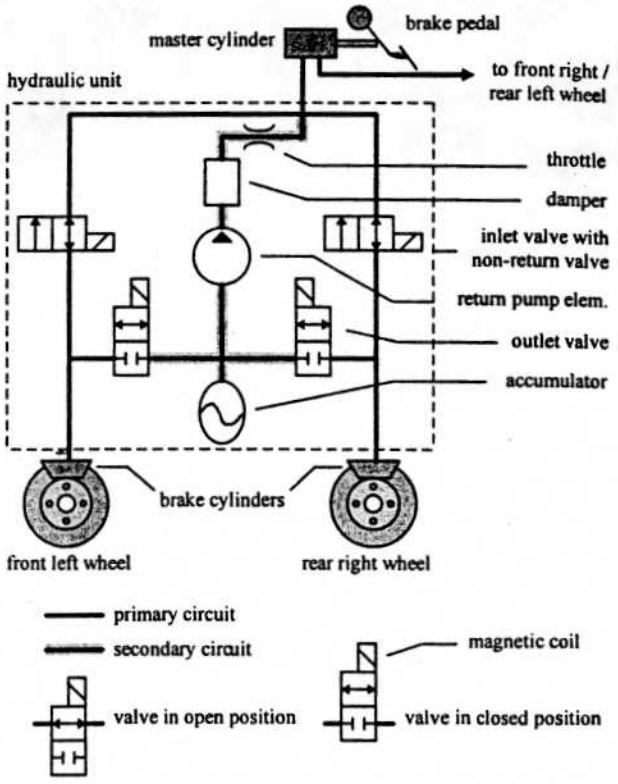


Figure 1: Hydraulic circuit of the ABS (diagonal distribution pattern)

cylinders while the pedal is pushed. In this mode, only the so-called primary circuit (see Figure 1) is active with the outlet valves closed. If the ABS is activated, reduction of pressure on the brake cylinders involves also the secondary circuit.

Control of the brake cylinders' pressure is achieved by stepping through different operation modes, as shown in Figure 2:
- **pressure-buildup**: for each wheel, an increase in pressure is achieved by an open inlet valve and a closed outlet valve, as in the regular braking mode.
- **pressure-holding**: the inlet valve is closed.
- **pressure-reduction**: the outlet valve is opened, and the accumulator fills quickly. Also, the return pump starts immediately to transport the fluid back towards the main cylinder.

If necessary, the brake pressure is then increased again to ensure that the wheel is not under-braked, and the next cycle may start.
- **pulsed pressure-buildup**: in some cases it might be useful to quickly interleave pressure-holding and buildup mode (the inlet valve receives a pulsed signal), to achieve a more smoothly raise of pressure.

The finite state machine shown in Figure 3 models in more detail the modes of the ABS control and the transition conditions which lead from one state to another. The essential condition is given by the wheel acceleration a, which is computed from the measured wheel speed v_w, and thresholds $a_1 < 0 < a_2 < a_3$. Additional variables are the vehicle speed v_{veh} and the

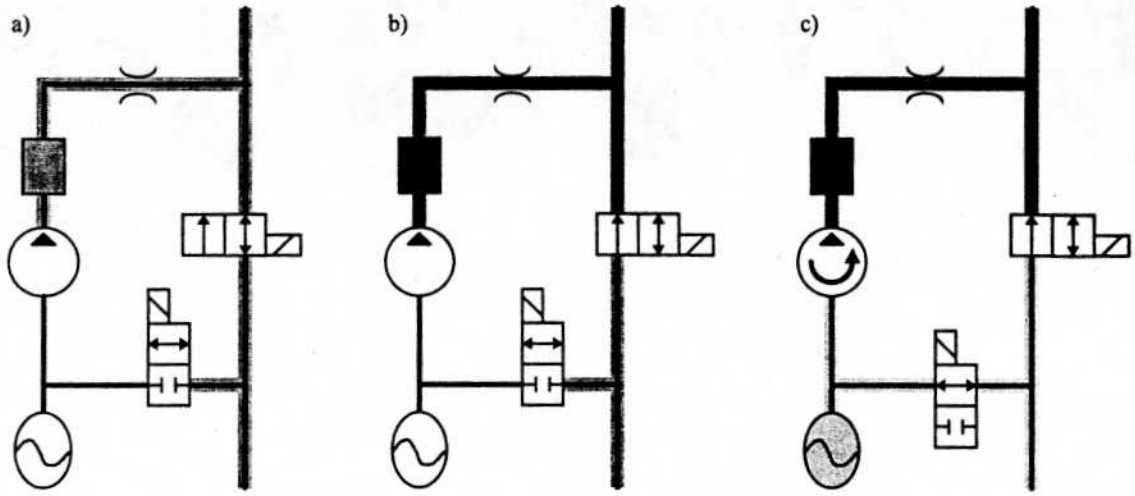


Figure 2: Operation modes of the ABS: a) pressure-buildup, b) pressure-holding and c) pressure-reduction

pedal position s_{ped}, with thresholds v_0 and s_0, respectively, which serve as termination conditions to switch off the ABS control (because the driver stopped emergency braking or the vehicle speed has been reduced appropriately). In fact, this is still a description of a rather simple or simplified ABS control. It should be noted that the above-mentioned parameters are not available under workshop conditions, nor would they be particularly useful for diagnosis, as the behavior of the control loop depends to a large extent on (unknown) factors like the adhesion of the road surface, tire condition and vehicle load.

2.2 The Diagnostic Problem

The problem we address in our work is to support detection and localization of faults in the hydraulic circuit under workshop conditions. [Struss et al. 95] reports our first results in model-based automation of the generation of diagnosis guidelines for the ABS. Usually, off-board diagnosis starts by reading information off the ECU. The ECU is equipped with built-in monitoring capabilities and produces error codes if it detects implausible signals. It already performs fault detection and a weak form of fault localization. However, this only applies to the electrical parts of the system. The reason is that there are simply no sensors, e.g. for pressure, in the hydraulic circuit (except for a sensor indicating that the brake fluid level has dropped below a critical threshold, which is of no help for immediate detection of misbehaviors and irrelevant for fault localization). Even in the garages, there exist no specific test-benches or analyzers that check the function of the entire ABS. Instead, information about pressures inside of the hydraulic circuit can only be obtained indirectly from observing the (de-)acceleration of the wheels.

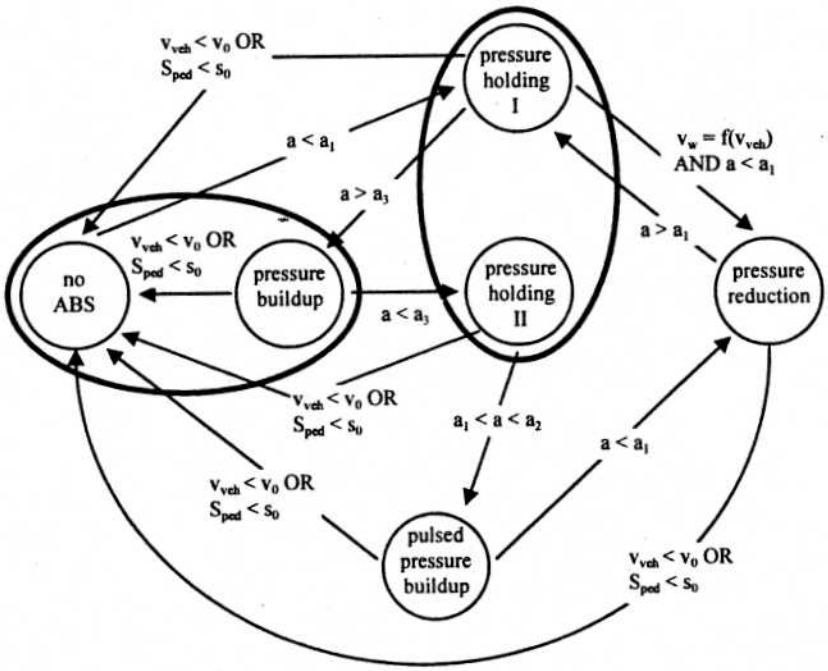


Figure 3: States and transition conditions of the ECU

However, it is not realistic that the driver or even a mechanic can exactly measure wheel acceleration or deceleration. As a result, diagnosis of the hydraulic subsystem has two major sources of information:

- **Symptoms reported by the driver.** Except for a lit control lamp, all a driver can perceive is some unexpected behavior of the vehicle w.r.t. braking and steering. This bears a chance of being translated into features of the individual wheels, perhaps a suspect response by the brake pedal, and possibly some sounds. For instance, typical observations could be that a wheel tends to lock up (indicating too high pressure in the respective brake cylinder) or that the brake pedal is too soft (as a result of an unusually low pressure in the main cylinder). We should emphasize however, that it is not guaranteed that an ordinary driver is able to provide even this kind of information, simply because most drivers do not gain extensive experience with braking in ABS mode. It can be produced more reliably by the mechanic in the workshop.
- **Tests** under defined operation modes **in the workshop**. With the same tool that is used to read off the error codes of the ECU, each operation mode of the ABS can be activated individually. The test e.g. for the pressure-holding phase consists of pushing the brake pedal while the pressure-holding mode is activated and checking if the respective wheel can still be moved freely, indicating that the system could indeed maintain the low brake cylinder pressure.

A typical diagnosis scenario which we will use for illustration in the following sections is that when braking,

- the car is yawing to the right, while
- the brake pedal feels somewhat harder than normal.

We assume that the first symptom can be refined to

- under-braking at the left-hand and
- over-braking at the right-hand side.

Actually, the symptoms are taken from a failure mode and effects analysis for the ABS. This analysis is carried out during the design of a system and lists a number of possible component faults such as clogged or enlarged valve profiles, valves stuck open or punctured, a defective pump element or air included in the circuit, together with their (potential) effects (e.g. the symptoms stated above).

We emphasize that observations like the ones mentioned above

- are **qualitative** in nature,
- are sparse, and only **indirectly related** to the important **internal system variables**, and
- have an **unspecified temporal extent.**

For instance, under-braking is a phenomenon that characterizes the behavior of a wheel over the entire period of braking, not even related to a particular phase. Only under the described testing conditions in the workshop, observations can be associated with the operation mode of the test, but even then, no detailed temporal aspects can be measured.

This fact contrasts sharply with the

- **dynamic behavior** of the device,

thus making the diagnosis problem a real challenge for modeling and automated diagnosis.

However, a human observer who is familiar with the components of the circuit and has a basic understanding of the functionality of an ABS as given in this section, is able to come up with reasonable diagnostic hypotheses; e.g. based on the symptoms of our example scenario:

Under-braking on the left-hand side indicates insufficient pressure. This could be due to a clogged inlet valve or an open outlet valve. The former would also explain why too high pressure remains in the master cylinder (hence the hard pedal) and in the primary circuit of the right-hand wheel (possibly causing over-braking). So, this seems to be a plausible diagnosis.

The question is what is required to perform this kind of reasoning in an automated diagnosis system. The following sections present our answer to this question, first, regarding the modeling formalism and, second, the diagnostic procedure.

3 Qualitative Deviation Models

3.1 Models of Hydraulic Components

In response to the nature of the observations, we adopted an approach that states models in terms of qualitative deviations of variables and parameters from some unspecified and even potentially changing nominal value.

The above-mentioned failure causes and effects qualitatively describe deviations of component parameters from such a nominal value (e.g. "inlet valve profile enlarged") or deviations of system variables from values one would expect normally (e.g. "over-braked"). The successful use of models which capture the qualitative relations between such discrepancies has already been presented in [Malik, Struss 96]. We briefly summarize the foundations of this approach.

Each variable domain is limited to signs

$$[x] := \mathrm{sign}(x),$$

especially derivatives of time

$$\partial x := [dx / dt],$$

and the deviation of an actual value from its reference value

$$\Delta x := x_{act} - x_{ref}.$$

In this case, the reference value is defined as the value that would occur under normal behavior of the ABS given the same situation in terms of road condition, force exerted on the pedal etc. Obviously, there is no way of explicitly specifying these values of a nominal behavior and their changes over time because of the unmeasurable or even unknown context. There are two basic insights: first, even under these conditions, it can be possible to predict the effect, or, likewise, the potential cause of a deviation in one system variable, and, second, many possible faults

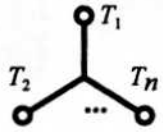
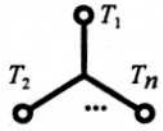
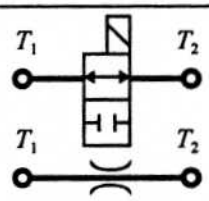
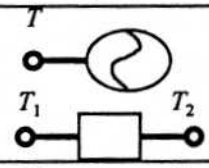
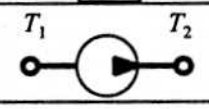
Component	Symbol	Constraints
n-node		$T_1.[p] = T_2.[p] = \ldots = T_n.[p]; \sum_{i=1}^{n} T_i.[Q] = \partial p \otimes [\beta_T]$ $T_1.[\Delta p] = T_2.[\Delta p] = \ldots = T_n.[\Delta p];$ $\sum_{i=1}^{n} T_i.[\Delta Q] = \partial p \otimes [\Delta\beta_T] \oplus \partial\Delta p \ominus \partial\Delta p \otimes [\Delta\beta_T]$
n-node (with invariant compressibility)		$T_1.[p] = T_2.[p] = \ldots = T_n.[p]; \sum_{i=1}^{n} T_i.[Q] = \partial p$ $T_1.[\Delta p] = T_2.[\Delta p] = \ldots = T_n.[\Delta p]; \sum_{i=1}^{n} T_i.[\Delta Q] = \partial\Delta p$
resistive element e.g. valve, throttle		$T_1.[Q] = [A] \otimes (T_1.[p] \ominus T_2.[p]); T_1.[Q] \oplus T_2.[Q] = 0$ $T_1.[\Delta Q] \oplus T_2.[\Delta Q] = 0$ $T_1.[\Delta Q] = [A] \otimes (T_1.[\Delta p] \ominus T_2.[\Delta p])$ $\oplus [\Delta A] \otimes (T_1.[p] \ominus T_2.[p])$ $\ominus [\Delta A] \otimes (T_1.[\Delta p] \ominus T_2.[\Delta p])$
volume element e.g. accumulator, damper		$T.[p] = [p]; T.[Q] = \partial p$ $T.[\Delta p] = [\Delta p]; T.[\Delta Q] = \partial\Delta p$ $T_1.[p] = T_2.[p]; T_1.[Q] \oplus T_2.[Q] = \partial p$ $T_1.[\Delta p] = T_2.[\Delta p]; T_1.[\Delta Q] \oplus T_2.[\Delta Q] = \partial\Delta p$
pump element		$T_1.[p] = [+] \Rightarrow T_1.[Q] = [D]; T_1.[p] = 0 \wedge [D] \neq [-] \Rightarrow T_1.[Q] = 0$ $T_1.[p] = 0 \wedge [D] = [-] \Rightarrow T_1.[Q] = [-]$ $T_1.[Q] \oplus T_2.[Q] = 0$

Figure 5: Qualitative model fragments for basic hydraulic components

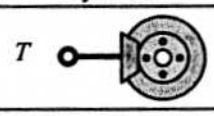
Component	Symbol	Constraints
wheel (with brake cylinder)		$T.[\Delta p] = -\partial\Delta v_w$
brake pedal		$T_1.[Q] = T_1.[p] \ominus T_2.[f]; T_1.[Q] \oplus T_2.\partial s = 0$ $T_1.[\Delta Q] = T_1.[\Delta p] \ominus T_2.[\Delta f]; T_1.[\Delta Q] \oplus T_2.\partial\Delta s = 0$

Figure 4: Qualitative model fragments for the brake pedal and wheels

can be characterized in terms of parameters deviating from their nominal values. For instance, a_clogged valve can be described by its profile, A, being smaller than normal: $\Delta A<0$. Models capturing the relationships of such qualitative deviations can be generated from the equations that describe the normal behavior of the respective components.

Table 1 lists a number of basic equations for types of hydraulic elements. They are meant to model basic aspects of hydraulic components and can be combined to describe a particular component type. Using the operators, [.], ∂, and Δ, defined above, qualitative deviation models of components can then be derived from these equations. Figure 5 shows the resulting qualitative models of basic hydraulic component types, whilst Figure 4 lists additional ones for ABS-specific components. In the notation, Q stands for flow, p for pressure, A for profile area and D for the pump delivery rate, whereas k and β_T are (material-dependent) factors. Thus, in the notation of the model fragments, e.g. $T_1.[p]$ denotes qualitative pressure at terminal T_1.

Component	Quantitative equations
conduit with zero resistance	$p_1 = p_2$ $Q_1 + Q_2 = 0$
resistive element	$Q = kA\sqrt{\lvert p_1 - p_2 \rvert}\ \mathrm{sign}(p_1 - p_2)$ $Q_1 + Q_2 = 0$
volume element with compressibility	$Q = k\frac{dp}{dt}\beta_T$
volume element without compressibility	$Q = k\frac{dp}{dt}$

Table 1:Basic equations for hydraulic elements

3.2 Coding of Observations

The inherently vague and qualitative observations of the ABS behavior can now be captured by our modeling formalism. For the symptoms of the scenario described in section 2, we obtain the following translations:

- under-braked left-hand wheel, i.e. it rotates faster than under normal conditions: $[\Delta v_L] = [+]$.
- over-braked right wheel, i.e. it rotates slower than expected: $[\Delta v_R] = [-]$.
- too hard brake pedal, which, given the usual pedal force, moves a shorter distance than normally: $\partial\Delta s_{PED} = [-]$.

Together with the characterization of the operation modes of the hydraulic circuit given in terms of states of valves and pump, these observations represent the only directly and somewhat reliably available input for model-based prediction and consistency-checking.

4 Using the Model for Consistency-based Diagnosis

4.1 State-based Diagnosis

Consistency-based diagnosis requires checking whether observations about the actual device behavior are consistent with the behavior predicted by a model:

$$\text{model} \cup \text{OBS} \stackrel{?}{\vdash} \perp .$$

For fault detection, the system checks the model of correct behavior. Fault localization is based on identifying inconsistent subsets thereof. Fault identification is done by checking models of faulty behavior for consistency with observations.

Since, in our domain, we have neither a chance to predict the dynamics reliably, nor a way to observe changes over time, we cannot perform what is often associated with the task of diagnosis of dynamic systems: tracking of the actual behavior over time and simulation of the modeled behavior. In previous work ([Malik, Struss 96], [Struss 97]), we have shown that, in theory and practice, checking only the observed states (rather than the temporal behavior) for consistency with the device model often suffices to obtain the desired diagnostic results and that, under certain conditions, these results are even equivalent to the ones generated by simulation-based approaches. In our case, we have no choice but trying to apply **state-based diagnosis**. Stated more systematically, this means that we ignore part of the model, namely the part that captures the laws of evolution over time (which, in practice, is often implicit in the predictive engine): if the model is divided into a set of constraints on the permissible states and a set of constraints expressing rules of continuity, integration, and derivatives („CID"),

$$\text{model} = \text{state-constraints} \cup \text{CID-constraints},$$

then we confine the consistency check to

$$\text{state-constraints} \cup \text{OBS} \stackrel{?}{\vdash} \perp .$$

It turns out that the observations together with the model do not suffice to generate appropriate conflicts. The "measurements" characterized above, enable the models to infer deviations in the pressure in different parts of the circuit. This, trivially, suffices to establish measurability for fault detection, but not measurability for fault identification and localization. The reason lies in the lack of information about the derivatives of pressures, which cannot be provided by the observations and the constraints of the model fragments alone. Basically, this information would help to detect significant inconsistencies because resistive elements like valves relate flow to pressure, whereas pipes and other containers link flow and derivatives of pressure and, respectively, their deviations.

In our example („yawing to the right"), the observation about the pedal, $\partial\Delta s_{PED} = [-]$, allows to infer a positive deviation of the pressure in the master cylinder (see Figure 6 for reference),

$$[\Delta p_{MC}] = [+],$$

and from the under-braked left-hand wheel, we obtain a lower pressure in the respective wheel brake cylinder,

$$[\Delta p_{WBC}] = [-].$$

From this information, the model left inlet valve can predict an increased flow across the valve:

$$[\Delta Q_{LIV}] = [+],$$

which does not establish any contradiction. What is it that makes us not feel comfortable with this situation? Well, the state description obtained may be consistent with the (part of the) model. However, an increased flow across the valve causes the pressure in the wheel brake cylinder to **rise** which conflicts with the **reduction** in pressure in this component. In other words, we squeeze more information out of the observations of the variables, namely information about their derivatives.

4.2 Adding CID-Constraints

If we would like our system to perform this kind of reasoning, we have to exploit additional knowledge which can compensate for this limited measurability. This is actually implied by the constraints we dropped in the previous subsection, *CID-constraints*. However, they are not used for simulation of correct or faulty behavior modes (for integration), i.e. by drawing inferences based on

$$\text{state-constraints} \cup \text{CID-constraints}.$$

Instead, they are applied to complement the observations with derivative information, i.e. we combine

$$\text{CID-constraints} \cup \text{OBS}.$$

More specifically, a version of the following theorem is applied:

Theorem 1

Let $f(t)$ be a continuously differentiable function and $t_0<t_e$. If $f(t_0)=0$ and $f(t)>0$ for $t \in (t_0, t_e)$ then $\exists\, t_1$ such that $t_0 < t_1 < t_e$ and $df(t)/dt > 0$ for $t \in (t_0, t_1)$.

Or, stated in its qualitative version,

CID_1

If $[f(t_0)]=[0]$ and $[f(t)]=[+]$ for $t \in (t_0, t_e)$ then $\exists t_1$ such that $t_0 < t_1 < t_e$ and $\partial f(t)=[+]$ for $t \in (t_0, t_1)$.

Informally, this says: if a variable is zero initially and then becomes positive in an interval, there must exist an initial (but potentially shorter) time interval during which both the variable and its derivative are positive (no matter what happens after this interval). This rule and other variants of it can be encoded as constraints and used to create state descriptions that contain information about derivatives, in our case about qualitative derivatives of deviations. Because the observations themselves are not explicitly related to specific time periods, the same holds for this derived information. We need to state more properties of the problem domain, or introduce more assumptions.

4.3 Adding Assumptions

Checking consistency of the set of observations with the *state-constraints* makes only sense if the individual observations refer to the same state. This means we need to assume that those **observations** that, together with a part of the model, establish a **discrepancy**, actually occur during **overlapping time intervals.**

The intervals (t_0, t_1) introduced by the CID_1 rule for the different deviations must have a non-empty intersection. Note, that we do **not** have to postulate that **all** existing deviations have to occur at the same time, but only those that are used to detect one discrepancy. In our application, we make an assumption that entails the first one, namely that the related effects of faults occur at the beginning of some phase (operation mode of the ABS), which provides the „synchronizing" initial time point t_0. This means, the phase starts with no deviation : $[\Delta f] = 0$ at t_0.

Furthermore, in this case study, we make the assumption that only valves, throttles with dampers or pump elements can be faulty.

4.4 Using Models and CID_1 for Prediction

In this subsection, we illustrate how the approach described, namely

- state-based diagnosis with
- qualitative deviation models and
- observations extended through CID-constraints,

works on our example (see Figure 6 for reference). Recall that the initial observations were:

- under-braked left-hand wheel: $[\Delta v_L] = [+]$.
- over-braked right wheel: $[\Delta v_R] = [-]$.
- too hard brake pedal: $\partial \Delta s_{PED} = [-]$.

Under the assumption that the pressure-buildup phase started at t_0 with no deviation, CID_1 yields that

$[\Delta v_L] = 0$ at $t_0 \wedge [\Delta v_L] = [+]$ after t_0
$\Rightarrow [\partial \Delta v_L] = [+]$ after t_0 ,

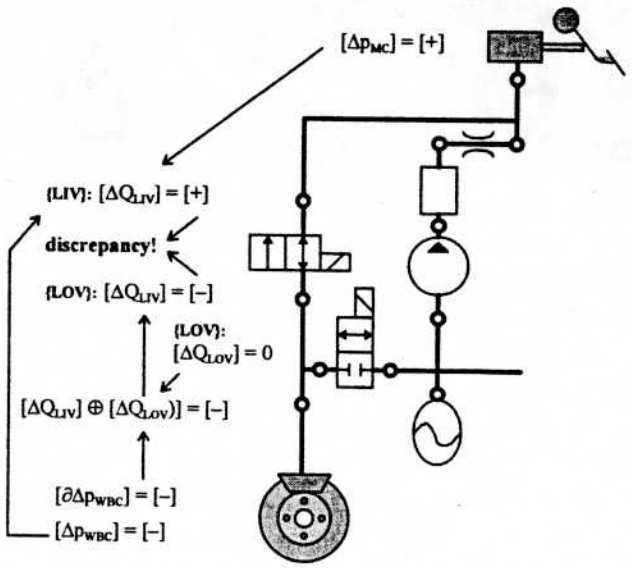


Figure 6: Inferences at left wheel brake cylinder

From this, the model of the left wheel brake cylinder infers

$[\partial \Delta v_L] = 0$ at $t_0 \Rightarrow [\Delta p_{WBC}] = 0$ at t_0
$[\partial \Delta v_L] = [+]$ after $t_0 \Rightarrow [\Delta p_{WBC}] = [-]$ after t_0.

By applying CID_1 again, we establish a link between this deviation of the brake cylinder pressure and the deviation of its derivative:

$[\Delta p_{WBC}] = 0$ at $t_0 \wedge [\Delta p_{WBC}] = [-]$ after t_0
$\Rightarrow [\partial \Delta p_{WBC}] = [-]$ after t_0.

The model of the node that joins the terminals of wheel brake cylinder, left outlet valve and left inlet valve then derives

$[\partial \Delta p_{WBC}] = [-]$ after t_0
$\Rightarrow [\Delta Q_{LOV}] \oplus [\Delta Q_{LIV}] = [-]$ after t_0.

The correct behavior of the left outlet valve in the pressure-buildup mode states that

$[\Delta Q_{LOV}] = 0$ at t_0 and after t_0.

This, together with the model of the node, yields a negative deviation of the flow through the left inlet valve:

$[\Delta Q_{LIV}] = [-]$ after t_0.

Note that we cannot determine the actual direction of flow, i.e. it is not possible to distinguish whether there is a flow from the master cylinder to the wheel brake cylinder which is smaller than usual, or there exists an increased fluid flow in the opposite direction.

From the observation at the brake pedal, the pedal model infers that the pressure in the master cylinder deviates in positive direction:

$[\partial \Delta s_{PED}] = [-]$ after $t_0 \wedge [\Delta f_{PED}] = 0$ after t_0
$\Rightarrow [\Delta p_{MC}] = [+]$ after t_0.

The increased pressure of the master cylinder and the decreased left wheel brake cylinder imply an increase in pressure drop across the left inlet valve:

$[\Delta p_{MC}] \ominus [\Delta p_{WBC}] = [+]$ after t_0.

Failure cause	Failure effect	
inlet valve profile clogged	pressure increase rate too small	under-braking of the respective wheel, over-braking of other wheels possible, hard braking pedal, worst case: car yawing
inlet valve stuck open or punctured	pressure retaining not possible	too high retardation on one wheel due to pressure on main cylinder, wheel tends to lock up
outlet valve stuck open or punctured	pressure retaining not possible	accumulator gets filled, pedal has to be moved a greater distance, braking less effective on diagonally opposite wheels
pump element defective	low pressure level not achieved	affected wheels tend to lock up
hydraulic unit not properly vented	air in primary circle	under-braking on the affected diagonally opposite wheels, pedal soft

Table 2: Failure effects for the hydraulic unit from a system FMEA

With the information that the left inlet valve is opened in the pressure-buildup phase, the model of the valve predicts a positive deviation of flow through the component:

$[\Delta Q_{LIV}] = [+]$ after t_0.

This contradicts the negative deviation of flow that has been inferred first, and a discrepancy is detected with the underlying conflicting correctness assumptions

{left inlet valve, left outlet valve},

i.e. one of these components must be broken. The observations for the right-hand wheel brake cylinder can be processed in a similar manner and reveal a second conflict

{left inlet valve, right inlet valve,
right outlet valve, throttle, pump element}.

These two conflicts suffice to produce the **left inlet valve** as the **only** possible **single fault** candidate and a number of potential double faults.

4.5 Adding Domain Axioms

In principle, to further refine conflicts, we could use fault models for the components in the style of GDE$^+$ ([Struss, Dressler 89]). The problem is that the models stated above can only derive deviations, but not the direction of flow through a component. However, meaningful fault models would require actual directions of pressure drops and flow. For example, a valve with no deviation of the pressure drop but a flow which is too low is consistent both with a too low and too high valve profile, if the direction of flow is unknown. Deriving this information would need a richer domain than just signs.

Instead, we adopted an approach using domain axioms to further refine the conflicts. The domain of the profile A of a valve is {0, [+]}, and its deviation ΔA can either be negative, zero or positive. We make model-based prediction more complete by adding the disjunctions of values local to components occurring in a conflict. It turns out that in our example, the right inlet valve then does not contribute to the second conflict in the sense that for each combination of values for A and ΔA, we obtain an inconsistency with the rest of the components in the conflict. Therefore, the conflict is reduced to

{left inlet valve, right outlet valve, throttle,
pump element}.

With this reduced conflict, we get

{left inlet valve}

as the only single fault candidate, as before, and

{left outlet valve, right outlet valve},
{left outlet valve, throttle},
{left outlet valve, pump element}

as the possible double faults. Indeed, the system successfully inferred a fault in the left inlet valve from the failure effects listed for a clogged left inlet valve in the FMEA.

4.6 Empirical Results

We carried out a number of experiments for several relevant failures (Table 2). They were selected based on an existing failure mode and effects analysis of the system. The guiding criteria which led to this selection were on the one hand the estimated probabilities of occurrence (as stated in the FMEA), and on the other hand concrete experience of workshop technicians. In addition, wrong mounting of the device or leaks are also relevant in practice. However, most likely, leaks would trigger the switch for the level of brake fluid and activate a warning lamp before affecting the functionality of the ABS.

For evaluation of the models and the approach, the symptoms of a particular failure cause listed by the FMEA were fed into the diagnosis procedure, and the success criteria was whether the respective cause occurred in the candidates generated and how well it could be isolated. The approach turned out to be fairly successful: for each sample of failure effects, fault localization was successful in the sense that the respective component failures were included in the set of single fault diagnoses, sometimes being the only possible single fault (Table 3).

Observation: Failure effects for fault	Candidates generated
left inlet valve profile clogged	**{left inlet valve}**, {left outlet valve, right outlet valve}, {left outlet valve, pump element}, {left outlet valve, throttle}
left inlet valve stuck open or punctured	**{left inlet valve}**, {left outlet valve, right inlet valve}, {left outlet valve, right outlet valve}, {left outlet valve, pump element}
left outlet valve stuck open or punctured	**{left outlet valve}**, {right outlet valve}, {throttle}, {pump element}
pump element defective	**{pump element}**, {left outlet valve}, {right outlet valve}, {right inlet valve}, {damper}
hydraulic unit not properly vented	**{compressibility}**, {throttle}, {pump element}, {left outlet valve}, {right outlet valve}

Table 3: Candidates generated with the failure effects as observations

5 Discussion

This case study extends the list of pieces of evidence that state-based diagnosis can very well suffice to diagnose dynamic systems (related work is described in [Dressler 96], [Chantler et al. 96], [Malik, Struss 96]). In [Struss 97], we present a more formal analysis of preconditions and limitations to this approach. Much more work is needed to develop good designs and criteria for it to be advantageous. This will require a more detailed analysis of the form and contents of the *CID-constraints* and their possible applications and relating their results to various limitations in measurability.

Our example also demonstrates that very weak qualitative observations can be exploited to get close to human diagnostic results under such conditions. This is a benefit of qualitative modeling combined with deviation models. However, we have to make a number of fairly strong assumptions to make diagnosis work, in particular, to compensate for the unspecified temporal scope of the observations. The assumption that the occurrence of symptoms is synchronized appears questionable, especially if we take multiple faults into consideration. Also, in our example, we presented diagnosis only for the pressure buildup phase. This is reasonable, but, in principle, deviating pressure could also result from a malfunction that affects the pressure-reduction phase. A diagnostic system would either need to exhaustively perform the analysis for all phases or require some (model-based) reasoning to pick the informative phases.

Acknowledgments

We would like to thank the members of the model-based systems and qualitative reasoning group Munich, O. Dressler, U. Heller, A. Malik and J. Mauss for their valuable contributions and T. Beschta, G. Biswas, M. Chantler, P. Nayak, and B. Williams, as well as many participants of the QR-96 and DX-96 workshops for interesting discussions and contributions. This work was supported in part by the Commission of the European Union (Project VMBD, #BE 95/2128) and by the German Ministry of Education and Research (# 01 IN 509 41).

References

[Bosch 96] Robert Bosch GmbH (ed.): Automotive Handbook (4th edition). *Society of Automotive Engineers (SAE)*, Warrendale, 1996

[Chantler et al. 96] M. J. Chantler, S. Daus, T. Vikatos and G. M. Coghill, The Use of Quantitative Dynamic Models and Dependency Recording for Diagnosis. *Workshop Notes of the 7th International Workshop on Principles of Diagnosis (DX-96)*, Montreal, 1996

[Dressler, Struss 96] Dressler, O., Struss, P., The Consistency-based Approach to Automated Diagnosis of Devices. *In: Brewka, G. (ed.), Principles of Knowledge Representation, CSLI Publications*, Stanford, 1996

[Dressler 96] Dressler O., On-line Diagnosis and Monitoring of Dynamic Systems based on Qualitative Models and Dependency-based Diagnosis Engines. *In: Wahlster, W., (ed.), Proceedings of the European Conference on Artificial Intelligence (ECAI-96)*, John Wiley & Sons, 1996

[Malik, Struss 96] Malik, A., Struss, P., Diagnosis of Dynamic Systems Does Not Necessarily Require Simulation. *Workshop Notes of the 10th International Workshop on Qualitative Reasoning (QR-96)*, AAAI Press, 1996

[Struss 97] Struss, P., Fundamentals of Model-Based Diagnosis of Dynamic Systems. *To appear in: Proceedings of the 15th International Joint Conference on Artificial Intelligence (IJCAI-97)*, Nagoya, Japan, 1997

[Struss, Dressler 89] Struss, P., Dressler, O., Physical Negation - Integrating Fault Models into the General Diagnostic Engine. *Proceedings of the 11th International Joint Conference on Artificial Intelligence (IJCAI-89)*, Morgan Kaufmann Publishers, San Mateo, CA, 1989

[Struss et al. 95] Struss, P., Malik, A., Sachenbacher, M., Qualitative Modeling is the Key. *Workshop Notes of the 6th International Workshop on Principles of Diagnosis (DX-95)*, Goslar, Germany, 1995