In: Dearden, R. and Snooke, N. (eds.). Proceedings of the 23rd Workshop on the Principles of Diagnosis. Great Malvern, UK. 2012

Modeling Hydraulic and Software Components for Automated FMEA of a Braking System

P. Struss, A. Fraracci

Tech. Univ. of Munich
Munich, Germany
struss@in.tum.de, fraracci@in.tum.de

ABSTRACT

This paper presents work on model-based automation of failure-modes-and-effects analysis (FMEA) applied to the hydraulic part of a vehicle braking system. We describe the FMEA task and the application problem and outline the foundations for automating the task based on a (compositional) system model. Models of the essential hydraulic components suitable to generate the predictions needed for the FMEA are introduced and the required models of the control software outlined. These models are based on constraints, rather than simulation (or envisionment construction), and capture the dynamic response of the systems to an initial situation based on one global integration step and determine deviations from nominal functionality of the device. We also present the FMEA results based on this model.

1 INTRODUCTION

Failure-modes-and-effects Analysis (FMEA) has attracted some qualitative modeling work pursuing the goal of automating the task. FMEA, a mandatory task in the automotive and aeronautics industries, is performed by groups of experts during the design phase of a system. Its core is to exhaustively go over all potential component faults and predict their impact on the functionality of the system in order to assess whether it can lead to a critical situation and violate safety requirements.

There are several reasons why FMEA is a suitable application, but also a challenge to qualitative modeling:

- During early design stages, only a blueprint may be available, and even when a physical prototype exists, it may be too costly, risky, or even impossible to implant certain faults in the physical system. Hence, a **model-based** solution is required.
- Exact parameter values of the design may still be undetermined. Hence, the analysis cannot be based on numerical, but only on **qualitative** models.
- Even if the parameters do have fixed numerical values, the analysis is inherently **qualitative** both w.r.t input (classes of faults, such as “a leakage”, rather than “leakage of size x”) and relevant effects (“loss of pressure in wheel brake” and “potentially reduced deceleration”).
- The modeling effort must be low to handle a class of systems and to support repetitive FMEA of design variants and modifications. This needs to be addressed by **compositional modeling**, which has to be based on a library of generic, context-independent component models.

In fact, FMEA has been (to our knowledge) the first of up-to-date few successful applications of qualitative modeling. The AutoSteve system [Price, 2000] was specialized on performing FMEA of electrical car subsystems. The AUTAS project developed a generic FMEA tool with applications to electrical, hydraulic, pneumatic, and mechanical systems in aeronautic systems [Picardi *et al.*, 2004].

In collaboration with a German car manufacturer, we applied this algorithm to FMEA of a novel braking system.

In particular the requirement of compositionality and re-use of models leads us to base the analysis on first-principles models of the **physical behavior**, rather than on **functional** models. It turns out that this also provides a key to modeling the embedded software and its faults in a straightforward and manageable way.

This confronts us with the need for models of hydraulic components, especially valves, that are, on the one hand, general enough to be reusable and, on the other hand, powerful enough to deliver the predictions relevant to FMEA of braking systems. In addition, they should be simple enough to be inspected and maintained easily and also efficient. The qualitative modeling and diagnosis literature contains quite a few presentations of valve models. But, to say the least, most of them may serve the purpose of illustrating a principled idea, but are not a suitable basis for a serious industrial application.

In this paper, we present the core of models that have proven to successfully produce the results needed for FMEA of the braking system. The key features of the models are that they

- capture one integration step, but avoid simulation or generating envisionments and are stated in terms of constraints (finite relations),
- are compositional and context-independent,
- analyze how a stimulus in terms of a local pressure change (e.g. pushing a brake pedal) propagates through the system,
- capture qualitative deviations of pressure and flow from their nominal values resulting from component faults,
- can be complemented by models of the control software functions for both their correct and their faulty behavior, due to the high level of abstraction.

The paper first describes the application context, FMEA of braking systems, and then summarizes the foundations of model-based FMEA. In section 4, we present the key parts of the models. The results obtained for FMEA are discussed in section 5. Section 6 outlines the software model.

2 APPLICATION CONTEXT

2.1 FMEA

"Failure mode and effects analysis (FMEA) is a logical and structured analysis of a system, subsystem, piece part, or function. Identified in the analysis are potential failure modes, their causes and the effects associated with the failure mode's occurrence at the piece part, subsystem and system levels and its severity rating." ([SAE, 1993]).

In practice, this means that a group of experts goes through the design of a system, considers all possible faults of all involved components, and attempts to identify their impact on the functionality of the system and on safety requirements. Its first purpose is the early identification of all catastrophic and critical failures in order to avoid or minimize/mitigate them through a design correction. Performing the task is costly, because precious expert working hours are spent, and it is error prone, because human analysis tends to be incomplete. It is also repetitive, because, at least in theory, it should be applied after major design modifications. The procedure is described in [MIL, 1980; SAE, 1993]. A conceptualization and examples are given in [Fraracci, 2009].

The focus of the work reported in this paper is on automatically determining the local and global effects of each failure mode (i.e. component fault).

2.2 The Braking System

The target is a novel braking system whose details are proprietary. For safety reasons, it still has to comprise the traditional braking function. Therefore, we use this part of the system in order to illustrate our solution.

A standard braking system is mainly composed of hydraulic and mechanical components and the electronic control unit (ECU) and its software. It contains a tandem pedal actuation unit (with two pistons and two chambers), valves (inlet and outlet types) and wheel brakes, shown in Figure 1.

The pedal actuation block (top right) comprises two

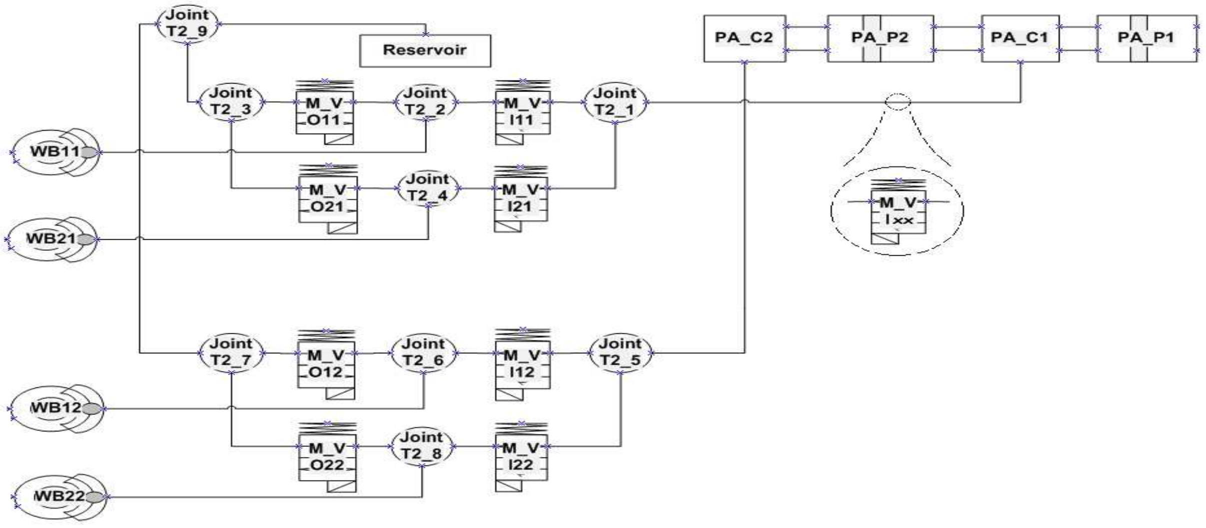


Figure 1 - Braking system. Pressure is generated by two pistons, PA_P1,2, in two chambers, PA_CA1,2, and reaches the wheel brakes, WBij, via open inlet valves, M_VIij, while outflow is blocked by closed outlet valves, M_VOij. The impact of inserting another valve, M_Vixx, is discussed in section 5.3

pistons (PA_P1 and PA_P2) and the two chambers (PA_C1 and PA_C2), where PA_P1 is directly affected by pushing the brake pedal. Each chamber produces pressure for one diagonal wheel pair, and each wheel brake (WB11, 12, 21, 22) sits between an inlet valve and an outlet valve.

The inlet-valves (M_VI11, 12, 21, 22) behave as piloted check valves; during standard braking (i.e. with no command), they are open, while the outlet-valves (M_VO11, 12, 21, 22) are closed. Pushing the brake pedal causes pressure to build up in the wheel brakes. Inlet valves always allow a flow back from the wheel brakes, which causes the diminishing of the wheel brake pressure if the brake pedal is released.

When operated under the Anti-lock-braking system (ABS), the valves are controlled by commands from the ECU. The pressure-build-up phase is the scenario described above. For pressure maintenance, the inlet valve is closed. If the speed sensors indicate that the wheels tend to lock up, the outlet valves are opened to release pressure, let the wheels spin again and, thus, enable steering of the vehicle. Then the cycle is entered again.

Typical inferences required for FMEA are

- If an inlet valve is stuck closed under normal braking, the respective wheel will be underbraked (reduced deceleration).
- The same holds if an outlet valve is stuck open under normal braking.
- If an outlet valve is stuck closed during the pressure release phase of ABS braking, the respective wheel will be overbraked, because the pressure is not released.
- An inlet valve being stuck open during this phase will have the same impact.

Other faults are leakages of the wheel brakes and the chambers, the wheel brakes and pistons being stuck etc.

3 MODEL-BASED FMEA

Predicting the impact of (classes of) faults is the core of the FMEA task. As argued in the introduction, this is a challenge to model-based systems technology. In this section, we illustrate the logical foundation of model-based FMEA.

3.1 Relational Models

Our models are qualitative, and they use finite qualitative relations over variables; hence, a behavior model is regarded as a relation *R* over a set of variables that characterize a component or system: $R\subset DOM(\underline{v})$, where $\underline{v}$ is a vector of system variables with the domain $DOM(\underline{v})$, which is the Cartesian product

$$DOM(\underline{v}) = DOM(v_1) \times DOM(v_2) \times ... \times DOM(v_n).$$

So, a relation *R* (i.e. a *constraint*) is a subset of the possible behavior space.

If elementary model fragments R_{ij} are related to behavior modes $mode_i(C_j)$ of the component C_j, then an aggregate system (under correct or faulty conditions) is defined by a mode assignment $MA = \{mode_i(C_j)\}$ which specifies a unique behavior mode for each component of this aggregate whose model is obtained as the join of the mode models, i.e. the result of applying a (complete version of) constraint satisfaction to $\{R_{ij}\}$:

$$R_{MA}= \bowtie R_{ij} .$$

3.2 Formalization of FMEA

To support FMEA, it is necessary to determine whether the effects of a certain component fault (represented as a mode assignment *MA*) violate an intended function of the system. If the function is considered as part of *GOALS*, then the task might mean to check whether the fault model FM_{MA} is inconsistent with the function:

$$FM_{MA} \cup GOALS \vdash^{?} \perp$$

Often, the analysis is carried out for particular mission phases (such and “cruising” or “landing” of an aircraft) or scenario S_k (e.g. the three phases of the ABS braking as explained above):

$$FM_{MA} \cup S_k \cup GOALS \vdash^{?} \perp$$

In practice, FMEA is not carried out this way, but by specifying effects E_i, which are specific violations of the intended function (*GOALS*), for instance too high and too low deceleration of a wheel, i.e. underbraking and overbraking:

$$S_k \cup E_i \vdash \neg GOALS \ ,$$

and the analysis determines the effects that may occur under a particular failure mode:

$$FM_{MA} \cup S_k \cup E_i \nvdash \perp$$

Since models, scenarios, and effects can all be represented by relations, we can characterize and compute the effects of the FM_{MA} as follows:

- $R_{MA} \bowtie S_k \subset E_1$
  if the failure mode is included in effect, then the effect will **definitely occur** (case E_1 in Figure 2)
- $R_{MA} \bowtie S_k \cap E_2 = \emptyset$
  if the intersection is empty, the effect **does not occur** (case E_2)
- otherwise
  the effect **may occur**: E_3

An example can be found in [Fraracci, 2009].

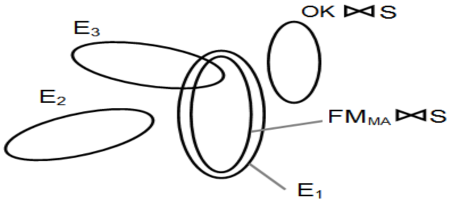


Figure 2 - Effects computation

3.3 Deviation Models - Formalization

FMEA is about inferring deviations from nominal system function due to a deviation from nominal component behavior. Hence, not the magnitude of certain quantities matter, but the fact whether or not they deviate from what is expected under normal or safe behavior.

This is why deviation models [Struss, 2004] offer the basis for a solution: they express constraints on the deviations of system variables and parameters from the nominal behavior and capture how they are propagated through the system.

For each system variable and parameter v_i, the deviation is defined as the difference between the actual and a reference value: $\Delta v := v_{act} - v_{ref}$.

Then algebraic expressions in an equation can be transformed to deviation models according to rules like

$$a + b = c \Rightarrow \Delta a + \Delta b = \Delta c$$

$$a * b = c \Rightarrow a_{act} * \Delta b + b_{act} * \Delta a - \Delta a * \Delta b = \Delta c$$

Furthermore, for any monotonically growing (section of a) function $y = \mathrm{f}(x)$, we obtain $\Delta y = \Delta x$ as an element of a qualitative deviation model.

For instance, the deviation model of a valve is given by the constraint

$$\Delta Q = A * (\Delta P_1 - \Delta P_2) + \Delta A * (P_1 - P_2) - \Delta A * (\Delta P_1 - \Delta P_2)$$

on the signs of the deviations of pressure (ΔP_i), flow (ΔQ), and area (ΔA). This constraint allows, for instance, to infer that P_1 being too large ($\Delta P_1 = +$) causes an increased flow ($\Delta Q = +$), if P_2 and the area remain unchanged ($\Delta P_2 = 0$, $\Delta A = 0$) and the valve is not closed ($A = +$). Such qualitative deviation models can be constructed from equational component models, if they exist.

4 HYDRAULIC MODELS

As stated in the introduction, the literature on qualitative modeling does not deliver a ready-made library of hydraulic models that could be used for real applications like the one we are tackling. Rather than arguing about particular trials on valve models in the literature, we ask why qualitative modeling of hydraulic systems is hard – compared, for instance, to modeling of digital circuits or resistive networks, the favorites of many qualitative modeling and model-based systems research.

One of the crucial differences is, of course, that for hydraulic circuits the dynamics are in the focus of interest. While for a resistive network, the steady state matters, rather than how it is established almost instantaneously, the analysis of hydraulic systems focuses on the transition, while the finally reached equilibrium may be boring (all connected parts with equal pressure). Pressures determine flows, which in turn determine change of pressure. Hence, the analysis has to include some integration step (in the mathematical sense). Of course, the same applies to electrical circuits with capacitors and inductors.

Another problem dimension, which is not the focus of this paper, is related to the fact that often, the nature of the stuff that flows cannot be ignored, e.g. when there is air in a hydraulic circuit.

In the following, we present the core pieces of qualitative hydraulic model that we used to solve the FMEA task. Our starting point was our early work on modeling for diagnosis of braking systems ([Struss *et al.*, 1997]), and we created

- a **relational** model that
- **qualitatively** captures the system's direct **response** to some **initial condition**, especially
- in terms of **deviations** from nominal behavior, and
- can be **used by the FMEA engine** whose basis was outlined in section 3.2.

Despite its simplicity, it turns out to be quite powerful and appropriate for generating the kind of information needed for the FMEA task. We first characterize its scope by discussing the most important requirements and modeling assumptions underlying it and then present the various "slices" of the key component models, namely valve and volume.

4.1 Modeling Assumptions and Requirements

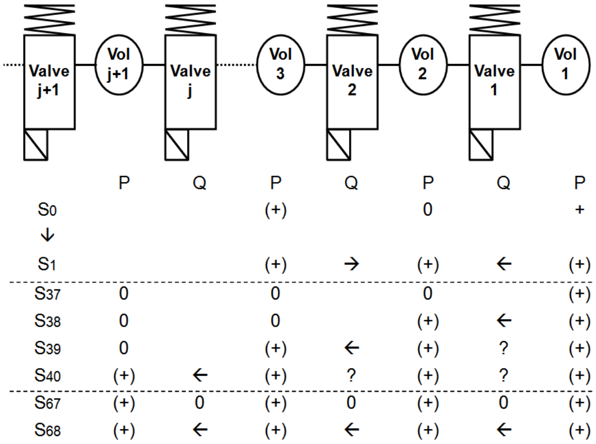
In the current model, we assume that there is one source of pressure, or, more precisely, a unique maximal pressure level generated by components or some external force. In our application, this is determined by the driver pushing the brake pedal. It is not fixed to a particular numerical value, but, rather, by the fact that the pressure in the system cannot exceed it. We are convinced that the approach can be extended to multiple source levels, but did not implement such a model and make no claims.

This assumption is reflected by the chosen domain for pressure:

PosSign3:={0, (+), +},

where + is the source pressure (and maximal), 0 corresponds to the sink (in our case the reservoir of the liquid), and (+) is any pressure in between. For pressure drops and flows, only their direction matters, i.e. their domain is Sign = {-, 0, +}. Valves are assumed to be either closed ($A = 0$) or open ($A = +$), which does not imply they are **completely** open.

The next assumption (a requirement of our application) is that the interest is in determining the systems direct response to an initial situation. To illustrate what this means (and what is excluded), consider the right-hand part of Fig. 3 with a volume component Vol_2, with initial pressure 0, connected via open valves on the right to a volume Vol_1 with pressure



	P	Q	P	Q	P	Q	P
S_0			(+)		0		+
↓							
S_1			(+)	→	(+)	←	(+)
S_{37}	0		0		0		(+)
S_{38}	0		0		(+)	←	(+)
S_{39}	0		(+)	←	(+)	?	(+)
S_{40}	(+)	←	(+)	?	(+)	?	(+)
S_{67}	(+)	0	(+)	0	(+)	0	(+)
S_{68}	(+)	←	(+)	←	(+)	←	(+)

Figure 3 - Volume-Valve sequence

P=+ in the initial scenario S_0, and on the left to another volume Vol_3 with initial pressure (+). The state following this initial situation will be a state with positive inflows Q into Vol_2, and this is what the model should predict (scenario S_1 in Fig. 3). There may be a next state, in which the pressure in Vol_2 exceeds the one in Vol_3, and the flow through the respective valve reverses. Capturing this in general, may lead to ambiguous predictions, since in case of several such events, their presence and order is undetermined, and several alternatives may result.

As a consequence, we also assume that no other event occurs during the period of interest, especially that no valve changes its state. We furthermore assume pressure to be homogeneous in a volume and ignore time required to achieve or approximate the situation.

To simplify the presentation in this paper, we assume that there are no deviations in the initial situation. This assumption can be dropped if the system response to a deviating initial situation is of interest.

We now present the different elements of the models, which are summarized in Figure 4.

4.2 Base Models

The core of the models is given by the qualitative abstractions of the standard (differential) equations. A key requirement is that the component models are local and context-independent in order to be compositional as required by the application task.

For the valve, the terminals T_i are its hydraulic connections (it has another one for the control command). With the convention that a positive flow is going into the respective component, we obtain

$$T_1.Q = A^* (T_1.P\text{-}T_2.P) \text{ ,}$$

where pressure subtraction

$$- : \{0, (+), +\}\ \{0, (+), +\} \rightarrow \{-, 0, +\}$$

is defined as

$$0 - 0 = + - + = 0,$$

$$+ - (+) = + - 0 = (+) - 0 = +$$

$$0 - (+) = 0 - + = (+) - + = -$$

$$(+) - (+) \text{ unrestricted.}$$

The second element is Kirchhoff's Law (see Fig. 4).

Since A is the **actual** opening of the valve, these elements apply to all behavior modes of a valve except leakages.

The base model of a **volume** is straightforward. To simplify the presentation, we consider a volume with only one terminal (like the wheel brake). If there is more than one terminal, $T_1.Q$ is replaced by the sum of all flows across all terminals (or the volume is connected to a joint capturing the various flows, as done in the brake model). In case of a leakage, also the resulting leak flow has to be included. ∂P denotes the qualitative derivative with the domain Sign.

The results obtained by this base model do not always contain an answer relevant to the FMEA task. In our brake system, normal braking happens when the inlet valve is open and the outlet valve is closed. The consequence is pressure (+) in the wheel brake. If the outlet valve is stuck-open, there will be an outflow (after one integration step). The wheel brake pressure is still (+). But the important point is: it is less than under nominal conditions. Therefore, we add a layer of deviation models, as shown in Figure 4.

<table>
<tr><th></th><th>Valve</th><th>Volume</th></tr>
<tr><td>Base model</td><td>$T_1.Q=A^*(T_1.P\text{-}T_2.P)$
$T_1.Q = \text{-}T_2.Q$</td><td>$T_1.Q = \partial P$</td></tr>
<tr><td>Base model derivative</td><td>$T_1. \partial Q = A^*(T_1. \partial P\text{-}T_2. \partial P)$
$T_1. \partial Q = \text{-}T_2. \partial Q$</td><td></td></tr>
<tr><td>Deviation model</td><td>$T_1.\Delta Q = \Delta A^*P_{diff} + +A^*\Delta P_{diff}\text{-}\Delta A^*\Delta P_{diff}$
$P_{diff} = T_1.P\text{-}T_2.P$
$T_1.\Delta Q = \text{-}T_2.\Delta Q$</td><td>$T_1.\Delta Q = \Delta\partial P$</td></tr>
<tr><td>Continuity Integration Persistence</td><td>
<table>
<tr><th>Q_0</th><th>∂Q</th><th>Q</th></tr>
<tr><td>-</td><td>□</td><td>-</td></tr>
<tr><td>0</td><td>-</td><td>-</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>+</td><td>+</td></tr>
<tr><td>+</td><td>□</td><td>+</td></tr>
</table>
</td><td>
<table>
<tr><th>P_0</th><th>∂P</th><th>P</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>+</td><td>(+)</td></tr>
<tr><td>(+)</td><td>*</td><td>(+)</td></tr>
<tr><td>+</td><td>-</td><td>(+)</td></tr>
<tr><td>+</td><td>0</td><td>+</td></tr>
</table>
</td></tr>
<tr><td>Integration Deviation</td><td>$T_i. \Delta\partial Q = T_i. \Delta Q$</td><td>$\Delta P = \Delta\partial P$</td></tr>
</table>

Figure 4 - The elements of valve and volume models

4.3 Deviation Models

The deviation models are easily obtained from the algebraic equations of the base model. However, they are quite powerful and provide the predictions we need for FMEA. In the above scenario, the inflow via the inlet valve will have a deviation 0, while the flow towards the outlet valve has a negative deviation (being negative instead of 0), and, hence, will cause a negative deviation $\Delta\partial P$ ("reduced pressure built-up").

Again, the deviation model applies to each instance of time. But still, we need to answer the question how we represent and predict the overall system response properly.

4.4 Integration, Continuity, Persistence

This model, which applies to every point in time, has limited utility. Consider again a sequence of three or more connected volumes (as in Figure 3), each with initial pressure 0, except for Vol_1, which has a pressure (+). What we would like to predict is a flow through all valves from right to left (scenario S_{37} in Fig. 3). The model as it stands will predict a flow into Vol_2 and zero flows, otherwise (S_{38}). Of course, the pressure derivative in Vol_2 is positive. Hence, after integration, the pressure becomes (+), too, and applying the model will lead to a flow from Vol_2 to Vol_3 – but leave the flow from Vol_1 to the second Vol_2 unrestricted, because of pressure=(+) for both (S_{39}). If there are n more volumes, n integration steps are required in order to let the flow reach the last one – and leave all other flows undetermined. – Obviously, this is not what we need.

In our model, we consider two temporal slices of the system behavior: the initial situation and the one capturing the direct global system response, i.e. a representation of the state after the effect of pressure differences has been propagated to all (connected) parts of the system. This means, we neglect the time needed for this propagation and apply some kind of "temporal factorization" ([Pietersma and van Gemund, 2007]).

The initial state is characterized by variables P_0, Q_0, etc., while the next state is represented by P, Q, etc.

Then the integration step can be represented as a constraint on different variables, namely P_0, ∂P, P. The crucial point is that we do **not** choose ∂P_0, but ∂P, i.e. the derivative **after** the impact. Figure 4 shows the respective constraint in row 4. It expresses more than the continuous transition from P_0 to P dependent on ∂P. It excludes transitions from (+) to + or 0, expressing the restriction of the predictions to the next state (which implies the exclusion of state-changing events).

Starting from some initial situation and the respective values of P_0, Q_0, etc., how can we determine ∂P instead of only ∂P_0? This is supported by the constraint on flows shown in row 4 of Figure 4. Again, it captures more than continuity: non-zero flows are considered to be persistent, which again expresses the restriction to the next qualitative state and the exclusion of events that change the direction of flow. This achieves the intended prediction, for instance, for the volume sequence discussed above: Q_0 and hence, also Q from Vol_1 to Vol_2 is determined to be non-zero, which suffices to determine ∂P = + and P = (+) for Vol_2. This implies a positive flow into Vol_3, etc.

Without further distinctions between sink and source pressures, i.e. within (+), the model developed, so far, may appear quite weak, being unable to determine the direction of flow between two volumes with pressure (+). Consider another initial scenario, S_{67}, for the hydraulic chain in Fig. 3, where initially, all volumes have pressure (+), the valves are open, but there are no flows across them (because all volumes have exactly the same pressure). If we connect Vol_1 to a source (pressure +) and the left-most valve to a sink (pressure 0), again we expect a flow from right to left (S_{68}). However, the presented model is unable to derive this, because the inflow to Vol_1 leaves its pressure at (+), and the flow through Valve_1 remains undetermined. What enables us to predict the change is the consideration that the pressure in Vol_1 has increased, exceeds the one in Vol_2 and, hence, produces a flow into Vol_2, and so on. We can capture this by adding a derivative of the base model that links change in pressure and change in flow, as shown in row 2 of Fig. 4. This model successfully generates the expected result S_{68}.

Finally, we add a constraint that integrates the deviations (row 5 of Figure 4). Intuitively, this states that if the derivative of a quantity deviates from the nominal value, then so does the quantity itself. This is based on the assumption that the initial situation does not contain deviations. If it is dropped, an initial pressure deviation has to be added.

5 FMEA RESULTS

5.1 Scenarios

We used the model whose core has been outlined in section 4 to produce an FMEA of the braking system outlined in section 2 for a number of scenarios: braking and non-braking with/without ABS for a moving/no-moving car. In the following, we focus on the scenario "Standard braking while car moving", which is identical to the 1st phase of ABS braking as explained in section 2.2. This scenario is defined as:

- no commands to all valves: Cmd = 0 (i.e. under normal conditions inlet valves open, outlet valves closed)
- the initial hydraulic pressure of all wheel-brakes are zero: $\text{WB}_{xy}.P_0 = 0$
- velocity $v > 0$ for all: $\text{WB}_{xy}.v$ = +

- constant pressure P on the piston PA_P$_1$ exerted by the brake pedal: PA_P$_1$.P = +.
- no deviation of the pedal pressure: PA_P$_1$.$\Delta P = 0$ and PA_P$_1$.$\Delta\partial P = 0$

For the "maintain pressure" phase, the commands to the inlet valves are set to 1, and the wheel brake pressures are (+) (from the previous phase). In the "release pressure" scenario, the commands to the outlet valves also become 1.

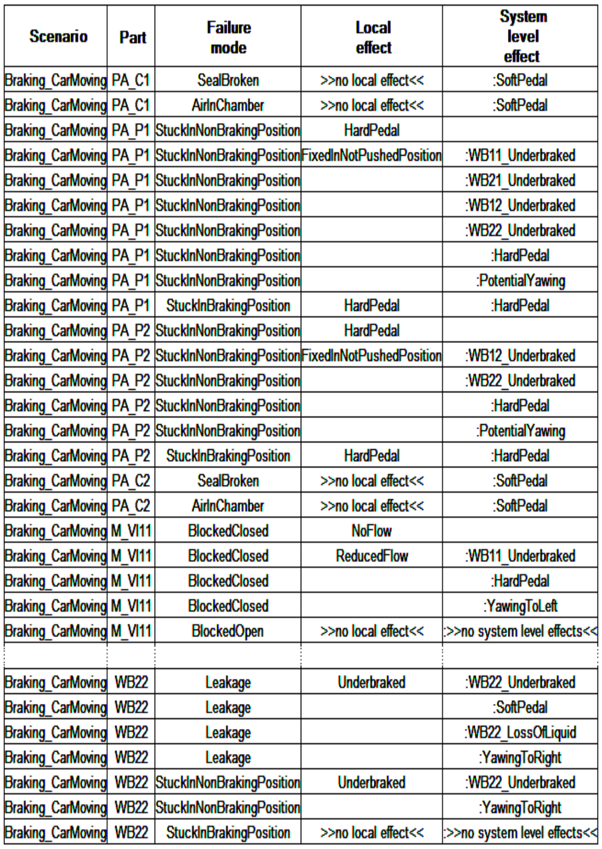
5.2 System Level Effects

The system effects are defined by the experts as the relevant deviations from the intended function. For the braking system, this includes the following effects:

- **soft pedal,** P = +; $\Delta P = 0$ and $\Delta\partial pos$ = +; where *pos* indicates the position of piston PA_P$_1$: when pushed (without deviation), the piston (and, hence, the pedal) moves faster than normal
- **hard pedal,** like soft pedal with $\Delta\partial pos$ = -
- **underbraking,** reduced deceleration of a wheel: WB$_{xy}$.$\Delta\partial v$ = + where xy indicates the wheel involved
- **overbraking,**
  too much deceleration: WB$_{xy}$.$\Delta\partial v$ = -
- **potential no steering,** both front wheels are underbraked (and, hence, may lock up)
- **yawing to left,**
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$ + WB$_{22}$.$\Delta\partial v$-WB$_{12}$.$\Delta\partial v$ = +
  AND NOT
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$+WB$_{22}$.$\Delta\partial v$ -WB$_{12}$$\Delta\partial v$ = -
  where:
  WB$_{21}$: left front wheel; WB$_{11}$: right front wheel;
  WB$_{22}$: left rear wheel; WB$_{12}$: right rear wheel .
  This means: underbraking of at least one wheel on the right-hand side or overbraking of at least one wheel on the left-hand side and no possibly counteracting under/overbraking.
- **yawing to right**
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$ + WB$_{22}$.$\Delta\partial v$-WB$_{12}$.$\Delta\partial v$ = -
  AND NOT
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$+WB$_{22}$.$\Delta\partial v$ -WB$_{12}$$\Delta\partial v$ = +
- **potential yawing**
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$ + WB$_{22}$.$\Delta\partial v$-WB$_{12}$.$\Delta\partial v$ = -
  WB$_{21}$.$\Delta\partial v$-WB$_{11}$.$\Delta\partial v$ + WB$_{22}$.$\Delta\partial v$-WB$_{12}$$\Delta\partial v$ = +
  Some over/underbraking, but none of the above cases (i.e. potential compensation of yawing)
- **loss of liquid,** $Qleak_x$ =+, where $Qleak_x$ is the leakage liquid flow and x indicates (as above) the respective wheel involved.

5.3 Results

The qualitative model has been implemented in Raz'r [OCC'M, 2011], an environment for model-based diagnosis, prediction, and FMEA. Partial results for the scenario “Standard braking while car is moving” are shown in Fig. 5. Columns 2 and 3 refer to the respective component and failure mode, while column 4 states the effects local to this component and column 5 the system level effects. This table is complete and correct when compared to FMEA tables produced by experts.



Scenario	Part	Failure mode	Local effect	System level effect
Braking_CarMoving	PA_C1	SealBroken	>>no local effect<<	:SoftPedal
Braking_CarMoving	PA_C1	AirInChamber	>>no local effect<<	:SoftPedal
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition	HardPedal	
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition	FixedInNotPushedPosition	:WB11_Underbraked
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition		:WB21_Underbraked
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition		:WB12_Underbraked
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition		:WB22_Underbraked
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition		:HardPedal
Braking_CarMoving	PA_P1	StuckInNonBrakingPosition		:PotentialYawing
Braking_CarMoving	PA_P1	StuckInBrakingPosition	HardPedal	:HardPedal
Braking_CarMoving	PA_P2	StuckInNonBrakingPosition	HardPedal	
Braking_CarMoving	PA_P2	StuckInNonBrakingPosition	FixedInNotPushedPosition	:WB12_Underbraked
Braking_CarMoving	PA_P2	StuckInNonBrakingPosition		:WB22_Underbraked
Braking_CarMoving	PA_P2	StuckInNonBrakingPosition		:HardPedal
Braking_CarMoving	PA_P2	StuckInNonBrakingPosition		:PotentialYawing
Braking_CarMoving	PA_P2	StuckInBrakingPosition	HardPedal	:HardPedal
Braking_CarMoving	PA_C2	SealBroken	>>no local effect<<	:SoftPedal
Braking_CarMoving	PA_C2	AirInChamber	>>no local effect<<	:SoftPedal
Braking_CarMoving	M_VI11	BlockedClosed	NoFlow	
Braking_CarMoving	M_VI11	BlockedClosed	ReducedFlow	:WB11_Underbraked
Braking_CarMoving	M_VI11	BlockedClosed		:HardPedal
Braking_CarMoving	M_VI11	BlockedClosed		:YawingToLeft
Braking_CarMoving	M_VI11	BlockedOpen	>>no local effect<<	:>>no system level effects<<
Braking_CarMoving	WB22	Leakage	Underbraked	:WB22_Underbraked
Braking_CarMoving	WB22	Leakage		:SoftPedal
Braking_CarMoving	WB22	Leakage		:WB22_LossOfLiquid
Braking_CarMoving	WB22	Leakage		:YawingToRight
Braking_CarMoving	WB22	StuckInNonBrakingPosition	Underbraked	:WB22_Underbraked
Braking_CarMoving	WB22	StuckInNonBrakingPosition		:YawingToRight
Braking_CarMoving	WB22	StuckInBrakingPosition	>>no local effect<<	:>>no system level effects<<

Figure 5 – Partial FMEA (omitting repetitive results)

Despite its simplicity, the model turns out to be quite powerful. To illustrate this, consider the table entry for the inlet valve M_VI$_{11}$ BlockedClosed in Figure 5. It predicts that the respective Wheel brake, WB$_{11}$ is underbraked, while WB$_{21}$ behaves normally, because, after all, it receives the proper pressure.

When we insert another valve between the chamber PA_C1 (with pressure +) and JointT2_1 the valve M_IV$_{xx}$ indicated in Fig. 1), then besides WB$_{11}$ underbraked, also WB$_{21}$ overbraked is predicted, because of a higher flow through M_IV$_{21}$ due to the blockage of M_IV$_{11}$.

6 SOFTWARE MODELS

In order to investigate the impact of a failure of a sensor that measures the rotational speed of a, we need a model of the intended behavior of the ECU, more precisely the software functions that control the valves based on the measured wheel speed: it has to issue a command, *cmd=1*, when the wheel speed drops below a certain threshold. For two different thresholds, the commands cause an inlet valve to close and an outlet valve to open, respectively. In our context, the only interesting aspect is how the (correct) function propagates a deviation of a sensor value (or a missing one).

Slightly simplified, this can be stated as

$$\Delta cmd = -\Delta v\_s \ ,$$

where v_s is the sensor signal and Δcmd is defined on the domain {0, 1} of cmd. If the v_s is too low (high), i.e. deviates negatively (positively) and, hence, reaches the threshold too early (too late), this causes the command to be set too early (too late), i.e. deviate positively (negatively). The OK model of the inlet valve contains

$$\Delta A = -\Delta cmd \ ,$$

while the outlet valve includes

$$\Delta A = \Delta cmd \ .$$

Hence, the impact of the sensor failure will be the same as for the respective valve failures, in particular overbraking and underbraking.

The relevant failures of the software itself are

- untimely command (which includes “command sent too early”, e.g. due to a high threshold value, and “command always”): Δcmd =+ and
- missing command (“command too late or never”): $\Delta cmd = -$, triggering the same effects as ΔA =+ ($\Delta A = -$) for the inlet (outlet) valve.

7 DISCUSSION AND OUTLOOK

According to the evaluation, so far, we succeeded in developing a set of models of hydraulic components that generate the results required by FMEA.

We emphasize that FMEA and also the broader safety analysis is ultimately targeted at determining the failure behavior of the **physical** system and its criticality, and that software bugs are relevant only with regard to their impact on this, which is totally specified by (deviating) actuator signals. This boils down to faults “untimely/no command” for Boolean signals as discussed above and “signal too high/too low” for analogue ones. Hence, this “physics-centered” perspective makes modeling software faults feasible.

Currently, functional safety analysis gains increased importance in the automotive industries through the new ISO 26262 standard. This analysis has to go beyond the pure characterization of the physical behavior, but has to assess its consequences for hazards in various situations, such as collisions, personal damage, and environmental impact. We are currently extending the analysis in order to also derive such conclusions automatically.

ACKNOWLEDGEMENTS

This work benefited from the collaboration with partners in the AUTAS project. Especially, we thank Oskar Dressler for producing a very efficient implementation of the FMEA algorithm.

REFERENCES

[Fraracci, 2009] Fraracci, A. *Model-based Failure-modes-and-effects Analysis and its Application to Aircraft Subsystems*. Dissertationen zur Künstlichen Intelligenz DISKI 326, AKA Verlag, ISBN 978-3-89838-326-4, IOS Press, ISBN 978-1-60750-081-0

[MIL, 1980] Department of defence USA. *Military standard - procedures for performing a failure mode, effects and criticality analysis*. MIL-STD-1629A, 1980

[OCC'M, 2011] OCC'M Software GmbH. *Raz'r Model Editor Version 3*. Interactive Development Environment for Model-based Systems. http://www.occm.de/, (c) 1995-2011

[Picardi *et al.*, 2004] C. Picardi, L. Console, F. Berger, J. Breeman, T. Kanakis, J. Moelands, S. Collas, E. Arbaretier, N. De Domenico, E. Girardelli, O. Dressler, P. Struss, B. Zilbermann. *AUTAS: a tool for supporting FMECA generation in aeronautic systems*. In: Proceedings ECAI-2004 Valencia, Spain, pp. 750-754

[Pietersma and van Gemund, 2007] J. Pietersma and A.J.C. van Gemund. *Symbolic Factorization of Propagation Delays out of Diagnostic System Models*. In 18th International Workshop on Principles of Diagnosis (DX-07), 2007.

[Price, 2000] Price, C. *Autosteve: automated electrical design analysis*. In Proceedings ECAI-2000, p.721-725, 2000

[SAE, 1993] Society of Automotive Engineers (SAE). *The FMECA process in the Concurrent Engineering (CE) Environment*. SAE AIR4845, 1993

[Struss *et al.*, 1997] Struss, P., Sachenbacher, M. Dummert, F.: *Diagnosing a Dynamic System with (almost) no Observations*. Workshop Notes of the 11th International Workshop on Qualitative Reasoning, (QR-97) Cortona, Italy, June 3-6, pp. 193-201, 1997.

[Struss and Price, 2003] Struss, P., Price, C. *Model-based systems in the automotive industry*. In AI magazine. AAAI Press, Menlo Park (USA) 2003, pp.17-34

[Struss, 2004] Struss, P. *Models of Behavior Deviations in Model-based Systems*. In. Proceeding of ECAI-2004 Valencia, Spain, pp. 883-887.