Enhancing safety of independent metering systems for mobile machines by means of fault detection

B. Beck, J. Weber

Chair of fluid-mechatronic systems, Technische Universität Dresden, Dresden, Germany
E-mail: benjamin.beck@tu-dresden.de, fluidtronik@mailbox.tu-dresden.de

Abstract

Systems with independent metering offer a high potential for increasing the functionality and efficiency of valve-controlled hydraulic drives. But nowadays there are only a few prototypical applications. One reason for that are the so far insufficient safety investigations. Besides the structural investigations carried out at the research institute, this contribution deals with a fault detection by means of limit checking of the applied pressure sensors. A detection algorithm is derived from several software-in-the-loop simulations of the independent metering system applied at an excavator arm. The functionality and limits of the fault detection will be shown by means of measurements. As a result, all safety-critical faults can be detected which leads to a Diagnostic Coverage of DC = 99% and thus allows the use of independent metering up to a Performance Level PL = e.

Keywords: hydraulic systems, independent metering, machine safety, ISO 13849, fault detection

1 Introduction

A significant contribution to the improvement of machine and process efficiency of mobile working machines is the use of (semi-)automated functions. Hydraulic drive systems with independent metering offer outstanding prerequisites to fulfill the requirements of (semi-)automated functions. Besides good structural properties and the further degree of freedom to control the system, there are additional potentials by transferring the functionality into the electronic control device and for the software. Thereby, the function's flexibility increases. Furthermore, the use of standardized valves becomes possible leading to reduced component costs. Despite these potentials there are only a few industrial applications with independent metering systems. One main reason is the so far insufficient analysis of safety and reliability aspects.

Previous contributions have shown which kind of system architectures meet the different safety requirements of mobile machines [1]. One suitable valve structure in combination with pressure sensors and a single-variable control approach was applied to the boom function of an excavator test rig at the research institute [2]. This system can reach a maximum Performance Level PL = e if the Diagnostic Coverage is DC = 99%, which depends on the fault detection. Fault detection methods were categorized and evaluated by Isermann [3]. An overview over these fault detection methods with corresponding publications on hydraulic drive systems is displayed in Figure 1. Additional publications for example on electrical drives can be found in [4]. There is a variety of publications on model-based fault detection methods as it can be seen in Figure 1.

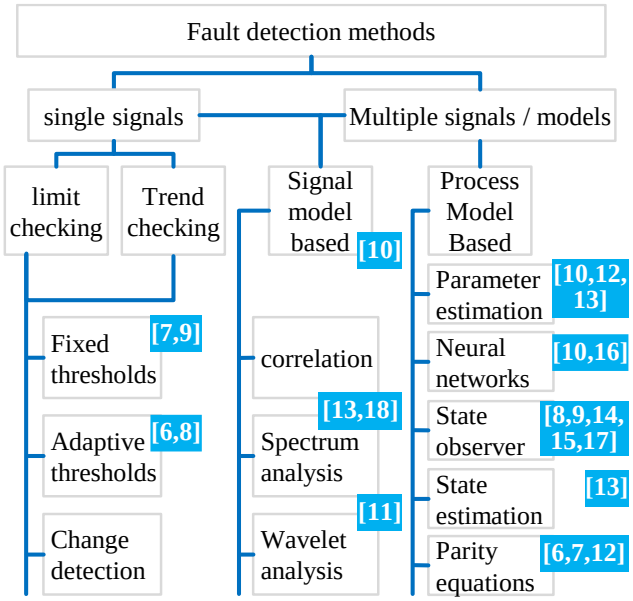

Figure 1: Fault detection methods [3] and related publications

On the one hand this is due to the fast detection and the diagnosis possibility of faults. On the other hand model-based methods require sufficient system models which result in a high implementation and computing effort [5]. These are reasons for simple approaches like limit checking being

widely spread in mobile hydraulic applications. Nevertheless, Nurmi and Mattila used a model-based approach to detect faults in typical mobile hydraulic valves in a crane application. With a reduced-order model, the measurement of the cylinder positions, the chamber pressures, the tank pressure, the pilot pressure and the intermediate pressure between the pressure compensator and the main spool as well as an adaptive threshold generating algorithm sensor biases of 3 bar can be detected [6]. But this contribution on the one hand only makes investigations on component level (focus on the valves). On the other hand a constant pressure system is assumed which is not typical for a mobile hydraulic system.

Concerning safety aspects of independent metering systems, there are only a few publications. Schmitz presents a steer-by-wire system consisting of eight 2/2 valves, two electronic control units (ECU), a redundant supply unit and two sensors to measure the steering wheel and wheel angle respectively. The main focus of this work is the development of a robust closed loop angle control of the wheels in order to compensate certain faults. In case of high control deviations, an off-duty self-test as well as an on-duty model-based fault detection on the basis of parity equations is introduced. Tests show that the fault detection only works sufficient with pressure compensated valves with a very low hysteresis [7]. To avoid the high component effort Fischer presents a superimposed steering system with independent metering. As well as Schmitz, Fischer focuses on fault compensation through an appropriate control concept. This makes the use of limit and trend checking methods for fault detection possible, because the safety shutdown of the electrohydraulic steering part is not time-critical any more [19]. The requirements on the working hydraulics' drive system vary greatly from the steering system's requirements. Besides the well-known load situation, there are mostly no cross-influences between several actuators due to the priority valve in steering systems. Furthermore, energy efficient operation modes have an impact on the system states. Similar to Schmitz and Fischer, Siivonen developed a fault tolerant controller for a digital hydraulic valve system consisting of 20 seat-type screw-in on/off valves. He uses an online fault diagnosis on the basis of measuring electrical quantities for re-configuration [20]. But the problem is the detection of sensor faults. Additionally, Siivonen developed an off-line fault detection algorithm based on pressure sensors [21]. He proved the functionality of both detection methods on a mobile crane test rig using a constant pressure net and a dSpace microcontroller system [22]. But during the off-line test the system cannot be used. To the author`s best knowledge, there are no publications on online fault detection for the working hydraulic of mobile machines using independent metering systems. Rannow introduces a fault tolerant algorithm for the reconfiguration of an existing independent metering valve product. But in his paper he assumes that faults are already detected and diagnosed [23].

In this paper the development of an online fault detection based on limit checking of pressure signals, using software-in-the-loop, is described. Therefore, the system model and validation will be shown firstly. After that, the fault detection algorithm will be derived from system simulation. The parameters of the limit checking are tuned by measurements on an excavator test rig. Finally, these tests as well as a discussion about the accuracy and the limits of the fault detection will be described.

2 Design of fault detection

Basis of the design of the fault detection is a model of the excavator test rig at the research institute. The system layout is displayed in Figure 2. It consists of the subsystems supply unit, input, logic, output, actuator and the work equipment. The supply unit comprises an electric motor, which is operated at a constant speed of $n_1 = 1450\ \text{min}^{-1}$, an electronically controlled variable displacement axial piston pump, a pressure relief valve and oil treatment elements like a filter. The operator generates a command signal through the joystick as part of the subsystem input, which are connected via CAN with the ECU (subsystem logic). The ECU calculates the valve`s control current depending on the operator command. Therefore, the ECU contains the control algorithm for each axis, the operation mode management, the failure insertion for the test of system faults and the fault detection algorithm. The subsystem output represents the valve block with independent metering. The displayed valve system is just one possible solution but provides a high flexibility, so that different control concepts can be investigated. It consists of two 2/2 bidirectional proportional spool valves (no. 5-6) for velocity and pressure control and four 2/2 bidirectional switching poppet valves (no. 1-4) for connecting each cylinder chamber with pump or tank line. A load independent movement is achieved through the individual pressure compensator (IPC – no. 8). To ensure that the inlet flow is always regulated from the IPC, an additional switching valve (no. 7) is installed. The system is described in detail in [2].

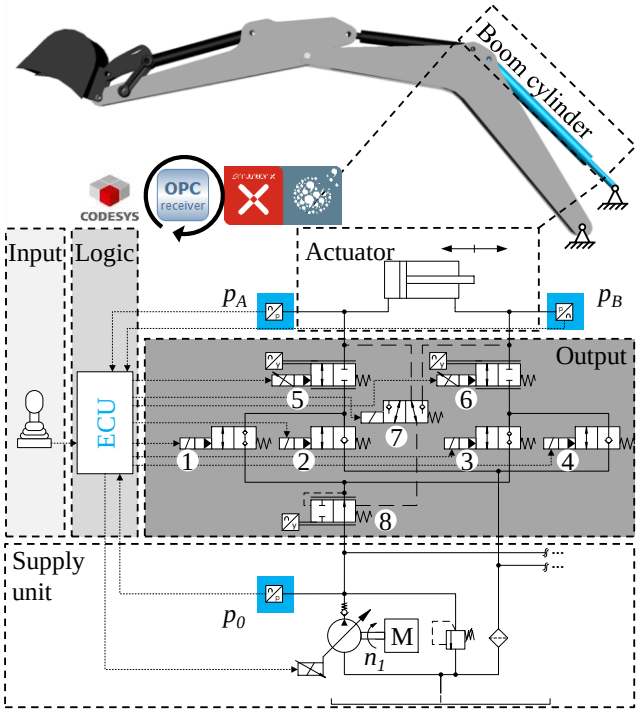

Figure 2: System structure / Test rig setup

At the test rig, pressure sensors in the pump line and each cylinder chamber, displacements sensors on the proportional valves and the pressure compensator as well as angle sensors for the boom, stick and bucket from which the position of the concerning cylinders are derived are installed. But for the proposed fault detection only the pressure sensors are used. Due to the fact that load on each cylinder depends on the equipment's mass distribution, a multi body-system with CAD-data has been built up. The valves have been measured separately on a valve test rig. The static characteristic diagram of the proportional valves and their dynamics are implemented in the model. The pump is modeled as a volume flow rate with its efficiency and dynamic. The model parameters especially the volumes are gained from the excavator test rig. The supply unit, the valves, the actuator, the work equipment and the input are modelled by using the system simulation software *SimulationX*. The control algorithm and fault treatment is directly programmed in the development environment *CODESYS*. This has two main advantages: Firstly, the restrictions from the hardware (discrete cycle time of 10 ms) should have taken into account by developing the algorithms. Secondly, a premature software implementation reduces commissioning costs. An *OPC* Server is used for the communication between the tools *CODESYS* and *SimulationX*. Since a fully extended equipment without loaded mass delivers high frequent pressure signals, the fault detection will be developed using the boom cylinder as a worst case scenario in this paper. Because of the kinematics of the work equipment the rod side of the boom cylinder is always on the high pressure side. This results in a retraction with a resistive load and an extension with an overrunning load during the lifting and lowering cycle.

2.1 Model Validation

The main goal of a fault detection is the feature generation. Therefore, it is necessary to know about the system's usual behavior. For that the built-up system model must be validated. Figure 3 displays the comparison of the software-in-the-loop simulation and measurements on the test rig of the lifting / lowering cycle using the boom cylinder.

The lift movement proceeds from 0 – 10 s and the lowering movement from 10 – 20 s. In the upper diagram the target and actual nominal velocity of the boom cylinder and in the diagrams at the bottom the corresponding pressure values are displayed. The simulation results, displayed in dashed lines, fit well to the measurements, displayed in solid lines. Deviations in the velocity signal are due to neglected leakage in the valve model. The higher velocity in the simulation leads to a movement of the boom cylinder into the end stop by using the same target velocity (operator command). This is why the pressure p_0 rises up to 250 bar at approx. 9 s. Due to the internal leakage of the cylinder, the pressure difference between the cylinder chambers equals slowly from 9 -16 s. During this time the set velocity is zero. At approx. 16 s the lowering movement starts. To that, the valve 6 has to control the volume flow, so that the overrunning load can be controlled and therefore the cylinder pressure p_A does not drop to zero (anti cavitation). During the movement phase from 16 – 20 s the simulation results fit well to the measurement. Overall, the system model represents the normal behavior very well and is therefore suitable for the development of fault detection.

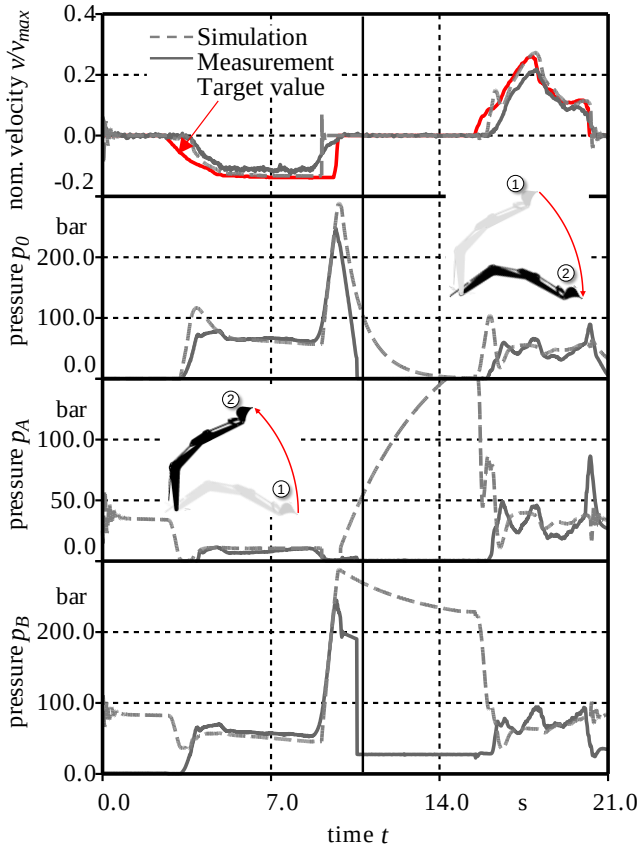

Figure 3: Model validation on lifting / lowering cycle

2.2 Analysis of fault behavior

To analyze the fault behavior, faults must be impressed upon the model. The fault insertion can be divided into four different levels:

1. Machine condition
2. Fault location
3. Type of fault
4. Moment of the fault occurrence

The machine condition is given through the considered cycle. Regarding the fault location, faults will be impressed upon the three pressure sensors and the valves 1 – 7. Faults of the IPC are not investigated because the compensator is (hydraulically-) mechanically controlled and thus basic and proven safety principles can be applied. The standard ISO 13849-2 defines fault types for mechanical, electrical, electronical, pneumatic and hydraulic elements [24]. The relevant faults for the insertion upon the model are summarized in Table 1.

Table 1: fault types regarding to ISO 13849-2

Valves	1	Change in switching times
	2	Failing to switch (stay fully closed or fully open or in every single position between)
	3	Change of neutral position without command
	4	Leakage
	5	Change of leakage volume flow during operation time
	6	Burst of housing and fasteners
	7	Hydraulic faults which cause uncontrollable behavior
sensors	1	Changes in the data acquisition and the output

Concerning a deep fault diagnosis a good description of the fault is necessary to identify the cause of the failure. But for the detection it is sufficient to know that there is a fault. Therefore, a fault needs to have an impact on the system behavior. The bigger the impact, the more critical the system behavior will be. Another question is how to insert these fault types into the model and the test rig. Because of the use of electronic controlled components it is obvious to use synthesized signals to manipulate the set values. To cover the fault types from ISO 13849 except valve fault six the signals in Figure 4 are used. The burst of the valve housing can be covered through the basic and proven safety principles like oversizing.

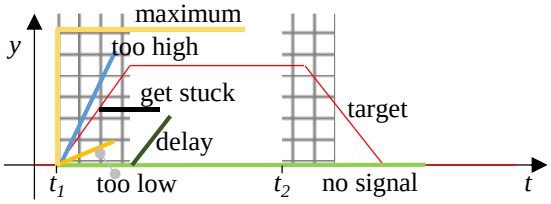

Figure 4: Synthesized signals to insert fault types

From the system's view a maximum signal equals a signal which is too high but with a bigger impact. In the same way no signal equals a signal which is too low and a signal delay with regard to a certain time. In the context of detecting safety critical states and to limit the variant only the signals "maximum", "delay" and "no signal" will be investigated in this paper. Finally, the time of the fault insertion can be varied as it is displayed in Figure 4. Therefore, it has to be mentioned that there are fault combinations which are not appropriate, e.g. the fault type "get stuck" when the set signal is constant or the fault "no signal" on a valve which already gets no signal due to the control algorithm. On the basis of this investigations a failure insertion unit with a related visualization as user interface has been programmed in *CODESYS*. The SIL simulation has been used to analyze the fault variations displayed in Table 2. Here only valve faults are shown. The simulation results with inserted sensor faults has shown that the impact on the cylinder movement is the same as inserting valve faults. This is due to the control algorithm, which reacts on the pressure signals to set the valve currents.

The simulation results show that there are six safety critical faults, which are highlighted in Table 2. A fault is safety critical within the context of the excavator application if:

- The boom will move faster than commanded from the operator or,
- The boom will move in the opposite direction than commanded from the operator or,
- The cylinder pressure will rise higher than the set value of the pressure relief valve.

The last case occurs when the boom cylinder extends and the downstream valves are closed. Due to the differential cylinder the chamber pressure p_B will be precisely higher by the amount of the area ratio of the differential cylinder (see section 3.1). The other fault variations lead to no movement or cavitation while the target movement is reached. Due to the defined safety function "safe stop", these faults do not need to be detected. But in the context of availability the identification of these faults enables countermeasures like a quick repair or reconfiguration. But in the following the safety critical faults will be described and a fault detection algorithm derived.

Table 2: fault variations for SIL simulation

	no.	**location**	**type**	**time**
Lifting movement	1	Valve 1	Maximum	t_2
	2	Valve 2	No signal	t_1
	3	Valve 2	Maximum	t_2
	4	Valve 3	No signal	t_1
	5	Valve 3	Maximum	t_2
	6	Valve 4	Maximum	t_2
	7	Valve 5	No signal	t_1
	8	Valve 5	Maximum	t_2
	9	Valve 5	Get stuck	t_2
	10	Valve 6	No signal	t_1
	11	Valve 6	Maximum	t_2
	12	Valve 6	Get stuck	t_2
	13	Valve 7	No signal	t_1
Lowering movement	14	Valve 1	Maximum	t_2
	15	Valve 1	No signal	t_1
	16	Valve 2	Maximum	t_2
	17	Valve 3	Maximum	t_2
	18	Valve 4	No signal	t_1
	19	Valve 4	Maximum	t_2
	20	Valve 5	No signal	t_1
	21	Valve 5	Maximum	t_2
	22	Valve 5	Get stuck	t_2
	23	Valve 6	No signal	t_1
	24	Valve 6	Maximum	t_2
	25	Valve 6	Get stuck	t_2
	26	Valve 7	No signal	t_1

In the following fault no. 1 and 24 will be investigated exemplary. Therefore, both simulation and measurements were taken out. The measurements complement the

simulation and serve to analyze the behavior of the operator. The simulation and measurement results of fault no. 1 are displayed in Figure 5. During the cycle, the work equipment lifts due to a retracting boom cylinder which drives against the load. In the fault-free state from 0 – 4.8 s the pump volume flow is directed into the rod side (chamber B) of the boom cylinder through the open switching valve 3 and the correspondingly open proportional valve 6. This leads to a pressure built-up in cylinder chamber B at approx. 2.5 s. At the same time, the valves 5 and 2 are open which allow a volume flow from cylinder chamber A to the tank. As a result, the cylinder begins to move as it can be seen in the solid grey line in the velocity diagram of Figure 5. During the movement, the simulation results (dashed lines) fit again well to the measurements. Since there is no ground contact in the model, the initial values of the pressure p_A and p_B are higher than in the measurement.

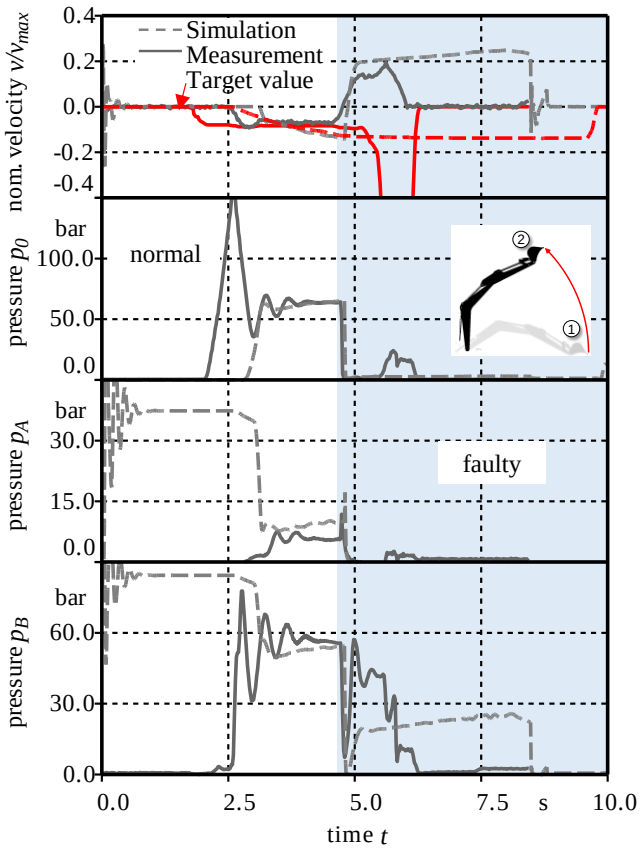

Figure 5: Results of fault no. 1

If the switching valve 1 unintentionally opens in the event of a fault at approx. 4.8 s, the pump is connected to the tank via the normally open switching valve 2. The pump pressure falls to a pressure level of approx. 10 bar at 5 s, determined by the pressure losses across the IPC and the switching valves. Likewise, the rod side of the boom cylinder, which is under pressure, is connected to the tank via the valves 1, 2 and 3. Thus p_B falls and the load force can no longer be overcome by the cylinder force. The boom sinks downwards due to its weight, which can be seen in the solid grey line of the nominal velocity v/v_{max}. Since the velocity of the piston and thus also the direction of the volume flow through valve 6 is reversed, p_B initially drops to 0 bar, and then rises again to the value of the pressure loss over valve 6. Since the piston speed slows down before the movement direction reverses, the volume flow conveyed via valve 5 also drops. By the same opening cross section of valve 5, the pressure drop decreases and thus also p_A. Since only p_T prevails before valve 5, not enough oil flows into the piston chamber as would be required by the cylinder velocity v. As a result, p_A falls further and remains at 0 bar. While the target velocity in the simulation (displayed in dashed red lines) remains constant due to a not modelled operator the reaction of a real operator can be seen in the solid red line. The measurements were performed in pairs. One controlled the fault insertion and the other one moved the joysticks. The operator reinforces the faulty lowering movement intuitively which can be seen in the velocity diagram of Figure 5 between 5 – 6 s.

Looking on the fault-free case of the lowering movement between 0 – 5.5 s in Figure 6, the rod side is connected to the tank by the correspondingly open valve 6 and the open valve 4. The piston side is connected to the pump by the correspondingly open valve 5 and the open valve 1. When sinking, a pulling load is applied to the piston (load force and velocity vector point to the same direction). The control edge on the load side *B* has the task of braking the piston. The ECU calculates the opening cross-section, so that a feed pressure p_A of approx. 10 bar is maintained on the piston side.

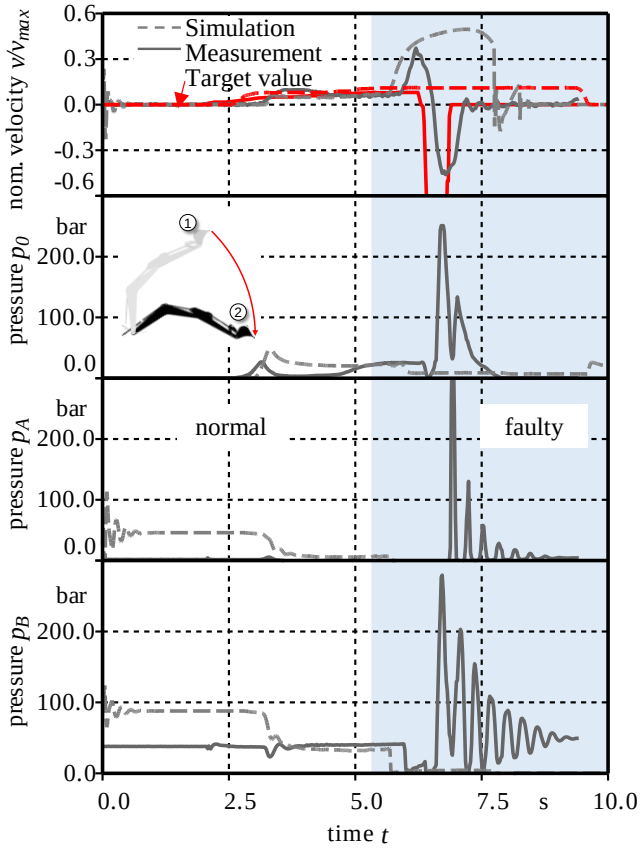

Figure 6: Results of fault no. 24

Fault no. 24 is displayed in Figure 6 from 5.5 s to the end of the movement. In this case, the proportional valve 6 on the load side opens to the maximum. This valve error has an immediate effect on the boom axis since there is a deviation between the required and actual opening cross-section immediately. The piston speed v rises significantly. This results in a pressure drop p_B and due to the equilibrium of forces at the cylinder also in p_A. Since the boom falls much faster, it moves into the end position of the cylinder with a given joystick presetting before the switching valves close in the simulation. Therefore, there is no pressure peak in p_B. The measurements show a slightly different situation. As it can be seen in the target velocity (solid red line) the operator is overwhelmed with the situation. A quick and strong displacement of the joystick in the opposite direction indicates that the operator firstly wants to compensate the fault. Due to that command p_0 increases to the maximum bounded by the pressure relief valve at approx. 6.6 s. Shortly after that he releases the joystick. The target velocity is at zero and all the valves are closed at approx. 7 s. The high velocity of the boom cylinder is braked by the closed valves. This leads to the stop of the cylinder and to high frequency oscillations in the pressure signals p_A and p_B. As mentioned above, this leads also to the risk of bursting hoses. A countermeasure is a secondary pressure limitation function (see section 3.1).

2.3 Description of fault detection algorithm

As described above, all fault variants displayed in Table 2 were simulated. Concerning the lifting movement, the comparison of the pressure signals in every simulation run leads to the following equation for the fault detection:

$$p_B > p_0 \text{ when } v_{set} < 0 \quad (1)$$

$$p_A < p_T \text{ when } v_{set} < 0 \quad (2)$$

Relation 2 has the disadvantage that it is likely also true in the error-free case. A fault detection based on this equation would then provide false alarms. Valve 5 acts as an outlet throttle during lifting and generates power loss due to the pressure drop. To save energy, valve 5 can be fully opened due to the independent metering system. This minimizes the pressure drop across valve 5 and thus also the pressure losses. The pressure p_A is consequently also minimal and calculated as the sum of tank pressure p_T, the pressure losses of the fully open proportional valve 5 Δp_{v5} and the open switching valve 2 Δp_{v2}.

$$p_A = p_T + \Delta p_{v2} + \Delta p_{v5} \quad (3)$$

Then, p_A will be only slightly above p_T especially at slow movements, and fall below p_T when the boom oscillates. Due to the application of more energy efficient operation modes, relation 1 should be preferred. Either way, relation 2 also occurs in the error-free case at the beginning of the movement between 2 s and 2.5 s (see measurements in Figure 5). Due to the applied flow matching control algorithm the pump pressure p_0 is zero at the beginning of the movement, and thus lower than p_B. As a result, the boom would lower and p_A falls to 0 bar.

Concerning the lowering movement, the comparison of the pressure signals in every simulation run lead to relation 4 for the fault detection:

$$p_A < p_T \text{ when } v_{set} > 0 \quad (4)$$

Equation 4 can also be true in the error-free case. This occurs in particular when the valves are being opened at the start of the movement and the necessary pump pressure has not been established yet, similar to the lifting movement. One countermeasure for this problem is a delay between the control of the pump and the valves (virtual load holding valve). By opening the proportional valves at a later time, the pump has an appropriate amount of time to increase the swash plate angle and thus build up a pressure p_0 upstream of the valves. A time constant is however not effective, because the pressure build – up is dependent on the required volume flow, and also the valve dynamics depend on the target value. An alternative solution is discussed in the next chapter. At the very least, error detection should be designed in such a way that short – term minima of p_A are tolerated. For that a fault must remain for a certain amount of time until the fault reaction (close every valve) is initiated. Because from the dynamical pressure signal view, lifting and lowering are different, the following relations are used to check the faulty time:

$$t_{fault} \geq \Delta t_{max,lift} \quad (5)$$

$$t_{fault} \geq \Delta t_{max,lowering} \quad (6)$$

Regardless of the type of fault detection, a well – tuned system with a robust control concept allows a simpler and safer parameter finding. As it is displayed exemplarily in the p_A-signal in Figure 6 between 3.5 s and 5.5 s a good pressure control wouldn't cause false alarms. Aspects of the control algorithm are discussed in detail in [2]. Another aspect is the pressure built – up problem which will be discussed below.

2.4 Special event handling

Particularly in the case of low volumetric flow requirements, the disadvantages of the use of a time constant for the query of the pressure build – up become clear. If sufficient pressure has not yet been built up in the pump line and the valves are actuated, the boom first drops. During lowering, the proposed error detection in equation 4 would report false alarms for the period shortly after the pressure build-up phase. In order to solve these problems, the pressure build – up phase has to be determined by pressure signals. The pressure build – up phase (*p_up*) is terminated for lifting when $p_0 = p_B$. Thus, the pumping pressure can support the load force in any case and sagging is prevented. In the case of lowering, the pressure build – up phase (*p_up*) is not to be terminated until the pump has built up a pressure of $p_A = 10$ bar in the piston chamber. As a result, the pump has already been increased its swash plate angle and can deliver the full required volume flow from the time in the valve 6. As a result, a sufficient volume flow can be fed into the piston chamber from the beginning, and p_A does not drop. During the pressure build – up phase, the currents of the load – side valves are zero, whereby single valve errors are also intercepted during this phase due to the

series circuit. The effect of the pressure build-up phase can be seen exemplarily in Figure 5. There is a time – delay between the target (red line) and the actual (grey line) velocity at between 2 s and 2.5 s.

To summarize the aforementioned arguments, the proposed fault detection with limit checking is based on the equations and parameters, which are derived from several SIL simulations.

Table 3: Fault detection equations and parameters

Lifting movement: $v_{set} < 0$	
Equation	$p_B - p_1 > p_{tol,1} \cap p\_up = False$
$p_{tol,1}$ [bar]	3
$\Delta t_{max,lift}$ [ms]	200
Lowering movement: $v_{set} > 0$	
Equation	$p_A < p_{tol,2} \cap p\_up = False$
$p_{tol,2}$ [bar]	3
$\Delta t_{max,lowering}$ [ms]	200

3 Implementation and test of fault detection

The presented fault detection algorithm has been integrated into the control software and has first been tested by means of SIL simulations on the model. Here again the advantage of the SIL simulation has been demonstrated. By means of early detection of programming errors, a quick commissioning on the test stand was possible. The tests for the secondary pressure limiting function and the safety function "safe stop" at the excavator arm test stand are presented below.

3.1 Test of the electronic secondary pressure relief function

As described in section 2.2 there are high cylinder chamber pressure in some cases, which can lead to bursting hoses. Usually, separate valves are used in mobile machines for this function. Since systems with independent metering require a higher number of components on the one hand and lead to flexible flow paths and thus a high degree of functional diversity on the other hand, it is presented here how an electronic secondary pressure limitation can be implemented. To avoid influences of this function on the movement of the cylinder, the valves on the load side must not be changed in their control. This means that a pressure reduction is only possible via the opposite side of the load. This control has two stages. If the pressure of a cylinder chamber exceeds the first threshold value, the switching valve which controls the incoming volume flow (valve 1 or 3) is first closed. Thus, the pressure which in the unfavorable case is reinforced by the cylinder, cannot increase further. If the pressure of a cylinder chamber exceeds the second threshold value, the tank valve (valve 2 or 4) on the opposite chamber side of the load is being opened. The hydraulic clamping of the cylinder is thereby canceled and both of the cylinder chamber pressures can be reduced down to the static pressure resulting from the applied load force. The functionality of this algorithm is displayed in Figure 7 exemplarily for the case of fault no. 23 (closed downstream valve, here valve 6). The normalized target and actual cylinder speed is shown in the upper part of the diagram. Below, the pressure signals and the normalized control currents of the switching valves of the opposite side of the load are shown. For an improved representation of the results, the time interval in which the pressure stages are exceeded is selected. The values of the pressure stages, which are selected exemplarily, are p_{Stage_I} = 180 bar and p_{Stage_II} = 240 bar.

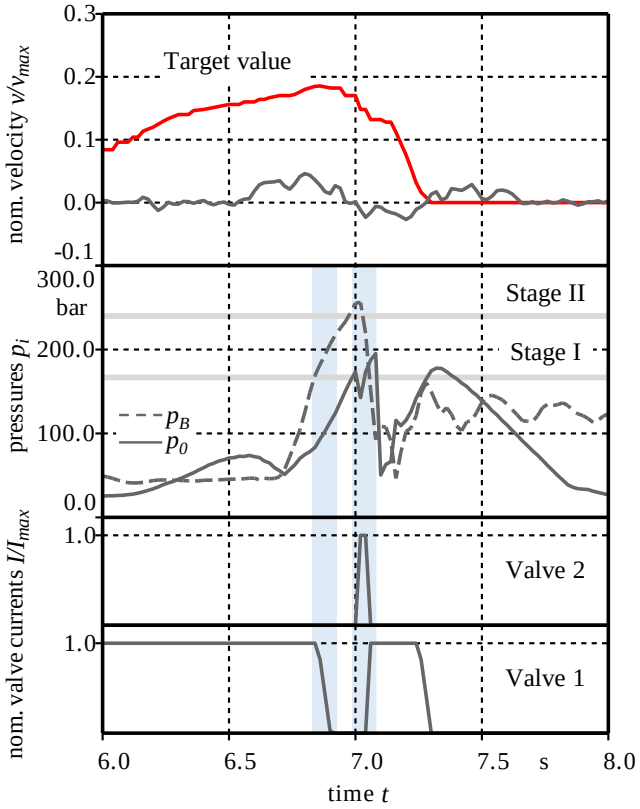

Figure 7: Experimental test of secondary pressure limitation at occurrence of fault no. 23

It can be seen how valve 1 closes when the first pressure stage is exceeded and valve 2 opens when the second pressure stage is exceeded. The functionality of the secondary pressure limitation function has thus been demonstrated. This complies with the requirements of ISO 4413. However, it should be checked which additional requirements apply by the use of electronic pressure relief valves. But overall this shows which functions can be integrated into independent metering systems.

3.2 Test of the safe stop function

Finally, the functionality of the developed fault detection is demonstrated, both in the normal operation and in the event of a fault. In Figure 8, the lifting and lowering cycle is depicted as in the case of the model validation. The equipment is lifted by the retracting boom cylinder between 0 s and 10 s. The pressure built – up phase can be seen in the time delay between the target and actual velocity again. In that time (between 4 s and 5 s) the fault variable t_{fault} rises up to a value of 90 ms. This is because the switching valve 2 of the load opposite side is already controlled. Thereby the pressure p_A drops under 3 bar. However, to detect valve faults during this phase, for example a faulty open tank valve 2 or 4 which would prevent the pressure built – up, a smaller increase of the fault variable t_{fault} is used. On the one hand this ensures the required pressure built – up and allows the fault detection on the other hand. Subsequently, the lowering movement takes place by the extension of the boom cylinder. At approx. 13.8 s the fault no. 24 (fully open valve 6) is inserted. The error begins to affect the movement at approx. 14 s. A detailed view of this phase is displayed in Figure 9.

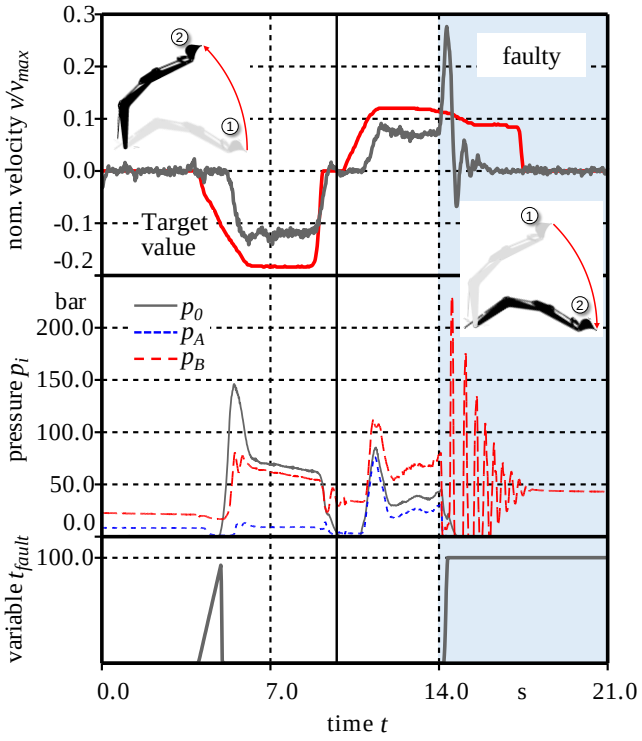

Figure 8: Experimental test of safe stop function by occurrence of fault no. 24

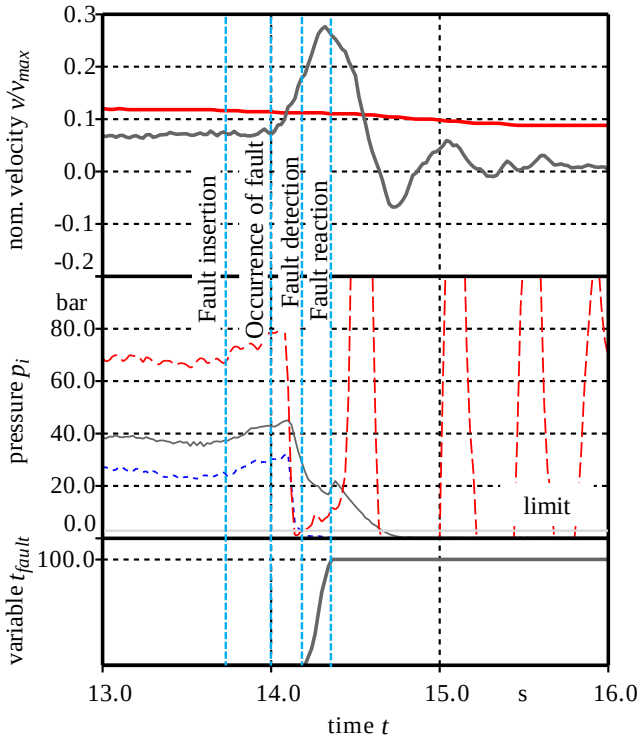

Figure 9: Enlarged section of Figure 8

The effect of the fault can be seen in the increasing cylinder velocity v. As a result of that p_A drops under the specified limit of 3 bar at approx. 14.2 s. This leads to the rise of the fault variable t_{fault} up to the specified limit of 100 ms. Therefore, all valve currents are set to zero at 14.3 s. The falling boom is hydraulically stopped by the closing switching valve 4 at 14.36 s. Because of the high velocity difference, the pressure peaks in p_B and thus also in p_A are significantly high (need for secondary pressure limitation; see section 3.1). An enlarged section of the error phase is shown in Figure 10.

3.3 Discussion of limits and accuracy

Fault no. 24 is the most safety critical fault due to the high boom cylinder velocity. Thus, the accuracy and limits of the proposed fault detection will be discussed using fault no.24. Figure 10 shows the trajectory of the excavator arm. The red dots highlight the movement during the occurrence of the fault. In the time between fault formation and fault reaction, the excavator arm lowers by approx. 593 mm. This drop height can be quantified with the difference of the Tool-Center-Point height Δy_{TCP} and is made up of the following parts.

$$\Delta y_{TCP} = \Delta y_{detect} + \Delta y_{remain} + \Delta y_{react} \qquad (7)$$

The first part is the fall height Δy_{detect} of the equipment, which arises in the time of the fault occurrence to fault detection and, therefore, the limit p_{tol} is exceeded.

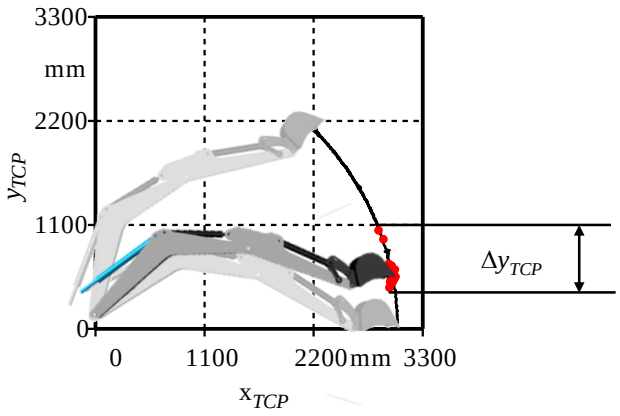

Figure 10: Trajectory of the excavator arm in case of fault no. 24

The required detection time depends on the following influencing factors:

- The current load situation,
- The current cylinder velocity,
- The pressure reduction time which depends on the dead volumes in the tubing and
- The specified limit p_{tol}.

Because the first two aspects are given through the operator command only the last two can be influenced in construction. The second part is the fall height Δy_{remain} of the equipment, which is given during the time of the selected limit Δt_{max} of the fault variable t_{fault}. If the system immediately reported an error according to the detection algorithm, this component of the fall height could be reduced to zero. To ensure that this fraction of the drop height is kept small and the fault detection is still robust against false alarms, Δt_{max} should be as small as possible. The value was successively reduced from 200 ms over 150 ms to 100 ms on the test bench. As a result, the overall fall height could be reduced by 244 mm. Here, there is little optimization potential for reasons of machine availability.

The last part of equation 7 represents the fall height Δy_{react} which is returned in the time of the fault reaction. The fault reaction measures related to the safety function "safe stop" are the simultaneous closing of all valves and the reduction of the swash plate angle of the pump. Influence factors of Δy_{react} are:

- The dynamic behavior of the applied components in combination with
- The control concept and thereby the cycle time of the ECU and again
- The operation point of the drive (load and velocity).

Again, the last aspect cannot be influenced because the operation point is given through the work task and the operator, respectively. But with fast components and an adequate control algorithm this time and the fall height respectively can be reduced. The measurements with the aforementioned variations of Δt_{max} showed that the overall fall height Δy_{TCP} is significantly influenced by the reaction time of the system (Δy_{react} / Δy_{TCP} = 66 %). 32 % of that value are attributable to the valve dynamics. The rest of Δy_{react} (68 %) arises from the boom cylinder oscillations before the static value of Δy_{TCP} is reached. Only 25 % of Δy_{TCP} are related to the selected maximum time limit Δt_{max} when the fault is detected and another 9 % arise from the detection itself ($p_A < p_{tol,2}$). As a result, a large part of the fault detection's optimization potential lies in the system parameters (volumes between valve and cylinder) and the dynamic of the components.

Finally, Table 4 gives an overview of the determined fall heights of the safety critical tests carried out.

Table 4: sensitivity of detection parameters

Fault no.	**Description**	**Δt_{max} [ms]**	**Δy_{TCP} [mm]**
1	Valve 1 maximum signal	200	144
6	Valve 2 maximum signal	200	132
24	Valve 6 maximum signal	200	837
24	Valve 6 maximum signal	150	751
24	Valve 6 maximum signal	100	593
25	Valve 6 get stuck	100	465

4 Conclusion and outlook

With the help of the validated simulation model, calculations with a targeted imprinting of previously defined errors could be carried out. The result of these simulations is on the one hand the knowledge about the safety-critical conditions in the system. On the other hand, information on deviations from error cases to normal behavior is provided. By analyzing the simulation results, it was possible to derive clear error patterns. These form the basis for the developed fault detection by means of pressure sensors. The use of the same pressure sensors for function and error detection does not incur any additional costs, which makes this solution particularly attractive.

Final tests at the test stand excavator arm show the functionality of the fault detection and the safety function. Unintentional false alarms are not reported during the movement in the normal mode of the independent metering system and all safety critical faults can be detected. Thus a Diagnostic Coverage of DC = 99 % can be assumed. This allows the use of this drive structure up to a performance level of PL = e. But unfortunately, the fall height during the detection and reaction is very high. Future work should address this problem. Nevertheless, the results provide a good basis for the further development of fault detection by means of pressure sensors and show the limits of simple detection methods like limit checking for mobile hydraulic systems. However, the dynamics of fault detection and the consideration of extended operating modes of the

independent metering system, dynamic load changes as well as parallel driven consumers still offer considerable development potential. An expansion of fault detection for fault locating would also significantly improve the availability of systems with independent metering.

5 Acknowledgements

The presented research activities are part of the project "Safety concepts for mobile hydraulic systems using independent metering "(Sicherheitskonzepte für mobilhydraulische Antriebsstrukturen mit getrennten Steuerkanten - Ref. No. 702910). The authors would like to thank the Fluid Power Research Fund of the VDMA for the funding and support.

Nomenclature

Designation	Denotation	Unit
DC	Diagnostic Coverage	-
n_1	Rotational speed of motor	min^{-1}
p_A	Cylinder chamber pressure A	bar
p_B	Cylinder chamber pressure B	bar
p_0	Pump pressure	bar
p_T	Tank pressure	bar
$p_{tol,i}$	Tolerated pressure limit	bar
$p_{Stage,i}$	Secondary Pressure limitation stage i	bar
p_up	Internal pressure built-up var.	-
Δp_{vi}	Pressure drop over valve i	bar
PL	Performance Level	-
t_{fault}	Fault variable	ms
$\Delta t_{max,i}$	Time limit i	ms
v	Cylinder velocity	mm/s
v_{max}	Maximum cylinder velocity	mm/s
v_{set}	Target cylinder velocity	mm/s
y_{TCP}	Height of tool center point	mm
Δy_{TCP}	Height difference of TCP	mm
Δy_{detect}	Height difference of TCP during fault detection	mm
Δy_{remain}	Height difference of TCP during $\Delta t_{max,i}$	mm
Δy_{react}	Height difference of TCP during fault reaction	mm

References

[1] B. Beck and J. Weber. Safety and Reliability of Independent Metering Systems in Mobile Machinery. Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016, Tylor & Francis Group, London, 2017.

[2] J. Lübbert, A. Sitte, and J. Weber. Pressure compensator control – a novel independent metering architecture. 10th International Fluid Power Conference (10. IFK) March 8 - 10, 2016 in Dresden, Dresden, 2016, vol. 1, pp. 231–246.

[3] R. Isermann. Fault-Diagnosis Applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[4] M. Münchhof, M. Beck, and R. Isermann, "Fault-tolerant actuators and drives—Structures, fault detection principles and applications. Annual Reviews in Control, vol. 33, no. 2, pp. 136–148, 2009.

[5] J. Richalet. Industrial applications of model based predictive control. Automatica, vol. 29, no. 5, pp. 1251–1274, 1993.

[6] J. Nurmi and J. Mattila. Detection and Isolation of Faults in Mobile Hydraulic Valves Based on a Reduced-Order Model and Adaptive Thresholds. Proceedings of ASME/BATH 2013 Symposium on Fluid Power and Motion Control, Sarasota, 2013.

[7] D. Schmitz. Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren. Karlsruher Institut für Technologie (KIT), Karlsruhe, 2014.

[8] Z. Shi, F. Gu, B. Lennox, and A. D. Ball. The development of an adaptive threshold for model-based fault detection of a nonlinear electro-hydraulic system. Control Engineering Practice, vol. 13, no. 11, pp. 1357–1367, 2005.

[9] H. Khan, S. C. Abou, and N. Sepehri. Nonlinear observer-based fault detection technique for electro-hydraulic servo-positioning systems. Mechatronics, vol. 15, no. 9, pp. 1037–1059, 2005.

[10] T. Ramdén. Condition monitoring and fault diagnosis of fluid power systems: approaches with neural networks and parameter identification. Linköping: Dep. of Mechanical Engineering, Linköping Univ, 1998.

[11] Y. Gao, Q. Zhang, and X. Kong. Wavelet-based pressure analysis for hydraulic pump health diagnosis. Transactions of the ASAE, vol. 46, no. 4, pp. 969–976, 2003.

[12] M. Münchhof. Fehlerdiagnose für hydraulische Servo-Achsen (Fault Diagnosis for Hydraulic Servo Axes). at – Automatisierungstechnik, vol. 55, no. 2, 2007.

[13] A. Kazemi-Moghaddam. Fehlerfrühidentifikation und-diagnose eines elektrohydraulischen Linearantriebssystems. TU Darmstadt, 2000.

[14] C. Stammen. Condition Monitoring für intelligente hydraulische Linearantriebe. RWTH Aachen, Aachen, 2005.

[15] S. Richter and J. Weber. Sicherheit geregelter Antriebe der Fluidtechnik - Weiterentwicklung von Sicherheitskonzepten. Institut für Fluidtechnik, Dresden, Abschlussbericht FKM-Nr.: 702390, 2011.

[16] J. Schaab, M. Muenchhof, M. Vogt, and R. Isermann. IDENTIFICATION OF A HYDRAULIC SERVO-AXIS USING SUPPORT VECTOR MACHINES. IFAC Proceedings Volumes, vol. 38, no. 1, pp. 722–727, 2005.

[17] P. Garimella and B. Yao. Fault detection of an electro-hydraulic cylinder using adaptive robust observers. ASME 2004 International Mechanical Engineering Congress and Exposition, pp. 119–128, 2004.

[18] K. Mollazade, H. Ahmadi, M. Omid, and R. Alimardani. Vibration-based fault diagnosis of hydraulic pump of tractor steering system by using energy technique. Modern Applied Science, vol. 3, no. 6, p. 59, 2009.

[19] E. Fischer, A. Sitte, J. Weber, E. Bergmann, and M. de la Motte. Performance of an electro-hydraulic active steering system. 10th International Fluid Power Conference (10. IFK) March 8 - 10, 2016 in Dresden, Dresden, 2016, vol. 1, pp. 375–386.

[20] L. Siivonen, M. Huova, and M. Vilenius. FAULT DETECTION AND DIAGNOSIS OF DIGITAL HYDRAULIC VALVE SYSTEM. The Tenth Scandinavian International Conference on Fluid Power, May 21-23, 2007 Tampere, Finland, Tampere, 2007.

[21] L. Siivonen, M. Linjama, M. Huova, and M. Vilenius. Pressure Based Fault Detection and Diagnosis of a Digital Valve System. Power Transmission and Motion Control (PTMC 2007), Bath, 2007, pp. 67–82.

[22] L. Siivonen, M. Linjama, M. Huova, and M. Vilenius. Jammed on/off Valve Fault Compensation with Distributed Digital Valve System. International Journal of Fluid Power, vol. 10, no. 2, pp. 73–82, 2009.

[23] M. Rannow. Fail Operational Controls for an Independent Metering Valve. 10th International Fluid Power Conference. Dresden: Dresdner Verein zur Förderung der Fluidtechnik e.V., 2016.

[24] DIN Deutsches Institut für Normung e.V. Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2012), 2013.