Simulation for verification and validation of functional safety

Lars Mikelsons, Zhou Su

Angaben zur Veröffentlichung / Publication details:

Mikelsons, Lars, and Zhou Su. 2014. "Simulation for verification and validation of functional safety." In *Proceedings of the 10th International Modelica Conference, March 10-12, 2014, Lund, Sweden*, edited by Hubertus Tummescheit and Karl-Erik Arzén, 455–64. Linköping: Linköping University Electronic Press. https://doi.org/10.3384/ecp14096455.

Simulation for verification and validation of functional safety

Lars Mikelsons Zhou Su
Bosch Rexroth AG
Rexrothstr. 3, 97816 Lohr am Main

Abstract

Safety of machinery is the most critical issue in the design of mechatronic systems. The verification and validation procedure for functional safety of machinery is thoroughly discussed in ISO 13849-2. Following this procedure, the system behavior in case of a component failure has to be analyzed. Up to now this analysis bases on expert knowledge and real experiments. In this contribution a simulation based approach is presented. This approach has several advantages over the state-of-the-art. First, real experiments are more time consuming and costly than simulation. Moreover, according models can be used for further investigations like optimizing the sensor setup.
To enable failure simulation as a substitute of testing on real machinery for validation of functional safety, typical hydraulic failures are added to safety-related components of an in-house Modelica hydraulics library. This library is then used for the verification and validation of functional safety of a hydraulic test bench. Moreover, error propagation is considered.

Keywords: functional safety; hydraulics; simulation; failure modeling

1 Introduction

1.1 Motivation

Safety is of primary concern for all machine designers. The functional safety of a mechatronic system is assured by the correct execution of safety functions. Those parts of the complete system that are relevant for the execution of safety-functions are denoted as safety-related part of the control system (SRP/CS). ISO 13849 provides guidelines to assure safety of mechatronic systems. While ISO 13849-1 [1] concentrates on the design of the SRP/CS, ISO 13849-2 [2] focuses on the validation of functional safety. Thereby, the reliability of the execution of a safety function is evaluated by a discrete measure called performance level (PL). The determination of the PL of a safety function requires the analysis of the system behavior in case of one or more component failures of the SRP/CS. The failures that need to be considered for that analysis are also standardized in ISO 13849. The PL is then used to verify that a mechatronic system is functional safe, by checking that the PL of the SRP/CS is greater or equal to the required performance level (PL_r) of the system. Obviously, the PL_r has to be derived beforehand from a risk assessment.
It is obviously desirable, that the validation of a safety function can be done solely by analysis, using mainstream failure analysis techniques like Failure Mode and Effect Analysis (FMEA) [3] or Fault Tree Analysis (FTA). However, in most industrial applications, the SRP/CS of a safety function are too complex to analyze the system behavior by the engineers intuition. Hence, the result of these failure analysis techniques is seldom conclusive. Consequently, testing on the real system must be carried out in order to get a reliable result. For these tests usually a prototype of the SRP/CS has to be constructed, which is a time consuming and costly task. Furthermore, correct insertion of the desired component failure into the test setup is not only difficult, but can also damage the prototype, e.g. if the influence of contaminated oil is investigated. In some applications, testing on actual constructed systems might not even be possible, e.g. if the considered failure leads to an hazardous situation for the operator. This is the case in hydraulic applications, when the housing of a component breaks, because this leads to an eruption of the oil at high pressure. To overcome the same problems (costly and time consuming prototypes), years ago simulation was established as a development tool. The use of simulation for the verification and validation of requirements is visualized in the mechatronic V-Model (see figure 1). However, up to now the requirements were mostly functional requirements. To the author's knowledge there exists no methodology to use simulation for the verification and validation of functional safety with respect to ISO 13849. Consequently, there are no libraries available

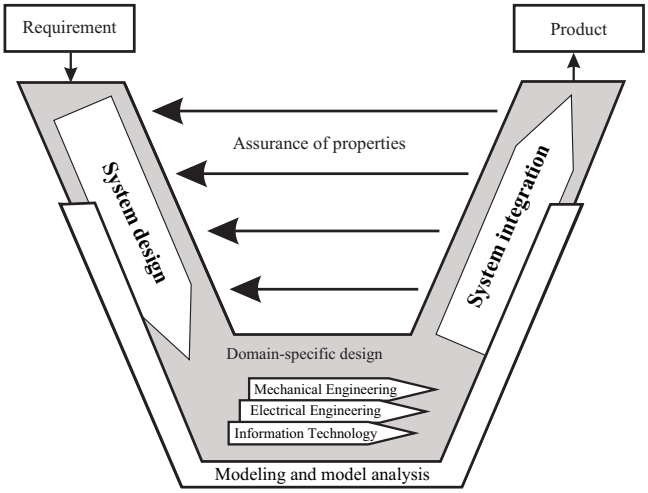

Figure 1: The mechatronic V-Model

that have a suitable level of detail, i.e. libraries including failure models. Obviously, it is desirable to model components including failures in such a way that

- the failures can be attached to a model without a failure (the original model),
- modification of the original model does not require modifications of the failures,
- the different failures can be easily exchanged,
- new failures can be added.

According to the first requirement physical models are needed. The remaining requirements aim for an object oriented model. Thus, Modelica seems to be appropriate to set up such models.
In this contribution an in-house hydraulics library is extended by components with failures, where the failures are modeled according to the requirements mentioned before. On the basis of that library it is shown how simulation can support and ease the design of a functional safe system. Moreover, an approach for error propagation is presented. A hydraulic test bench, which is used for testing hydraulic components like valves, is used as an application example. To summarize, the major benefits of the methodology presented here are:

- Optimization the typical work flow of design with respect to functional safety of mechatronic systems [4], i.e. replacing conventional analysis techniques and tests on prototypes by failure-simulation.
- Automated identification of the safety-critical failures in the SRP/CS.
- Investigation of error propagation.
- Future: Possibility to determine whether a failure can be detected by the sensor arrangements in the SRP/CS.

1.2 State-of-the-art

The concept of functional safety is derived from a functional system representation. Thus, most approaches for computer aided design of functional safe systems use functional models. A functional model is a block diagram of the system under consideration, where the blocks represent functions of the model and the connections represent a flow of energy, material or signals. Functional models can be generated at very early design stages, but suffer from the fact that they are rather rough, e.g. they do not include any dynamics.

Using these functional models, a Functional Failure Identification and Propagation framework is proposed for the analysis of functional failure propagation in [5]. However, this approach differs significantly from the method shown here and suffers from two major drawbacks. First, the level of detail of functional models is very low. Thus, the value of the gathered information is limited. Moreover, a special syntax and semantics are developed, so that existing models can not be used or upgraded for safety considerations. The same holds the methods described in [6] and [7] since the authors also use functional models. It is noteworthy, that the approach presented by Deng is originally intended for the verification of general requirements and can hence also be used for the verification of functional safety.

Most functional model-based analysis approaches are supported by failure analysis techniques like FMEA or FTA. An approach for combining both is presented in [8]. The coupling is done using the Systems Modeling language (SysML), a general-purpose modeling language. This method allows for automatic computation of a FMEA from a functional model, but suffers from the drawbacks described above. The use of ModelicaML [9] could be a promising future direction of the work presented here.

Although most simulation-based safety analysis methods use functional models, examples of physical models used for safety investigation can be found. A simple hydraulic system including a 4/3 directional valve, a motor-pump group and a cylinder is modeled with the help of bond graphs in [10] for

DOI 10.3384/ECP14096455

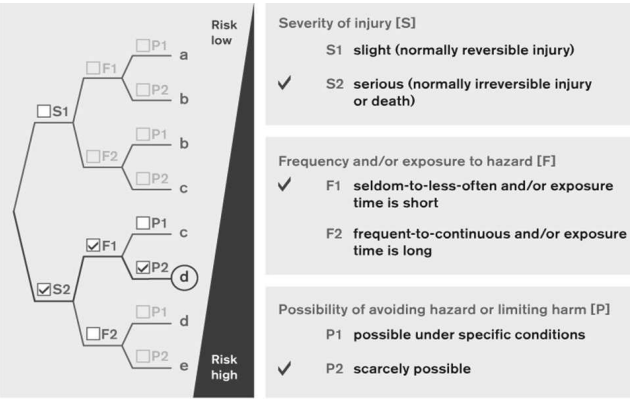

Figure 2: Determination of the required performance level using the risk graph

proactive fault diagnosis. However, without the help of powerful object-oriented equation-based modeling languages like Modelica, even modeling this simple hydraulic system is tedious and difficult. Therefore, the fault diagnosis is restricted to erroneous spool movement in the 4/3 directional valve. Moreover, this method does not satisfy the requirements stated in the motivation.

In the following section a brief introduction to functional safety is given. After that, a hydraulic library including models of failures is presented. Section 4 shows the application example mentioned before. The paper closes with a conclusion and an outlook.

2 Functional safety

Safety is the primary concern for every machine designer. ISO 12100 defines machine safety as:

"*the ability of a machine to perform its intended function(s) during its life cycle where risk has been adequately reduced.*"

If the machine safety depends on the correct functioning of a control system, the term *functional safety* is used. ISO 13849 contains guidelines for the design of a system with respect to functional safety. In [4] ten steps to reach the required performance level are presented. In the first step possible risks are identified and evaluated in a risk assessment. If required, measures to reduce the risks are chosen. These measures can be information for the use of the system, improved system design or safeguarding. If such a measure depends on the control system it is called a *safety function*. De-energizing of the system in order to reach a safe state is a common safety function. In the second step the safety functions of the system are identified. In the third step the PL_r is determined for every safety function using the risk graph in figure 2. In the shown example the possibility of serious injuries (irreversible or death), that can happen only in short time span (e.g. 10min per hour) and are hard to avoid (e.g. fast moving machine) lead to a required performance limit PL_r =d. The PL_r quantifies the required reduction of the risk (see figure 3). Hence, after the third step the requirements for the SCRP/CS are known. Thus, in the fourth step the structure of the control system can be outlined. Following directive EN 954-1, control systems can be realized in the form of five categories (B, 1, 2, 3, 4) mapping the typical architectures, e.g. redundancy or additional shut-off paths. With each category only certain performance levels can be reached as can be seen in table 1. On the other hand, different choices for the category in order to reach a certain PL are possible. The fourth step is completed after the selection of an appropriate category. In the fifth step a functional model of the system is generated. That model is used in the sixth step order to analyze failures of the SCRP/CS. Therefore, a list of relevant failures is included in [2]. Basing on the functional model and the engineers expertise it is judged whether the failures from the failure list lead to a dangerous situation or the system remains in a safe state. Then, for each component the diagnostic coverage (DC) is determined as the ratio between failure rate of detected dangerous failures and the failure rate of total dangerous failures. Thereby, the failure rate is the inverse of the mean-time-to-failure (MTTF), which can usually requested for each component at the manufacturer (MTTF and $MTTF_d$). The MTTF is the number of years at which approximately 63% would fail. Hence, the MTTF corresponds to a statistical, expected value and does not guarantee for a failure free time. The sixth step is completed after calculating the average diagnostic coverage for the complete SCRP/CS (consisting of N components) by

Category:	PL (possible)
B	a-b
1	b-c
2	a-d
3	a-e
4	e

Table 1: Reachable performance level

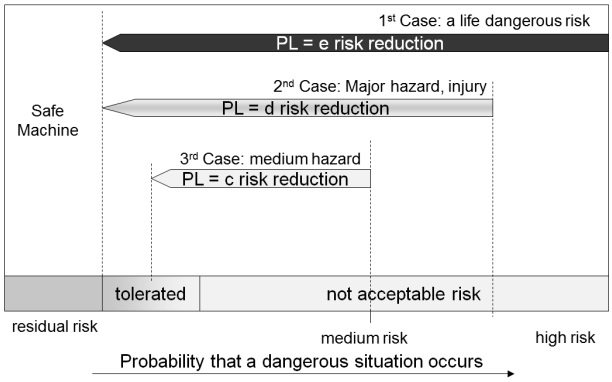

Figure 3: Principle of the risk reduction by the safety function

$$\mathrm{DC}_{avg} = \frac{\frac{\mathrm{DC}_1}{\mathrm{MTTF}_{d1}} + \frac{\mathrm{DC}_2}{\mathrm{MTTF}_{d2}} + \ldots + \frac{\mathrm{DC}_N}{\mathrm{MTTF}_{dN}}}{\frac{1}{\mathrm{MTTF}_{d1}} + \frac{1}{\mathrm{MTTF}_{d2}} + \ldots + \frac{1}{\mathrm{MTTF}_{dN}}}, \quad (1)$$

where MTTF_d denotes the mean time to a dangerous failure. In the seventh step the PL of the designed SCRP/CS is determined. The PL depends on

- the category of the PLC,
- the reliability of the SCRP/CS (MTTF_d),
- the diagnostic coverage (DC_{avg}).

There exist different approaches to compute the MTTF_d of the SCRP/CS from the MTTF_d of the single components, e.g. Parts-Count-Procedure [4]. Using the MTTF_d, the category chosen in the fourth step and DC_{avg} determined in the sixth step, the PL can be read from a table given in [4]. Afterwards, the robustness of the PLC with respect to situations, that are not considered in the first steps, is analyzed in the eighth step. For example, in a redundant controller design all channels could fail due to violation of the maximum admissible operating temperature. In such cases adequate measures are taken. In the ninth step the software for the controller is developed with respect to state-of-the-art techniques and processes. In the last step the results from the previous steps are verified and validated. During the verification it is checked whether the required performance level has been reached. Otherwise the SCRP/CS has to be improved, e.g. with components with a longer life cycle or a higher category. The plausibility of all the mentioned reliability parameters (MTTF_d, PL, category, DC), must be validated, either by analysis or with the help of testing/simulation. The complete validation procedure can be summarized as follows:

1. validation of safety functions
2. validation of performance level which includes:
   - validation of category specifications
   - validation of $MTTF_d$ and DC_{avg}
   - Validation of measures against systematic failure
   - validation of safety-related software
3. validation of combination and integration of all SRP/CS

Theoretically, this verification and validation can be performed solely by analysis. However, due to the complexity of most control systems, testing or simulation must be carried out to support inconclusive failure analysis.
Besides the use of simulation for validation it is useful for some other tasks. In the sixth step dangerous failures are identified. Up to now this is done basing on a functional model and the engineers expertise. Due to typically big and complex systems this approach is time consuming and error prone. Hence, the use of simulation would not only speed up the design process, but also lead to more meaningful results.

3 Failure models in Modelica

The DC_HydrauLib is a Modelica library for the simulation of hydraulic systems developed by Bosch Rexroth. It contains hydraulic components like pumps, cylinders and valves. In this contribution it is used to present a possible approach for failure modeling in Modelica. This approach respects the requirements stated in the introduction. Using the language features of Modelica these requirements can be satisfied in the following way: Each failure is implemented in a new model that extends from the nominal model. All these models are then collected in a wrapper model (via replaceable), which is denoted as the failure model. Modeling this way one failure model consists of multiple models including failures. During application the user can choose the failure, that should be investigated by a parameter. The failures are implemented according to the list from ISO 13849-2 containing typical hydraulic failures. This list is developed without consideration of modeling and simulation. Hence, each failure is described on the base of the actual component construction. Examples for failures of a switching valve are

DOI 10.3384/ECP14096455

- Change of switching times
- Non-Switching (sticking at the end or zero position) or incomplete switching (sticking at a random intermediate position)
- Spontaneous change of the initial switching position (without an input signal)
- Leakage
- Bursting of the valve housing or breakage of the moving component(s) as well as breakage/ fracture of the mounting or housing screws

However, the hydraulic library contains only models with a level of detail suited for system simulation. Thus, a translation into implementable descriptions fitting to the abstraction level of the existing hydraulic library is required first. While the translation for the first two failures is straight forward, different translations for the remaining failures are possible, e.g.

- Spontaneous change of the initial switching position (without an input signal): A white noise input signal replaces the control signal when the failure is triggered.
- Leakage: Internal leakage with user-specified leakage coefficient.
- Bursting of the valve housing or breakage of the moving component(s) as well as breakage/ fracture of the mounting or housing screws: External leakage with a (big) user-specified leakage coefficient.

A brief overview on a possible implementation of the failures is given below.

Change of switching times The switching behavior of a switching valve is modeled by a trapezoidal profile, that is parametrized by the switching times (on/off separately). In addition to the parameters and variables inherited from the base model, two new parameters, r_{on} and r_{off} are introduced, which are defined as

$$r_{on} = \frac{T'_{on}}{T_{on}} \tag{2}$$

$$r_{off} = \frac{T'_{off}}{T_{off}}, \tag{3}$$

where T and T' are the original and the erroneous switching time of the valve, respectively. In case of a failure the erroneous switching times are used in the calculation of the spool dynamics.

Non-switching This failure is split into two failures, non-switching and random sticking. Non-switching means that the valve cannot open or close upon the next opening or closing input signal. Thus, this failure does not take effect immediately at the moment the failure is triggered. However, at the moment the failure is triggered the current spool position is saved and from that moment on used for the flow rate calculation instead of the spool position calculated in the spool dynamics.
Random sticking, takes effect when the failure type is triggered, which means that the spool stays at the current position when the failure is activated at any random time. The sticking position can either be the two end positions or any intermediate position. This failure is very common in directional valves, when the spring holding the spool at the end position is broken. The implementation is very similar to the non-switching behavior.

Spontaneous position change This failure describes the situation when the valve becomes totally uncontrollable, most likely due to breakage of the spool. For this failure, a white noise generator producing filtered noise with a user-specified bandwidth is used as the input for the spool dynamics. Notice that this noise generator is not really random. Only different seeds generate different noise output.

Leakage Leakage is an unavoidable problem in the construction of hydraulic valves. Leakage between two hydraulic ports is models as a volume flow rate proportional to the pressure difference Δp between the two ports

$$q = c \cdot \Delta p \tag{4}$$

with c as the leakage coefficient. Here, one has to distinguish between internal and external leakage. Internal leakage takes place between the two hydraulic ports of a the valve. In the example of a switching valve with two ports (A and B), oil might flow from port_A to port_B, even when the valve is fully closed. External leakage is leakage to the environment (modeled as a tank). This model can also be used to simulate the breaking of the housing or similar failures.

Looking at the failures it is clear that there should be some kind of triggering mechanism. In this work two different triggering mechanisms have been implemented. In the first case the failure is

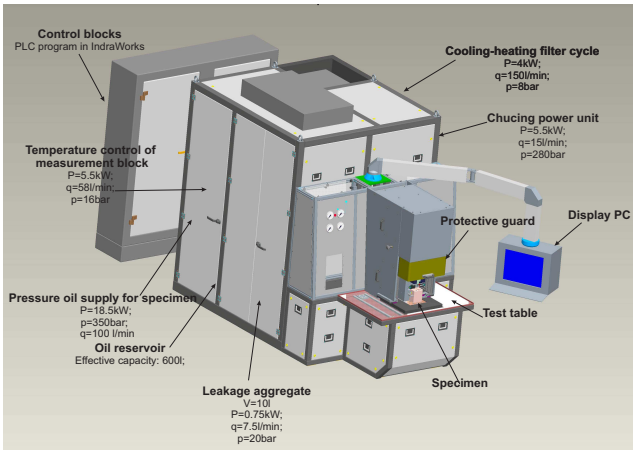

Figure 4: Hydraulic test bench

triggered at a user specified time. In the second case the failure is triggered by the violation of the working conditions of the corresponding component, e.g. pressure limitation, temperature range or fluid contamination. In this contribution only one working condition (pressure limits) is implemented. According to the specifications of the DC_HydrauLib, both ambient and fluid temperature are constant during one simulation run, so exceeding the temperature range cannot be modeled using that library (until now). Similarly, fluid quality is also a fixed property of a selected oil type, thus contamination of oil can also not be modeled. Though, the user can specify a maximal operating pressure. If this maximal pressure is exceeded the chosen failure is triggered.

4 Application Example

In this section a test bench for hydraulic valves is used to present possibilities of the usage of failure simulation during the design phase of a hydraulic system. A typical safety function of this test bench (emergency stop initiated by user), is thoroughly investigated by simulation on the SRP/CS that executes this safety function.

4.1 Test bench

The hydraulic test bench (Figure 4) is designed for the testing of directional valves. The test bench is manufactured by Bosch Rexroth and applied in the production line of a Rexroth plant. Typical valve characteristics of the test item (specimen in figure 4) like leakage, characteristics curves and switching times can be tested. To perform all tests required for a test item, the test bench must be able to provide various pressure and volume flow rates. During the productive period of the test bench, a trained operator stands in front of the test table to mount the test item. A test can only be started when the safety door (protective safeguard in figure 4) is open. On the other hand this door can only be lowered when the test item is correctly mounted. The test results are automatically recorded by the control devices of the test bench. Thereby, the test results can be severely impaired by a malfunction of the test bench, especially by component failures in the motor-pump group and the test table. For example, internal leakage inside the test bench may lead to test results, that indicate too big leakage of the test item. Moreover, if one of the safety functions, which are measures against risks, cannot be carried out due to internal component failures, the consequence can be even more disastrous. Thus, each time before the test bench is started a checking routine has to be performed. To reduce this non-productive period, and at the same time ensure the correct functioning of safety functions like emergency stop and safe door locking, is one of the most challenging issues in the designing of hydraulic test benches.

4.2 Circuit example

The safety function to be investigated for the hydraulic test bench (emergency stop initiated by user), is activated by pressing the emergency button on the control panel, and executed by de-energizing all engaged valves. Notice that in the execution of this safety function only the relevant actuators, namely valves engaged in cutting off the pressure supply, are de-energized. The energy supplier (the electrical motor within the motor-pump group) is still working, because it might be employed in other crucial functions of the test bench.

Two functional blocks exist between the oil pressure supply and the test table, where the test item is mounted. The block directly below the base frame of test table is the measurement block, which contains mainly sensors for measuring and valves for channel selection. This measurement block is designed to carry out all important tests on the test item. Notwithstanding its importance in the correct functioning of the test bench, it is not safety-related, since it does not execute a safety function. Moreover, malfunction of this measurement block only results in the non-execution of the designed tests on the test item. No danger is caused by the loss or degradation of this function. So the measurement block is out of the investigation scope of this

DOI 10.3384/ECP14096455

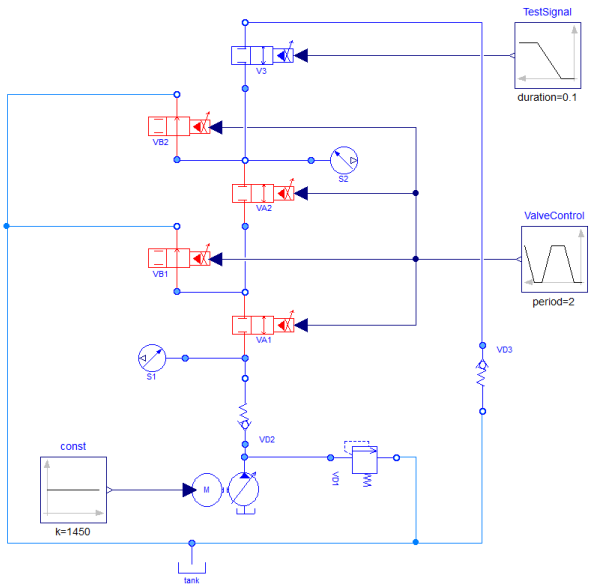

Figure 5: Simplified circuit diagram

contribution.

The other block is directly connected to the pressure supply. This block is designed to cut off the oil supply from the pump as fast as possible by de-energizing all engaged valves upon emergency. So this functional block is the active part to execute the safety function under consideration, and thus in the focus of the investigation in this contribution. The original system consists of several identical channels that can be connected to the test item. However, for the following investigations only one channel is considered for the reason of simplicity. Some additional simplifications lead to the circuit diagram in figure 5. Here, the red components (valve VA1, VB1, VA2 and VB2) are failure models. An explanation of the essential components is given in the following:

- VA1 and VA2: These 2/2 directional valves control the pressure supply of the test table. The valves have a switching time of 10ms and an internal induction sensor for spool monitoring (high DC value).
- VB1 and VB2: These 2/2 directional valves are opened in order to let the remaining oil between two valves flow back to the tank. The valves have a switching time of 10ms.
- VD1: This pressure relief valve limits the pressure in the circuit to 250bar.
- V3: This 2/2 switching valve imitates a test item.

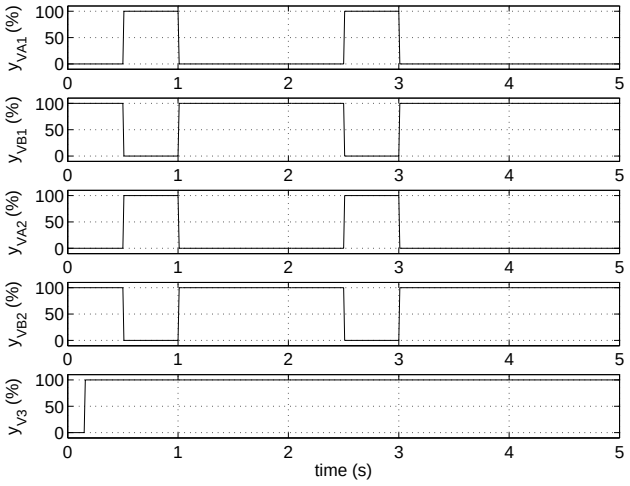

Figure 6: Spool position of the valves in the reference simulation

4.3 Failure simulation

Before performing failure simulations, a failure-free simulation is first carried out as a reference behavior. During this reference simulation the safety function is triggered twice within five seconds. Thereby, the motor-pump group provides a constant volume flow rate of 40 l/min. Figure 6 shows the spool position y of all controlled valves (VA1, VB1, VA2, VB2 and V3). The safety function is triggered at 1s and 3s, respectively. Thus, at these times the valves VA1 and VA2 are de-energized (closed). Moreover, VB1 and VB2 also de-energized (opened) and thus let the residue oil flow back to the tank. Valve V3, which represents the test item, is controlled by a separate testing signal, and is not engaged in the execution of the safety function. It opens at 0.15 s and stays completely open throughout the whole simulation. The volume flow rate into the test item q_{V3} is the output variable since this variable is a measure for the danger of extruding oil. The volume flow rate into each major (VA1, VA2, VB1, VB2 and V3) is shown in figure 7. Valve VB1 and VB2 are auxiliary valves designed to let out residue flow when the main channel is suddenly cut off. Hence, the flow rate trough these valves is much smaller than the flow rate through VA1 and VA2.

The results of the reference simulation is used as the reference for all failure simulations performed in the following.

4.3.1 Time triggered failures

In the first step described in Sec. 2 a risk assessment is performed. Here, simulation with failures injected

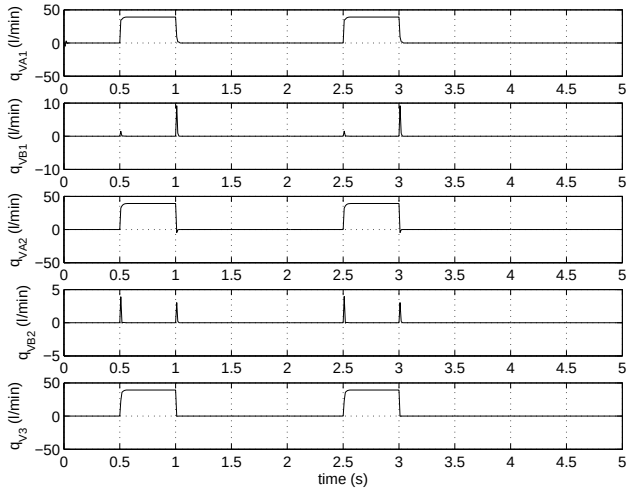

Figure 7: Volume flow rate at port_A of all controlled valves in the reference simulation

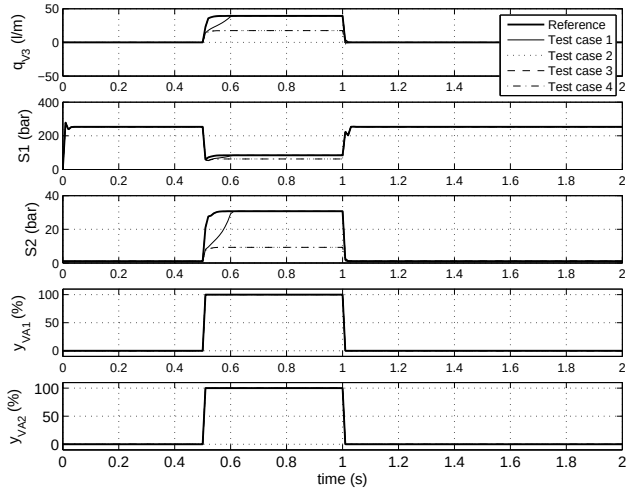

Figure 8: Comparison of four failure simulations with the reference simulation

into only one of the safety-related components (VA1, VA2, VB1 and VB2) can be used in order to get better estimates of the consequences of component failures. In the sixth step it judged whether a failure leads to dangerous situation or not. Clearly, also here simulation can be used. However, here the use of simulation in the tenth step is shown, i.e. how to use simulation for validation. Therefore, the category of the SRP/CS is validated in the following. The chosen category for the system at hand is three (PL_r=d). According to ISO 13849-2 this requires that a single failure does not lead to the loss of the safety function. Therefore, a Dymola script is used to simulate possible single failures. In figure 8 some typical results are presented. The trajectories under investigation are the system output q_{V3}, which is the volume flow rate into the test item valve V3, and all measurable states, which are the displays of the two pressure sensors S1, S2 and the two internal sensors monitoring the spool position for valve VA1 and VA2. Sensor S1 is placed near the pump, and is used to monitor the pressure source of the whole system. Sensor S2 is placed at the inlet port of the test item valve V3, and is used to monitor the pressure provided to the test item.

It can be easily seen that the trajectories of q_{V3} and the two pressure sensor displays in the four test cases in figure 8 differ from the reference trajectories around 0.5s (valve VA1 and VA2 are opened). However, after the first triggering of the safety function at 1s, q_{V3} becomes almost identical to the reference trajectory for each test case. The same holds for all test cases not shown here. Thus, the safety function is successfully executed in all the four test cases and the safety function is not lost in case of a single failure.

Note that the validation of the category can thus be performed only based on simulation, which saves time and money (especially for more complex systems). Clearly, during the risk assessment also combinations of failures can be simulated.

4.4 Error propagation

For the previous simulations, only time-triggered failures are considered. Another option for the failure triggering mechanism, in which a component failure is activated when a safety principle is violated, is considered in this section, for the investigation of error propagation.

Therefore, the failure-free pressure relief valve VD1 in figure 5, which is used for pressure limitation of the whole system, is replaced by an equivalent failure model. Note that the failure lists for pressure valves differs from the failure list for directional valves. The only investigated failure in this contribution is non-opening, which means that the valve cannot open completely (maximal 1%).

In the test case for error propagation the failure of the valve VD1 is triggered at 1s. Additionally, VA1 becomes uncontrollable (spontaneous spool movement), if the pressure at the inlet port exceeds the pressure limit of 400bar. The other valves (VA2, VB1 and VB2) exhibit a big external leakage (corresponds to the breaking of the housing), if the pressure limit (same as for VA1) is exceeded. Once again, a simulation of five seconds with two requests on the safety function is performed (denoted as Testcase 1 in the fig-

DOI 10.3384/ECP14096455

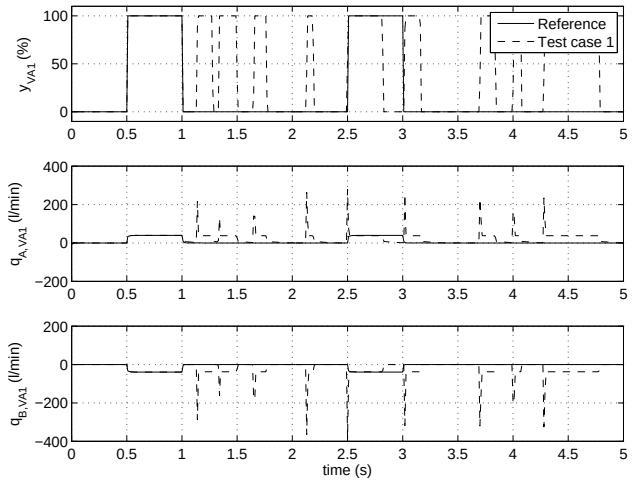

Figure 9: Results of the valve VA1 compared with the reference simulation

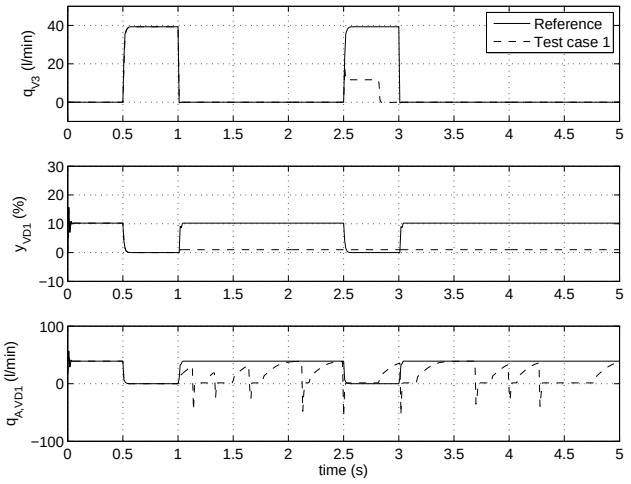

Figure 10: Results of the valves V3 and VD1 compared with the reference simulation

ures). In figure 9 the simulation results for valve VA1 are shown. It can be seen that the valve VA1 breaks down shortly (at 1.01s) after the failure of valve VD1 is triggered, because the pressure at the input port gets bigger than the pressure limit. From that time on the spool moves uncontrolled, which results in the presented volume flow. The valves VA2 and VB1 break down simultaneously shortly after the break-down of valve VA1 at 1.13s. This is, because the inlet ports of these two valves are connected to the same hydraulic port. The break-down of the valves VA2 and VB1 is modeled as big external leakage and hence these valves nearly act a tank for the rest of the simulation. That behavior explains the simulation results of the valve V3 (shown in figure 10). It can be seen that the volume flow after the failure of VA2 is much smaller than in the reference simulation. Note that the valve VB2 works properly, which indicates that the pressure at the end connector to the test item does not exceeds the maximum allowed pressure. This can also be confirmed by a look at the pressure sensor S2, which is even lower as in the reference simulation. This behavior occurs, because the valves VB1 and VA2, which are nearer to the pressure supply, break down earlier (and exhibit a big external leakage as explained before).

This example shows that it is possible to perform a model based estimation of the consequences of component failures, where even error propagation is considered.

5 Summary

In this contribution an approach for the use of simulation for the verification and validation of functional safety is presented. Therefore, a hydraulics library is extended by failure models. Thereby, the failure models depend on the original model in such a way, that the requirements stated in the introduction are satisfied. One possible use of these failure models is a risk assessment. The simulation of single failures lead to insight in the consequences of component failures. Here, also error propagation can be considered. Furthermore, the failure models can be used for the verification and validation step, e.g. the verification of the category as shown before.

In the future, optimization will be used for the identification of the worst case combination of failures. The results can either be used for the risk assessment or the identification of critical components. Moreover, the approach can be used in order to identify an optimal sensor setup. Therefore, on the one hand better sensor models have to been implemented and on the other hand algorithms for failure identification are required.

References

[1] ISO 13849-1: Safety of machinery-safety-related parts of control systems - Part 1: General principles for design. International Organization for Standardization (ISO), 2006.

[2] ISO 13849-2: Safety of machinery-safety-related parts of control systems - Part 2: Validation.

International Organization for Standardization (ISO), 2010.

[3] Bertsche B. Reliability in Automotive and Mechanical Engineering. VDI-Buch, Springer-Verlag Berlin Heidelberg, 2008.

[4] Barg J., Eisenhut-Fuchsberger F., Orth A. 10 steps to peformance level - Handbook for the implementation of functional safety according to ISO 13849, 2012, Bosch Rexroth AG

[5] Sierla S., Tumer I., Papakonstantinou N., Koskinen K., Jensen D. Early integration of safety to the mechatronic system design process by the functional failure indentification and propagation framework. In: Mechatronics, Volume 22, 2012.

[6] Belmonte F., Schön W., Heurley L., Capel R. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. In: Reliability Engineering and System Safety, Volume 96, 2010.

[7] Deng A., Britton G., Tor S. Constraint-based functional design verification for conceptual design. In: Computer-Aided Design, Volume 32, 2000.

[8] David P., Idasiak V., Kratz F. Reliability study of complex physical systems using SysML. In:Reliability Engineering and System Safety, Volume 95, 2009.

[9] Schamai W., Fritzson P., Paredis, C., Pop A. Towards unified system modeling and simulation with ModelicaML: modeling of executable behavior using graphical notations, In: Proceedings 7th Modelica Conference, Como, Italy, 2009

[10] Athanasatos P., Costopoulos T. Proactive fault finding in a 4/3-way direction control valve of a high pressure hydraulic system using the bond graph method with digital simulation, In: Mechanism and Machine Theory, Volume 50, 2012

DOI 10.3384/ECP14096455