15th IFK
Proc. of the 15th International Fluid Power Conference <Symposium/Conference>
<DOI>

Automated Processing of FMEA-Induced Fault-Injection Simulation for Safety Functions in Dangerous Machinery

Dipl.-Ing. Christa Düsing, Dipl.-Ing. Benjamin Erzberger

Authors affiliation, duesing@xcmg-erc.com, benjamin.erzberger@fluidon.com

Abstract.

Safety-critical and hazardous mobile machines must not only be technically safe, but also require a validation process with increasing demands on process quality, traceability, and reproducibility as the required safety level rises. Since safety functions (SF) often operate close to safety limits, validation by physical testing is associated with high effort and late availability; therefore, systematic simulation-based testing is considered as an early, safe and repeatable alternative. This paper presents a systematic simulation-based validation approach using a digital model that represents the aspects of machine structure and kinematics, drive and control subsystems, and safety-related software algorithms within a physics-based simulation environment. The method is derived from a Safety Function-FMEA (Failure Modes & Effects Analysis) [4, 10] in combination with Failure Modes, Effects & Diagnostic Analysis (FMEDA) [3, 10] to define relevant failure modes, test conditions, and diagnostic expectations. These failures are implemented in the digital model as targeted fault injections via virtual sensors and manipulators, enabling controlled and adjustable experiments for machine-level assessment of system response, failure detection, and diagnostic performance. The implementation is carried out using a digital model [1, 14] in DSHplus® [1, 2] (1D simulation of hydraulics, mechanics and controls) By integrating the digital model into the Cube® platform [1,2], the simulation environment is extended to a digital twin, enabling automated parameter management, test execution, and result evaluation in a reproducible workflow according to established definitions. In addition to verifying logic and algorithms, the approach is aligned with relevant functional safety requirements and processes such as ISO 13849 [8], ISO 19014 [7] and ISO 26262-8, Clause 11 [9], supported by tool assessment and complemented by model validation and plausibility checks. The approach is demonstrated using the safety function for working range limitation of an excavator and shows how digital-twin-based fault injection testing can provide traceable evidence for early, standard-compliant validation before physical prototypes are available or dangerous tests have to be carried out.

Keywords. Simulation-based testing, Fault-Injection-Test, FMEA-induced Failure Modes, Digital model, Digital twins, Cube Platform, Verification & Validation, Safety Assessment

1. INTRODUCTION

The development of safety-related parts of control systems (SRP/CS) [8] in mobile machinery with increasing levels of automation requires a systematic evaluation of safety functions to ensure reliable operation in the event of failures. Functional safety is not only a regulatory requirement defined by standards such as ISO 13849 [8], ISO 19014 [7], but also a key contributor to the operational performance and acceptance of automated and (semi-) autonomous mobile machines. With increasing automation, safety functions are required to operate close to physical and functional limits, which significantly increases the complexity of their development and validation. In conventional development processes, the validation of safety functions is often time-consuming, labour-intensive, and usually only feasible in late development stages. This late availability delays the detection of safety-relevant design weaknesses and increases development effort and costs, particularly when design iterations become necessary. At the same time, safety standards demand traceable and reproducible evidence that safety functions meet the required Performance Level (PL) [8], which further increases the pressure on high-quality development and validation processes, especially for highly dangerous machines according to new machinery directive in which notified bodies have to be involved along with the development. In current industrial practice, these challenges are primarily addressed through extensive hardware-based testing and analytical safety assessments such as FMEA [4,10] and FMEDA [3, 10], which are however largely limited to late development stages and component-level evaluation. To address these challenges, automated and simulation-based validation methods are increasingly considered as a means to enable early, repeatable, and cost-efficient testing of safety functions. In addition, such methods must not only reproduce nominal machine behaviour, but also allow systematic investigation of failure conditions in order to support functional safety validation. In this context, safety functions are distributed across multiple technical domains, including machine structure and kinematics, hydraulic or electric actuators, electronic hardware such as sensor, controllers and software algorithms. Ensuring functional consistency across these domains requires validation methods that operate at machine level rather than at isolated subsystem or component level. The approach presented in this paper follows a structured validation process in which Safety Function-FMEA [4, 10] and FMEDA [3, 10] results are transferred into a physical-based digital model of the machine. This digital model is used to execute systematic fault-injection simulations, enabling automated evaluation of safety function behaviour at machine level. By embedding the simulation model into an automated workflow environment, parameter variations, test execution, and result evaluation can be managed in a traceable and reproducible manner. Figure 1-1. illustrates the structured validation process followed in this work.

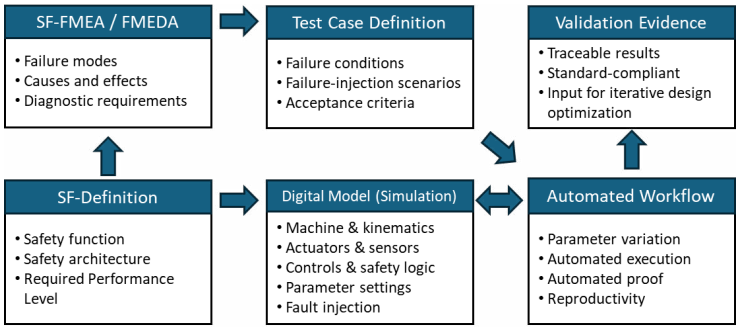

Figure 1-1. Process Flow of the proposed Simulation-based Validation approach for SF

2. EXCAVATOR USE CASE AND SAFETY FUNCTION SCENARIO

The proposed approach is applied to a representative use case of a (semi-)autonomous excavator equipped with the safety function *"Avoid bucket collision with detected obstacle"* for a hydraulic excavator. This function ensures that the bucket movement is automatically stopped before a potential impact occurs and requires a performance level PL = d. The presented simulation model represents the safety-relevant machine behaviour and includes the subsystems kinematics, the hydraulic system, sensors and the control algorithms required to analyse the selected safety function. Figure 2-1 shows in the top the excavator test without failure injections. The sequence illustrates the excavator bucket approaching the obstacle (a), detecting it (b), and stopping automatically before contact (c). This test verifies the correct operation of the implemented safety function under nominal conditions.

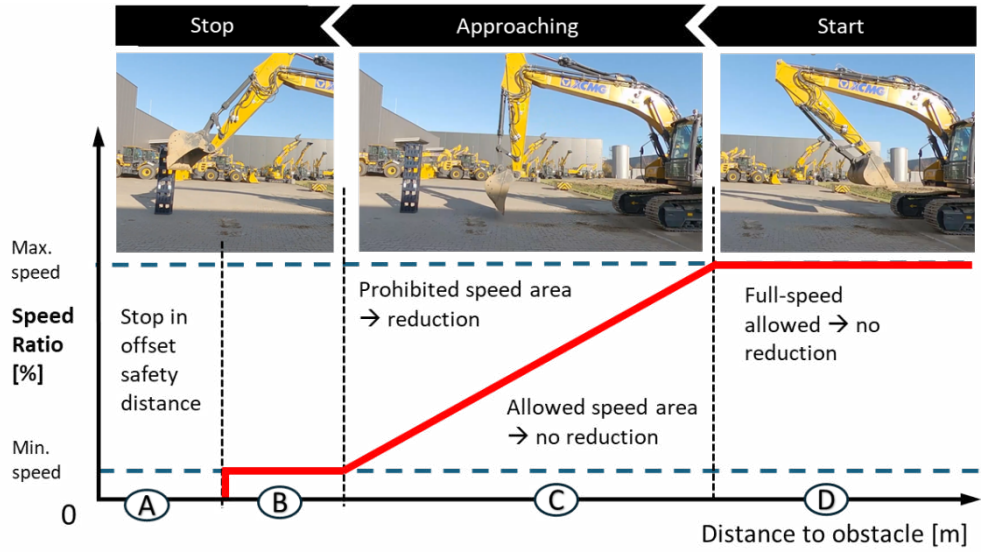

Figure 2-1. Excavator movement limit function: (c) Bucket approaching, (b) entering critical Obstacle Distance, (a) Bucket stopped [11, 12]

The bottom area of Figure 2-1 illustrates the determination of the speed scaling factor for the movement limiter. The speed scale on Y-axis is tracked against the distance to the obstacle on the X-axis. The red line shows the maximum speed curve for each distance. In section D, full speed is allowed and now speed reduction is applied. In the section C, set speed is limited along the red line. Values above the red line are reduced accordingly, values below the red line pass without reduction. Minimum speed is applied in the section B to approach obstacle slowly until safe stop is achieved in a safe offset distance to the obstacle in section A. Based on the operator-defined boundary limits, potential collision points of the work equipment are identified and extended by circular safety offsets this way. The maximum and minimum x- and z-position of these points are assigned to the corresponding boundaries. If multiple boundaries are active, the smallest scaling factor is applied to all drives of the excavator. The resulting scaling factor is multiplied with the set speed input and transmitted to the valve solenoid via the main PLC.

2.1. Possible Failures and Effects

During approach of an obstacle, various failure conditions can affect the safe execution of the movement limiter function. The following failure modes are typical examples derived from the Safety Function-FMEA [4, 10] and do not constitute a complete list:

(A.) **Sensor drift or sensor offset,** i.e. a gradual or constant deviation of the sensor signal from the actual value, can delay obstacle detection, increase the stopping distance or cause a collision;

(B.) **Hydraulic valve malfunction**, e.g. a stuck spool, can prevent the actuator from stopping even when the stop command is issued;

(C.) **Signal loss or signal degradation,** i.e. a temporary or intermittent reduction in signal quality (e.g. noise, dropouts or reduced resolution), can lead to incorrect interpretation of the machine status and uncontrolled movements of the actuator;

These effects directly influence the reliability of the stop function and must be validated to ensure compliance with ISO 13849 [8] and the associated functional safety standards.

2.2. Objective of the Investigation

The objective of this investigation is to evaluate the diagnostic behaviour of the safety function *"Avoid bucket collision with detected obstacle"* implemented by the movement limiter under selected failure conditions derived from the Safety Function-FMEA [4,10]. The safety function limits hazardous machine movements in the relevant directions, with the bucket–obstacle collision used as a representative use case. The focus is on assessing failure detection, system response, and diagnostic coverage using simulation-based fault-injection tests. Test success is evaluated by comparing the achieved diagnostic coverage (DC) with the required DC larger than 90% for PL d in a Category 2 safety function structure.

3. SIMULATION MODEL

3.1. Machine Model

The simulation model represents the excavator including its hydraulic actuators, control logic and virtual sensing system. All safety-relevant components are connected according to a Category 2 structure, consisting of a functional channel and an independent test channel for periodic diagnostic checking, as defined in ISO 13849 [8]. Figure 3-1 shows the simulation model consisting of an excavator model (2) that is moved by the hydraulic control system (1). The excavator model provides information about coordinates of the bucket tip (2B), but also outputs the angular values for each steel part of the attachment, so that sensor raw data can be generated and signals used in the test equipment (4). Sensor data feeds the movement limiter function (3) that can scale the control command (7). The test equipment (B) compares deviations between the redundant sensors signals and can deactivate a hydraulic pilot pressure switch (6) if critical deviations outside the tolerance band of +/- 2°are detected. The model also features an integrated manipulator (A) used for failure injection and signal variation of the arm angle sensor. The functional channel processes the sensor signals of the safety function, including redundant sensor inputs, whereas periodic diagnostic checking is realised via an independent test path in accordance with the applied Category 2 architecture. The manipulator (A) is used exclusively in the simulation to inject

defined failures derived from the Safety Function-FMEA [1, 10] into the signal paths, shown in Figure 3-1 to extend the simulation model for the representation of sensor-related failure scenarios. The hydraulic enable block (C) represents the actuation path for implementing and observing failure effects on the physical system behaviour. This setup supports the systematic assessment of the diagnostic performance by analysing failure detection behaviour and achievable diagnostic coverage under controlled failure conditions, following established principles of model-based diagnosis and failure-tolerant control [15, 16]. The simulation model as such represents a digital model of the machine, as it reproduces structure, behaviour, and failure responses without direct coupling to a physical asset. Figure 3-1 shows the simulation model structure with manipulator (A), test equipment (B), and hydraulic enable path (C) according to a Category 2 architecture.

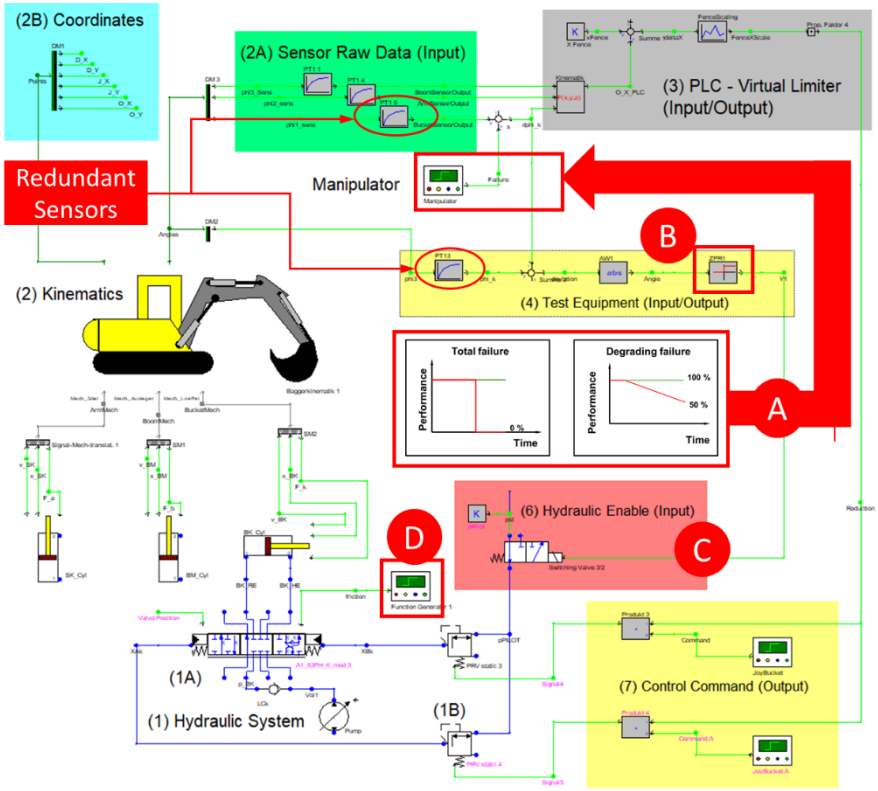

Figure 3-1. Simulation Example of Digital Model with Manipulator for an Excavator Arm representing Category 2 Structure according to ISO 13849 [8, 11, 12]

3.2. Valve Model

The directional control valve (1A in Figure 3-1) is modelled in detail to analyse the influence of mechanical failures on system behaviour. The focus is on the main valve stage, where effects such as increased friction, temperature-dependent spool motion, or a stuck valve spool can occur. Such failures can lead to unsafe machine states if the hydraulic actuation continues even though a stop command is requested. For this purpose, the valve position is derived from the equilibrium of forces on the spool that includes also terms for viscous

friction in the housing bore and a dry friction force that can be externally applied by the force manipulator D. The valve is actuated via electro-hydraulic pilot valves, which generate a differential pilot pressure acting on the ends of the main valve spool. This pilot pressure shifts the spool against spring forces, which in turn controls the hydraulic flow to the actuator. In the simulation model, external manipulation of the spool friction is used to reproduce an undesired stuck condition of the valve spool. The simulation example Figure 3-1 illustrates a failure scenario in which the valve spool remains stuck after a stop command. Although a corresponding closing signal is activated, the hydraulic flow is not fully interrupted and the actuator does not stop as intended. Reproducing this malfunction in the simulation allows the evaluation of control logic responses and virtual sensing mechanisms, as well as the assessment of potential countermeasures such as additional stroke sensing or parameter monitoring.

3.3. Test Procedure derived from FMEA

This section describes the execution of the simulation-based fault-injection tests and the associated evaluation workflow. The excavator simulation starts with arm and bucket cylinder at total extension, so that bucket is close to the cabin and bucket teeth. Both, arm and bucket cylinder are simultaneously retracted, so that arm moves away from the cabin and bucket turns leading to a bucket moving towards the obstacle. Under normal conditions, a movement limiter reduces speeds of arm and bucket with regard to the distance and stops without colliding. Defined failure scenarios are introduced at specific simulation times, and the system response is analysed using consistent evaluation criteria. An overview of the considered failure scenarios and their corresponding test objectives is provided in Table 3.1.

Table 3.1. Simulation-based Fault-Injection Scenarios and Evaluation Objectives for the Safety Function “Avoid bucket collision with detected obstacle” [10, 11, 12, 15, 16]

Injected failure scenario	**Description**	**Diagram reference**
Calibration / degrading failure	Evaluation of the influence of sensor drift on failure detection time and final stop position during bucket motion.	Failure Detection – Drift vs. Movement / Time
Performance test of bucket movement	Assessment of start and stop dynamics and their effect on the timing accuracy of failure detection and controlled stopping behaviour.	Failure Detection – Drift vs. Stop Position over Time
Total failure of inclination sensor	Analysis of the impact of complete inclination sensor signal loss on stop distance, safety margin to the obstacle, and diagnostic response.	Failure Detection – Inclination Sensor Offset
Stop behaviour	Evaluation of the influence of increasing angular offsets on stop distance and diagnostic tolerance within the specified sensor accuracy range.	Failure Detection – Inclination Sensor Angular Offset

Each virtual experiment follows a defined sequence answering the key questions of the test design:

(A.) **Baseline simulation:** The machine is simulated under nominal conditions to establish reference curves for pressure, flow and velocity. This serves as a benchmark for later comparison with failure scenarios;

(B.) **Fault-injection:** A selected failure mode, such as sensor drift, offset, or valve friction is activated at a predefined simulation time using the manipulator module. All test parameters are managed and executed automatically within Cube® [1, 2], ensuring repeatability and efficient data handling.;

(C.) **Detection analysis:** The system response is analysed to determine the safe failure detection time t_{detect}, defined as the interval between failure activation and detection by the diagnostic logic. Diagnostic performance is evaluated using two complementary coverage measures: $DC_{t\_failure}$, addressing time-based detection behaviour, and $DC_{x\_position}$ addressing the remaining permissible positional margin at the time of detection. This combined assessment supports a differentiated evaluation of diagnostic effectiveness with respect to temporal detection and positional safety, particularly for slowly developing failures;

(D.) **Diagnostic evaluation:** Based on ISO 13849 [8], the Diagnostic Coverage (DC) [8] is used to assess the effectiveness of the implemented diagnostic logic, while the time-resolved evaluation of failure detection follows system-level validation principles as defined in ISO 26262 [9]. The critical detection time $t_{detect.critical}$ is defined as the maximum allowable detection time interval derived from the safety function requirements. DC is calculated as the ratio of this critical detection time to the reference cycle time $t_{cycle,ref}$ and expresses the proportion of failures that can be detected within the allowable detection time interval;

The described evaluation approach enables a quantitative basis for comparing diagnostic quality across different failure types. The systematic approach enables direct comparison of failure scenarios and yields quantitative results on detection speed, reaction behaviour, and overall robustness. By combining DSHplus® [1, 2] with Cube® [1, 2] automated evaluation functions, a large number of test cases can be executed efficiently, forming the basis for the result analysis presented in Chapter 4.

3.4. Data management system structure for automated simulation

The virtual test setup for evaluating the excavator's stop function was realised in a combined simulation and automation environment. The excavator system model, including the machine structure, kinematics hydraulic components, and safety-related logic, was implemented in DSHplus® [1, 2], while parameter management, simulation control, and result evaluation were executed in the Cube® platform [1, 2]. The interaction between the simulation model and the workflow environment is based on a structured exchange of parameters, simulation control signals and result data, enabling automated, repeatable and traceable fault-injection testing of safety-relevant functions. Based on the system structure and data flow shown in Figure 3-2, the automated testing approach relies on a systematic parameterisation of test conditions applied within the simulation model. Test-relevant parameters are provided to the DSHplus® [1, 2] simulation model, where the fault-injection tests are executed and the dynamic system behaviour is calculated. The resulting simulation data are then transferred to the Cube® [1, 2] workflow environment for automated processing, evaluation, and visualisation, ensuring that every test case is executed under

clearly defined and reproducible conditions. This separation between simulation execution and result evaluation allows fault-injection tests to be automated and repeated without manual interaction with the simulation model.

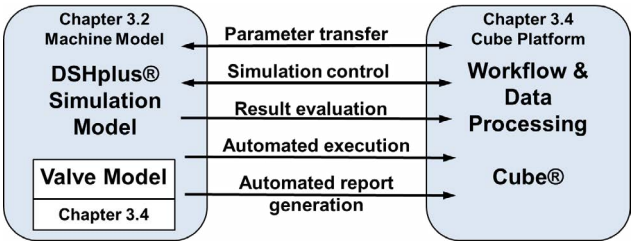

Figure 3-2. System Structure and Data Flow between DSHplus® and Cube® [1, 2]

The parameter set used for automated testing comprises several categories. Failure-related parameters describe the type and characteristics of the injected failure, such as the failure mode, activation time, magnitude, and duration. These parameters are directly derived from the Safety Function-FMEA [4, 10] and FMEDA [3, 10] results and represent the analytical basis for fault-injection testing. Machine operating conditions define the system state at the start of each test, including machine position, velocity, load conditions, and actuator states, ensuring that safety functions are evaluated under representative operating scenarios. In addition, environment-related parameters may be considered, for example the presence of obstacles or moving objects within the working area, if relevant for the investigated safety function. Sensor-related parameters, such as sensor placement or signal availability, allow the influence of sensing configurations on failure detection and diagnostic behaviour to be analysed. Finally, software-related parameters define internal settings of the safety function implementation, including limit values, timing parameters, and logic configurations used for monitoring and failure detection. All parameter variations are defined at workflow level and transmitted automatically from Cube® [1 ,2] to DSHplus® [1, 2] as input data for simulation execution. Simulation control, parameter transfer, and result feedback are handled within the automated workflow, allowing a large number of test cases to be executed efficiently. The resulting data, including system response, detection times, and diagnostic states, are returned to Cube® [1, 2] for structured processing and evaluation.

4. SIMULATION RESULTS

The conducted simulations show how the digital machine model and the automated workflow can be used to analyse functional safety aspects under defined failure conditions. The results illustrate how individual component and system failures influence the diagnostic behaviour of the safety function *"Avoid bucket collision with detected obstacle"*. The evaluation is performed both at virtual machine level and at system level with a focus on hardware-related failures. Based on simulation-based fault-injection, the diagnostic coverage is assessed in a structured and reproducible manner. The automated Cube workflow enables a process-safe and transparent evaluation, comparable to established SIL (Software-in-the-Loop) or HIL (Hardware-in-the-Loop) test procedures and allows efficient iterations in the process, e.g. when modifications in the algorithms become necessary. It can be used to automatically generate diagrams and key-figures that support the approval process. In addition, the simulation results are compared with the original data-

sheet-based evaluation approach, allowing additional insights and recommendations for the assessment of diagnostic coverage to be derived.

4.1. Investigation of Sensors Failures

Sensor-related failure effects on the safety function are analysed based on time-dependent signal behaviour. Characteristic signal trajectories of sensor output, hydraulic enable signal, cylinder position and actuator pressure are evaluated to illustrate the interaction between sensor failures, diagnostic logic, and system response. This allows a clear distinction between normal operation, detected failures and undetected failures, as well as the assessment of delayed failure recognition and its impact on the stop response. To represent safety-relevant sensor failures derived from the Safety Function FMEA, one of the redundant inclination sensor signals is manipulated. The applied failure patterns include time-dependent drift and step-like deviations, while the second redundant sensor provides the nominal reference signal. The diagnostic logic monitors the deviation between both signals and classifies a failure as detected once the predefined diagnostic threshold is exceeded. The resulting system behaviour is illustrated in Figure 4-1.

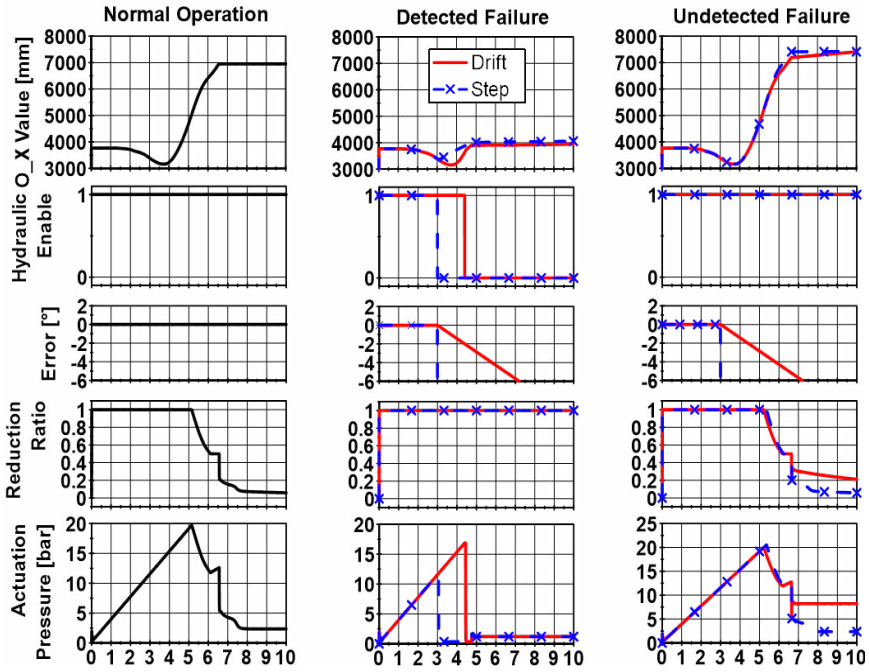

Figure 4-1. Sensor Drift, normal Operation, detected & undetected Failures [11, 12, 15, 16]

Normal operation has no error and applies the reduction ratio from the movement limiter to stop the bucket at 7000 mm in a reference cycle time $t_{cycle,ref} = 6.6\,sec.$ In the detected failure case, the injected deviation exceeds the diagnostic threshold, leading to deactivation of the hydraulic enable signal and thus, immediately stops movement at 4000 mm. Undetected failures remain below the threshold and therefore do not trigger the stop command, despite deviation of the manipulated sensor signal from the nominal signal. The failure causes a stop exceeding 7m and thus causes a collision with the obstacle. The results demonstrate the influence of failure severity on detection capability and confirm the

suitability of the simulation-based approach for assessing diagnostic coverage for sensor-related failures.

4.1.1 Sensor Drift

Figure 4-2(a) shows the bucket position at failure detection and the corresponding stop position for different sensor drift rates. Higher drift rates lead to earlier detection and shorter stopping distances, ensuring collision avoidance. Medium drift rates are detected sufficiently early but operate closer to the defined safety limit. Very small drift rates result in late detection or remain within tolerance, reducing the available safety margin. The results highlight the relevance of defined tolerance bands for achieving sufficient diagnostic coverage. The left-shift of the −0.5 °/s curve results from late detection at small bucket displacement.

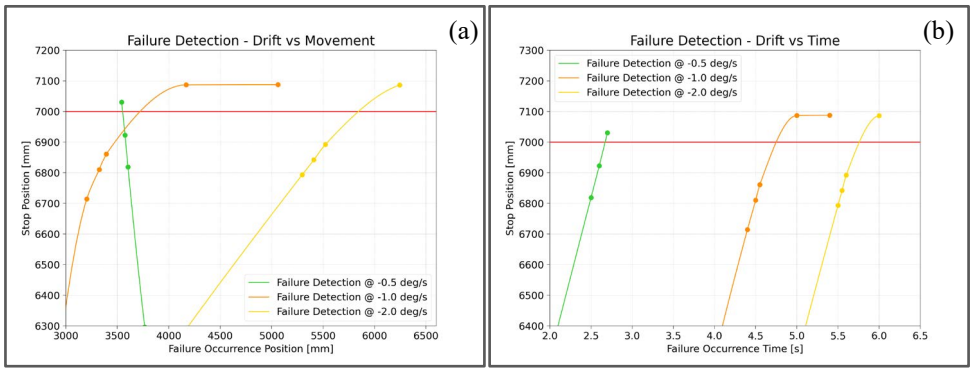

Figure 4-2. Failure Detection Characteristics [11, 12, 15, 16]

Figure 4-2(b) relates the time of fault-injection to the bucket position at stop. Faster drift rates cause early detection shortly after failure onset, whereas slower drifts lead to delayed detection closer to the obstacle. This behaviour demonstrates the time-dependent nature of drift faults and underlines the criticality of slow sensor drifts for diagnostic algorithms. For the automated data processing, the time-based diagnostic coverage $DC_{t\_failure}$ is calculated according to equation (4.1) using the simulation-derived detection timing for the failure setting crashing into the obstacle and the reference cycle time $t_{cycle,ref}$:

$$\mathrm{DC_{t\_failure}} = \frac{\mathrm{t_{failure\ occurance,crash}} + \Delta \mathrm{t_{detect}}}{\mathrm{t_{cycle,ref}}} \times 100 \qquad (4.1)$$

In addition, a position-based diagnostic coverage $DC_{x\_position}$ is introduced. The $DC_{position}$ describes the ratio of the position at which failure occurrence leads to a crash and the position of the obstacle and is defined as equation (4.2):

$$\mathrm{DC_{x\_position}} = \frac{\mathrm{x_{failure\ occurance,crash}}}{\mathrm{x_{obstacle}}} \times 100 \qquad (4.2)$$

The quantitative results for the investigated drift cases are summarised in Table 4.2. The results show that the two DC values differ from each other, but also that the demanded rate of 90% and higher could not be performed by the current design and algorithm of the movement limiter. A higher absolute drift rate corresponds to a more severe sensor failure, leading to a faster deviation of the perceived inclination from the actual machine state,

whereas smaller drift rates represent slowly developing failures that are typically more challenging to detect in time. The selected drift rates of −2°/s, −1°/s, and −0.5°/s therefore allow the diagnostic behaviour to be evaluated under clearly differentiated failure dynamics, while all other boundary conditions remain unchanged. This ensures that differences in detection time and diagnostic coverage can be directly attributed to the severity of the injected sensor drift.

Table 4.1. Quantitative Results for different Inclination Sensor Drift Rates obtained from Simulation-based Fault-Injection Test for a reference Cycle Time of 6.6 sec

Case	Drift rate [°/s]	Δt_{detect} [s]	Δt_{detect} [s]	$DC_{tfailure}$ [%]	x [mm]	$DC_{xposition}$ x [%]
D1	-2°/s	5.6	0.89	98.33	5750	82.14
D2	-1°/s	4.6	1.42	91.21	3600	51.43
D3	-0,5°/s	2.6	2.93	83.78	3600	51.43

The results in Table 4.1 show a clear relationship between drift severity, detection time, and diagnostic coverage. Larger drift rates lead to shorter detection times, as the sensor signal reaches the diagnostic decision limits more rapidly. Consequently, the proportion of the admissible reference cycle time during which the failure is detected increases, resulting in higher DC_{time} values. In contrast, smaller drift rates result in a more gradual signal deviation and longer detection times. This reduces the available safety margin before the permissible displacement is exceeded and leads to lower diagnostic coverage. The complementary metric $DC_{position}$ further highlights how early failure detection preserves spatial safety margins, underlining the criticality of slow sensor drifts. The result illustrates that the diagnostic effectiveness is not only determined by the implemented logic itself, but also strongly depends on the temporal characteristics of the failure itself. This underlines the importance of time-resolved, system-level fault-injection testing for evaluating diagnostic coverage beyond static or datasheet-based assumptions.

Figure 4-3 illustrates the relationship between the sensor drift rate and the time to failure detection Δt. Failure detection occurs once the predefined ±2° tolerance band is exceeded (to be verified in the simulation). The results show that higher drift rates are detected earlier, while slow drift rates lead to significantly delayed failure detection. The depicted trend follows a nonlinear inverse relationship.

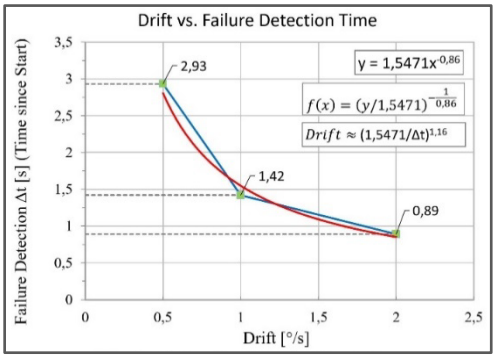

Figure 4-3. Failure Detection Characteristics [11, 12, 15, 16]

In addition, Figure 4-3 shows clearly that high drift rates are uncritical, as detection occurs early and sufficient safety margins remain. In contrast, slow sensor drifts are critical, since failure detection happens late and close to the safety limit, reducing the available stopping distance. This behaviour of slowly developing sensor drifts motivates the introduction of an intermediate Zone B in the safety algorithm, where operation continues at reduced speed before a safe stop in Zone A with a defined distance to the obstacle is initiated. Figure 4-3 therefore emphasizes the importance of defined tolerance bands and staged safety reactions to ensure adequate diagnostic coverage for slow sensor drifts.

4.1.2 Total and offset failures

Figure 4-4 illustrates the influence of inclination sensor offset failures on the diagnostic behaviour of the safety function in accordance with the principles of ISO 13849 [8] and ISO 19014 [17]. In contrast to drift failures, an offset represents a static deviation and leads to a constant discrepancy between the redundant inclination sensor signals. Figure 4-4(a) shows the resulting bucket stop position for angular offsets of 3° started at different time instants during the bucket approaching the obstacle. As the offset does not increase over time, failure detection is determined by the absolute deviation relative to the defined tolerance band of +/- 2°. Variations in the resulting stop position are caused by the system state at the time of fault-injection. The distance shown represents the absolute bucket position relative to the obstacle highlighted by the red line. Figure 4-4(b) presents the evaluation for increasing offset magnitudes. Offset values within the permissible angular tolerance band of +/- 2° are handled by plausibility monitoring in the test equipment of the safety function and do not lead to a safety reaction. The system fails to react for negative offset values as stop positions are beyond the limit of 7000 mm. Positive offset values bring the system to the safer side and stop in front of the obstacle instead. Once the offset exceeds the predefined diagnostic threshold, the inconsistency between both sensor signals is detected and the stop command is initiated. This behaviour is consistent with the diagnostic principles defined for Category 2 architectures according to ISO 13849 [8], where systematic sensor failures are detected by periodic or continuous plausibility checks. The results indicate that the applied tolerance band method in the movement limiter may lead to stop position deviations of up to 100 mm, therefore an additional safety offset distance in stop area Zone A, Figure 2-1, is recommended.

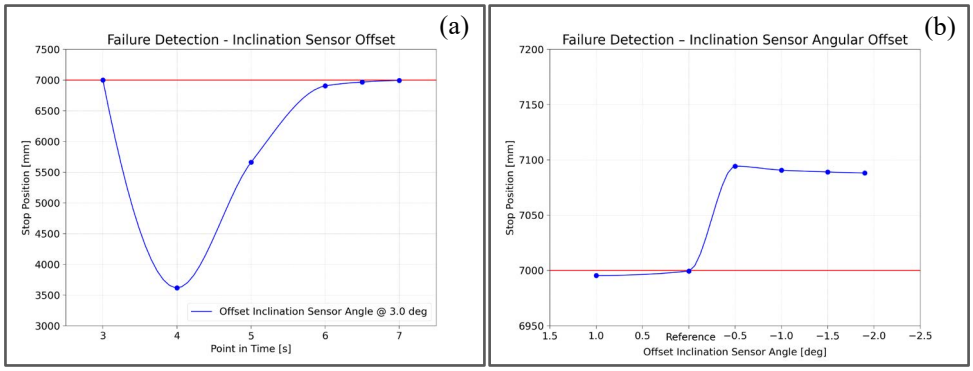

Figure 4-4. Total Failure of Inclination Sensor & Inclination Sensor Angular Offset [11, 12, 15, 16]

4.2. Valve spool behaviour

The results for wrong valve actuation behaviour and an active movement limiter are illustrated in Figure 4-5. In the friction scenario shown in Figure 4-5a, the valve spool opens to 40% that only allows a slow movement of the bucket while approaching the obstacle. The friction in the valve spool gap delays the valve closing after the stop demand at 4 sec. As a consequence, the valve spool stroke decreases progressively until the actuator motion comes to a standstill at an effective stroke of approximated 20% that is below the positive overlap of the metering edge geometry. The valve closing time of few seconds indicate, that the such frictions can become more serious when the valve already has higher openings before stop command is initiated. In contrast, the stuck piston failure illustrated in Figure 4-5b represents a mechanical blockage of the valve spool that avoids the valve closing. The stop command at 5 sec cannot be executed by the valve spool. The valve opening remains at 60%, so that the hydraulic flow is still further transmitted to the actuator. As a result, the bucket does not stop in front of the obstacle. Both behaviours indicate a total loss of controllability and a decoupling between the control signal and the physical actuator response.

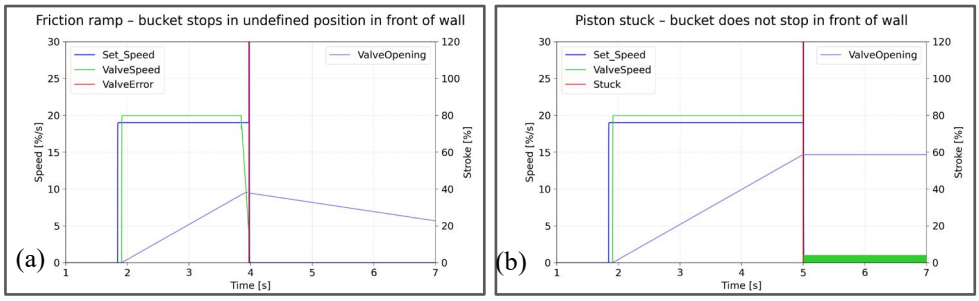

Figure 4-5. Comparison of friction-induced and mechanically blocked piston behaviour in the hydraulic valve section [11, 12, 15, 16]

The resulting bucket stop behaviour is shown in Figure 4-6(c) and Figure 4-6(d). In the friction ramp scenario shown in Figure 4-6(c), the reduced actuator speed leads to a controlled deceleration of the bucket, which comes to rest in front of the obstacle.

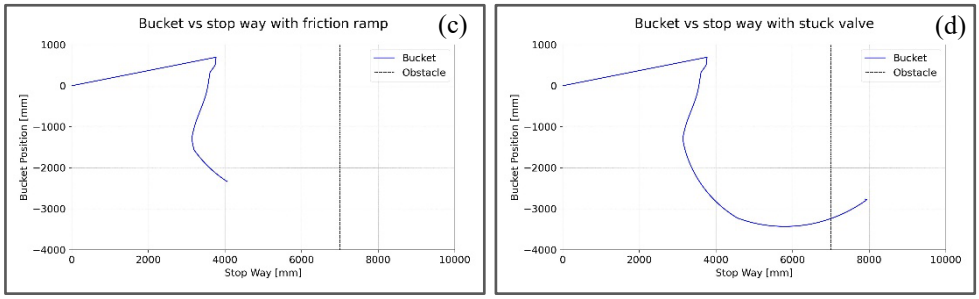

Figure 4-6. Bucket stopping behaviour under valve failure behaviour

In contrast, the stuck valve failure shown in Figure 4-6(d) causes continued bucket motion beyond the defined stopping position. The movement stops in the mechanical end position of the excavator attachment. This behaviour indicates that the hydraulic flow through the

valve is not interrupted, despite the presence of a stop command, and illustrates a safety-relevant failure mode in which unintended motion persists due to clamping of the valve.

4.3. Evaluation

The simulation results show that the implemented diagnostic concept reliably detects sensor drifts, signal offsets and hydraulic malfunctions before the defined safety limit is exceeded. The Category 2 architecture [8] with redundant sensors which is consistent with the functional safety objectives for earth-moving machinery as defined in ISO 19014 [7], increases failure tolerance and enables early detection of degrading behaviour. The combination of DSHplus® [1, 2] and Cube® [1, 2] allows systematic execution and evaluation of extensive test series while maintaining traceability. To place the obtained diagnostic coverage results in a broader context, Table 4.2 compares the proposed simulation-based DC evaluation with conventional datasheet-based approaches. The comparison highlights differences in scope, validation depth, and the integration of FMEA-derived failure modes [4, 10], illustrating the added value of time-resolved, system-level fault-injection-tests for assessing diagnostic effectiveness.

Table 4.2. Comparison of datasheet-based & simulation-based DC evaluation

Aspect	**Datasheet-based Evaluation**	**Simulation-based Evaluation (Fault-Injection-Test)**
Scope	Component Level	System level (including software logic)
Basis	Static manufacturer data (MTTFD, DC values)	Dynamic failure behaviour under realistic conditions
Focus	Hardware reliability	Algorithmic failure detection and reaction
Detection proof	Assumed via design parameters	Verified through time-resolved detection response
Performance Level Validation	Theoretical	Practical validation within virtual environment
Limitation	Cannot assess control algorithm or reaction time	Requires modelling and simulation effort
Added value	Quick estimation	Realistic validation of functional safety behaviour of the machine
Integration of FMEA results	Not considered - datasheet assumes ideal operation	FMEA-identified failure used for targeted fault-injection tests
Phase in V-Model	Hardware validation	System and machine validation

4.4. Cube-Based Evaluation

The simulated test cases are evaluated using the automated Cube® [1, 2] workflow environment, which coordinates simulation execution, data processing, result visualisation, and documentation in a predefined and reproducible sequence. In combination with the automated Cube® workflow for execution, parameter management, and result evaluation, the virtual twin is extended to a digital twin [1, 14] representation in accordance with the concepts described in the literature [14] and their implementation in an automated simulation and workflow [1]. Coupling the DSHplus® [1, 2] simulation model with the Cube® workflow enables automatic execution of parameter variations and failure scenarios

under consistent test conditions. The evaluation shows a substantial reduction in manual engineering effort, while the numerical simulation runtime per test case remains comparable for manual and automated execution. The observed efficiency gain is achieved by eliminating repetitive manual tasks such as parameter configuration, data storage, post-processing, and result documentation rather than by accelerating the simulation itself. Individual simulation runs require only a few seconds, allowing parameter studies with numerous failure scenarios to be completed within minutes. In contrast, equivalent real-machine tests typically require several minutes per test case due to machine setup, repeated execution, and data acquisition, which limits the number of scenarios that can be investigated. In a manual simulation workflow, the surrounding engineering activities typically dominate the total effort per test case, whereas the Cube®-based execution performs these steps deterministically without user interaction. In addition, the automated workflow improves reproducibility and result quality by applying all test parameters consistently and eliminating handling errors associated with repeated manual testing. The simulation environment further allows the investigation of critical or hazardous scenarios, such as collision conditions or complete failure of safety functions, which cannot be systematically explored in real-machine experiments. Overall, the Cube-based evaluation provides a reproducible framework for system-level assessment of diagnostic performance, enabling higher test coverage with significantly reduced engineering effort compared to conventional manual or real-machine testing. The benefit of the Cube®-based approach therefore lies not in faster simulation, but in the systematic reduction of manual effort and variability in the evaluation process.

5. SUMMARY AND CONCLUSION

This work shows that simulation-based fault-injection testing can be used to evaluate diagnostic behaviour of safety-related control functions in a time-resolved and system-level manner. The purpose of the presented approach is not the simulation itself, but the generation of early and reproducible evidence for diagnostic performance under defined failure conditions, which is difficult to obtain by conventional testing methods. The results demonstrate that diagnostic coverage is strongly influenced by the temporal characteristics of failures and by the domain in which failures occur. Slowly developing sensor degradations and hydraulically induced effects may lead to delayed detection, even if the implemented diagnostic logic is functionally correct. This highlights that diagnostic effectiveness cannot be assessed solely on a structural or datasheet level, but requires dynamic evaluation under realistic operating conditions. From a development perspective, the approach supports decision-making by shifting extensive diagnostic validation from late-stage physical testing to an earlier simulation-based phase. This enables systematic comparison of design variants, monitoring strategies, and parameter settings before hardware availability, while maintaining traceability to FMEA-derived failure assumptions. In summary, the presented methodology provides a means to validate diagnostic concepts with respect to timing, coverage, and system interaction, thereby supporting robust safety design and reducing the risk of late-stage design iterations. Although the movement limiter already provides a high level of operational safety, the results indicate that the dynamic diagnostic coverage identified by the FMEA-based digital model cannot yet fully satisfy the performance requirements. Consequently, the simulation results reveal the need for further refinement of both the movement limiter algorithms and the associated diagnostic strategy.

6. REFERENCES

[1] R. Alt, et. al., 'Seamless Integration of Device and Field Data into the System Simulation of a Hydraulic Servo-Press using AAS', 14th Int. Fluid Power Conf. (14th IFK), pp. 553-569, Dresden, March 2024.

[2] H. Baum, 'Cube – A SaaS development environment for technical system', Drivetrain and System Engineering Conf. (DSEC), Aachen, March, 2025.

[3] International Standard, 'DIN EN ISO 61508-5:2011-02. Functional safety of electrical/ electronic/ programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels;

[4] Ch. Düsing, D. Prust, 'Supplementary failure mode and effect analysis (FMEA) for safety application standards DIN EN ISO 135849 Safety Function-FMEA', 12th Int. Fluid Power Conf. (12th IFK), pp. 349-358, Dresden, Oct. 2020.

[5] Ch. Düsing, 'Integration of a Safety Function-FMEA into a Professional FMEA-Software Tool to meet the New Draft of ISO 13849', 13th Int. Fluid Power Conf. (13th IFK), pp. 297-308, Aachen, June, 2022.

[6] International Standard, 'DIN EN ISO 12100:2011-03, Safety of machinery - General principles for design – Risk assessment and risk reduction', DIN Media Verlag, Berlin, March 2011.

[7] International Standard, 'DIN EN ISO 19014-1:2025-5 Earth-moving machinery – Functional safety – Part 5: Tables of performance levels', DIN Media Verlag, Berlin, Sept.2025

[8] International Standard, 'ISO 13849-1:2023-04, Safety of machinery – Safety related parts of control systems – Part 1: General principles of design', DIN Media Verlag, Berlin, April 2023.

[9] International Standard, 'ISO 26262-4:2018-12 Road Vehicles – Product development at the system level', DIN Media Verlag, Berlin, December 2018

[10] International Standard, 'IEC 60812:2018-08, Failure modes and effects analysis (FMEA and FMECA)', DIN Media Verlag, Berlin, August 2018

[11] Ch. Düsing, M. Inderelst, 'Evaluation of the Diagnostic Coverage for safety-relevant components in automated drive systems for mobile construction machinery', 9th Symposium Construction Machinery, pp. 199-217, Dresden, Sept. 2022.

[12] Ch. Düsing, F. Will, 'Safety Function Failure Mode and Effect Analysis (S-FMEA) – A Novel Approach of FMEA for Safety Application in Mobil Working Machinery, Global Fluid Power Society (GFPS), pp. 157-182, Springer Nature, 2025. ISBN 978-3-031-84505-5

[13] IFA Report 1/2025, 'Functional safety of machine controls – Application of DIN EN ISO 13849' Online Version, Germany, May 2025.
ISBN-978-3-948657-66-6

[14] Werner Kritzinger, Digital Twin in manufacturing. A categorical literature review and classification, IFAC Papers OnLine, June, 2018, Bergamo, Italy, pp. 51-11, DOI: 10.1016/j.ifacol.2018.08.474

[15] R. Isermann, Fault-Diagnosis Systems – An Introduction from Fault Detection to Fault Tolerance, Springer Verlag, Berlin, 2006. ISBN-978-3-540-30368-8, https://doi.org/10.1007/3-540-30368-5

[16] Blanke et al., Diagnosis and Fault-Tolerant Control, Springer Verlag, Berlin, October, 2016. ISBN-978-3-662-47943-8

Biographies

Christa Düsing received a diploma in mechanical engineering from Rheinische Hochschule Köln (RH Köln). She is currently FMEA coordinator and certified FMEA moderator (DGQ) at XCMG European Research Center GmbH in Krefeld. She is responsible for conducting FMEA analyses of mobile working machines, including mobile cranes, graders, and loading cranes. In addition, she provides FMEA training for the XCMG team across the group worldwide. She has extensive experience as a development engineer focusing on the optimization and further development of hydraulic systems and components for mobile machinery. Since September 2020, she has been pursuing an external doctorate at the Technical University of Dresden.

Benjamin Erzberger received a diploma in mechanical engineering from RWTH Aachen University in 2012, and has since worked for FLUIDON GmbH. He is mostly involved in hydraulic system simulation and pressure pulsation problems. This involves stationary systems like forging presses or articulated bridges as well as mobile applications, reaching from cranes, excavators and agricultural machinery to airplanes. Apart from enjoying fixing stability issues of load control valves he has developed a special fondness of solving acoustic problems in all kinds of hydraulic systems.