

SUPPLEMENTARY FAILURE MODE AND EFFECT ANALYSIS (FMEA) FOR SAFETY APPLICATION STANDARDS DIN EN ISO 13849 SAFETY FUNCTION-FMEA

Dipl.-Ing. Christa Düsing*, Dr.-Ing. David Prust

XCMG, European Research Center GmbH, Europark Fichtenhain B4, 47807 Krefeld,

* Corresponding author: Tel.: +49 2151 7830380; E-mail address: duesing@xcmg-erc.com

ABSTRACT

In the automotive industry, the Safety Function-FMEA according to ISO 26262 and its application to functional safety relevant systems is a well-established process in the form of Automotive Safety Integrity Levels (ASILs). These represent the failure mitigation that must be applied to ensure an acceptable residual risk of malfunctioning behaviour. The DIN EN ISO 13849 (ISO 13849) already describes a process to reduce risks for machines which starts with a Hazard And Risk Analysis (HARA) as described in DIN EN ISO 12100 and concludes with the Safety Requirements Specification (SRS). The SRS is a functional and technical safety concept defining requirements and guidelines to make sure the design conforms to defined safety goals. ISO 13849 lists important faults and failures for various technologies. The defined Safety Functions (SFs) can be classified in corresponding categories that lead to the particular hardware/system structure. This applies to mechatronic systems consisting of at least one sensor, one control unit and one actuator to monitor the system and effect a response in case of failure. Compared to the methods described in ISO 13849, the Safety Function-FMEA allows systematic identification of additional failures resulting from combinations of effects, rather than only listing the main failure causes. Based on the complexity of the machines it is highly recommended to perform a Safety Function-FMEA as a complementary method to assess and improve the overall safety of machinery.

Keywords: Mobile hydraulic machine, DIN EN ISO 13849, Failure Mode and Effects Analysis, FMEA, Safety Function-FMEA

1. INTRODUCTION

The standard ISO 13849 [1] [2] provides safety requirements of machinery for the design and integration of Safety-Related Parts of Control Systems (SRP/CS), e.g. in the hydraulic boom system for a loader crane. Amongst other issues, it provides general principles of design and validation. One of the main topics is to generate safety standards for machinery.

According to ISO 13849, a separate FMEA is proposed or recommended for quantification purposes for each of these described four steps:

- Risk assessment according to DIN EN ISO 12100 [3]
- Identification of preventive measures that are converted in the form of SFs
- Determine the required Performance Level (PL_r)
- Selection of the categories

The first step in the FMEA process is the risk assessment according to DIN EN ISO 12100 (ISO 12100), followed by the identification of the Performance Level (PL) according to ISO 13849 [1] [2]. Once completed, the first step outlines the hazards involved in the design, the process of risk analysis and risk evaluation and the strategy for risk reduction.

The second step details the identification of preventive measures that are converted in the form of SFs, according to ISO 13849. The SF is defined in this standard as “function of the machine whose failure can result in an immediate increase of the risk(s)” [4]. As an example, types of SFs for a hydraulic loader crane are:

- Avoiding unexpected start-up movements
- Emergency Stop function
- Safety-related stop function – initiated by a safeguard, e.g. *Overturing Protection*

Relationship between categories and PL

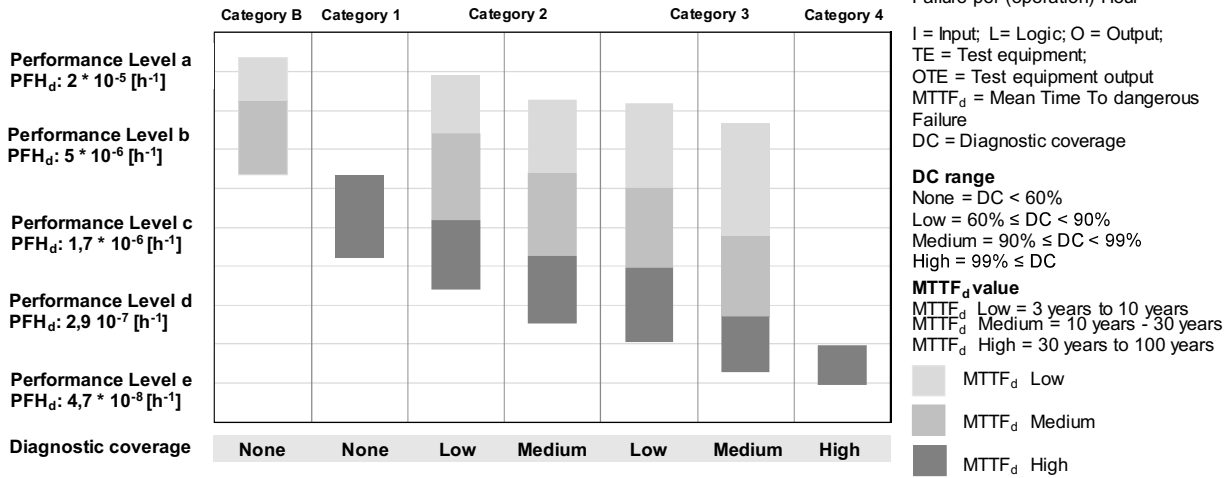


Figure 2: Relationship between categories and PL according to ISO 13849 [1] [2]

Figure 1 shows the *Overtuning Protection* as an example. To avoid the loader crane from tipping over, the overturning torque (T) must be less than the counter torque for stability realized through the stabilizers, shown in equation (1):

$$T_{\text{Overtuning}} < T_{\text{Stability}} \quad (1)$$

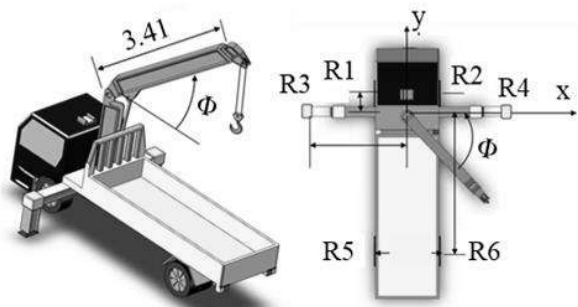


Figure 1: Detailed example for the calculation – *Overtuning Protection* [5]

The third step is to determine the PLr by selecting the level of requirements for each SF. ISO 13849 [1] provides a risk graph for the elementary determination of the appropriate PLr, which includes:

- Severity of injury (S),
- Frequency and/or exposure to hazard (F)
- Possibility of avoiding hazard or limiting harm (P)

The defined risk parameters lead directly to the PLr and represent the level of risk. The higher the PLr, the higher the fault resistance of the control system has to be designed.

Next, the categories are selected. Depending on the category selection, the influence on the design of the SRP/CS becomes apparent; for the

relationship between the categories and the PL, see **Figure 2**. Each category shows typical hardware architectures of the SRP/CS and a corresponding assignment is required for each defined SF. The quantification is using the Mean Time to Dangerous Failure ($MTTF_d$) values, the Diagnostic Coverage (DC) values, and the Probability of dangerous Failure per Hour (PFH_d) values for the PL. These are integrated into the Category table according to ISO 13849 [1] see **Figure 2**, to realize the classification of the categories. The $MTTF_d$ values give a statistical probability of the failure of a specific component, e.g. a main control valve section, thus rating the reliability of the SFs. The DC defines the effectiveness of diagnostics, being the ratio between the rate of dangerous failures or total dangerous failures. All these parameters in total define the PL. The design architecture for each SF of the SRP/CS, for each Category is shown in **Figure 3**, **Figure 4** and **Figure 5**.

The structure of the architecture for Category B and Category 1 corresponds to a single-channel system (not redundant), as shown in **Figure 3**, with input, logic – processing and output. With Category B PL b is the maximum achievable performance level, see **Figure 2**. In Category B the minimum standard shall be designed, constructed, selected, assembled, and combined in accordance to fulfil the basic safety principles for the specific application. Category 1 shall be designed and built to use well-tried components and well-tried safety principles, according to ISO 13849 [1].

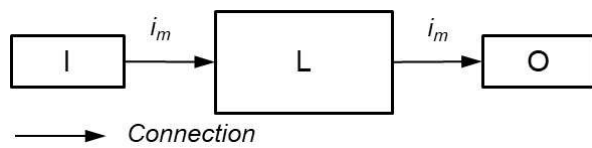


Figure 3: Designated architecture for Category B and Category 1 according to ISO 13849 [1]

Therefore, Category 1 requires that the customer can request a component which is well-tries and state of the art. Applying the standards guides manufacturers on how to confirm the achievement of well-tries components. The Category 1, supports PL b to c. In Category 2, the occurrence of a failure can result in the loss of the SFs, see **Figure 4**. As well as in Category B and Category 1, the architecture corresponds to a single-channel and continuously monitored system. The test allows detecting a dangerous failure of a component. Thereby, the choice of the frequency of the test rate decreases the occurrence of dangerous failures. With the output of the test equipment, the hardware structure includes a supplementary shutdown path.

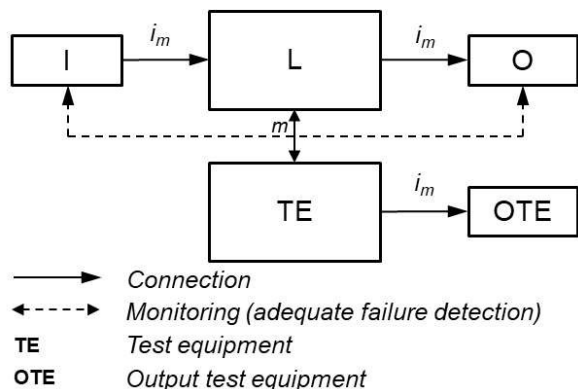


Figure 4: Designated architecture for Category 2 according to ISO 13849 [1]

As shown in **Figure 5**, the architecture for Category 3 illustrates that the performance of the SF detects some single failures with a two-channel structure (redundant), but not all failures. However, a loss of the SF can result from the accumulation of undetected failures. Category 4 additionally uses extensive monitoring to limit undetected failures and hence the accumulation thereof. Here, the SFs always come into action when switching the machine on or during the working cycles, regardless of the accumulation of failures.

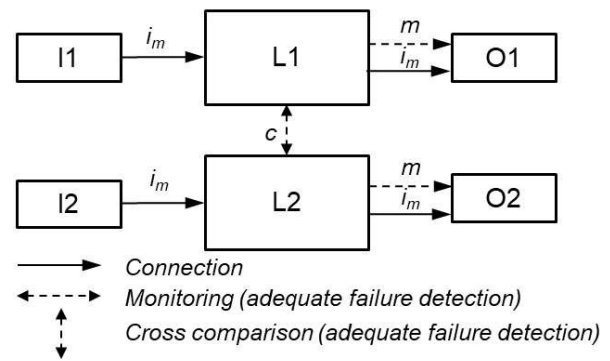


Figure 5: Designated architecture for Category 3 and Category 4 according to ISO 13849 [1]

2. FMEA GENERAL STRUCTURE

The Automotive Industry Action Group (AIAG) and the German Association of the Automotive Industry (VDA) released the latest publication on FMEA in 2019 [6]. FMEA structures have been completely revised and expanded by adding a new method, the “FMEA Supplement for Monitoring and System Responses” (FMEA - MSR) according to ISO 26262 [7]. The AIAG & VDA FMEA [6] standards are tailored to the automotive industry and thus, do not include a process of ISO 13849 [1] [2] for the required SFs in hydraulic control systems.

This circumstance serves the following fundamental question:

“How to integrate the defined SFs and the corresponding categories within the structure of the FMEA process?”

As guidance, this paper proposes several approaches how to perform an FMEA process for SFs in hydraulic control systems in practice. A function - as a non-safety-related function - usually describes the intended purpose of an object or a system element. One or more functions can be assigned to each other respectively AIAG & VDA [6]. Unlike this definition, safety-related functions of a mobile machine, e.g. for a hydraulic loader crane, are higher-level functions, supplemented as an add-on. These usually monitor the state of a functional system consisting of one to multiple inputs, one logic and several outputs. In the event of safety-relevant failures, the system will switch off or fall back to a safe state to maintain required safety levels.

3. INTEGRATION OF SFS INTO THE FMEA PROCESS FOR HYDRAULIC CONTROL SYSTEMS

When preparing a system or sub-system FMEA, it is recommended to implement a P - Diagram. The P - Diagram is a graphical representation of the system structure and shows the relationship between systems parameters, system elements and their functions in form of a block diagram. They are determined and elementarily visualized. For the standard FMEA process, the P - Diagram is built around the object under consideration of the product, system, sub-system and single component according to the scope of the analysis. It shows the input signals, the output signals, the unintended outputs, the control factors and the confounders [8]. **Figure 6** shows an example of a modified P - Diagram supplement including Failure Modes and the SFs.

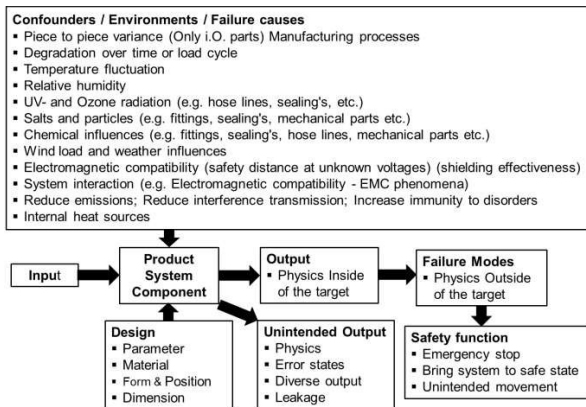


Figure 6: Proposed P – Diagram example, Quality in product development [8], with modified structure

The P - Diagram is advantageous when analysing complex systems with various system interactions, operating conditions, design parameters and complex relationships of functions. The focus in the P - Diagram may be on the input and output variables or the respective functions for the system, the sub-system or the single-components.

3.1. Theoretical models of a failure sequence chain

The analysis of each FMEA generally consists of three various failure aspects:

- Failure Effects
- Failure Modes
- Failure Causes

These three different aspects are linked together and show a failure sequence chain depending on the focus element. For connecting Failure Causes with Failure Modes, the question is: “Why does the failure occur?” [6] and for linking Failure Effects with Failure Modes, the question is: “What happens when the Failure Mode occurs?” [6]. The standard failure sequence chain according to AIAG & VDA [6], as shown in **Figure 7**, does not comprise the SFs. The following four models of failure sequence chains represent different solutions including the integration of SFs.

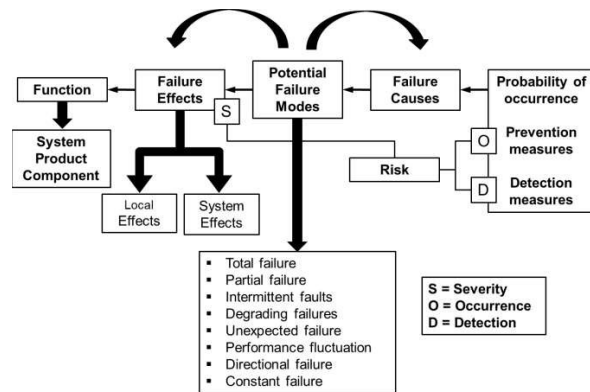


Figure 7: Standard model of a failure sequence chain according AIAG & VDA [6]

For better clarification, the following solutions show practical examples, using the sub-system first boom of a loader crane, as shown in **Figure 8** and shown as a hydraulic circuit diagram in **Figure 9**. According to the described process and the defined SFs, Category 2 PL d and Category 3 PL d are determined for the sub-system ‘first boom of a loader crane’.

In the case of the loader crane, the hydraulic pump is included in the scope of the truck hydraulics. The truck provides the required pressure supply and the corresponding flow rate via a specified hydraulic pump powered by the power take off (PTO) of the engine.

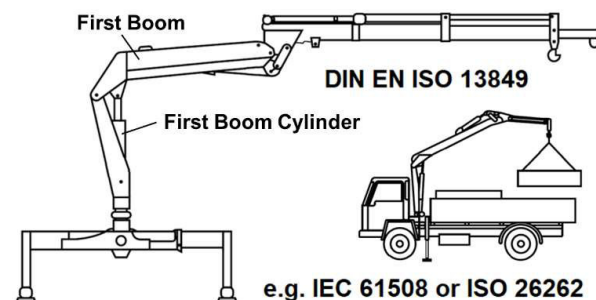


Figure 8: Loader Crane, First Boom, DIN EN 12999:2013-02+A2:2012 [9]

Thus, the hydraulics of the loader crane are directly connected to those of the truck.

The analysis of the hydraulic circuit diagram, **Figure 9**, shows all components that are essential for compliance with the SFs for the sub-system first boom.

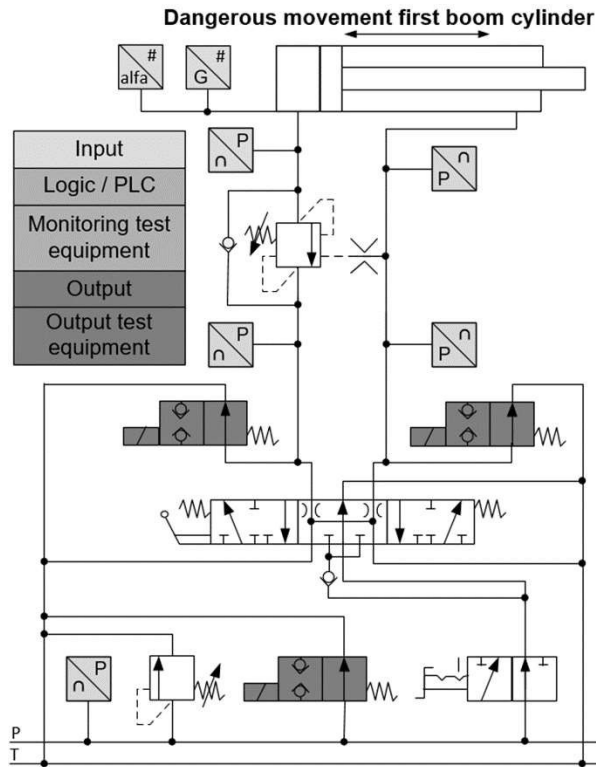


Figure 9: Hydraulic circuit diagram, First Boom, according to the IFA Report [10]

The sensors pointed out in light grey trigger the SFs. The switching valves, shown in dark grey, act as actuator of the logic and monitor values marked in mid-grey to prevent the dangerous movement of the first boom cylinder. This depends on the failure modes of the sensors and their interfaces. In compliance with basic and proven safety principles, safety valves (pressure relief valve and counterbalance valve) support the cylinder function. All electrical components are monitored by the Logic/PLC. According to the defined SFs and the corresponding Category 2 PL d the circuit implements two shutdown paths. Depending on the defined SFs, the first boom hydraulic also implements the Category 3 PL d with a two-channel structure.

First method of safety-related solution:

The first method of the safety-related solution of a failure sequence chain divides the Failure Modes into a safety-related part and non-safety related part. For all non-safety-related Failure Modes, the standard procedure of the FMEA process is applied according to AIAG & VDA [6]. If the Failure Modes are safety-related, further steps supplement the standard process see **Figure 10**. To achieve a better identification, a further column „How Failure Modes can disrupt safety goals/requirements“, supplements the failure sequence chain. Furthermore, the SFs are defined as preventive measures for the respective failures. The corresponding Categories defined in ISO 13849 [1] for the individual SF specify the detection structures for the relevant SFs, see **Chapter 1** Introduction. With the example of the respective SFs and their corresponding Category 2 PL d see **Figure 10**, the SFs will be defined as preventive measures to protect the system from damages. Additionally, the output of the test equipment is triggered by the safety detection measures; this reflects the two shutdown paths.

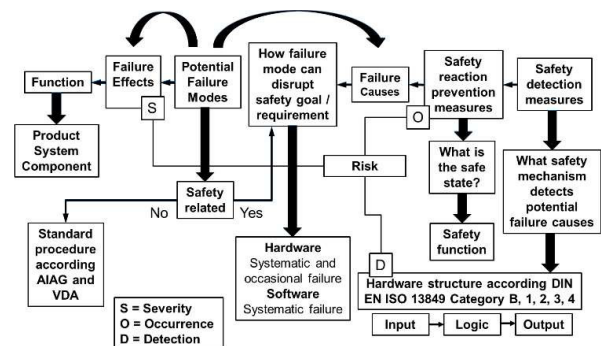


Figure 10: Proposed safety-related solution I, according ISO 26262 [7], kVA by UL [11], with modified structure to ISO 13849 [1]

The following example shows the conversion of the failure sequence chain into an FMEA structure, considering the SFs. This method of preliminary evaluation simplifies the system analysis and serves as a basis for the interface definition, and to generate the function and failure identification, see **Figure 10**.

XCMG				FMEA				Number:
System				First Boom Hydraulic of Loader Crane				Page: 1
Effect	S	C	Failure mode	How failure mode can disrupt safety goal / requirement	Cause INPUTS	Prevention action OUTPUTS	Detection action TE and OTE	RP AP
Loader Crane, First Boom Hydraulic								
System element: Main Control Block Q38 - Hydraulic supply for cylinder system								
Function: Crane Mode on (change from pressure free circulation to closed state)								
[Loader Crane] Doesn't transfer pressure supply from main pump determines the load (bar)	8	C	Crane Mode on not possible (Doesn't change from pressure free circulation to closed state)	Reasons, e.g.: - The cable is cut - Wires are cut - Loose cable connection - Wire inside cable are twisted - Short circuit to supply - Short circuit to ground - Input / output values are stucked	Initial state: 04/12/2019 [Logic / PLC] Doesn't read Sensor Signals	Safety communication: > CANopen safety BUS-System	Test equipment: Separate Processor -> Evaluation of status information, functional target ranges, time delays, and maintenance information in the context of built-in functions	4 96 L
Loss of main function								
[Loader Crane] Doesn't transfer volume power from main pump determines the flow rate (l/min.)	8	C		Reasons, e.g.: - Output value is stucked - Input value is stucked - Measured value is outside the defined range - Transferred values are corrupted	Initial state: 04/12/2019 [Position Sensor B3 Digital] Doesn't generate a Digital Signal that the 1st Boom is in Transport position	SF: Inclination monitoring -> The SF is used to block the boom movements if the inclination angle exceed the max. allowed value	Output of Test equipment: -> Monitoring the SF	4 96 L
Loss of main function								
[Loader Crane] Doesn't guide the power supply to actuate the magnetic of Main Control Valve and Cylinder Valves	8	C		Reasons, e.g.: - Output value is stucked - Input value is stucked - Measured value is outside the defined range - Transferred values are changed	Initial state: 04/12/2019 [Position Sensor B3 Digital] Generate an incorrect Digital Signal that the 1st Boom is in Transport position	SF: Inclination monitoring -> The SF is used to block the boom movements if the inclination angle exceed the max. allowed value	Output of Test equipment: -> Monitoring the SF	4 96 L
Loss of main function								

Figure 12: Proposed FMEA Form Sheet, First Boom Hydraulic, Loader Crane

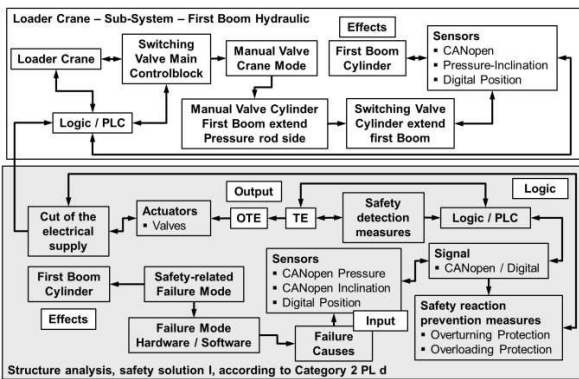


Figure 11: Proposed structure analysis, safety-related solution I

Figure 11 and Figure 12 show that the SFs are defined as safety reaction prevention measures. The task of these prevention measures is to bring the system to a safe state. The sensor signals of the respective components are monitored at start-up and/or during cyclical operation with the defined parameters for faulty signals outside the tolerance for value and time. The structure analysis also shows the two shutdown paths according to Category 2 PL d see Figure 11. Compared to the standard FMEA and their possibilities on how to integrate defined absolute characteristics into the FMEA structure, the SFs are implemented into the prevention action column of the form sheet, as shown in Figure 12. With this solution, it is not mandatory to build up the SFs with the corresponding Category 2 PL d in the function and failure networks. There is a possibility to integrate both FMEA processes (safety-related and non-safety-related) into one

structure. Accordingly, the disadvantage is that the structure gets very complex.

Second method of safety-related solution:

The second method of the safety-related solution of a failure sequence chain, see Figure 13, implements only SFs. Separately, a non-safety-related solution can be designed.

The standard model of a failure sequence chain was used as the basis. The difference to the standard model is that the Failure Causes are subdivided into three sections:

- Technical Failure Causes - Within the system
- Technical Failure Causes - Outside the system
- Failure Causes – Non-technical leads to Hazards

Additionally, there are safety-related causes triggered by the user, which influence the SFs. The implementation of the Category 2 PL d and Category 3 PL d, according to ISO 13849 [1], shall be realized in this solution through the function and failure networks.

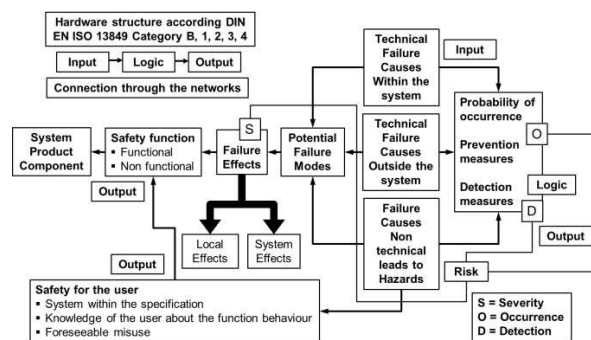


Figure 13: Safety-related solution II, Schellbach [12]

The structure analysis for the second solution into an FMEA structure, as shown in Figure 14

differs from the safety-related solution I. Depending on the level of the focus element, the failure detection, the safety for the user and the output of logic trigger the SFs. The prevention measures are designed as in the standard model in the context of development and planning.

It is recommended to include the hardware structure for the SFs and the corresponding Category 2 PL d and Category 3 PL d into the failure and function network.

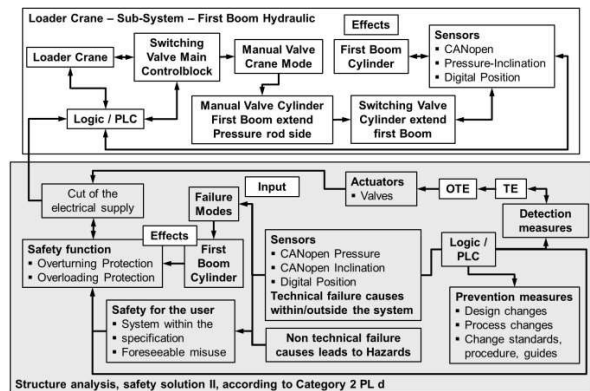


Figure 14: Proposed structure analysis, safety-related solution II

Third method of safety-related solution:

In the third method, as shown in Figure 15, the standard model of the failure sequence chain forms the basis of the procedure.

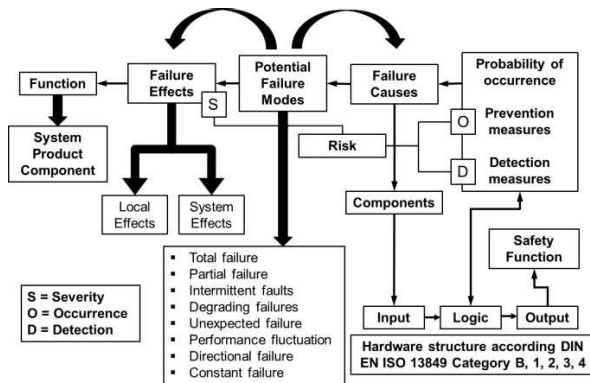


Figure 15: Proposed safety-related solution III, based on AIAG & VDA [6], with modified structure according to ISO 13849 [1] [2]

Non-safety-related functions and safety-related functions can be integrated into this solution. The sensors as safety-related failure-causing components supply the input signals for the respective functions. The failure detection is controlled through the logic, and the output triggers the corresponding SFs directly. Therefore, in this solution, the SFs are an add-on

to monitor the system elements. Depending on the SFs for Category 2 PL d and Category 3 PL “d”, only the sensors or each system element influences the SFs and their failure possibilities respectively, which are applicable for the relevant system or sub-system.

The following structure analysis, see Figure 16 illustrates an example of the defined hardware structure, Category 2 PL d for the ‘first boom hydraulic’ and corresponding SFs. The structure analysis in Figure 16 shows that the sensors trigger the SFs, the Logic/PLC controls the components, the test equipment monitors the sensors (how and how often), and the components which are responsible for the SFs.

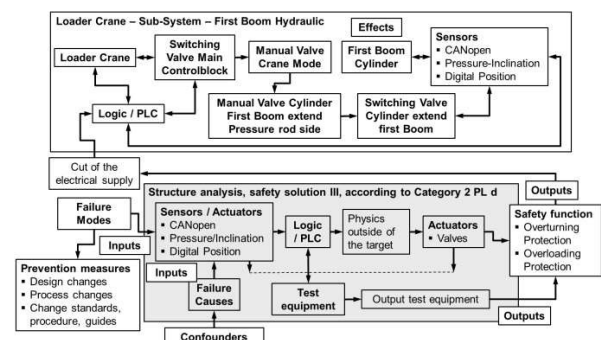


Figure 16: Proposed structure analysis, safety-related solution III

With this representation of the sub-system ‘first boom hydraulic’, the associated functions and failure networks become very clear. Figure 17 shows a simplified example of a function network with the focus on the pressure sensor of the ‘main block hydraulic supply’, which triggers the SF *Overturning Protection*. The function network builds up the hardware structure of the Category 2 PL d with the two shutdown paths. The sensor signal (e.g. outside functional target) as the causes, the Logic/PLC as the controls of components, the test equipment as a diagnostic part, the valves as actuators and as an add-on, e.g. for the SF *Overturning Protection*.

In the standard FMEA process each implemented sensor, every involved actuator and every SF in the complete loader crane system, must be connected into the function network with each other. The failure network is generated in the same way. In order to simplify the process structure, the function and failure networks can be created separately for each SF, which can then be linked together.

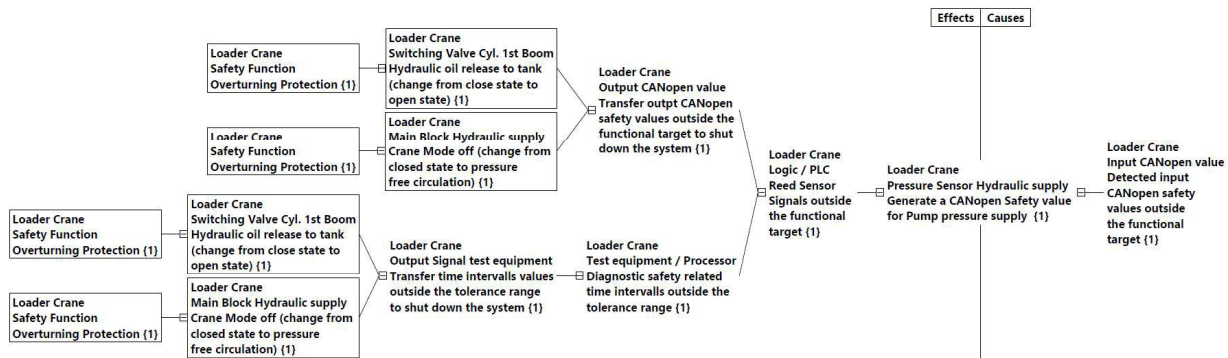


Figure 17: Proposed function network - Pressure sensor hydraulic supply - SF “Overturning Protection Category 2 PL d”

Fourth method of safety-related solution:

The fourth safety-related solution also divides the Failure Modes into non-safety related and safety-related Failure Modes. The difference to the other solutions is that all SFs and their corresponding categories are integrated into the failure sequence chain see **Figure 18**. The clear structure of the failure sequence chain thus simplifies the structure analysis and provides a good overview.

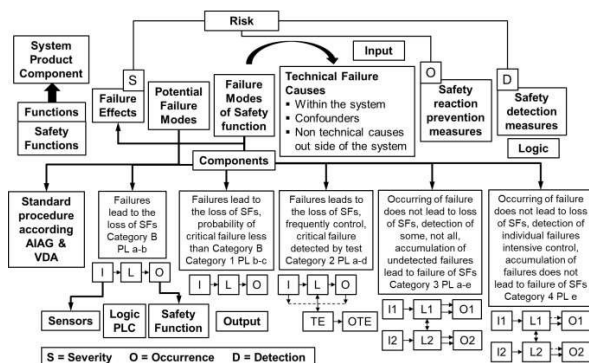


Figure 18: Proposed safety-related solution IV, according ISO 26262 [7], with modified structure to ISO 13849 [1] [2]

With this solution, the SFs are displayed directly with their associated category in the structure. The following example of a structure analysis see **Figure 19** shows the Category 3 PL d for the SF *Emergency Stop*. For this SF and depending on the focus of the failure causes, all involved components which are responsible for the subsystem ‘first boom hydraulics’ trigger the individual input. The SF as an add-on switches off the system depending on the output signals from the Logic/PLC. The structure analysis **Figure 19** illustrates the redundant functionality of the Category 3 PL d. The specified parameters and requirements for the Category 3 PL d controlled by the Logic/PLC cut off the electrical

supply if failures occur in channel 1 and channel 2 at the same time or when affecting the same function.

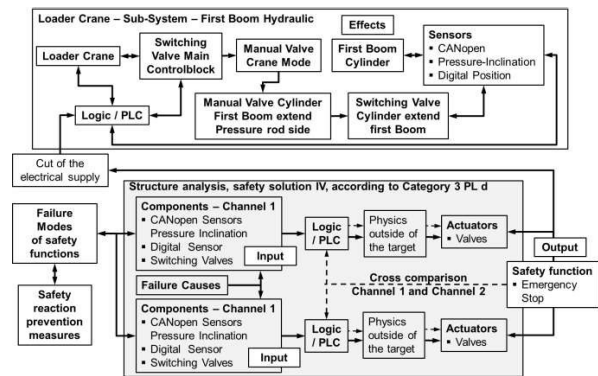


Figure 19: Proposed structure analysis, safety-related solution IV

When combined in one FMEA structure, the number of subsystems and the number of the defined SFs with different categories can easily make it very complex to build up a function and failure network including the non-safety-related functions, and the safety-related functions.

Figure 20 shows the proposed function network as a simplified example for the SF *Emergency Stop*, for the pressure sensor ‘hydraulic supply’ and the pressure sensor of the switching valve ‘cylinder bottom side’ of the sub-system ‘first boom hydraulics’ the proposed function network. Because all involved components on each sub-system influence the SF *Emergency Stop*, it is necessary to generate the function network for each component and for each sub-system, which triggers the SF.

For clear structuring, it is recommended to first create the individual function and failure networks of the responsible components for the SF *Emergency Stop* and then to combine these individual networks accordingly.

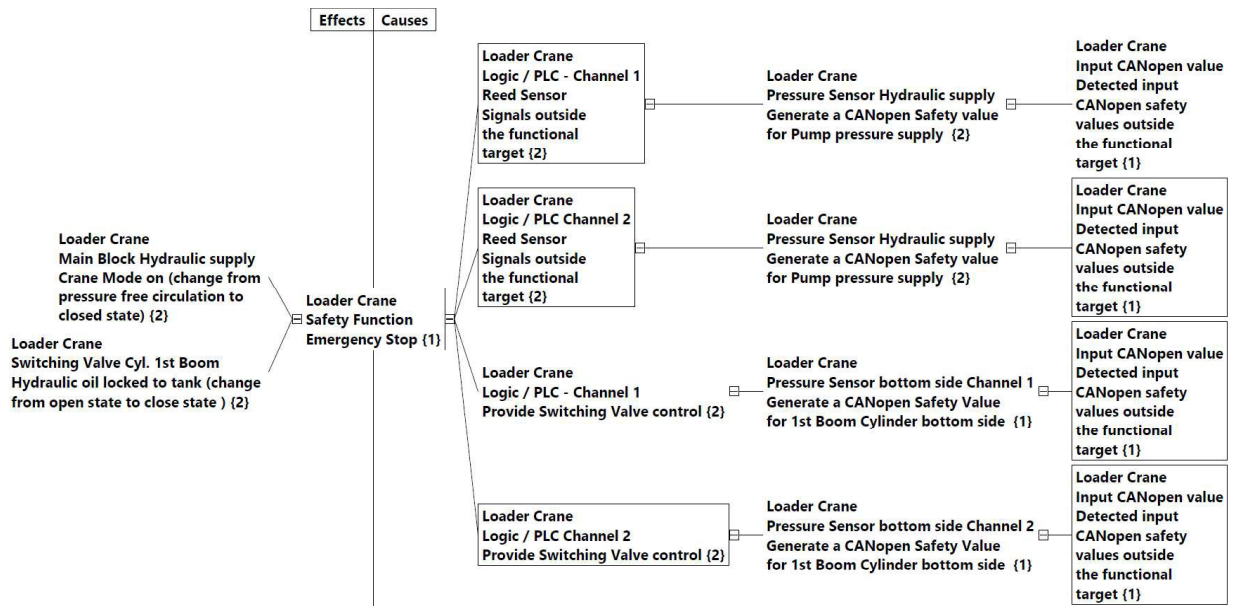


Figure 20: Proposed function network - Pressure sensor hydraulic supply - SF “Emergency Stop Category 3 PL d”

4. EVALUATION AND RESULTS

Four possible methods answer the question:

“How to integrate the defined SFs and the corresponding categories within the structure of the FMEA process?”

Figure 21 compares the four different methods, starting with a combination of a safety-related solution and a non-safety-related solution with the emphasis on the safety-related perspective, but with a complex FMEA structure when combined. The first and the fourth solution illustrate that the SFs are realized as preventive and detection measures. The second solution only looks at the safety-related parts and the SFs are realized as detection measures. Therefore, it has a clear structure in the function and failure networks. In the third and the fourth method, the SFs are supplemented as an add-on. Systematic four shows a fully integrated approach with a clear overview of the defined categories for all involved SFs, see **Figure 18**, but also includes a complex FMEA structure.

Comparison of possible safety-related solutions	First solution	Second solution	Third solution	Fourth solution
Various solutions				
Safety-related solution	x	x	x	x
Non-safety-related solution (Standard System FMEA)	x	possible	x	x
Combination of safety-related and non-safety-related solution (Standard System FMEA)	possible		possible	possible
Safety Functions				
Safety function as an add-on			x	x
Safety function as Prevention Measures	x			x
Test equipment with Outputs as Detection Measures	x	x	x	x
Category B, 1, 2, 3, 4 with corresponding hardware structure				
Integrated into the function and failure network		x	x	x
Failure Modes				
Divided the Failure Modes into safety-related and non-safety-related solution	x	x		x
Failure Causes				
Failure causes divide in different variants		x		
Structure of the function and failure networks				
Complicated structural design	x		x	x
Clear structural design		x		

Figure 21: Comparison of the methods

Figure 22 compares the advantages of the possible solutions based on the evaluation criteria. The practical implementation of the favoured third method can then be carried out as shown in for the example of the loader crane.

Evaluation criteria for the possible solutions Comparing the benefits	First solution	Second solution	Third solution	Fourth solution
Presentation of the categories into the FMEA process basically to be realized	-	+	++	++
Implementation into the structure feasible	+	+	+	+
Can be used as a starting point for functional analysis	+	+	+	+
Graphical representation of the scope of observation depended on a combination of safety-related and non-safety-related functions	+ -	+	++	- -
Adaption of evaluation criteria out of the FMEA-MSR possible	+	+	+	+
Can be used for various mobile machine systems	+	+ -	++	++

Figure 22: Evaluation criteria for possible solutions

5. CONCLUSION AND OUTLOOK

These methods not only apply to the one particular hydraulic mobile machine presented. Generally, they apply to all hydraulic mobile machines, which are a combination of a vehicle with a separate machine, such as loader cranes, fire trucks, truck-mounted concrete pumps or mobile cranes. The research using the loader crane example shows that separating the mobile machine and vehicle allows implementing the safety function and the corresponding categories into the FMEA structure.

For other mobile working machines, e.g. graders, wheel loaders or wheeled excavators where separation is not possible and where street approval must also be taken into account, the entire process must be re-examined to show whether the proposed approach can be applied as well. Therefore, the following question arises again:

“How to integrate SFs, corresponding categories and street approval with their risks within the structure of the FMEA process?”

NOMENCLATURE

<i>AIAG</i>	Automotive Industry Action Group
<i>ASILs</i>	Automotive Safety Integrity Levels
<i>DC</i>	Diagnostic Coverage
<i>DIN</i>	German institute for standardization
<i>EN</i>	European Standard
<i>F</i>	Frequency
<i>FMEA</i>	Failure Mode and Effects Analysis
<i>MSR</i>	Monitoring and System Response
<i>HARA</i>	Hazard And Risk Analysis
<i>ISO</i>	International Organisation for Standardization
<i>MTTF_d</i>	Mean Time To dangerous Failure
<i>P</i>	Possibility
<i>PFH_d</i>	Probability of dangerous Failure per Hour
<i>PL</i>	Performance Level
<i>PL_r</i>	Performance Level required
<i>PLC</i>	Programmable Logic Controller
<i>PTO</i>	Power take off
<i>S</i>	Severity
<i>SRP/CS</i>	Safety-Related Parts of Control System
<i>SRS</i>	Safety Requirements Specification
<i>T</i>	Torque
<i>VDA</i>	German Association of the Automotive Industry

REFERENCES

- [1] DIN EN ISO 13849-1, Safety of machinery – Safety related parts of control systems – Part 1: General principles of design (ISO 13849-1:2015)
- [2] DIN EN ISO 13849-2, Safety of machinery – Safety related parts of control systems – Part 2: Validation (ISO 13849-2:2012)
- [3] DIN EN ISO 12100, Safety of machinery – General principles for design – Risk assessment and risk reduction (ISO 1200:2010)
- [4] Barg J, Eisenhut-Fuchsberger F, Orth A, Ost J, Springhorn C (2012) 10 steps to performance level, Bosch Rexroth Group
- [5] Yang, Chia-Feng, (2010) Mechanics Based Design of Structures and Machines
- [6] AIAG & VDA, FMEA Handbook (2019), Failure Mode and Effect Analysis, AIAG
- [7] ISO 26262, Road vehicles – Functional Safety – (ISO 26262:2011-11-15)
- [8] von Regius B (2006) Qualität in der Produktentwicklung – Vom Kundenwunsch bis zum Fehlerfreien Produkt, Carl Hanser
- [9] DIN EN 12999, Cranes – Loader cranes; (DIN EN 12999:2013-02+A2:2012)
- [10] DGUV IFA Report (2/2017) Functional Safety of machine controls
- [11] kVA by UL, technical and management consulting group focused on functional safety and ISO 26262 standards
- [12] Schellbach A, Dörfel L (2019) Gesamtheitliche Betrachtung mittels der FMEA