Efficient Drive-Based Analysis of Fault Detection Measures in Safety-Related Pneumatic Systems

Andreas Barner[1, 2], Jan Bredau[1], Frank Schiller[2]

[1] *Festo AG & Co. KG, Esslingen-Berkheim, D-73734, Germany, {aban; jbre}@de.festo.com*

[2] *Institute of Information Technology in Mechanical Engineering*, Automation Group, Technische Universität München, Garching, D-85748, Germany, *{barner; schiller}@itm.tum.de*

ABSTRACT

The focus of this research is on safety-related open-loop controlled pneumatic systems. The top events of those fault trees (FT) would represent functional failures of the system at the highest level of the design. By monitoring the top event of FT by means of signal-based diagnostic methods, each possible failure within the system becomes potentially detectable. This property is deployed explicitly in the proposed approach regarding pneumatic systems. Thus, the system under control is encapsulated, and comprehensive fault detection up to a Diagnostic Coverage of greater than 99% is achievable with tremendously less effort compared to conventional solutions. In this way, a layered system model including a safety-layer similar to current safety-related solutions to fail-safe communication and data processing has been established.

1 INTRODUCTION

Industrial applications of pneumatic systems for automation can be found in variety of industrial sectors such as material handling, automotive, food and packaging. Upcoming safety regulations and new standards for functional safety led onto a growing demand to achieve safety goals with pneumatic systems. As well as other technologies, safety-related pneumatic systems are subject to a certain probability of failure. Therefore, proper probability risk assessment of these systems is necessary to fulfil national and international standards. The most important standard to evaluate safety-related pneumatics is ISO 13849. With this and other standards (IEC, 1998; GOBLE, W. M. and Cheddie, H., 2005), component failure rates are classified into failure mode categories safe and dangerous (ISO, 2006).

Whereas the safe failures, whether detectable or undetectable, have no influence on safety, the dangerous failures may lead to hazardous states or loss of operability of the system. Dangerous failures are furthermore divided into detectable and undetectable failures. Typical distribution of failure rates in safety-related pneumatic systems is shown in Figure 1.

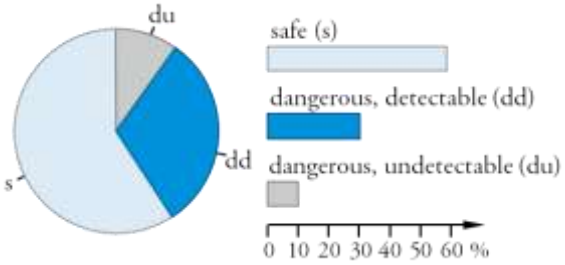

Figure 1: Typical distribution of failure rates (adapted from GOBLE, W. M. and Cheddie, H., 2005)

The parameter Diagnostic Coverage (DC) represents the ratio between failure mode categories, as in Eq. (**1**).

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{d}} \quad (1)$$

2 PROBLEM STATEMENT

To determine the parameter DC, the related standards propose several methods for system analysis. Failure Mode and Effect Analysis (FMEA) is the most common method to indentify the hazardous initiating events. However, the standards claim to evaluate a safety-related system but they refer to individual components. This component-state view is extraordinary apparent from ISO 13849-2 (ISO, 2003) fault-lists and exclusions. Since the initiating events are only identified and not systematically analysed by means of fault tree analysis (FTA) the failure rate distribution and the DC is incorrect or at best afflicted

with uncertainty (VESELY, W. et al., 2002). For example, a directional control valve is listed with 7 considerable failures (ISO, 2003). But the failure rate is only available for the whole component and there is no creditable scientific way to divide the failure rate between these 7 failures without making assumptions. Furthermore, reliability data is determined from laboratory testing and reliability modelling in accordance with (ISO, 2007). Hence test criteria are focused on functional failure, i.e. failure to switch and leakage between ports. In most cases, this is not the arrangement of directional control valves in safety-related pneumatics. Therefore, failure rates are not accurate for safety assessment (SCHAEFER, M. and Bork, T., 2007).

Some other remarks about these lists are necessary:

Some entries are repeatedly listed and make no sense from a standpoint of physical failure detection. For example, there is no difference in »Leakage« and »Change in the leakage flow rate over a long period of use« looking at a 3/2 directional control valve as shown in Figure 2.

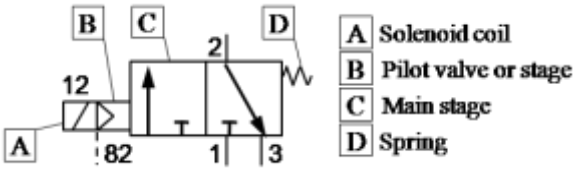

Figure 2: 3/2 directional control valve, pilot operated

Some entries are the cause for other entries i.e. »Leakage« within a pilot valve trigger the event »Change of switching times« for the main stage as Figure 3 reveals.

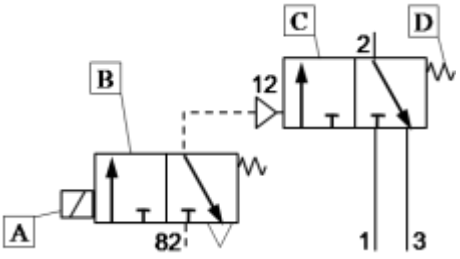

Figure 3: Schematic, disassembled view

Final actuators, i.e. a double-acting cylinder as shown in Figure 4, are not listed and considered in the standards at all. But this is necessary for some safety functions in fluidic systems. For example: if the protection goal for the safety-related control is to stop the cylinder movement on demand, an internal flow from one cylinder chamber to the other would be fatal.

Last but not least there is the question: is it really necessary for comprehensive failure detection (DC ≥ 99 %) to know every initiating event about every listed fault?

Conversely, the FTA provides another solution. FTA is a deductive (top-down) analytical tool used to study a specific undesired event, which was first introduced in 1961 in (WATSON, H. A., 1961). It starts with the undesired event and traces backward the necessary and sufficient causes. It ends with several initiating events or failures that are identified as primary causes. FTA is thus a suitable analysis method to apply if an undesired event is given and the aim is to find out what component or system behaviour contributes this final event.

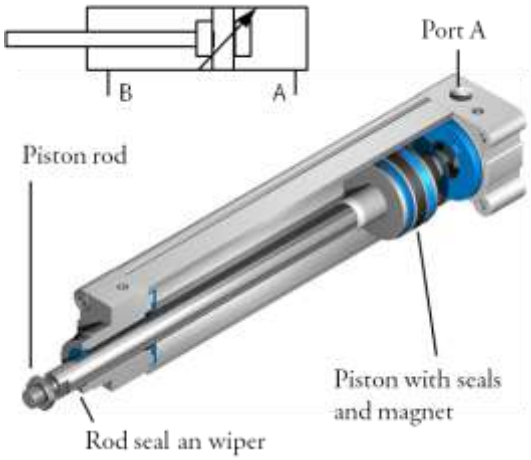

Figure 4: Cut-away view of a cylinder and symbol

Hence the FTA can be used as a proactive tool to discover the presence of an initiating cause through representing effects. Recent scientific work (BARNER, A. et al., 2009) discussed this idea in order to understand the consequences for failure detection and evaluate the amount of DC in safety-related pneumatics.

3 EXAMPLE 1 –A TYPICAL PNEUMATIC SYSTEM

3.1 Functional description

A typical pneumatic system in industrial applications is illustrated in Figure 5. Under normal or automatic operating conditions, the pneumatic circuit provides a linear movement (extension/retraction) of the piston rod. The pneumatic circuit also permits Safe Stopping and Blocking (SSB) of extension or retraction moves of the piston rod as a safety function. The functional dependencies are easily identified. The movement of cylinder 1A1 will stop when the 5/3 directional control

valve 1V1 switches to its closed centre position. Hence fluid flow from and to the cylinder chambers A and B is blocked. The one-way flow control valves 1V2 and 1V3 are used to adjust velocity while operating under regular conditions.

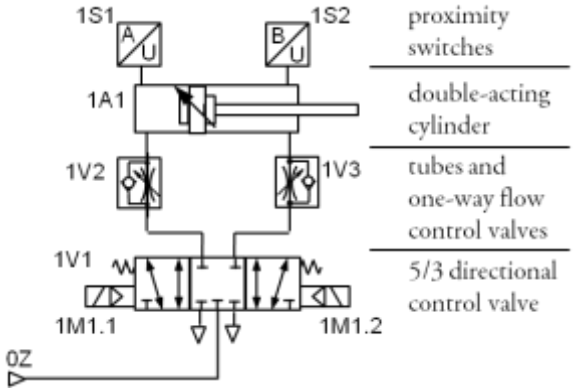

Figure 5: Typical pneumatic System

A worn component can cause faults in this system. If the valve fails to switch to its closed centre position for blocking the flow on demand, the cylinder movement will not stop. Also leakage between the cylinder chambers or a cylinder chamber and atmosphere is followed by loss of operability. That includes leakage from the one-way flow control valves and tubes. The paragraphs that follow conduct an analysis of the used pneumatics components and the complete circuit or system. Thus the background of the initial remarks will be further explained.

3.2 Analysis for Safe Stopping and Blocking (SSB)

In order to calculate a DC for SSB, understanding of behaviour of the safety-related components for all faults is necessary. The attempt to form a cause-effect-chain or FT for the safety-related directional valve including all faults from generic lists in ISO 13849-2 leads to the outcome in Figure 6. It is very easy to notice that certain generic fault is the cause for others. In addition, some generic faults are named repeatedly. Hence FMEAs cannot be combined to form a FT.

The analyst should strongly conduct the proper way of construction for FTs (IEC, 2006; VESELY, W. et al., 2002). Thus an undesired event should be first identified for the pneumatic system and second for components. The undesired event for pneumatic system derives from the protection goal stopping and blocking of piston rod movements, that is the piston rod velocity $\dot{x} = 0$.

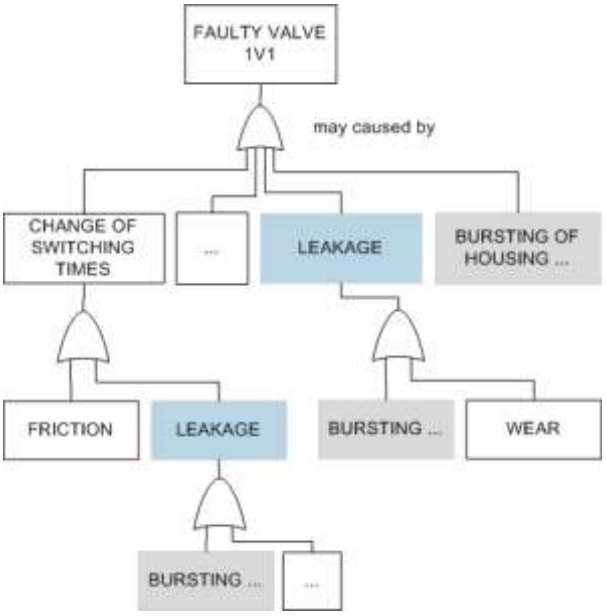

Figure 6: structured view of possible faults of a directional control valve

The velocity $\dot{x}$ of a double-acting cylinder depends upon flows to and from the cylinder chambers A and B. They are connected by Eq. (2) (MURRENHOFF, H., 2006).

$$\dot{x} = \frac{Q_A}{A_A} = \frac{Q_B}{A_A - A_R} \tag{2}$$

Considering flows caused by failure, i.e. external and internal leakages and piston movement as shown in Figure 7 the velocity $\dot{x}$ is applied in eq. (3) and (4).

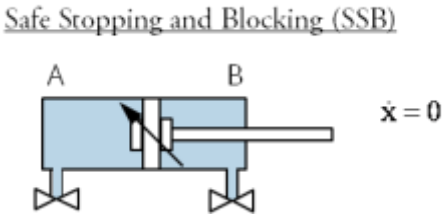

Figure 7: Double-acting cylinder in SSB

For steady state cylinder chamber A applies to Eq. (3) and Eq. (4). Whereas all flow rates Q are nominal flow rates. There many variations to calculate nominal flow rates, i.e. in accordance with physical reference conditions (DIN, 1990) or technical reference conditions (ISO, 2009). The same formula applies analogously for steady state in cylinder chamber B.

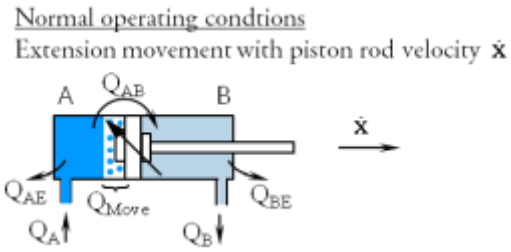

Figure 8: Flow in double-acting cylinder

$$\sum Q = Q_A - Q_{AE} - Q_{AB} - Q_{MOVE} \quad (3)$$

$$Q_{MOVE} = A_A \dot{x} \frac{\rho_A}{\rho_N} \quad (4)$$

It is obvious that SSB fails when the piston rod velocity $\dot{x} = 0$ or any flows occur. Thus the top event that occurs at the pneumatic drive and its cause (sub-top event) are identified (Figure 9).

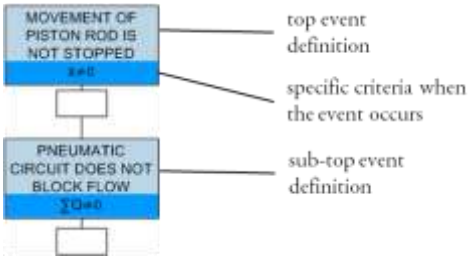

Figure 9: drive-based top and pneumatic sub-top event for FTA

From the given undesired event, trace backwards the logical and functional dependencies step by step. This is called immediate cause concept. This ensures the totality of FTA (VESELY, W. et al., 2002). The resulting FT for the pneumatic system in Example 1 is shown in Figure 10. Evidently, all initiating or other causes will lead to occurrence of the top event. A directional control valve fault is one example for a cause. If valve 1V1 fails to switch to its closed centre position there is no flow interruption to or from cylinder 1A1 (transfer gate T002). Hence piston rod velocity is not $\dot{x} = 0$.

The adjustable one-way flow control valves 1V2, 1V3 and the tubes to and from the double-acting cylinder 1A1 can cause two types of failures.

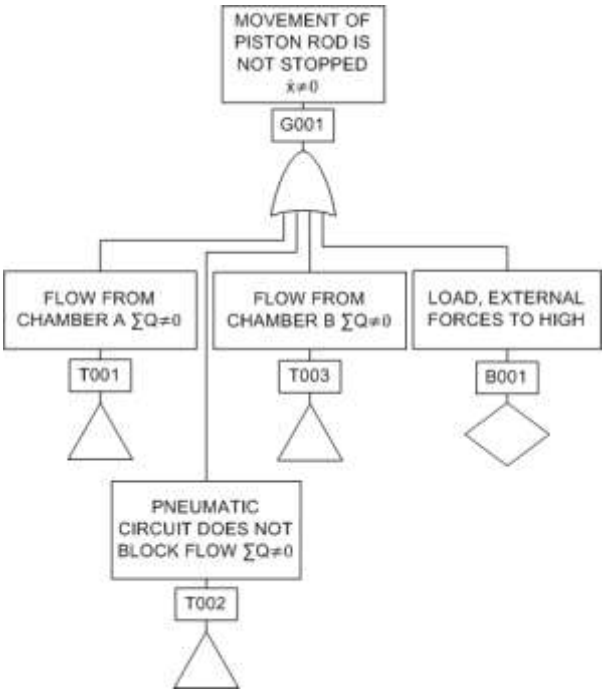

Figure 10: FT for the pneumatic system

Flow restriction can happen in case of a manipulated flow valve or narrowed line conduit. If the safety function had to stop the cylinder this failure would be irrelevant. The other cause is leakage in blocked direction. The latter endangers the protection goal of stopping and blocking the movement. Consideration of this dangerous component fault is already achieved by considering flow rates Q_A or Q_B in Eq. (2). Hereby tubes and one-way control valves are considered as additional volume to cylinder chamber A (transfer gate T001) or B (transfer gate T003). Another cause might be a high load which is not further discussed (gate B001). On this depth the FT is consistent with reliability data (failure rates) determined from laboratory testing and reliability. Further developed or depth of FT for probabilistic quantification is not sensible. But provide interesting insight for the goal of DC determination and efficient fault detection measures. Based on the event of gate T002, the pneumatic circuit is further analysed. Since faults of tubes and one-way flow control valves are considered in events T001 and T003, FTA is applied on the directional control valve. Utilising the deductive methodology, the result is shown in Figure 11.

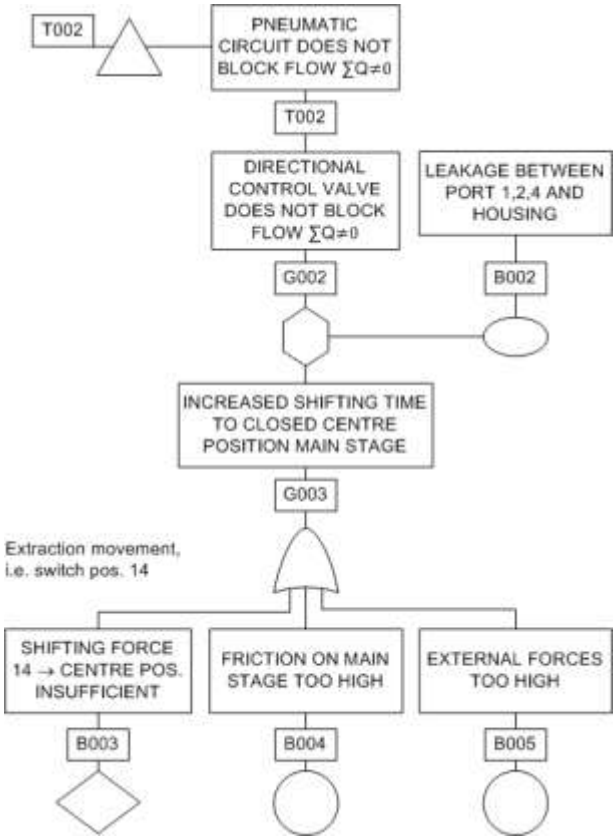

Figure 11: FT for 5/3 directional control valve

The FT in Figure 10 and Figure 11 describes the relationship among input conditions that triggers a undesirable effect on system and component level. Therefore the top event and its assigned specific criteria represent all conditions or failures inside a pneumatic system or components. Hence measuring aberration from the top events specific criteria provides a good starting point for comprehensive fault detection.

The considerable advantages of this drive-based approach are:

→ Minimal depth of FT to identify functional dependencies. It ends on component level: Therefore the depth is consistent with the available failure rates. The highly uncertain weighing of failures rates for each failure is dispensable. The calculation results from mathematical reliability and safety models way more accurate.

→ Entirety of result. No fault event is overlooked.

→ Justification of DC is based on deterministic cause-effect-chains.

→ It is sufficient to measure the single value of the top-event to cover all possible failures, whether they are dangerous or not.

→ Analysing DC and achieving DC ≥ 99% is less complicated.

4 EXAMPLE 2 – A COMPLEX PNEUMATIC SYSTEM

4.1 Functional description

In some cases pneumatic circuit are more complex. Reasons are manifold. Examples are high requirements for safety or availability which lead to functional redundancies. Figure 12 shows an adaptation that is based on example 1. The redundant channel is added to provide fault tolerant control for SSB. Channel 1 consists of the already introduced 5/3 directional control valve 1V1 and two adjustable one-way flow control valves (1V2 and 1V3). The latter are not directly safety-related but should also be considered for failures such as outlined in chapter 3.2. Channel 2 consists of the 3/2 directional control valve 1V4 that operates pilot operated non-return valves (1V5 and 1V6). Both channels are terminated by a double-acting cylinder. To stop the cylinder movement one of both channels have to block the flow to and from the cylinder chambers successfully. The undesired top event for FTA is a cylinder velocity x not equal zero. Drive-based definition of the sub-top event gives flow rate Q at A- and B-Side not equal zero as unwanted events.

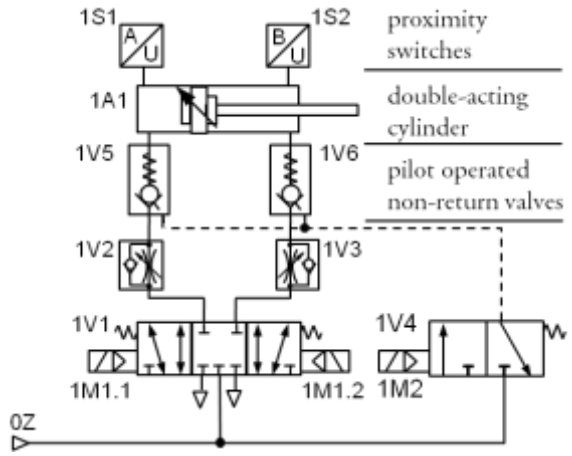

Figure 12: A complex pneumatic system

4.2 Analysis for Safe Stopping and blocking (SSB)

The drive-based approach to analyse the functional dependencies in this safety-related pneumatic systems leads to the same FT on top and sub-top event levels as for example 1! Derivations in further depth are the result of different circuit synthesis, i.e. the functional redundancy. Which is extraordinary evident in the AND gate.

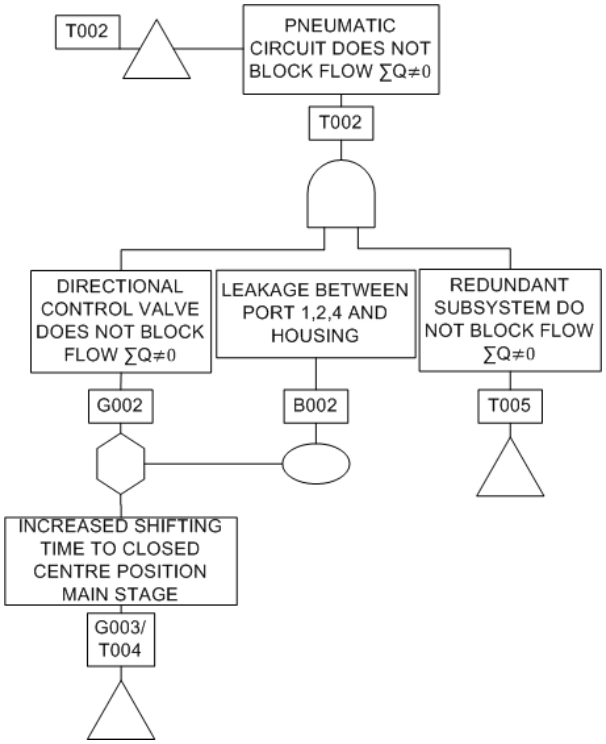

Figure 13: FT considering redundant structure

Obviously the conclusions as before are possible. The FTs top-event represents all its initiating events. All events and conditions in the FT would cause an aberration from specific criteria of top event, i.e. a change of velocity $\dot{x}$. Hence the top-event is a representative symptom of all failures.

5 GENERALISATION FOR THE SOLUTION: ENCAPSULATION

From these research results the analyst is able to encapsulate the safety-related pneumatic system as shown in Figure 14. Faults within the encapsulated system manifest themselves through symptoms, i.e. top and sub-top events.

By monitoring (measuring and checking) the limits of specified criteria the occurrence of any fault is detectable. Since most pneumatic systems in industrial automation come with electrically operated valves and proximity switches it is very easy to implement such monitoring or limit checking algorithms with signal based diagnosis methods. In case of SSB the pneumatic drive velocity $\dot{x}$ is the specified criteria when the undesired safety-related event occurs. It should be mentioned that leakage flow Q within the pneumatic circuit is evident in velocity $\dot{x}$ only above a certain value. This does not contradict conclusions made in this paper and is not discussed here in further depth.

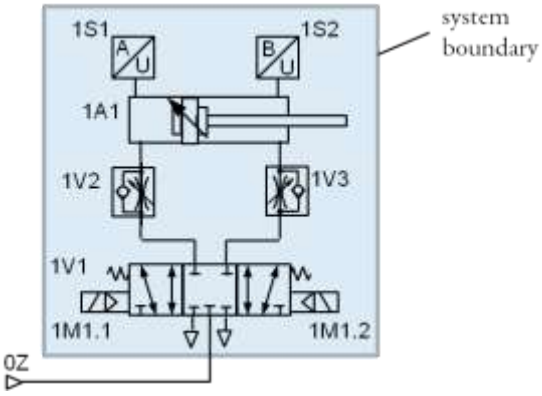

Figure 14: Encapsulated safety-related pneumatic system

This approach helps to detect that something within system boundaries is wrong. To locate or isolate a fault limit checking only is not sufficient. Plausibility checks and in some cases model based diagnostic approaches are necessary (GUTIÉRREZ GONZÁLEZ, R. et al., 2010). A structured overview for fault detection and diagnosis (FDD) in pneumatic systems gives (BREDAU, J. et al., 2008).

In conjunction with the encapsulation and methods for FDD in pneumatics it is possible to assign layers to the FT shown in Figure 15.Safety Layer (SL), Allocation Layer (AL) and Diagnosis Layer (DL) are in analogy with diagnostic concepts (GUTIÉRREZ GONZÁLEZ, R. et al., 2010; KELLER, R. and Bredau, J., 2008) and correspond to FT levels described in (DIN, 1990).

→ SL is equivalent to the top-event. Measuring the value of the assigned safety-related parameter ensures safety needs. Only signal-based diagnostic methods are necessary to implement that task. Discovery of faults (detection) is intended.

→ AL is equivalent to FT level 1 or the top-event in case of a component. Assessment of defective subsystems or components (localization) is intended.

→ DL deals with detailed diagnosis of initiating or other causes.

The latter levels needs signal processing by means of model-based diagnostics.

As mentioned before, for safety-related fault detection, only SL is necessary. Lower layers AL and DL are more a subject in a matter of availability and maintainability. Safety solutions in communications and software execution that are based on a similar layer-oriented view are well established (STRIPF, W. and Barthel, H., 2005; HUMMEL, M. et al., 2006).

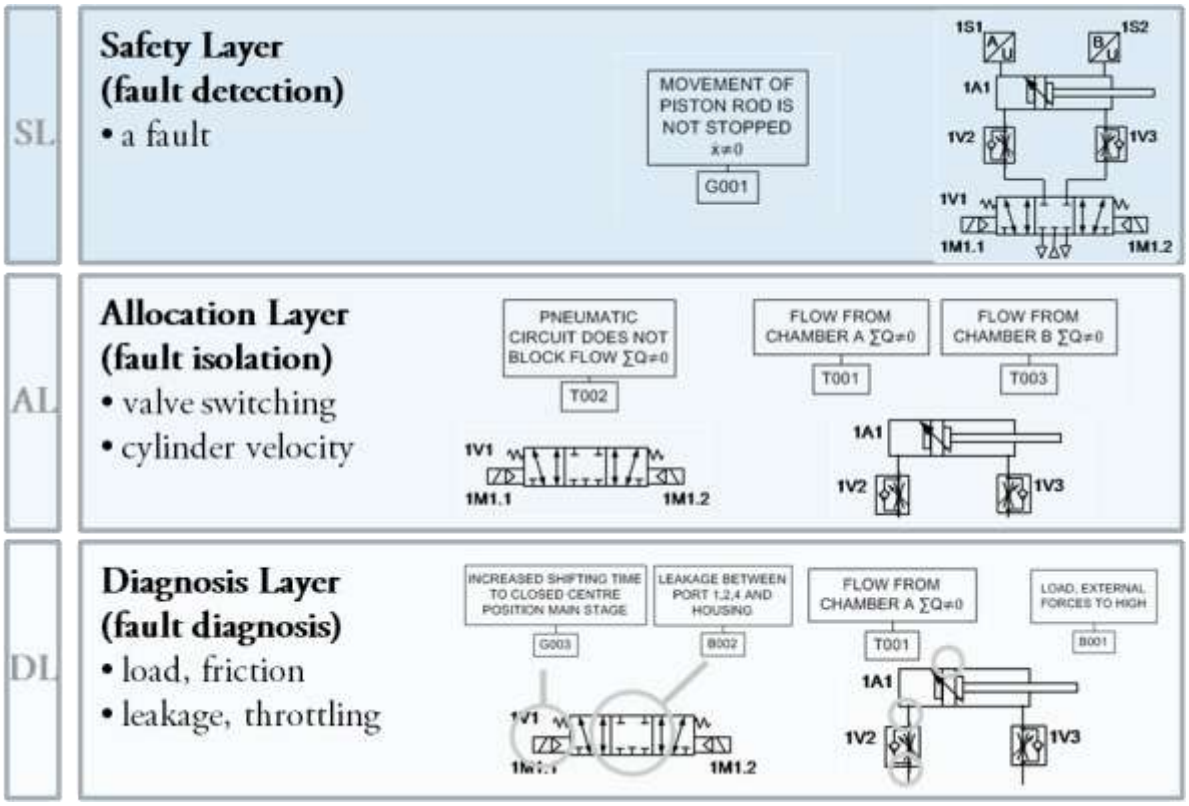

Figure 15: Safety and Fault Detection Layers

6 CONCLUSION

Developing the cause-effect-chains by FTA simplifies the insight in functional dependencies of safety-related pneumatic circuits. Any initiating event and other causes are represented by the top event. The proposed layered view will allow the encapsulation of the system. The FTs depth is consistent with the available failure rates. The highly uncertain weighting of failures rates for each failure is dispensable. The calculation results from mathematical reliability and safety models are way more accurate. Monitoring the top event by means of signal-based diagnostics covers every possible failure within the system. Comprehensive fault detection or achieving a DC ≥ 99% is less complicated. The abstraction and layered view will assist to reduce the problem of state explosion while calculating complex systems with Markov-chains. Because failures and events on low levels are depicted by high system levels. In summary the concept of conceptual encapsulation is an efficient way of fault detection in safety-related pneumatic circuits. The idea enables the automation industry to develop and validate machinery applications with powerful fault detection in safety and reliability with a minimised number of sensors. Hence expensive overhead on electronic sensor and safety equipment in safety-related pneumatics is dispensable.

7 FUTURE WORK

Following our current approach, we need to define drive-based SF. Motion actuating devices, i.e. pneumatic cylinders, induce hazards that are caused by dangerous movements or forces. Therefore SFs have to control velocity, direction of movements and forces to reduce risks. We will propose a generalised drive-based approach to define 8 SFs in open-loop controlled pneumatic systems.

Another property that is explored is the reduction and the refinement of system designs. Classical synthesis of safety-related pneumatic circuits depends on a specific application. Thus the variation of safety functions and solutions is manifold. In many cases adaption to a new process is not possible without replacing any hardware. We will work on a standardised, modularised system designs in pneumatics.

The goal is to contribute an alternative, traceable methodology in the area of safety monitoring and its assessment in pneumatics.

NOMENCLATURE

A_A	piston area side A
A_R	piston rod area
Q_A	flow rate into cylinder chamber A
Q_B	flow rate into cylinder chamber B
Q_{AB}	internal leakage flow rate from cylinder chamber A to B
Q_{AE}	external leakage flow rate from cylinder chamber A to environment
Q_{BE}	external leakage flow rate from cylinder chamber B to environment
$\dot{x}$	velocity

REFERENCES

BARNER, A., J. BREDAU, and F. SCHILLER. 2009. Efficient Fault Detection in Safety-Related Pneumatic Control by Conceptual Encapsulation. In: IFAC, (ed). 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, 2009. Barcelona.

BREDAU, J., W. GAUCHEL, and A. RIEK. 2008. Möglichkeiten von Diagnose für pneumatische Antriebstechnik. *In*: *Automation 2008, 2008*. Baden-Baden: VDI, pp.93-96.

DIN. 1990. *DIN 1343: Reference conditions, normal conditions, normal volume; concepts and values*. Berlin: Beuth.

DIN. 1990. *DIN 25424-2: Fault tree analysis; manual calculation procedures for the evaluation of a fault tree*. Berlin: Beuth.

GOBLE, W. M. and H. CHEDDIE. 2005. *Safety Instrumented Systems Verification: Practical Probalistic Calculations*. Research Triangle Park, NC: ISA.

GUTIÉRREZ GONZÁLEZ, R., J. BREDAU, and H. MURRENHOFF. 2010. Fault Diagnosis of a Pneumatic Subsystem. *In*: H. MURRENHOFF, (ed). *7th International Fluid Power Conference (IFK), 2010*. Aachen: Apprimus, pp.537-548.

HUMMEL, M., J. MOTTOK, and R. EGEN et al. 2006. Generische Safety-Architektur für Kfz-Software. *Hanser Automotive*, 11, pp.52-54.

IEC. 2006. *IEC 61025: Fault tree analysis (FTA)*. Geneva: IEC.

IEC. 1998. *IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*. Geneva: IEC.

ISO. 2009. *ISO 1217: Displacement compressors - Acceptance tests*. Geneva: ISO.

ISO. 2006. *ISO 13849-1:2006-11: Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*. Geneva.

ISO. 2003. *ISO 13849-2: Safety of machinery - Safety-related parts of control systems - Part 2: Validation*. Berlin: Beuth.

ISO. 2007. *ISO 19973-1: Pneumatic fluid power - Assessment of component reliability by testing - General procedures*. Geneva: ISO.

KELLER, R. and J. BREDAU. 2008. *Diagnostic Device for At Least One Pneumatic Value Actuator Arrangement*. US02008/0065355 A1.

MURRENHOFF, H. 2006. *Fundamentals of Fluid Power Technology*. Aachen: Shaker.

SCHAEFER, M. and T. BORK. 2007. Tangible and transparent use of reliability data for functional safety "The sense and nonsenes of quantification". *In*: T. N. E. C. E. I. A. (NECA), (ed). *5th International Conference "Safety of Industrial Automated Systems", 2007*. Tokio:, pp.370-375.

STRIPF, W. and H. BARTHEL. 2005. PROFIsafe - Safety Technology with PROFIBUS. *In*: R. ZURAWSKI, (ed). *The Industrial Information Technology Handbook, 2005*. Boca Raton: CRC Press, pp.1-20.

VESELY, W., J. DUGAN, and J. FRAGOLA et al. 2002. *Fault Tree Handbook with Aerospace Applications*. Washington, DC: NASA.

WATSON, H. A. 1961. Launch Control Safety Study. Murray Hill:, pp.Section VII, Volume 1.

Andreas Barner is research scientist at Future Technologies of Corporate Research Department at Festo AG & Co. KG, Esslingen. In addition he is a doctoral candidate at Technische Universität München. His research focuses on developing efficient methodologies to analyse and implement fault detection and diagnosis for safety-related open-loop controlled pneumatic systems. He served as an army officer and holds a 4-year degree in Mechatronics Engineering.

Jan Bredau graduated in Mechanical Engineering. He received a doctorate from Technische Universität Dresden for his dissertation in Fluid Dynamics. He has carried out applied research in the area of condition monitoring and diagnosis at Future Technologies of Corporate Research Department at Festo AG & Co. KG, Esslingen. Currently he is Product Manager.

Frank Schiller holds a degree of Diplom-Ingenieur of Technische Universität Dresden and later earned his doctorate with a dissertation in Qualitative Process Diagnosis. He worked for Siemens AG in Nuremberg and Berkeley, CA and has carried out applied research in the area of safety and diagnosis. Since 2004 he has been Professor at Technische Universität München.