15th IMEKO TC10 Workshop on Technical Diagnostics
Technical Diagnostics in Cyber-Physical Era
Budapest, Hungary, June 6-7, 2017

Logic Solver Diagnostics in Safety Applications

M. Catelani, L. Ciani, M. Venzi

Department of Information Engineering, University of Florence, via S.Marta 3, Florence (Italy)

***Abstract* – The Functional Safety is the part of overall safety of a system, called Safety Instrumented System that depends on the system operating correctly in response to its inputs. The paper focuses on safety loop assessment using the standard IEC 61508 and presents a case study concerning the evaluation of the Probability of Failure on demand (PFD) for a complex Safety Instrumented System including redundancy in modern application.**

***Keywords* –** *Safety Instrumented Systems, IEC61508, Safety Loop, Safety Assessment, Redundancy*

I. INTRODUCTION

Diagnostics plays a fundamental role in industrial engineering and nowadays is an essential part of performance requirements. Fault diagnosis and condition monitoring are almost mandatory in particular for Oil&Gas applications where products are forced to endure extreme process and environmental conditions.
With the introduction of fault diagnosis design engineers are allowed to improve standard scheduled maintenance methods based on planned actions and severe timetables: thanks to diagnostics both corrective and predictive maintenance procedures can be put onto practice [1-4].
Condition monitoring (CM) is the process of monitoring one or more condition parameters in machinery to identify some changes that are indicative of an incipient fault or equipment health degradation. Condition monitoring systems select and survey parameters from the sensors placed in the system in order to detect a change in the health machine condition [5].

II. LOCAL DIAGNOSTICS

Many devices used in manufacturing applications e.g. Oil&Gas are a two wire 4-20mA sensor assembly made of one or more sensing device (i.e. thermocouples or RTDs in temperature instruments) and one dedicated transmitter to communicate with system control panel. The outcome of a field sensor can vary in response of changes in the monitored physical quantity or in case of failure.
Diagnostics clearly play an essential role to distinguish between these two conditions.
If the sensor is provided with a dedicated on-board circuit, the device itself communicates its health status to the control logic using out-of-range outputs or dedicated communication channels. There are two main communication protocols:

- Highway Addressable Remote Transducer (HART®)
- Foundation™ Fieldbus (FF).

HART and FF both bring significant benefits to process industry using intelligent field devices with the difference that HART is a hybrid protocol fully compatible with 4-20mA wiring while FOUNDATION fieldbus is a distributed control system based on a multi-drop bus. The focus of HART protocol is to bring digital information maintaining compatibility with 4-20 mA signal; on the other hand, the focus of Foundation fieldbus is to bring the control architecture to the bus and bring down the control to device level [6].
The benefits of HART protocol are listed below [7]:

- It is compatible with the installed base of instrumentation in use in the pre-existing system so it doesn't require any change in the wiring.
- It improves plant performance and provides savings in commissioning and installation (in particular for wiring).
- It provides access to all information in multi-variable devices which can be used for verification and control of the whole plant.
- It guarantees to minimize the time required to identify failures and take corrective action.

FOUNDATION Fieldbus is a digital, bi-directional and multi-drop Local Area Network (LAN) for process control sensors, actuators, and control devices; its benefits are following shown [8]:

- The control unit computer is assessed at device level.
- Customers can choose interchangeably standard.
- The Fieldbus Foundation standardized the way the user can bring new devices into the network, set and configure them.
- The building block in this system is the Device Description (DD) which tells everything about the device and its functionality
- 4-20 mA systems require one pair of wires per device while FF requires only a single set of wires to connect multiple devices.

The major difference between these two protocols is that FF is used for real-time closed loop control. FF is completely digital end-to-end, from sensor to actuator and it has several benefits over loops using hardwired 4-20 mA and on/off signals.
Other pros of FF comparing with HART are the following:

- Balanced (non-grounded) signal with high amplitude for noise immunity;
- Multiple devices on the same pair of wires reducing cable;
- Easy addition of devices and signals in devices;
- Time synchronized control and fast control response period.

III. LOGIC SOLVER DIAGNOSTICS

In case field sensors are not equipped with on-board diagnostics or HART protocol is not put into practice, condition monitoring is submitted to the logic solver that analyses measure trends or compares different data coming from multiple devices (in case of redundant architectures). If the process signal moves to an undesirable high or low condition, the logic solver performs the safety loop e.g. warning relay output activation, on/off control or emergency shutdown.
Usually the control implementation is associated to different thresholds that are upper and lower limits of the physical quantity under analysis. During normal operation these thresholds are used to define the operative range; in case the measurement crosses those values, the control panel triggers the loop following the implemented logic[9].
Temperature, pressure, level and flow monitoring in Oil&Gas application is usually achieved with a four threshold strategy, shown in Fig. 1: “H, high”, “HH, high-high”, “L, low” and “LL, low-low”.

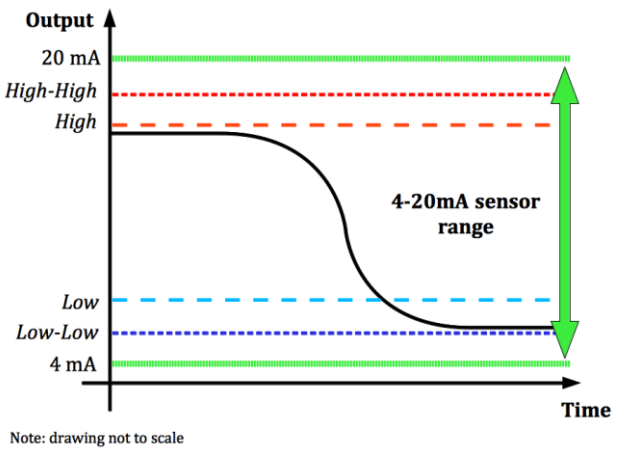

Fig. 1. Output range and safety thresholds for 4-20mA analog sensor

“H” and “L” threshold-crossing usually leads to a visual alarm on the control panel to make the operator aware of the problem; “HH” and “LL” values, instead, are associated with more dangerous conditions. They lead to a progressive load reduction and gradual system shutdown or, in case of extremely critical loop, to an emergency shutdown that instantly stops the machine (this kind of event is always associated to a concrete risk for environment and health and safety of operators).

IV. FUNCTIONAL SAFETY & SAFETY INSTRUMENTED SYSTEM

The operation of many industrial processes, especially in chemical and oil & gas fields, involves inherent risk to persons, property, and environment. The goal of functional safety is to design, built, operate and maintain systems in such a way to prevent dangerous failures or, at least, to be able to control them in case of hazardous conditions. A risk-based approach is mandatory to determine the required performance of safety systems [10-11].
IEC 61508 is a generic standard that provides the framework and core requirements for functional safety of safety related systems that use Electrical/Electronic/Programmable Electronic (E/E/PE) technologies in industrial applications [12].
In order to reduce the risk arising from industrial plants, it might be necessary to automatically activate safety measures when required to avoid dangerous situations: functional safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems is achieved with Safety Instrumented Systems (SIS). These systems are specifically designed to protect personnel, equipment, and the environment by reducing the likelihood or the impact severity of hazardous events.
Safety Instrumented Systems (see Fig. 2) are typically constituted by a combination of three fundamental blocks [12]:

- Sensor(s) detects a physical quantity and provides a corresponding electrical output. Field sensors evaluate process parameters (e.g. temperature, pressure, flow, etc.) in order to determine if single equipment or the whole process or plant is working properly and it is in a safe state. Such sensors do not monitor the normal process but they are usually dedicated to SIS.
- Logic solver(s) receives the information collected by the sensor and elaborates it to take the best response. It is typically a controller that takes actions according to the defined logic in order to prevent hazardous conditions.
- Final element(s) implements the outcomes of the logic solver. This actuator is the last element of the loop and in many industrial applications is represented by a pneumatic valve.

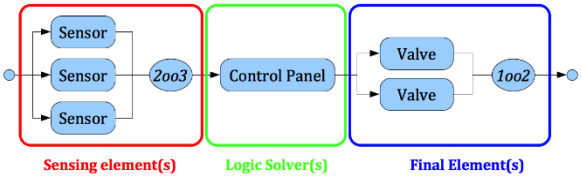

Fig. 2. Safety Instrumented System Functional Block Diagram

The aim of SIS is to implement one or more Safety Instrumented Functions (SIF) in order to guarantee a Safety Integrity Level (SIL): SIFs control critical processes and avoid unacceptable or dangerous conditions for health and environment. Each SIF is associated with a safety loop that is the process involving all the three stages described above (sensor, logic solver and final element) in order to detect a failure, elaborate the collected data and perform the corrective action. SIL is determined by the Risk Reduction Factor (RRF) provided by the SIS to the equipment under control. The inverse of the RRF is the Probability of Failure on Demand (PFD) that is a value that indicates the probability of a system failing to respond to a demand. Average Probability of Failure on Demand (PFDavg) is the average probability of a system failing to respond to a demand in a specified time interval, usually called Proof Test Interval.
There are two modes of operation for a safety function, low and high (or continuous) demand mode. In a low demand mode the safety function is only performed on demand in order to lead the EUC (Equipment Under Control) to a specified safe state; in this case the frequency of demands is no greater than one per year or twice the proof test frequency (frequency setting how often the safety system is completely tested and insured to be fully operational).
In a high demand mode the safety function is always performed on demand but more than twice the proof check frequency; in continuous mode of operation, instead, the safety function is part of normal operation.
Low demand mode is defined by PFD target while high demand and continuous mode follow the Probability of (dangerous) Failure per Hour (PFH).

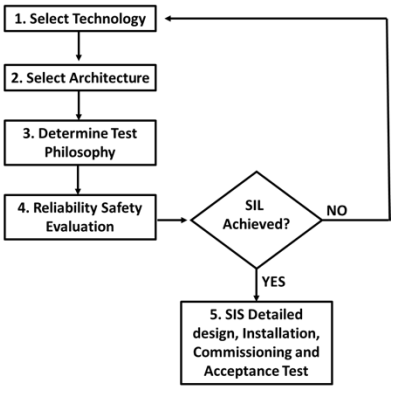

Fig. 3. Flow-chart of SIS design

According to IEC61508 the SIS design is composed by various step, as seen in Figure 3.
The first step considers the selection of element composing the safety loop. Each item must be certified for the use in a SIS. A FMEDA (Failure Mode, Effect and Diagnostic Analysis) must be developed in order to obtain the failure rate of the element, which is classified in four categories:

- Safe undetected (λ_{SU}): SIF can always be performed;
- Safe detected (λ_{SD}): SIF can always be performed;
- Dangerous detected (λ_{DD}): SIF cannot be performed but system will quickly go into the safe state;
- Dangerous undetected (λ_{DU}): failure occurs without notice and in case of demand the safety system cannot perform SIF.

Two important parameters for safety assessment are Diagnostic Coverage (DC) and Safe Failure Fraction (SFF) [3].
DC is the ratio of the probability of detected failures to the probability of all the dangerous failures and it is a measure of system ability to detect failures; SFF, instead, indicates the probability of the system failing in a safe state so it shows the percentage of possible failures that are self-identified by the device or are safe and have no effect.

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (1)$$

$$SFF = \frac{\lambda_{SU} + \lambda_{SD} + \lambda_{DD}}{\lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}} \quad (2)$$

In order to evaluate the PFD_{avg} of the SIS, and consequently the SIL index, the following step of Figure 3 are fully explained in the IEC 61508-6 [12].

V. SAFETY LOOP OPERATION

The loop activation is usually associated with two processes, low and high trip corresponding to lower and upper threshold monitoring:

- Low trip level: the risk is associated to measurements below a predefined value and, in case the sensor output crosses this threshold, the safety function is activated.
- High trip level: the risk is associated to measurements above the threshold and, in case the sensor output crosses it, the safety function is activated.

The logic solver is the second stage of the safety loop and its detection strategy can influence the effectiveness of the safety function.

VI. CASE STUDY

Logic solver diagnostics may be involved in safety applications: in this study we'll focus on diagnostic procedures of 2oo3 TIT architecture that is a sensor assembly dedicated to thermal analysis. It plays the role of sensing stage of a SIS. In this analysis it is assumed that the logic solver is able to detect under and over range currents so both fail-low and fail-high conditions are detectable.

In order to assess Probability of Failure on Demand (PFD), Safe Failure Fraction (SFF) and Diagnostic Coverage (DC), the necessary assumption are in compliance with IEC 61508 [12]. The average probability of failure on demand of a safety function for the SIS is determined by the combination of the average probability of failure on demand for all the subsystems involved in the safety function. Average PFD can be expressed as follows:

$$PFD_{SYS} = PFD_{SE} + PFD_{LS} + PFD_{FE} \quad (3)$$

A. Sensor stage

In this study the first stage of the safety loop under analysis is a 2-out-of-3 (2oo3) redundant architecture of temperature sensors widely used for Oil&Gas applications, Rosemount® 3144P HART Temperature Indicator Transmitter (TIT). TIT is a two wire 4-20mA temperature sensor assembly made of one or more temperature-sensing devices (e.g. Thermocouples or RTDs) and one dedicated transmitter to communicate with system control panel: for Safety Instrumented Systems the 4-20mA output is used as the primary safety variable by the safety logic solver. In this study the Temperature Transmitter is programmed to drive its output low on detected failure (fail-safe state is under-range).

Tab. 1. Failure rates, DC and SFF for sensor

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	DC	SFF
2275 FIT	109 FIT	28 FIT	83 FIT	25,23%	96,67%

Table 1 shows the Rosemount® 3144P HART Temperature Indicator Transmitter failure rate, the DC and SFF achieved with equation (1-2).

In compliance with IEC 61508, 2oo3 architecture consists of three channels connected in parallel with a major voting strategy: the safety function is required in case at least two channels demand it and the system state is not changed if only one channel gives a different result which disagrees with the other two channels. The introduction of a redundant architectures can mitigate the risk associated to dangerous event, but the real enemy of redundancy is common cause failures: if some conditions affect more than one sensor, that is a common cause condition that nullifies redundancy benefits.

The necessary assumption for PFD assessment are shown below:

- Low demand mode of operation;
- $\beta = 10\%$, $\beta_D = 5\%$;
- $MTTR = 8h$;
- 1 year proof test interval.

The average PFD for 2oo3 architecture is:

$$PFD_{SE} = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR = 3{,}68 \cdot 10^{-5} \quad (4)$$

Where:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}} MTTR = 3{,}28 \cdot 10^3 h \quad (5)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}} MTTR = 2{,}19 \cdot 10^3 h \quad (6)$$

B. Logic Solver stage

In this study the logic solver is the Moore Industries® Safety Trip Alarm (STA) logic solver. This device acts on potentially hazardous process conditions in order to:

- Warn of unwanted process conditions;
- Provide emergency shutdown;
- Provide on/off control in both Safety Instrumented Systems and traditional alarm trip applications.

In this study three STA logic solvers are required because the first stage is a 2oo3 Temperature Indicator Transmitter architecture and one Safety Trip Alarm is required for each sensor (using 4-20mA loop); the 2oo3 vote is then performed on the STA relay output.

Tab. 2. Failure rates, DC and SFF for logic solver

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	DC	SFF
0 FIT	660 FIT	170 FIT	86 FIT	66,41%	90,61%

Table 2 shows the Moore Industries® Safety Trip Alarm failure rate, the DC and SFF achieved with equation (1-2). The necessary assumption for PFD assessment are shown below:

- Low demand mode of operation;
- $\beta = 10\%$, $\beta_D = 10\%$;
- $MTTR = 8h$;
- 1 year proof test interval.

Using equations (3-6) with data contain in tab.2, the average PFD is:

$$PFD_{LS} = 3{,}83 \cdot 10^{-5} \quad (7)$$

C. Final Element stage

In this study the final element under analysis is a pneumatically actuated block valve controlled by ASCO® Redundant Control System (RCS): it is an electro-mechanical and pneumatic system consisting of two solenoid valves and one pneumatic valve (bypass valve). Three pressure switches are provided on each valve for diagnostic purpose to monitor the pneumatic pressures at critical points of the RCS assembly: switches are required to confirm the proper position of the valve.
In compliance with IEC 61508 for safety assessment Redundant Control System is considered part of the final element together with the controlled block valve.
The safe-state is achieved with de-energized signals so at least one of the two solenoid valves has to be energized to prevent the block valve from moving to the safe state. The pressure switch contacts are normally open so they are closed in presence of pressure. The mode of operation of the RCS is 1oo1HS: in this mode only one solenoid valve is on-line during normal operation. Any spurious trip of the on-line solenoid valve is detected by the logic solver using signals coming from the associated pressure switches; in response to spurious trip the logic command to energize the second solenoid valve in order to maintain air supply to the block valve.
The second item to take into account in the final element stage is the controlled block valve. In this study the final element is a ball valve with floating ball design (Abc. X Series Ball Valve): the safety function is to move to the designated safe position within the required time.

Tab. 3. Failure rates for final element stage

Device		λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
RCS	Solenoid Valve	594 FIT	216 FIT	502 FIT	10 FIT
	Bypass Valve	57 FIT	88 FIT	7 FIT	0 FIT
	Pressure Switch	444 FIT	5 FIT	0 FIT	0 FIT
Block Valve		0 FIT	0 FIT	149 FIT	330 FIT

Table 3 shows the ASCO® Redundant Control System (first three rows) and controlled block valve (last row) failure rates.
The necessary assumption for PFD assessment are shown below:

- Low demand mode of operation;
- $\beta = 1\%$;
- $MTTR = 24h$ and $ADT = 24h$;
- 1 year proof test interval.

Using Markov modelling the average PFD for RCS with ADT (Automated Diagnostic Tests) is the following:

$$PFD_{FE_{RCS}} = 1{,}24 \cdot 10^{-4} \quad (8)$$

Since the ball valve under analysis is provided of partial stroke testing (PVST), and the necessary assumptions and the procedure to assess the average PFD are the following:

- MTTR = 96 hours;
- 2 months partial proof test interval (1460h);
- 6 months full proof test interval (4380h);

Where the PVST coverage concerns only dangerous failures that are undetected by the diagnostics and that may be revealed by stroke tests. Since the PVST is put into practice, it is necessary to follow a different procedure to assess the average PFD.
In compliance to IEC 61508 [12] the Probability of Failure on Demand of the Ball Valve is the following:

$$PFD_{FE_{BV}} = 5{,}05 \cdot 10^{-4} \quad (9)$$

The average probability of failure on demand of the whole final element stage is:

$$PFD_{FE} = PFD_{FE_{RCS}} + PFD_{FE_{BV}} = 6{,}29 \cdot 10^{-4} \quad (10)$$

D. Safety loop PFD assessment

The average probability of failure on demand of a safety function for the safety instrumented system is determined by the combination of the average probability of failure on demand for all the subsystems involved in the safety function. Average PFD can be expressed by equation (3) as follows [12]:

$$PFD_{SYS} = 7{,}04 \cdot 10^{-4} \quad (11)$$

According to the conversion table between PFD values and SIL achieved reported on IEC 61508 [12], for the system under analysis SIL 3 range is achieved because the PFD_{SYS} belongs to the range of SIL3 attribution.

$$PFD_{SYS} \in [10^{-4}; 10^{-3}) \quad (12)$$

As possible to see in figure 4, in this application the main contribution to the whole PFD is attributed to the final element, (about 90% divided in 72% to the Block Valve and 18% to the RCS), the 10% remaining is divided equally between the sensor and the logic solver.

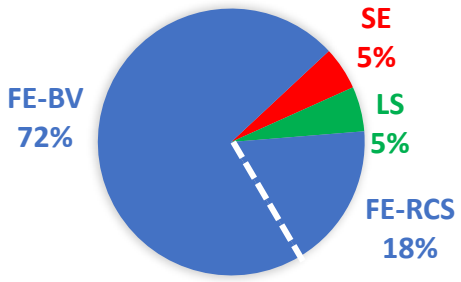

Fig. 4. Pie chart of each contribution of the probability of failure on demand

VII. CONCLUSIONS

The paper analyzes the local diagnostics in modern system and its benefits and drawback, then the focus is the safety loop assessment using the IEC 61508 issue.

A case study was developed to test the strength and the criticality of the design method of Safety Instrumented System proposed in the European Standard.

The system under analysis is composed by: three sensor in 2oo3 configuration making of the sensor stage; three logic solver (one of each sensor) able to elaborate data and active the Safety function; a final element composed by a RCS system and a block valve.

Redundant architectures (e.g. 2oo3) improve the system reliability and availability decreasing the probability of dangerous failures. Anyway the common cause failures (CCF) are the real problem of this kind of structure, that nullifies redundancy benefits. The CCF must be taken into account during design phase before introducing additional components. In order to reduce the probability of common cause failures diagnostic and diversity must be used in design phase. Obviously each choice is a trade-off between safety and costs: to take these decisions designers should select the best safety improvement considering real-world installed safety.

For the system under analysis the SIL 3 is achieved. A reasonable division of the system probability of failure on demand that seems to be widely accepted is 35-15-50% to the sensor, logic and final element subsystems respectively. As seen in figure 4 in this application about 90% of whole PFD is associated to the final stage, due to the 1oo1 architecture.

REFERENCES

[1] M. Catelani, L. Ciani, M. Venzi, *"Sensitivity analysis with MC simulation for the failure rate evaluation and reliability assessment"*, Measurement, Volume 74, October 2015, Pages 150-158, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.07.003

[2] MIL-HDBK-338B, Electronic Reliability Design Handbook – Department of Defence Washington DC, 1998

[3] M. Rausand, "*Reliability of safety-critical systems",* John Wiley & Sons Inc. Publication, 2014

[4] ReliaSoft Corporation, "*Life Data Analysis Reference",* Tucson, AZ, USA,, May 2015

[5] G. Kulwanoski; M. Gaynes; A. Smith; B. Darrow; "*Electrical contact failure mechanism relevant to electronic packages*", Electrical Contacts - 1991 Proceedings of the Thirty-Seventh IEEE HOLM Conference on Electrical Contacts, Pages: 184 - 192, DOI: 10.1109/HOLM.1991.170823

[6] Rolf Isermann, "*Mechatronic Systems - Foundamentals"* Springer-Verlag, London, 2005

[7] H. T. Grimmelius; P. P. Meiler; H. L. M. M. Maas; B. Bonnier; J. S. Grevink; R. F. van Kuilenburg, "*Three state-of-the-art methods for condition monitoring*", IEEE Transactions on Industrial Electronics, Volume: 46, Issue: 2, 1999, Pages: 407 - 416, DOI: 10.1109/41.753780

[8] Seung Ho Hong; Sung Min Song; "*Transmission of a Scheduled Message Using a Foundation Fieldbus Protocol*", IEEE Transactions on Instrumentation and Measurement, Volume: 57, Issue: 2, 2008, Pages: 268 - 275, DOI: 10.1109/TIM.2007.910100

[9] An Guochen; Meng Zhiyong; Ma Hongtao; Sui Bingdong, "*Design of Intelligent Transmitter Based on HART Protocol*", 2010 International Conference on Intelligent Computation Technology and Automation, Volume: 2, Year: 2010, Pages: 40 - 43, DOI: 10.1109/ICICTA.2010.167

[10] M. Catelani; L. Ciani; V. Luongo, "*Safety analysis in oil & gas industry in compliance with standards IEC61508 and IEC61511: Methods and applications*". IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 2013, Minneapolis, MN (USA), pp. 686-690, DOI: 10.1109/I2MTC.2013.6555503

[11] M. Catelani; L. Ciani; M. Mugnaini; V. Scarano; R. Singuaroli, "*Definition of Safety Levels and Performances of Safety: Applications for an Electronic Equipment Used on Rolling Stock*", 2007 IEEE Instrumentation & Measurement Technology Conference (IMTC), 2007, Pages: 1-4, DOI:10.1109/IMTC.2007.379086

[12] IEC61508, Electric / Electronic / Programmable Electronic safety-related systems, parts 1–7. Technical report, International Electrotechnical Commission, May 2010.