Fieldbus: A solution for safety and availability?

Wolfgang Velten-Philipp
TÜV SÜD
Automation, Software and Electronics - IQSE
Ridlerstraße 65, 80339 München
Germany

Dr. M.J.M. Houtermans
Risknowlogy B.V.
Brunner Bron 2,NL-6441 GX Brunssum
The Netherlands

Abstract: Fieldbus solutions are mainly used for control functions but the latest trend in fieldbus is to use the technology also for safety applications. Using fieldbus technology in theory is not a problem. There are international standards dealing with functional safety and if a fieldbus device meet these standards then it can easily be integrated in safety related solutions. For an end user, wanting to implement new technology for safety applications, it is important to understand whether fieldbus devices are at least as safe as existing traditional safety solutions, and do not reduce plant availability with spurious trips.

Key–Words: Process Availability, Safety, Fielbus, PLC

1 Introduction

Fieldbus technology has developed significantly during the past five years and is currently being used in plants all over the world. The ease of use of fieldbus solutions has also come to the attention of the safety industry. There are existing different solutions for field bus protocols which are supporting safety related communication, e.g. CAN-Open, Profibus and Foundation Fieldbus [1]. Fieldbus technology has several advantages compared to point to point field wiring:

- It saves field wiring as there is only one bus wire necessary which connects all bus participants.
- It allows decentralized execution of the logic.

On the other hand potential users of Fieldbus technology have concerns using the new technology for some reasons:

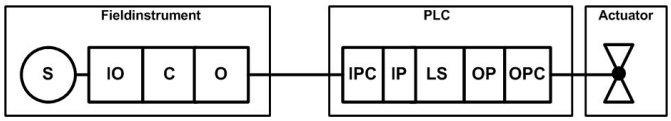
- They fear that fieldbus technology is not as safe as a conventional safety solution.
- They have concerns that fieldbus technology might cause more spurious trips as conventional safety techniques.
- The reaction time to execute the intended safety function is longer compared to PLC solutions.

The objective of this paper is to help answer the question whether fieldbus is a good solution for safety and process availability compared to a conventional solution using PLC technology. In the following a typical safety related application is selected which requires a safety instrumented system. For the purpose of this paper the safety instrumented system is implemented in two ways, i.e., first as traditional safety system using PLC equipment and then based on devices using fieldbus technology. For each technology a reliability model is created. The reliability models are used to calculate the probability of failure on demand (PFD) and the probability of fail safe (PFS) for both solutions.

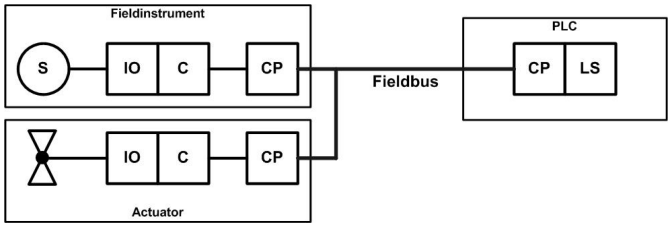
This paper will explain the architectures of the two safety instrumented systems and the data used to perform the calculations. Finally the results will be compared and the paper will finish with conclusions and a statement will be made whether fieldbus is a good solution for safety as well as process availability.

2 Definition of architectures

In order to compare fieldbus technology to traditional safety technology we first need to define a safety function which is implemented in a 1oo1 and 1oo2 architecture. These two basic architectures are shown in figure 1 and 2. Figure 1a and figure 2a shows the safety function implemented by a traditional safety instrumented system in a 1oo1 and 1oo2 architecture. Figure 1b and Figure 2b shows the same safety function implemented in Fieldbus technology. The traditional system uses conventional instrumentation where every single instrument or actuator is connected to a safety PLC which executes the logic. The fieldbus system uses instruments, actuators and the logic solvers connected via one bus system.



(a) 1oo1 Architecture with PLC



(b) 1oo1 Architecture with fieldbus

Figure 1: 1oo1 Architectures

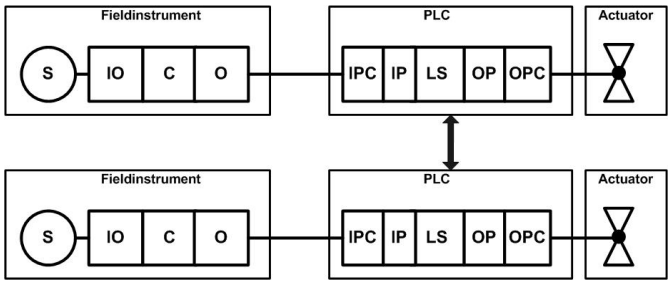
Independent of the technology chosen a safety instrumented system always consists of an input part, a logic solver part and an output part. In order to compare both technologies it has been decided to divide each system into its standard elements. In its core Fieldbus technology consists of the same components or standard building blocks as any other safety device. It only differs from traditional safety solutions in the way the safety plc communicates with its instrumentation and actuators. The following description applies to both technologies and explains the common parts of each system, see figure 1 and 2.

A typical field instrument, as it is in use today, consists of a sensing element and an input/output section. S is the real sensing element, e.g. a pressure sensor element, which consists of a diaphragm and a piezoelectric sensor element. The sensor element is connected to an I/O section. The I/O section interfaces the measured signals to a microcontroller which is connected to an output section. Usually this is a 20 mA current source.

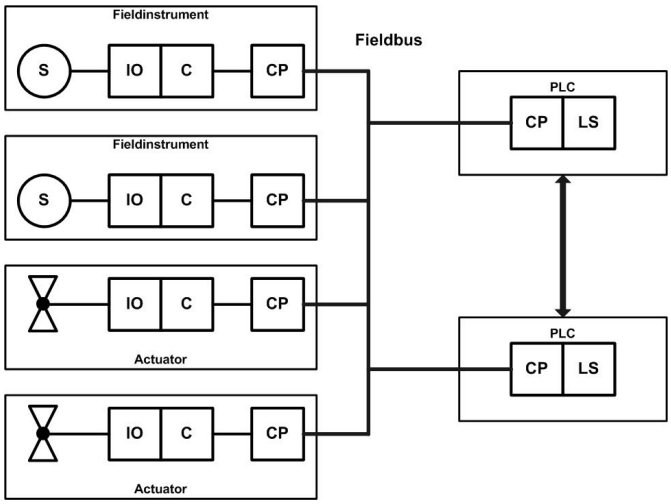
The current loop of the field instrument is connected to a safety plc which consists of an input module (IPC, IP), logic solver (LS) and output module (OP, OPC). Input and output modules are divided into a common part (IP, OP) which is used for all channels (IPC, OPC) on a module. The IPC section usually consists of discrete components which are protecting the inputs from over voltages and which are converting the input current into a voltage. The IP part itself consists likely of a multiplexer and an analogue to digital converter device which interfaces the logic solver device (LS) of the PLC. The logic solver receives and processes the data from the input modules and controls the output modules. The output modules are driving the output channels. In our example, the outputs are directly connected to the actuators. Each instrument consisting of S, IO,C,O requires one I/O point of the PLC.

The same architectures realised by using fieldbus technology is shown in fig.1b and fig.2b. Currently available fieldbus technology does not allow executing safety related functions decentralized in the fieldbus instruments. Therefore it is assumed that the fieldbus is connected to the PLC by an interface module (CP). Usually the CP bases on a microcontroller device or a complex ASIC.

In other words, even though the fieldbus solution is based on a new technology it does not mean that suddenly our safety systems are using new basic electronic components. The only thing fieldbus does is introducing the same electronic components on other positions in our safety solution.



(a) 1oo2 Architecture with PLC



(b) 1oo2 Architecture with fieldbus

Figure 2: 1oo2 Architectures

3 Model

Based on the architectures in figure 1 and 2 four reliability models have been developed. These models are basing on Markov technique [8, 9].

3.1 Failure Modes

Fault models are necessary to define the different modes how sub-systems can fail. For many sub-systems the main failure modes and their effects can be predicted. Passive components for example can fail stuck open, stuck close or they can change parameters over time (drift effects). In the safety world components are classified by two different types of fault effects. A sub-system is of type A in case a predictable fault model exists or of type B if the effect of a fault of this sub-system is not predictable (see [2]). This is normally the case if a sub-system consists of high complex devices like ASIC's or microcontrollers. For such kind of sub-systems it impossible to predict the effect of an internal fault of a single component (e.g. a failed transistor in a microcontroller). In this case IEC 61508-2 allows to assume that the fraction of safe to dangerous failures is 50% unless proof for better values are existing.

The effect of a sub-system fault is analysed by examining the related safety function. Every safety related system has a specified safety related function and in most cases a predefined safe state. A safety related system executes its safety function in case a demand from the connected process comes. An emergency shut down system for example turns off all outputs in case of a demand of the safety function (e.g. measured overpressure in a boiler). The safe state is the de-energized state in this case.

Generally, there are two types of fault effects. An internal fault is classified as dangerous if the safety function of the system cannot be executed upon demand after the fault occurred. A fault has no effect if the safety function is still available after the fault occurred. In case the fault itself has initiated the safety function (system has tripped the process), the fault effect is classified as safe. In case the fault has inhibited the safety function it is considered

as a dangerous failure. Safe and dangerous faults are additionally classified by the system capability to detect the faults. Considering these detection by online diagnostics [3] leads to following possible system states which have been used for the reliability analysis:

Effect	Description
SU	(Sub-) System has failed safe undetected
SD	(Sub-) System has failed safe detected
DU	(Sub-) System has failed dangerous undetected
DD	(Sub-) System has failed dangerous detected
NE	(Sub-) System failure has no effect on safety function

The Markov models generated are assuming that each block can fail to the previously explained states. In case the system fails not to a detected or safe state, faults of all other components were assumed. Furthermore common cause effects have been taken into account by introducing β -factors.

The following table defines the different system states for which the calculation has been executed:

State	Description
UP	Function is free of faults
AV	Function is available
FS	Function has tripped
FD	Function has failed dangerous

4 Reliability Data

In order to execute the reliability calculations reliability data is needed for each sub system of the safety system. Table1 gives an overview. The data is chosen in a way that allows fair comparison of the different technologies. The data used is based on the following assumptions:

- All microcontroller devices (C) have the same base failure rate.
- IO sections have the same base failure rate.
- The base failure rate of the PLC logic solvers (LS) is two times the base failure rate of microcontroller C[1].
- The base failure rates of the communication processors (CP) are 1.5 times higher than other microcontroller devices (C)[2].
- All complex components have 50% safe failures and 50% dangerous failures.
- All computer based devices have a diagnostic coverage for dangerous failures of 60%.
- The diagnostic coverage for safe and dangerous failures for the communication protocol and the related communication processor is 90%.
- The diagnostic coverage for safe and dangerous failures for the PLC related I/O is 90%.

It is important to understand that the absolute values in table1 are not essential for the calculations and for the comparison of the results. The comparison results are not affected by absolute values but by the relationship the values have to each other.

[1]The LS logic solver usually consists of more than one microcontroller and of other complex components.

[2]It is assumed that a communication processor has a higher failure rate that a normal microcontroller because it is connected to a communication interface [10].

Label	component	Characterisation	λ_b FIT	S_r	DC_d
S	Sensor element	Electro mechanic, electro hydraulic element	500	0.5	0
IO	Sensor Input /Output circuit	Electronic circuit, discrete components, ADC, DAC, Multiplexers	50	0.5	0
C	Embedded computer	Microcontroller	100	0.5	0.6
CP	Communication controller, interface circuitry	Microcontroller, interface chip sets	150	0.5	0.9
O	Output circuitry	DAC, analogue electronic	50	0.5	0.2
IP	Input module	Discrete components, ADC, multiplexers, embedded controller	200	0.5	0.9
IPC	Per channel input circuit	Discrete components, filter	25	0.5	0.9
LS	Logic Solver	Main CPU, communication processor, interface circuitry	200	0.5	0.6
OP	Output module	Discrete components, embedded controller	200	0.5	0.9
OPC	Per channel output circuit	Power transistors, filter, interface	50	0.5	0.9
A	Actuator	Mechanical components	700	0.5	0

Table 1: Reliability Data

5 Results of Markov analysis

In the safety world mean values for the reliability over a certain time span are used to compare systems and to evaluate safety integrity levels[2]. Figure 3 shows the results for the mean values of the state reliabilities P_{UP},P_{AV}, P_{FD}, P_{FS} defined before for the 1oo1 architectures. The tables in the figures are summarizing the results. The mean values of the probabilities are printed after a time interval of 1 and 10 years. Furthermore a ratio $P_{fieldbus}/P_{plc}$ is calculated to ease compare of the different values.

Figure 4 shows the results for the mean values of the reliabilities for the 1oo2 architectures.

5.1 Compare of FD values

First we compare the results for the 1oo1 and 1oo2 technologies. The FD state probabilities are providing the probability of a safety related loop to fail into a dangerous state. That means the safety function will not be executed on demand.

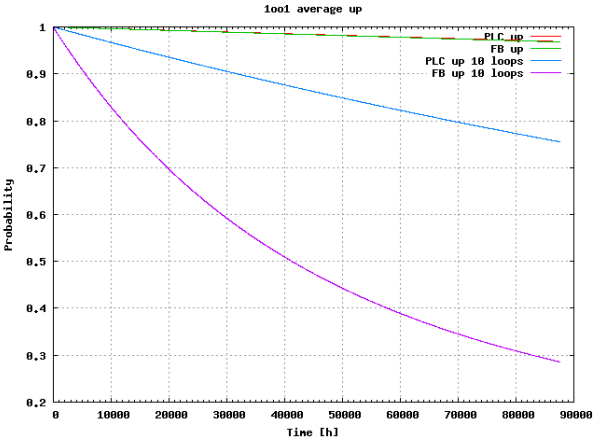
The probability to fail dangerous P_{FD}[3] for a safety related loop, realized either by Fieldbus or by PLC technology,is nearly equal, see fig.fig:res1oo1c and fig.fig:res1oo2c. By use of previous assumptions for the component data SIL 1 to SIL 2 level is gained, depending from the off-line proof test interval which is assumed to be 10 years. The 1oo2 solution shows similar results, but reaches a SIL 2 to SIL 3 level.

Summarized 1oo1 and 1oo2 Fieldbus and PLC systems are providing the same level of safety.

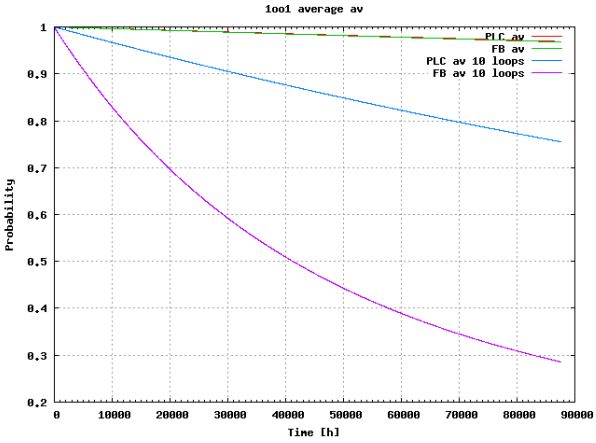
5.2 Compare of UP and AV-state probabilities

Next we discuss the results for the up states of the system. The system leaves up state as soon as a component fault occurred. An AV state is reached if a component fault occurs and the system is afterward still able to execute the safety function. AV represents therefore an intermediate state where the system has a fault, but is still operable.

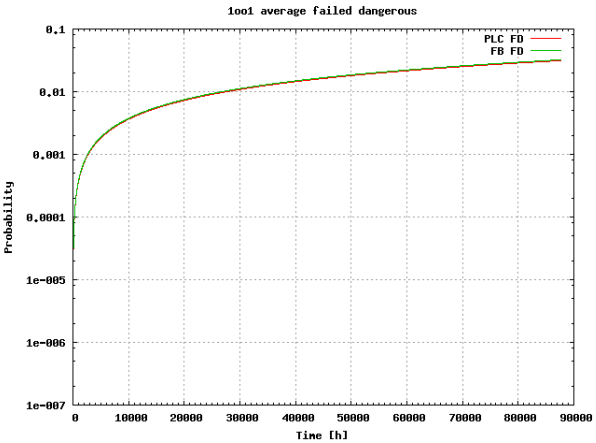
[3] P_{FD} is related to one single safety related loop because safety related systems usually fail dangerous, if one single loop has failed dangerous.



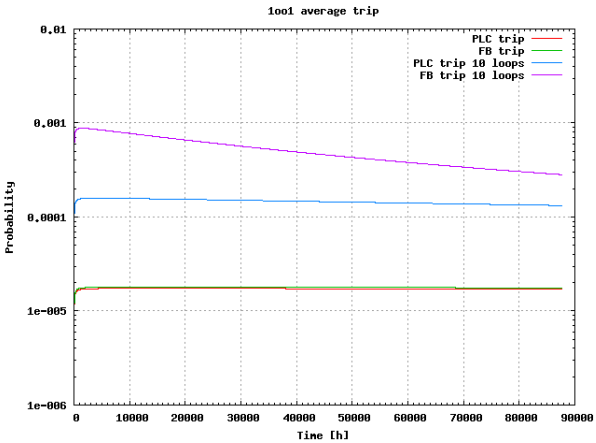
(a) Average Probability UP -States



(b) Average Probability AV -States



(c) Average Probability FD -States

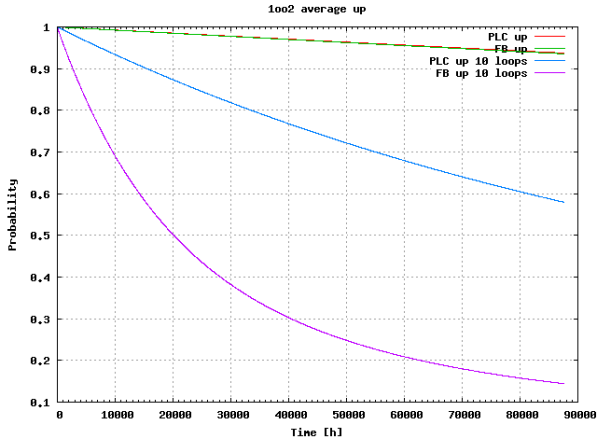


(d) Average Probability FS -States

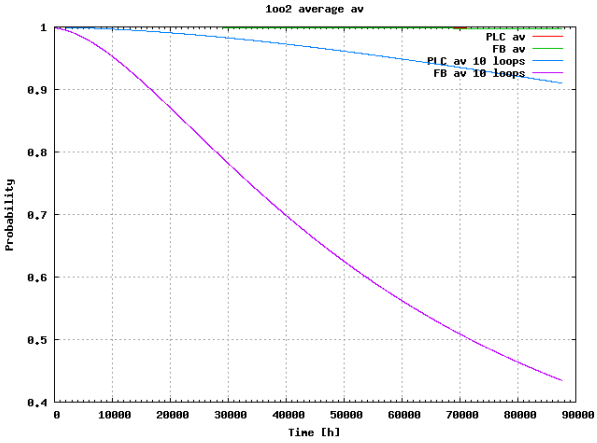
1oo1 architecture 1 Loop		**1 year**			**10 year**	
	PLC	FB	FB/PLC	PLC	FB	FB/PLC
up	9,97E-01	9,97E-01	1,00	9,69E-01	9,68E-01	1,00
av	9,97E-01	9,97E-01	1,00	9,69E-01	9,68E-01	1,00
fs	1,74E-05	1,79E-05	1,03	1,72E-05	1,76E-05	1,03
fd	3,19E-03	3,29E-03	1,03	3,12E-02	3,22E-02	1,03
10 Loop		**1 year**			**10 year**	
	PLC	FB	FB/PLC	PLC	FB	FB/PLC
up	9,71E-01	8,48E-01	0,87	7,55E-01	2,86E-01	0,38
av	9,71E-01	8,48E-01	0,87	7,55E-01	2,86E-01	0,38
fs	1,58E-04	7,91E-04	5,01	1,32E-04	2,82E-04	2,13
fd	2,90E-02	1,51E-01	5,22	2,45E-01	7,14E-01	2,92

(e) Average probabilities after 1 year and 10 years

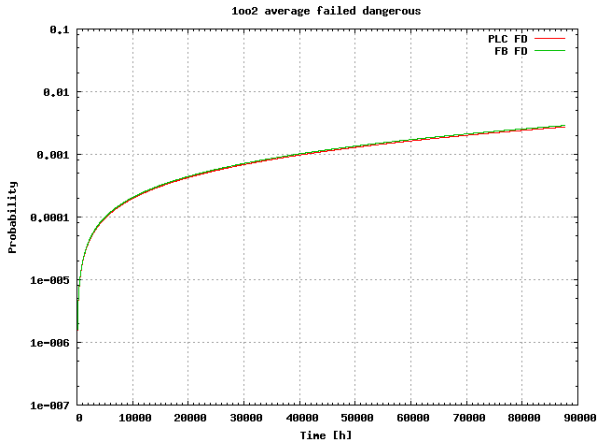
Figure 3: Markov calculation results for 1oo1 architectures



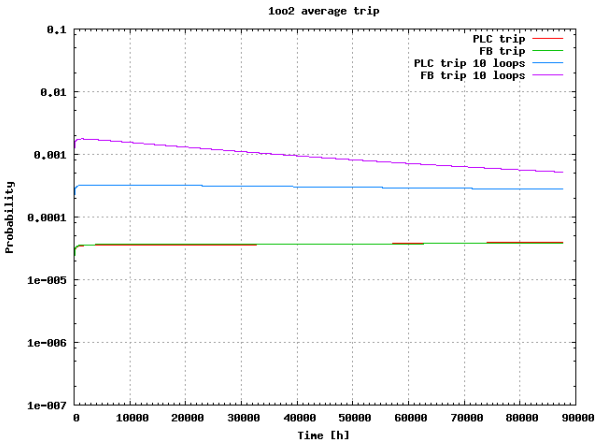
(a) Average Probability UP -State



(b) Average Probability AV -State



(c) Average Probability FD -State



(d) Average Probability FS -State

1oo2 architecture 1 Loop		**1 year**			**10 year**	
	PLC	FB	FB/PLC	PLC	FB	FB/PLC
up	9,93E-01	9,93E-01	1,00	9,37E-01	9,35E-01	1,00
av	1,00E+00	1,00E+00	1,00	9,97E-01	9,97E-01	1,00
fs	3,57E-05	3,65E-05	1,02	4,01E-05	3,87E-05	0,96
fd	1,72E-04	1,78E-04	1,04	2,73E-03	2,88E-03	1,05
10 Loop		**1 year**			**10 year**	
	PLC	FB	FB/PLC	PLC	FB	FB/PLC
up	9,41E-01	7,20E-01	0,77	5,80E-01	1,44E-01	0,25
av	9,97E-01	9,61E-01	0,96	9,10E-01	4,35E-01	0,48
fs	3,25E-04	1,58E-03	4,87	2,76E-04	5,21E-04	1,89
fd	2,51E-03	3,61E-02	14,35	8,01E-02	5,45E-01	6,80

(e) Average probabilities 1 year and 10 years

Figure 4: Markov calculation results for 1oo2 architectures

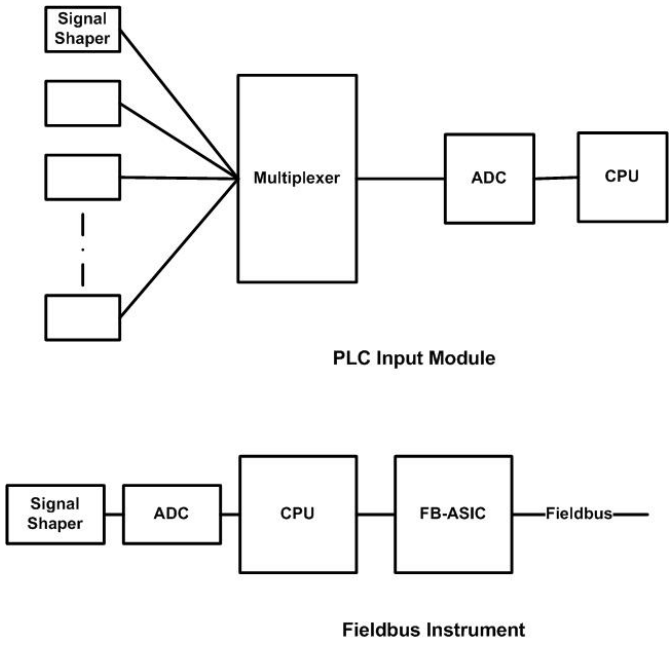


Figure 5: Typical I/O stage for PLC and fieldbus instrument

In case of a non fault tolerant 1oo1 system AV states are seldom because in most cases the system shuts down immediately after a fault occurs. In case of the fault tolerant 1oo2 architecture in opposite, numerous AV states are existing because the system can often be still operable after a fault had occurred.

For a single safety function the up state probability of a Fieldbus and a PLC system are nearly equal. This changes if we evaluate a system which includes more than one safety related function. The calculation performed assumes 10 loops and no redundancy for the system functions. If one loop fails the system leaves the up state.

The PLC has here significant advantages compared to the fieldbus solution. Reason for that behavior is obvious. In case of fielbus instrumented loops every channel which was added to the system requires an additional bus communication device, which is usually a complex microcomputer device or ASIC. The PLC in opposite requires only few passive components to add additional channels. Fig 5 shows a typical I/O architecture of a PLC compared to fieldbus instrument. Every channel which is added to the PLC architecture adds passive components responsible for signal shaping, filtering and isolation. In case of fieldbuses every channel requires a complex ASIC or microcontroller device to connect a device to the fieldbus. According to table 1 every additional PLC input channel adds 20 FIT, in case of fieldbuses each channel counts 150 FIT. Signal shaping, filter and IO computer are necessary in both cases and have equal failure rates. This explains why fieldbus has disadvantages compared to PLC structures if availability is compared.

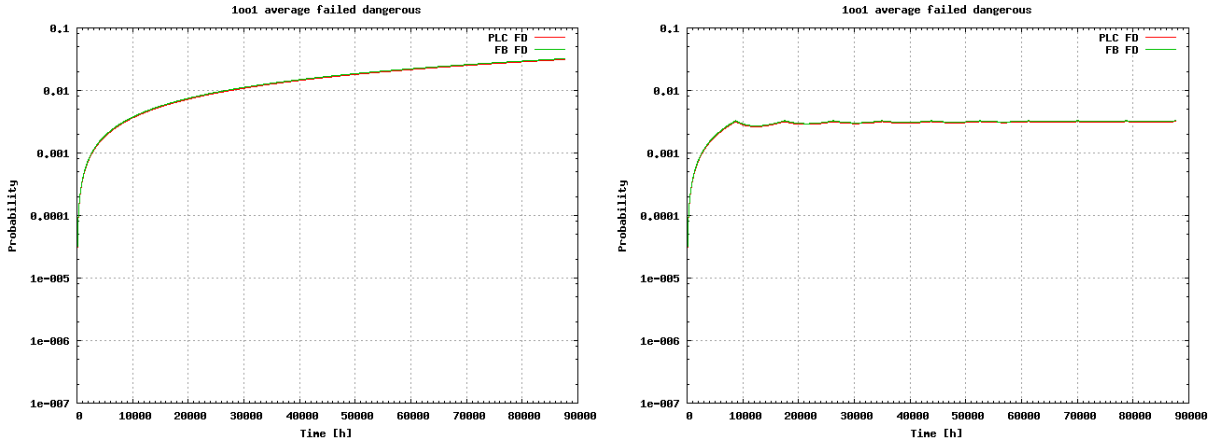
5.3 Compare of trip probabilities

The trip probability is one of the most interesting values as it shows the probability to shut down the connected process. For the same reasons explained before the trip rate of the fieldbus based solution is is significantly higher (2-5 times) than the PLC based solution.

5.4 Influence of proof test

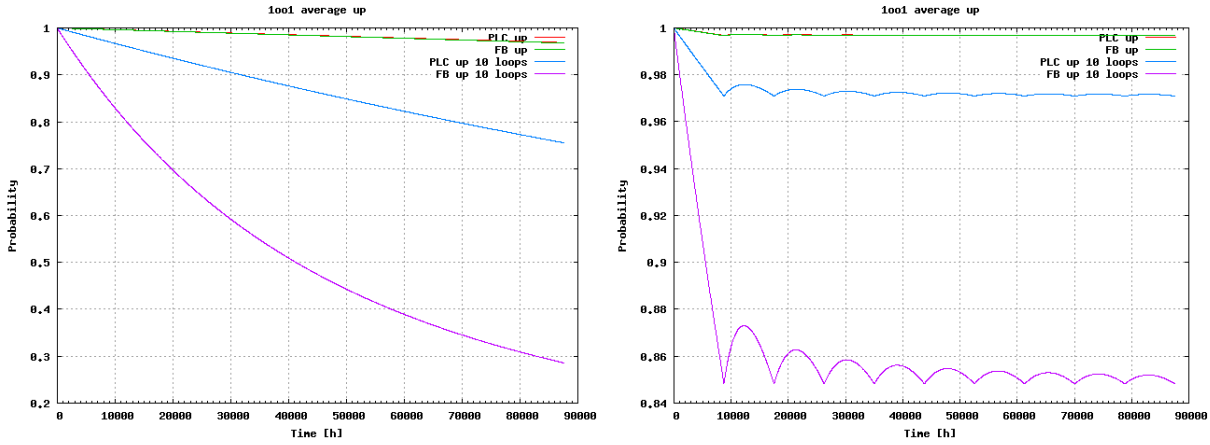
Proof testing means that the safety function of the control equipment is tested manually. Proof testing has a big impact on safety related parameters like probability to fail to a dangerous state. Figure 6 shows the effect of proof testing on both architectures. The proof test prevents the probability to fail to danger from increasing over a certain level.

Also the probabilities for the UP and AV state are decreasing to a certain level in case of periodically executed proof tests. Figure 7 shows the UP probabilities with and without proof testing.



(a) (b)

Figure 6: Effect of a proof test every year on the PFD



(a) (b)

Figure 7: Effect of a proof test every year on the UP probability

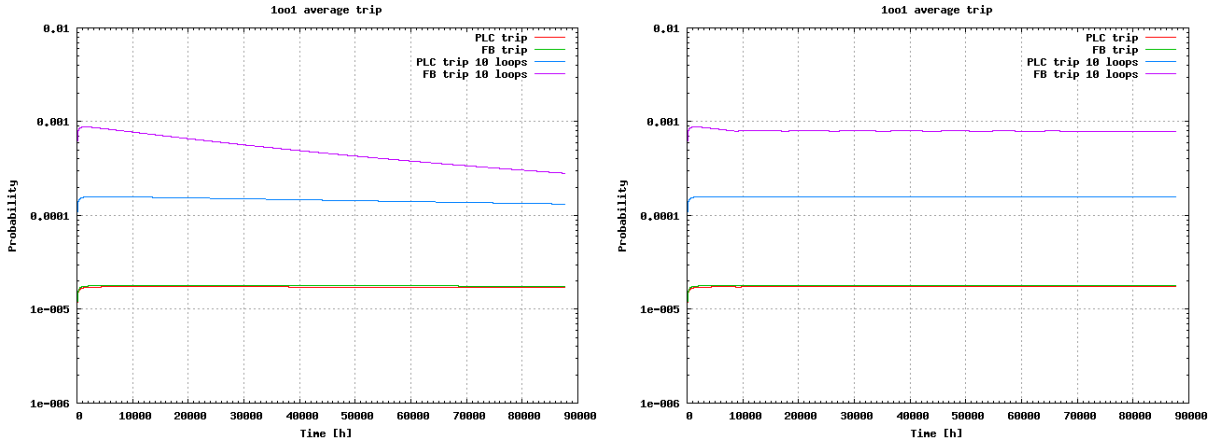
The probability to trip shows the same behavior, it decreases to a certain value and remains there. Without proof tests the probability decreases over time. The reason for that behavior which seems contradictory is that the probability of the UP and AV states are decreasing and therefore the absolute value for trip probability also decreases over time. Relative to the UP state probabilities both values for trip are with and without proof test nearly equal[4].

6 Conclusion

The compare of a safety related fieldbus solution and a PLC based solution for 1oo1 and 1oo2 architectures has shown that both solutions provide the same level of safety.

The compare of the other reliability parameters showed that Fieldbus based solutions have significant disadvantages regarding availability. Reason for that behavior are the higher failure rates of sub-systems which are necessary to interface the bus system and the fact that there is only one single bus system in place. This causes unavailability of the whole system if it fails to a state where the whole bus becomes unavailable. By improving the bus interfaces by minimizing component faults which are leading to complete unavailabilities of the bus system

[4] 5 percent deviation



(a) (b)

Figure 8: Effect of a proof test every year on the TRIP (FS) probability

and by use of interface components with low failure rates the problem could be relieved. Also frequent executed proof testing limits the unavailability of the system. The PLC solution in opposite has less components which are causing a complete unavailability of the system, but requires on the other hand more effort for field cabling.

Future filed bus systems might support redundant bus interfaces and buses to improve the availability of the system.

References:

[1] Fieldbus Foundation Receives TÜV Protocol Type Approval For Safety Instrumented Systems Specifications, *http://www.fieldbus.org/News/?news_x_language_id=624*, 2006

[2] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems, *International Standard,* IEC 2000

[3] Houtermans M.J.M., Velten-Philipp W.
Diagnostic Test versus Proof Test, *Whitepaper www.risknowlogy.com*

[4] M.J.M. Houtermans
Definition of spurious trip levels, *Whitepaper www.risknowlogy.com*

[5] Börscök J. Electronic Safety Systems, Hardware Concepts, Models, and Calculations, *Huthig GmbH & Co. KG Heidelberg*, Germany 2004

[6] Houtermans M.J.M., Rouvroye J.L., The Influence Of Design Parameters On The Performance Of Safety-Related Systems, *International Conference on Safety, IRRST*, 1999 Montreal, Canada

[7] Houtermans M.J.M., Brombacher A.C., Karydas D.M., Diagnostic Systems of Programmable Electronic Systems, *PSAM IV, New York*, 1998 U.S.A

[8] William J.Stewart, Introduction to the Numerical Solution of Markov Chains, *Princeton University Press*, 1994

[9] Technical Report 84.0.02, Version 4
Safety Instrumented Systems (SIS)
–Safety Integrity Level (SIL)
Evaluation Techniques
Part 4: Determining the SIL of a SIS via Markov Analysis, *ISA*

[10] Technical Report IEC TR 62380
Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment, *IEC*, 2004