

TECHNICAL WHITE PAPER

FIELDBUS AND AVAILABILITY

The difference between theory and practice

In process automation, fieldbus is gaining more attention, not only because of the robustness it delivers for day-to-day operations, but also for its ability to integrate safety-related controls. It boils down to extremely high availability of the fieldbus infrastructure itself, as with any critical production process.

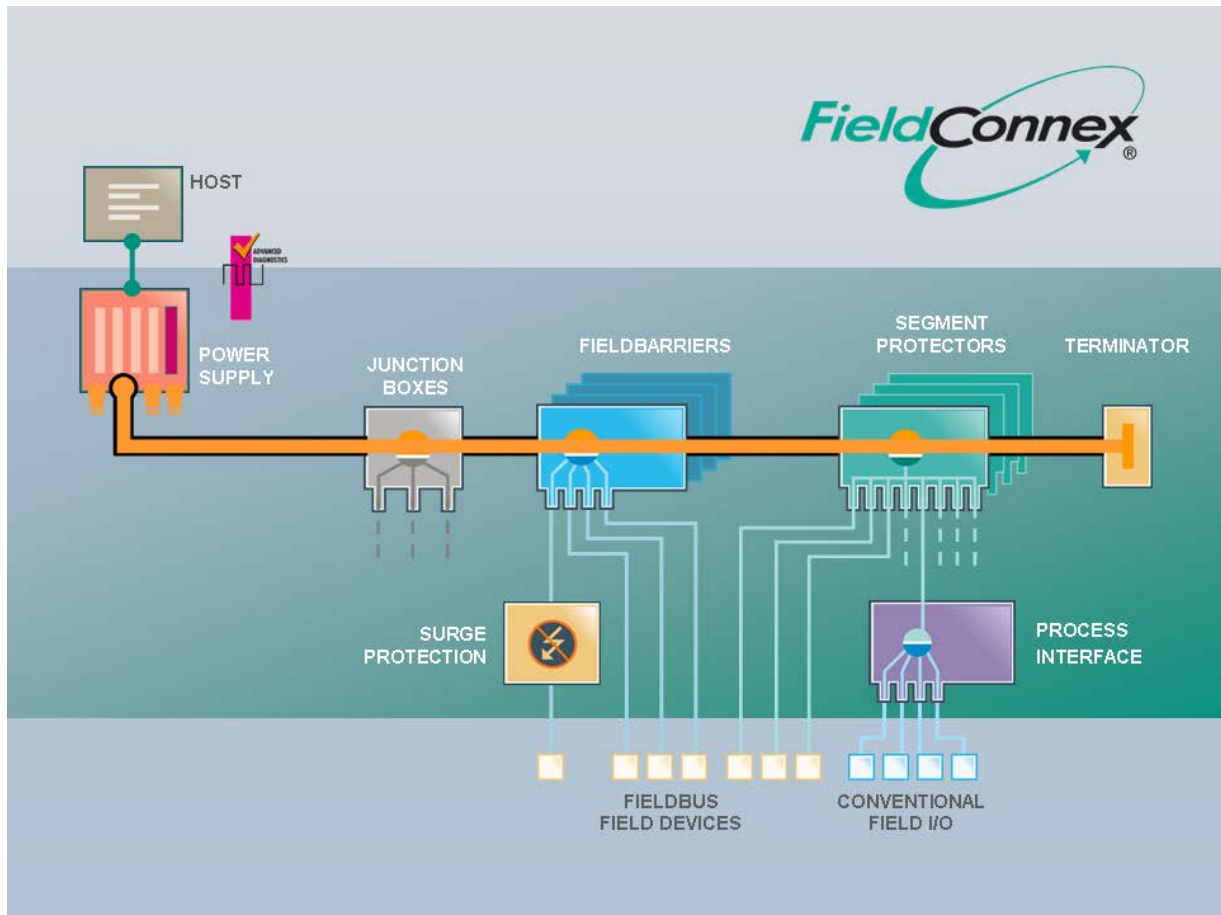
This technical white paper provides facts and reasonable assumptions relevant to the availability of fieldbus infrastructures. It provides the knowledge for decisions based on facts about handling fieldbus. Components, dimensioning and automatic fault isolation, diagnostics, and redundancy all have a part in it. With the information provided, you are enabled to form your own opinion and judgment.

Prepared by:

Andreas Hennecke
Product marketing manager

Thomas Klatt
Support manager

Andreas Hildebrandt
Training manager



Quality Information from a Quality Supplier

This technical white paper utilizes Pepperl+Fuchs' expertise and knowledge to provide a clear insight into the many new technological and application issues you may face with a fieldbus installation. It corresponds to our way of working and thinking: combining state-of-the-art technologies with years of research and innovation to simplify planning, installation and commissioning, operation, and plant upkeep.

If the content of this paper sparks comments or questions, we invite you to contact your Pepperl+Fuchs office or representative to get in touch with the experts. We are glad to share our expertise with you for your business success.

Our promise is to simplify your work processes: You can stay focused on your day-to-day business with a reliable FieldConnex® fieldbus infrastructure. It ensures the connection between DCS and instruments, fully digital with explosion protection for any hazardous area. We are driven to provide innovation with proven reliability for process automation practitioners:

- FieldConnex is robust, reliable, and the first choice of many well-known end users worldwide.
- Advanced physical layer diagnostics reach down to spurs, accessories, and instruments; interpret data, and provide detailed fault analysis. Water ingress and worn-out surge protectors are identified without manual inspection.
- The High-Power Trunk concept allows long cable runs and high device counts and is now an industry standard. DART Fieldbus makes the High-Power Trunk intrinsically safe.

We hope that the contents of this paper are helpful in your daily work or decision-making process. We look forward to hearing from you.

Table of Contents

1	Introduction and overview.....	2
2	The fieldbus infrastructure.....	2
2.1	System structure	2
2.2	The added value of digital communication	3
2.3	Technology and progress.....	4
2.4	Designing digital technologies	4
3	Availability considerations.....	5
3.1	Calculated availability	5
3.2	Observed availability.....	7
3.3	Methods for mitigating risks of failure	8
4	Fault statuses during normal operations	8
4.1	Typical Fault Scenarios	8
4.1.1	Direct low Ohm short circuits	9
4.1.2	Water ingress	9
4.1.3	Attaching and disconnecting a device	10
4.1.4	Vibration/Machine-induced intermittent faults	10
4.2	Fieldbus components and availability	11
4.2.1	Field device	11
4.2.2	Fieldbus power supply and DCS connection	11
4.2.3	Device coupler: FieldBarrier or Segment Protector.....	11
4.2.4	Device connection, cable at the spur	12
4.2.5	Trunk cable.....	12
4.3	Heuristic assessment of availability	13
4.3.1	Causes of malfunction	13
4.3.2	Solutions and components	14
4.4	Effectively increasing availability	14
5	Summary.....	16
6	Bibliography.....	16

1 Introduction and overview

In the field of process automation, fieldbus enables complete and integrated access to all information relating to instrumentation: measured values, configuration, and device diagnostics. Those who wish to use information from the field for proactive control of the system and for active management of maintenance rely on the digital fieldbus. There is a requirement for a detailed look at availability, particularly with regard to productivity and the now fully defined protocols for safety-related control systems.

In particular, the bus systems FOUNDATION Fieldbus H1 and PROFIBUS PA are characterized by, in some cases, exceptional improvements from generation to generation. The general advantages and the history of these somewhat revolutionary changes are described in chapter 2, The fieldbus infrastructure.

The mathematical examination of the service life and reliability of components is only a small step towards achieving high availability, but the reliability data of the instruments does not in itself produce the difference between good perfor-

mance and maximum reliability. Chapter 3, Availability considerations provides further details and prepares to disclose some questionable or just plain incorrect assumptions that we have come across in presentations and forums.

Practical experience with fieldbus and details of fault scenarios on the installation are described in chapter 4: Fault statuses during normal operations. The chapter describes a heuristic approach, raising awareness of how devices, handling, and ambient conditions can have an effect and at which point of the fieldbus installation, and how they can be influenced in terms of their probability of occurrence. This approach enables opportunities and risks to be dealt with in an appropriate way. Making fact-based decisions relating to application and design optimizes the fieldbus infrastructure in terms of costs and availability for the required application.

The authors are advocates of fieldbus and hope that this paper will provide you with the information you need.

2 The fieldbus infrastructure

2.1 System structure

Fieldbuses in process automation, in particular FOUNDATION Fieldbus H1 and PROFIBUS PA, digitalize signals on the last kilometer from the control room to the field device. Since compressed air control systems were replaced by analog data transmitters (4...20 mA) about 60 years ago, digital communication is the next step in the development process with complete data integration to the control system level. As with analog transmission of measured values, fieldbus transmits the data communication and power supply via a shielded twisted pair cable to up to 31 devices (realistically eight to 22). Various types of protection are used for installation in hazardous areas.

Fieldbus infrastructure consists of a power supply, cables, and marshaling cabinets. (Figure 1) Master cables, also known as trunks, lead from the control room to the marshaling cabinets that are installed in the field so that they are easily accessible to technicians. Spurs lead from the marshaling cabinets to the field devices.

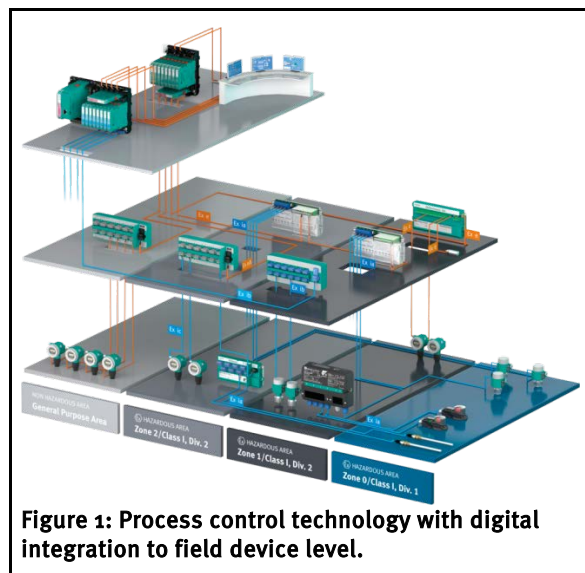


Figure 1: Process control technology with digital integration to field device level.

2.2 The added value of digital communication

Less instrumentation required: Instruments can transfer multiple measured values. A flow transmitter can simultaneously provide temperature and density. Measuring points can thus be saved. This data is transmitted in native form, i.e., without special engineering or configuration requirements.

Predictive maintenance: Instrumentation sends diagnostics data in addition to the measured values. Maintenance teams intervene less frequently and purposefully, and thus contribute to the overall availability of the system. This is due to better information, which makes cause and necessity transparent. This data transmission is part of the protocol definition and is carried out in parallel with the transmission of measured values. Access is simple, fast, and accurate from the control room; here, also, additional engineering is not required.

Remote parameterization: The parameterization of field devices can be adjusted from the safety of the control room. In the event of frequent product changes or other necessary adjustments, the settings are made quickly and efficiently. If a device needs to be replaced, the parameterization is imported from the control system.

The documentation of the process automation equipment is always up to date and available in the control system.

Digital communication transmits more information and with greater accuracy. The signal is converted from analog to digital only once in the instrument and transmitted at a very high resolution. In fact, the process is so accurate that two different instruments, such as two pressure transmitters, can be used for a differential measurement (Figure 2).

Space saving in the control room and in the field: Power supplies, each serving one segment with realistically eight to 22 devices, require space in the control cabinet. Compared to classic analog technology there is at least one wiring level not required, and thus a saving on costs for planning, purchasing, installation, and testing is achieved.

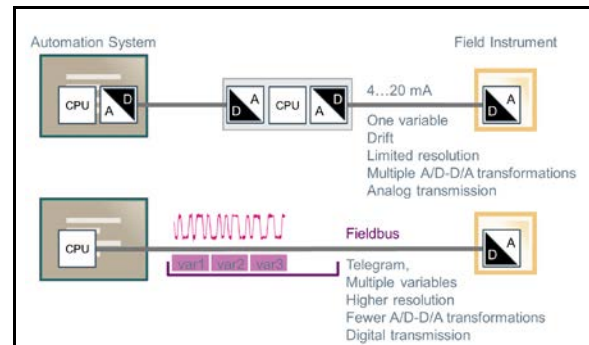


Figure 2: A comparison of analog and digital transmission of measured values.

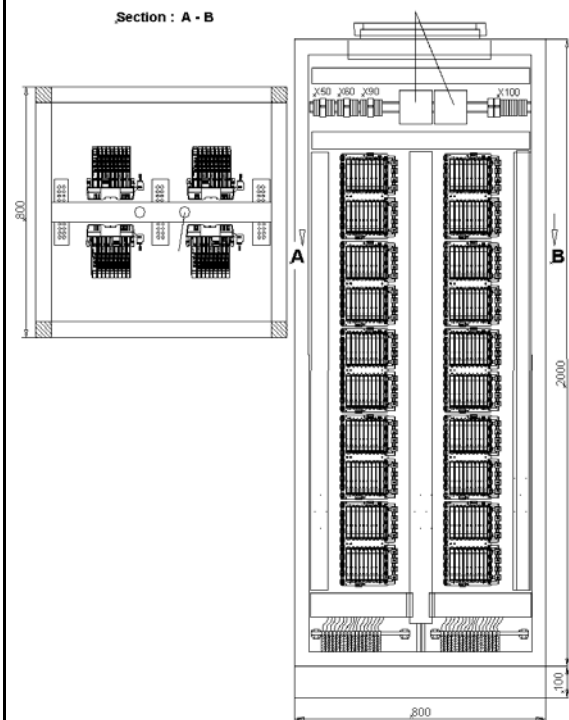


Figure 3: Control cabinet with space for up to 160 segments.

Figure 3 shows the design drawing for a typical control cabinet with fieldbus power supplies. Mechanically, there is space for up to 160 segments. The power supplies per square meter of surface area realistically supply about 100 segments, and thus between 800 and 2,200 field devices and control technology boards.

Faster go-live: Testing the physical layer in advance ensures communication with each individual device. The loop check is thus performed earlier and faster. A case study demonstrates significant savings in terms of the time and effort required for the loop check by fieldbus with diagnostics in [1].

Simple proof of explosion protection: Variants of the intrinsic safety type of ignition protection,

specially developed for fieldbus, provide proof of intrinsic safety without any calculations. A parts list with links to the certificates, as well as a few requirements that must be adhered to, are that proof. Examples of this include FISCO, the Fieldbus Intrinsically Safe Concept, and a special section in the standard IEC 60079 and DART Fieldbus. DART technology significantly increases the effective power of an intrinsically safe installation. DART Fieldbus is a solution developed by Pepperl+Fuchs and certified according to IEC 60079-11.

Safety-related data transmission with fieldbus is tested and used on a trial basis. Additional mechanisms in the protocol secure the transfer of process and security signals via the same cable without the need for additional hardware. The connection, including power supply, and barriers for explosion protection are not taken into consideration. Calculations, evidence, and testing can be realized more easily than is customary at present. Background information can be found in [2].

2.3 Technology and progress

Fieldbus achieves excellent availability of communication through the use of signals modulated to the supply voltage. The low data speed of 31.25 kbit/sec is more than sufficient for process signals. The data is transmitted not as a signal level, but as a transition between steady states (Figure 4). These very sharp events can be easily detected by the input modules, and are very resistant to interference.

In the early stages, the fieldbus cable was looped from field device to field device. Necessary work on a field device inevitably led to failure. Today, junction boxes, which contain installation components known as device couplers, with spurs, have become the de facto standard. Junction boxes with spurs create a clear design that is easy to install and maintain.

Device couplers with short circuit current limitation are the preferred method, so that work can take place on a device during ongoing operations without impairing the function of the segment. This short circuit protection has recently been enhanced with the addition of new technologies, resulting in fault protection that can detect and eliminate complex, dynamic faults that occur during practical usage (Figure 5). These faults include: contact bounce, short circuiting, and

opening, as well as “jabber”—excessive and unauthorized communication of a field device due to an internal fault.

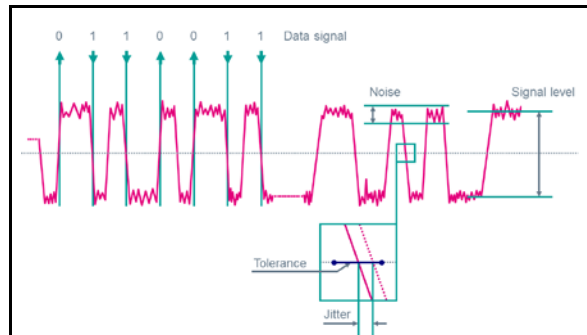


Figure 4: Digital signal: reliable transmission at high resolution and without drift.

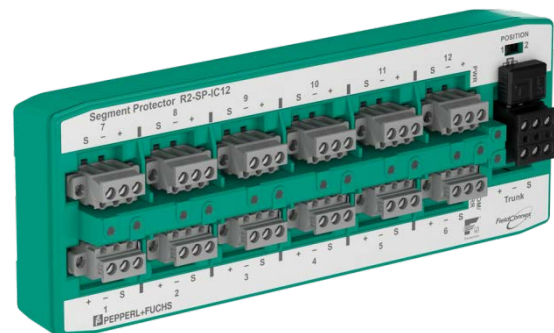


Figure 5: Segment Protector with modern fault protection and diagnostics at each output. Protects against the many possible causes of malfunction.

Routine monitoring of the installation is economically feasible with fieldbus. Signal noise, ground faults, and many other measured values from the fieldbus communication can be permanently monitored. The associated software evaluates the signals and interprets and translates them into relevant messages for maintenance teams. Using the diagnostics of the physical layer, causes can become visible before a failure occurs. [3]

2.4 Designing digital technologies

In addition to the simple measured value, planners, owners, operators, and maintenance personnel will receive additional information through digital communication to the field device. Information can be translated into higher availability on the one hand, and reduced maintenance effort on the other. The safety of personnel and equipment are also improved. Since communication of up to 31 components is controlled via one infrastructure, it must be ensured that this infrastructure can be operated with a very good level of availability.

3 Availability considerations

Availability calculations are always based on information, assumptions, and observations from the theory of probabilities. In many discussions we discover that results are derived from sometimes unrealistic, sometimes even just plain incorrect, assumptions. Their validity is doubtful to say the least.

To begin with, this chapter quotes various definitions of availability that are relevant to the practice of process automation. A thought experiment involving an unusual example illustrates the criteria that are used to produce a realistic assessment of availability. Based on this example, the discrepancy between theory and practice

becomes clear. The calculated values that are generally far too high do not correspond to the reality experienced in process automation. Finally, methods are discussed that have a positive impact on the availability of a system, if applied correctly.

3.1 Calculated availability

The following definitions can be found in the International Electrical Vocabulary (IEV) [4], which is also relevant for the creation and translation of standards. Here you will find 47 definitions under the term “availability.” The number given is the entry number in the IEV [4].

Table 1: Definitions according to the IEV

Name	Definition
191-02-05: Availability	The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.
191-11-01 Current availability	The probability that an item is in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided.
191-11-03 Mean availability $A(t_1, t_2)$	The mean of the instantaneous availability over a given time interval (t_1, t_2) Note – The mean availability is related to the instantaneous availability $A(t)$, as $\bar{A}(t_1, t_2) = \frac{1}{t_2 - t_1} * \int_{t_1}^{t_2} A(t) dt$
191-11-06 Stationary availability A	the mean of the instantaneous availability under steady-state conditions over a given time interval. Note – Under certain conditions, for instance constant failure rate and constant repair rate, the steady-state availability may be expressed by the ratio of the mean up time to the sum of the mean up time and mean down time. Under these conditions, asymptotic and steady-state availability are identical and are often simply referred to as “availability.”
191-12-07 Mean time to failure, MTTF	The expectation of the time to failure
191-11-12 Mean down time, MDT	The expectation of the down time
191-12-03: Mean failure rate, $\lambda(t_1, t_2)$	the mean of the instantaneous failure rate over a given time interval (t_1, t_2) Note – The mean failure rate relates to instantaneous failure rate $\lambda(t)$ as $\bar{\lambda}(t_1, t_2) = \frac{1}{t_2 - t_1} * \int_{t_1}^{t_2} \lambda(t) dt$

First, let us look at the following simple thought experiment: how high is the availability of the system shown in Figure 6. The answer can be determined visually and proves trivial: the availability is 50%. This is the value for stationary availability.

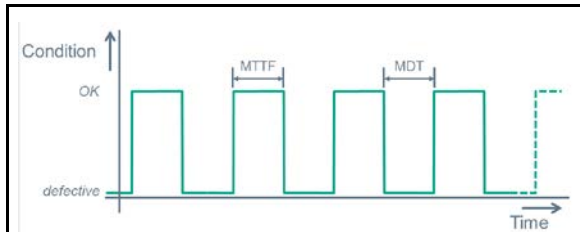


Figure 6: Availability of a system over time.

As shown in the comment under 191-11-05, stationary availability is also shortened to “availability.”

The availability assumed in the preceding example is confirmed with the calculation based on the following formula if $MTTF = MDT$:

$$A = \frac{MTTF}{MTTF + MDT} = 50\%$$

So that the calculated availability reflects the real situation, it is necessary to use realistic numerical values for the MTTF and the MDT. The reciprocal of the failure rate lambda is incorrectly used for the MTTF. This type of calculation provides a meaningless result, because the factors that influence the MTTF, such as ageing or wear, are disregarded. Likewise, the influences of the mode of operation and of the environment to which the respective component is exposed are ignored. This is illustrated by means of the following example:

Let us consider a human male in his role as worker and calculate his availability. To do this, the MTTF of the person must first be determined. According to the incorrect procedure described above, this is derived from the reciprocal of the failure rate in the flat section of the bathtub curve (Figure 8).

The human bathtub curve can be derived from the mortality tables of the Federal Republic of Germany. In the flat section (bottom area, are 31, see Table 2), the failure rate for men is 0.71375 per thousand. For the MTTF (inverse of lambda), the figure is therefore 1,401 years, or 72,800 weeks.



Figure 7: Availability of humans illustrates random and systematic failures.

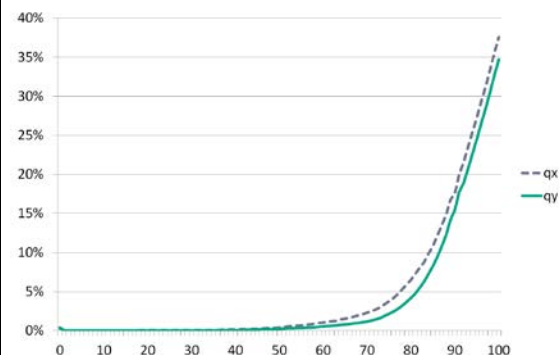


Figure 8: Bathtub curve of humans: Mortality rates 2011 of the Federal Republic of Germany [5].

Table 2: Extract from the mortality table of the Federal Republic of Germany 2011

Age	Px (male)	Py (female)
29	0.00065759	0.00028692
30	0.00063989	0.00028303
31	0.00071375	0.00030202
32	0.00073510	0.00035447
33	0.00076333	0.00036564

Based on the assumption that a replacement is found for a failed employee after six weeks, the availability is calculated as:

$$A = \frac{MTTF}{MTTF + MDT} = \frac{72,800}{72,800 + 6}$$

$$A = 0.99992 \text{ or } 99.992\%$$

3.2 Observed availability

In practice, significantly lower availability rates can be observed. Leave, sickness, doctor's visits, and business trips occur several times a year and are also causes of absence from the workplace. Assuming a failure will take place twice a year on average and the downtime is an average of two weeks in these cases, the result is an availability of:

$$A = \frac{MTTF}{MTTF + MDT} = \frac{26}{26 + 2} = 92.9\%$$

This value is realistic, i.e., it corresponds to actual observation in practice. The theoretical value calculated initially is simply incorrect, since the reciprocal of the failure rate was used for the MTTF, and this value does not represent the mean time to failure in real-life systems.

To correctly determine availability, two essential questions must realistically be answered: 1. How long does a system function on average without failing and 2. How long is the system down in the event of a failure? Based on these two responses, it is possible to calculate a realistic value for availability quickly and easily based on the above formula.

If the objective is a high level of availability, measures must be taken to extend the mean time to failure. To achieve this, you must first ask what the reason for the system failure is. Experience shows that randomly occurring equipment defects are rarely the cause of a system failure. In most cases, there are systematic faults arising from the application and environment, such as incorrect dimensioning, harsh ambient conditions, faults during maintenance and repair, ageing, corrosion, or wear, that lead to system failure.

Applied to automation technology, a higher level of availability is therefore primarily achieved by avoiding or overcoming the aforementioned systematic faults. As shown below, this can be achieved with particular ease by designing equipment that copes with systematic faults without a malfunction, or at least limits them locally to one instrument. Although devices with a lower failure rate produce better results in the case of the incorrect availability calculation first described, the availability observed in practice does not change. This availability improves only when the true causes of the failure are rectified or controlled, or at least their effects are limited.

Note: In the references, the MTBF is sometimes also used to calculate the availability, because the terms "MTTF" and "MTBF" are often used synonymously. Based on the above, this changes nothing, in principle.

It is important to bear two factors in mind when using technical devices. They are failures due to:

- The device itself because of random failures that are quantified with the failure rate; or
- The application and ambient conditions caused by systematic faults as described above, which could be avoided.

A glance at the alarm lists and failure statistics for process automation shows that influencing factors arising from the application and ambient conditions are much more likely causes than a random equipment failure. As part of a long-term project, the Pepperl+Fuchs experts studied fault statuses, their causes and effects on the fieldbus infrastructure. Risks arising from the application and ambient conditions are summarized below:

- Poor design of segments
- Faults in the installation
- Contact bounce through work on devices
- Moisture ingress
- Lightning strikes
- Ground faults

To determine realistic MTTF and MDT values for a fieldbus segment or process system, it is important to evaluate whether the devices can withstand the treatment and external influences to which they are exposed. These cause failures far more frequently than equipment defects involving components.

3.3 Methods for mitigating risks of failure

Systematically, there are four methods to protect against a component or part of a system failing. They include:

1. Preventive measures and standard operating procedures: External influences can often be reduced through knowledge and correct use of the technology.
2. Predictive, automated handling of faults: Technologies and components are used that can detect and isolate a fault. The effect of the fault is limited to the extent that the system remains in operation. An example would be the shutdown of a field device connection in the event of a short circuit. The fault is limited locally. The fieldbus segment will continue to function unaffected. The failure of a measuring point is usually tolerable.
3. Diagnostics: Monitoring detects a deviation in the current status from the best possible status and generates a message in the control room. Proactive intervention can rectify this status before it has a negative effect on the overall function. An example of this would be measuring the frequency of level sensors using a vibration fork. A change indicates that the sensor has become jammed, or measuring ground faults at a fieldbus segment. In the

case of single-pole ground faults, the effect of electromagnetic interference increases. This information can be used to plan maintenance work.

4. Redundancy: Redundancy protects against faults where the device itself is the cause, where these faults cannot be tolerated and must be controlled, power supplies and DCS interfaces, for example. Field devices are often configured in redundant design where the measuring circuit is required to have a very high level of availability.

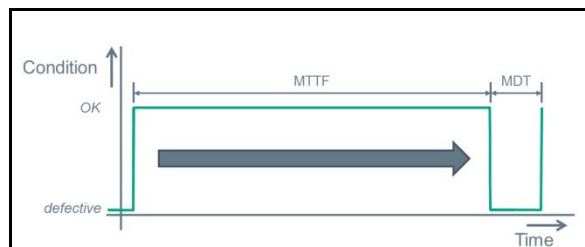


Figure 9: System status, qualitative representation. The MTTF must be maximized using appropriate measures.

Looking at the failure rate of devices and components alone produces meaningless results. It is possible to evaluate relevant fault statuses for system operation through a qualitative analysis of possible fault statuses with regard to individual components. This is much faster and explained in the following chapter.

4 Fault statuses during normal operations

All of the above methods are available to the operator and planner. Manufacturers provide the core building blocks with redundancy or diagnostic functions.

This chapter describes many of the causes identified by Pepperl+Fuchs that can lead to a segment failure if they remain undetected. These cases, taken from real-life operations, can occur on an ongoing basis or very sporadically. Proactive handling and elimination by the fieldbus infrastructure are possible in many cases. Other faults are identified through messages in the control room, enabling maintenance personnel to deal with the fault in a targeted manner according to demand.

The following section comes from the Technical White Paper “Advanced Failure Protection by Fieldbus Device Couplers” by Gunther Rogoll and

Ren Kitchener, which illustrates possible technical solutions for handling failures [7].

4.1 Typical Fault Scenarios

Spur faults discovered over the years have been known to cause the failure of a working segment even when fitted with typical spur short-circuit protection. Tests to replicate the failures in real applications have shown that the potential is real and fairly repeatable.

4.1.1 Direct low Ohm short circuits

Direct low Ohm short-circuit faults are commonly seen where a spur cable is cut, or where a ground fault exists on one pole, and the other pole is shorted to ground. They are also commonly seen where spur wires are drawn through electrical housings while removing the device for repair or calibration (although this often leads to a very noisy intermittent fault).

With a single clean “make” the spur protection system will react very quickly to isolate the spur where only one telegram will be affected (Figure 10).

4.1.2 Water ingress

Instrument housing water ingress is a failure that has been reported on more than one occasion. Replicating this in the laboratory revealed that the conventional short-circuit protection systems behave unpredictably at certain conductivity levels due to the dynamic impedance of water, which can rapidly change in conductivity.

With increasing conductivity between the wires at the spur, the wiring block with short-circuit protection increases the impedance of the output to prevent an overload condition on the trunk. This, in turn, dampens the communication signals (Figure 11).

Oscillation sometimes occurs when a fault current is at or marginally above the current limit set point, and the electronic circuit is just barely operating. At this point, the voltage to the fault decreases with a resulting decrease in current, turning off the current-limiting circuit. This cycle continues quite rapidly and can be amplified when a device is transmitting at the same time. The reaction during this narrow transition point can be unpredictable. Not every fault behaves in a repeatable way. For example, water’s impedance can be very nonlinear versus voltage or current, where this further varies with temperature and conductivity.

Also, water ingress can lead to mechanical failures such as irreversible corrosion damage to electronics, terminals, or cable parts (Figure 12).

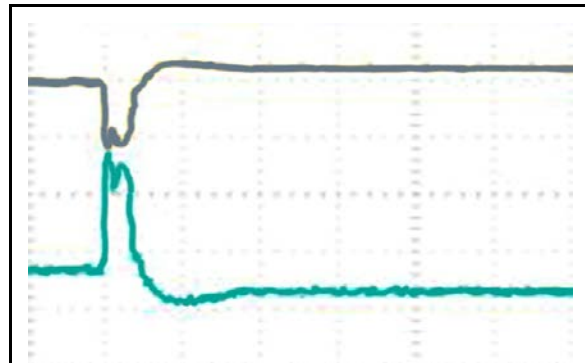


Figure 10: Fault measurement on the trunk due to a clean short circuit. The short-circuit protection circuit isolates the spur by switching off the current.

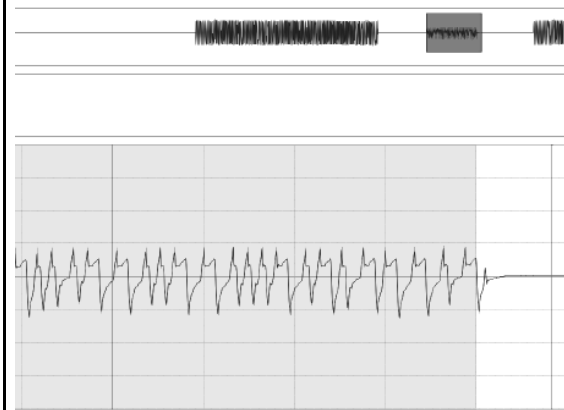


Figure 11: Oscilloscope trace showing a heavily distorted communication signal due to current draw near the short current limit, caused by water conductivity.



Figure 12: Corrosion of terminal arrangement in a transmitter housing due to water penetration.

One example shows the seriousness of the fault scenario: A field instrument with an active backup LAS loses communication to a host installed in the control room, due to the low communication signal during a progressive fault occurrence. The backup LAS activates while the host LAS remains active. At this point, field instruments on normally operating spurs still “see” the back-

up LAS, which is nearby, as well as the host. With two active LASs on the segment, communication clashes, and the segment fails.

4.1.3 Attaching and disconnecting a device

The use of device connectors is a safe way to connect a device without the possibility of shorting the wires; however, make or break must be done swiftly. Inserting the connector slowly may lead to systematically connecting and disconnecting the device over a one-second period or longer (Figure 13).

This type of fault is seen with loose connections, drawing cable through electrical housings with loose strands of copper making contact with other connections, connectors, and device electronic failure or faults (Figure 15).

This connection chatter or contact bounce severely disrupts communication, even with electronic short-circuit protection, due to the current being below the trip threshold to the point of segment failure (Figure 16).

4.1.4 Vibration/Machine-induced intermittent faults

In some cases, high-frequency mechanical vibration can cause a loose or poor contact to make and break or even loosen a terminal. This repeated interruption will cause the segment to fail if it is not isolated immediately (Figure 16).

In one case, the device was the cause of a vibration-induced fault, where the printed circuit board connection to the terminal contained a “dry joint” which was not easy to see without taking the instrument apart.

Industrial equipment for process industries is mostly designed to be installed in environments where vibration with a frequency of up to 150 Hz could occur.

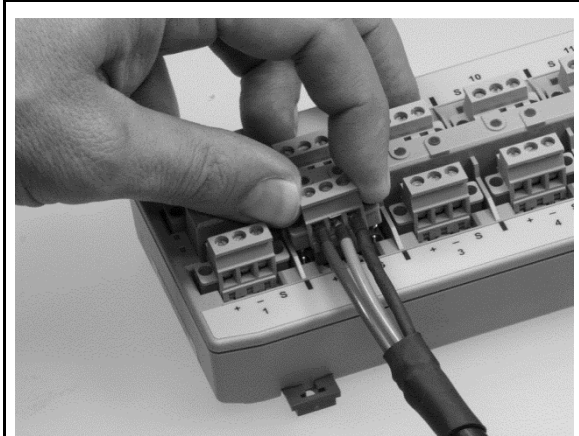


Figure 13: Contact bounce can be avoided when pulling the plug in the junction box.

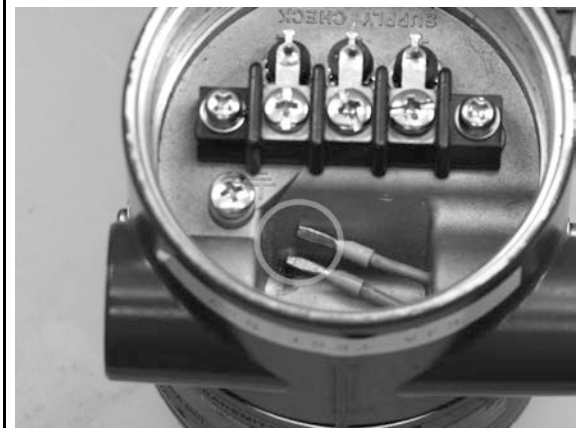


Figure 14: Example of the spur poles shorting through the terminal housing while the wires are being withdrawn.

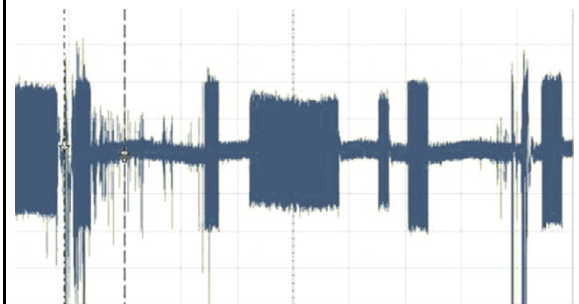


Figure 15: Voltage spikes caused by spur poles shorting through the terminal housing while the wires are being withdrawn.

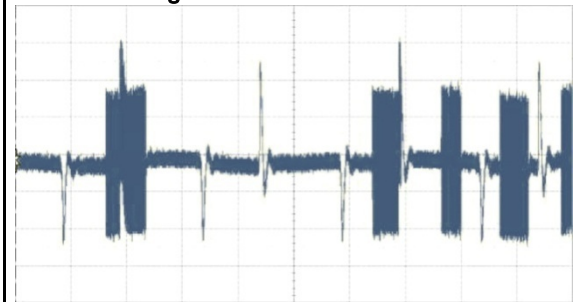


Figure 16: Vibration induced voltage spikes.

4.2 Fieldbus components and availability

This section describes the individual components of the fieldbus infrastructure in terms of availability, and summarizes the results of the studies. The four alternatives for influencing availability are described.

4.2.1 Field device

Aside from the DCS controller, the field device is the essential element in the transmission chain in terms of function. Because of the high levels of stress caused by the application, e.g., environmental factors, temperature, water, aggressive media, and lightning, it is the weakest link in the chain. All field device variants provide diagnostic functions that can detect the typical faults.

The field device is critical for the availability of the automation loop. Depending on the product and complexity, the MTTF is between 30 and 300 years. The range of the MTTF clearly shows that redundant design can have a positive impact on availability, depending on the type of device.

Figure 17 shows two principal options for implementing device redundancy. In version 1, each instrument is connected to a separate device coupler. In version 2, the two instruments are connected to two separate segments. In the latter case, device redundancy increases overall availability. The fieldbus infrastructure works also redundantly even if it is set up simplex.

4.2.2 Fieldbus power supply and DCS connection

Fieldbus power supplies consist of motherboards, usually equipped with passive components and demonstrating very low failure rates. The electronics are located in one or more plug-in modules. Since the fieldbus power supply supplies between five and 20 devices—according to the segment design—redundancy can also have a positive effect here.

With the single-channel version, the smallest possible unit is replaced in the event of redundancy—the power supply module for a channel. This design results in the lowest costs in terms of the spares inventory and replacement.

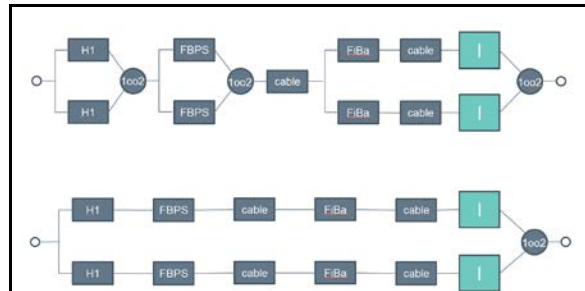


Figure 17: Topologies for device redundancy.

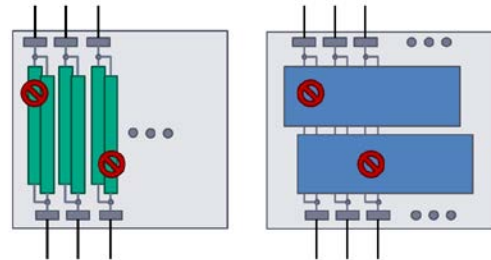


Figure 18: Fieldbus power supply with single segment block power modules.

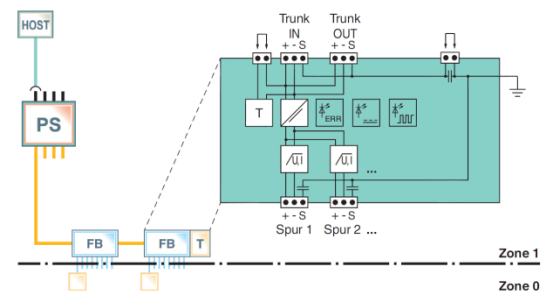


Figure 19: Simplified diagram of the FieldConnex FieldBarrier. Each output is equipped with modern fault and short circuit protection.

In multi-channel power supplies within a housing, a redundant configuration can result in a very unpleasant situation whereby channel x in module A and channel y in module B fail at the same time. In this case, replacement invariably involves shutting down a segment (Figure 18).

4.2.3 Device coupler: FieldBarrier or Segment Protector

Between four and 12 field devices are connected to the outputs on the device coupler. The majority of device couplers monitor the output for faults and switch it off to protect the segment (Figure 19). Modern day fault protection as offered by selected FieldConnex® components protect from the systematic causes of segment failure as described in section 4.1,

Device couplers from well-respected manufacturers are typically approved for hazardous areas and have oversized components according to

regulations. These are the main reasons for the very low failure rate of the device coupler.

Electronics, output and spur connection are comparable to any type of point-to-point connection with regards to failure. Redundancy is an unnecessary cost.

4.2.4 Device connection, cable at the spur

Similarly, the connection from the device coupler to an individual device is simplex by design. Cables and connections are highly reliable (see discussion on trunk cables below) so redundancy is not necessary.

4.2.5 Trunk cable

The trunk supplies all devices connected to the segment. Installation takes place in cable trays that provide good protection for the cable. Access to the trunk cable is not necessary in normal day-to-day operation. Cables are well protected in terms of compliance with the installation rules. They include:

- Separate cable trays for communication and power cable (Figure 20); and
- Minimum clearance within a tray.

For installations outdoors, there should be protection against weather-related environmental factors such as temperature, humidity, and UV radiation. Cables installed below ground should be installed in a plastic tube to provide protection against mechanical damage.

To protect against explosions, the trunk is installed with protection. According to standard [6], protection must be provided against inadvertent opening of a current circuit as a result of:

- Mechanical damage
- Reaction caused by chemicals
- Corrosion and water
- Accidental human intervention
- Temperature effects

These regulations are associated with the “increased safety Ex e” type of ignition protection attributed to the FieldBarrier and the cable glands on the housing.

Thanks to these installation requirements, the trunk resists external influences very well as there are no failure modes.



Figure 20: Fieldbus installation in cable trays.

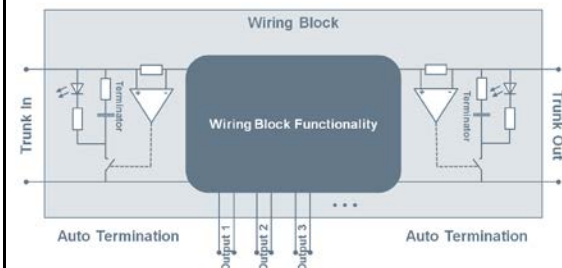


Figure 21: Principle diagram of a device coupler supported by redundant trunk connections. Additional electronics are necessary to achieve automatic switchover and termination.

A redundant version of the cable requires:

- A switchover at each end of the trunk and at each device coupler output;
- Automatic bus termination with electronic monitoring, twice per coupler; and
- Routing of cables in separate trays.

In addition to extensive installation work, trunk cable redundancy requires increased effort in terms of the electronics. This is counterproductive for availability. Only two fatal and very rare failure modes are covered by the redundancy:

- Manual intervention, which is very rarely necessary; and
- The fatal inadvertent opening of the current circuit in hazardous areas.

4.3 Heuristic assessment of availability

4.3.1 Causes of malfunction

The tool described in this section for assessing availability is derived from the FMEA analysis: all possible and conceivable causes of failure are weighted and allocated to possible solutions. The technical solution with the highest classification number offers the best protection. The causes of malfunction are evaluated according to two classification numbers. These figures illustrate the impact (I) and the frequency (F). The product of the two figures determines the risk (R) of this cause of malfunction.

For example, the following causes of malfunction can occur on a cable: hard short circuits, opening loose contacts due to vibration, short-circuiting loose contacts when pulling the cable through a cable gland, or creeping short circuits caused by water ingress. The faults are normally rare, with the ingress of water considered very rare. Work frequently takes place while the device is running. All faults lead to a failure of the segment

without intervention and are, therefore, classified as serious.

Table 3: Cause of malfunction	I	F	R
Hard short circuit	4	2	8
Opening loose contact due to vibration	4	2	8
Short-circuiting loose contact when pulling the cable through a cable gland	4	4	16
Creeping short circuit due to water ingress	4	1	4

The short-circuiting loose contact poses a significantly higher level of risk. A work instruction could provide a possible solution, for example: “Before removing the field device, the fieldbus lines must be isolated.” This is an instruction that may be frequently ignored in the hustle and bustle of daily operations or is ignored by professionals with limited fieldbus experience.

Curiosity of an availability calculation for cables

In an attempt to justify the redundancy of the trunk, we discovered a case study with an MTTF of 75 years—as high (or low) as a very complex field device. Such an assumption cannot be plausible for the reasons stated. The consequence of this would be: with 75 installed cables, there would be one cable defect per year—or with an average of 1,000 installed lines, more than one cable fault per month! The authors found this absurd.

We only consider an unnecessarily elevated fault rate due to careless mistakes or lack of installation knowledge as possible justifications, for example, as a result of:

- Insufficient or missing seals
- Incorrect tightening torque at cable glands
- Incorrectly mounted cable glands
- Poor EMC due to routing of data and power cables in a single tray
- Materials unsuitable for the location

Installation faults can result from the high cost pressure and deadline constraints placed on suppliers and installers. All of the causes referred to above can be significantly reduced through the following measures:

1. Training employees on special features in dealing with a fieldbus installation (approx. one day).
2. Network Acceptance Tests (NAT)—automates fieldbus infrastructure checks after installation, as well as each time the segment is accessed, for example, due to maintenance work on an instrument.

Rest assured: Practical studies show the occasional installation fault that is detected and rectified by the NAT. Installation with monitoring of the physical layer results in very high availability. Diagnostics is shown to have a significantly higher impact on availability than cable redundancy. The method explained below provides a plausibility.

4.3.2 Solutions and components

All technical solutions, components including their characteristics for fault handling, redundancy, and diagnostics are listed in columns. Causes are assigned to the components under two conditions: 1. The component handles the cause, and 2. The availability of the system is maintained.

The accumulation of all assigned risk indicators shows which component or solution can handle most causes of malfunctions. An assessment of the risks allows a comparison of cost and effort.

For example, fieldbus couplers with various technical characteristics are available for the fieldbus installation: a junction box with a single row of terminals and without short circuit current limitation, a Segment Protector with simple short circuit protection, a Segment Protector with fault handling and diagnostics, or a device coupler with redundancy.

Table 4 shows the assignment of the causes of malfunctions to the proposed technical solutions.

The Segment Protector with diagnostics is able to handle most causes of malfunctions and gets the highest score. The decision in favor of a specific technology is made after estimating the additional costs and the effort needed for the installation, shows possible causes, and links them to technical solutions currently available.

A complete sheet with possible causes of failure and known solutions is shown in Table 5 on page 15: a column I available for own interpretations and further measures to mitigate the respective risk.

A decision for a particular technology follows the evaluation based on an optimum of protection from intolerable causes of failures and estimation of costs. Costs are incurred for establishing standard operating procedures, training and components, including installation cost.

Table 4: Correlation between cause of malfunction and possible protection functions

Cause of failure	Impact	Frequency	Risk	Junction box	Segment Protector	Segment Protector with diagnostics SP	Device coupler with redundancy
Hard short circuit	4	2	8	0	8	8	8
Opening contact bounce	4	2	8	0	0	8	0
Short-circuiting contact bounce	4	4	16	0	0	16	0
Creeping short circuit condition	4	1	4	0	0	5	0
Total:				0	8	37	8

4.4 Effectively increasing availability

The White Paper quoted in chapter 4.1, "Typical Fault Scenarios," describes, in detail, potential solutions and product concepts that are able to control the faults listed in the event of the aforementioned possible fault scenarios. Com-

ponents intervene proactively where temporary faults occur, or report signs of possible causes of malfunctions to the control room. Targeted, proactive intervention by the maintenance team is based on detailed and reliable information on the physical layer and leads to higher availability of automation.

Fieldbus and availability: Causes of failure - risk and protection

Fieldbus and availability: Causes of failure - risk and protection																			
Cause of failure	Protecting component																		Comments, own thoughts, other strategies
	Performance indicator																		
	I	F	R	0	64	0	32	0	32	144	8	0	0	32	40	64	144	192	
Components																			
Fault in power supply electronics	3	3	64	1															
Fault in device coupler: Electronics at the spur	1	2	8								1								
Instrument fault due to external influences	2	3	32											1	1				
Instrument fault due to failure of electronics	2	1	8												1				
General Installation																			
Termination incorrect	1	3	16																
Electromagnetic interference	3	4	128																
Failure of surge protectors	3	3	64													1	1	1	
Wiring at the trunk																			
Interruption, e.g., due to cable damage (short-circuit or open circuit)	3	1	16																
Opening contact bounce, e.g., due to vibration	3	1	16																
Short-circuiting contact bounce	3	1	16																
Creeping overload, e.g., due to corrosion or moisture	3	1	16																
Wiring at the spur or field instrument																			
Solid short circuit	2	3	32																
Opening contact bounce, e.g., due to vibration	2	3	32																
Short-circuiting contact bounce, e.g. live maintenance at a device	2	4	64																
Creeping overload, e.g., due to corrosion or moisture	2	2	16																
(This line is intentionally not used. Please add additional lines as required above.)																			
Notes:																			
1 Check the impact and frequency fields to reflect your assessment of risk																			
2 Add or edit any field "in the grid" above.																			
3 Place a "1" where the measure listed in columns mitigates the risk listed in rows																			
4 Check for duplicates, e.g., where a risk is controlled by multiple measures																			
5 Select the measures that control risk																			
6 Start with highest performance indicators																			
Separate evaluation of monitoring and control loops can be beneficial.																			
Explanation																			
Impact, I																			
Very little, operation not in jeopardy (up to \$1,000.00 per incident)																			
Additional damage (up to \$10,000.00 per incident)																			
Serious damage (up to \$100,000.00 per incident)																			
Huge damage (up to \$1,000,000.00 per incident)																			
Frequency, F																			
Very seldom (you may have heard about it)																			
Very infrequent (one time in 100 years)																			
Infrequent (one time in ten years)																			
Frequent (one time per year)																			
Very frequent (ten times per year)																			
Risk Indicator = 2 * Impact * 2 * frequency																			
Actually, the product should be applied with impact and frequency to the power of ten; however, this would create unnecessarily large risk and performance indicators with no additional insight.																			

Table 5: Example evaluation of cause and effect.

5 Summary

This article explains and comments on the history and the technical improvements of fieldbus installations over the last two decades. It illustrates why the calculated, stationary availability and the availability observed in practice are not at all comparable. Distinguishing between failures caused by the component and failures caused by handling of the component and the ambient conditions shows that the latter is responsible for the large discrepancy.

An FMEA analysis shows the relationships between causes of malfunctions and solutions for mitigation and establishes the relationship between the two. Based on this analysis, the system planner and operator receive a clear overview of these relationships and of the potential for improvement, allowing them to weigh up various technical solutions. Based on this simple conceptual model, objective and focused decisions can be made to achieve a specific availability.

The influence of the electronic component on the availability of a fieldbus segment is minimal. That is why manufacturers offer diagnostic functions that signal systematic faults such as wear or failure before the effects become critical to the process. Diagnostics and monitoring ultimately ensure visibility of the numerous faults that oc-

cur and allow active intervention for rectification and maintenance purposes. As a concept, diagnostics is better than redundancy.

The analysis tool described above provides the reasons for the business success of FieldConnex® Advanced Diagnostics for the physical layer as it provides remedy for many of the causes of failure. This is because the diagnostics of the physical layer has uncovered many of the fault sources and causes of malfunctions discussed here. Fieldbus diagnostics and the new fieldbus components, capable of eliminating errors, enable users to reliably control fieldbus and to take advantage of an integrated solution for measurement data, remote configuration, and diagnostics.

By making reasonable decisions, the operator is the main contributor when it comes to achieving the specified availability. Decisions concern:

- Predictive automatic fault handling;
- Diagnostics for monitoring device status and physical layers;
- Preventive measures, procedural instructions, and training; and
- Redundancy where it works conceptually.

6 Bibliography

- | | |
|--|--|
| <p>[1] Fieldbus Testing with Online Physical Layer Diagnostics, Gunther Rogoll and Ren Kitchener, TDOCT-1107B, available as a publication from Pepperl+Fuchs, order number: 198636</p> <p>[2] Sicherheitsgerichtete Steuerung über den Feldbus [Safety-related control system via the fieldbus], Armin Beck and Andreas Hennecke, conference volume, VDI Automation 2009, available in electronic form from Pepperl+Fuchs</p> <p>[3] Advanced Online Physical Layer Diagnostics, Gunther Rogoll and Ren Kitchener, TDOCT-0995B_USA,, available as a publication from Pepperl+Fuchs, order number: 198641</p> | <p>[4] Electropedia: The World's Online Electrotechnical Vocabulary by the International Electrotechnical Commission http://www.electrical-dictionary.org/</p> <p>[5] Sterbetafel der Bundesrepublik Deutschland [Mortality table of the Federal Republic of Germany 2011]. Source: Federal Statistical Office, Federal Republic of Germany https://www.destatis.de/</p> <p>[6] IEC 60079-14: Explosive atmospheres—Electrical installations design, selection and erection</p> <p>[7] Advanced Failure Prevention by Fieldbus Device Couplers, Gunther Rogoll and Ren Kitchener, TDOCT-2860_EN available from www.pepperl-fuchs.com</p> |
|--|--|

- intentionally left blank -

YOUR DEMAND. OUR CHALLENGE.

PROCESS INTERFACES

- Isolated Barriers
- Zener Barriers
- Signal Conditioners
- Fieldbus Infrastructure
- Remote I/O Systems
- HART Interface Solutions
- Level Measurement
- Purge+Pressurization Systems
- Industrial Monitors+HMI Solutions
- Corrosion Monitoring
- Separator Alarm Systems
- Explosion Protection Equipment

INDUSTRIAL SENSORS

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- AS-Interface
- Identification Systems
- Logic Control Units

