CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648103

Modern Safety Diagnostics

Andy Crossland[a], Sven Lohmann*[b]

[a]Emerson Process Management, Leicester, UK
[b]Emerson Process Management, Haan, Germany
sven.lohmann@emerson.com

HART capable devices and their potential for the improvement of the performance of production plants in the processing industry has long time been a very underestimated and misunderstood topic. This contribution shows the benefits of diagnostics in general and particularly when used in combination with the HART protocol to transmit diagnostic data within the safety instrumented system. The argument is supported by an analysis carried out using the tool exSILentia for the calculation of the probability of failure on demand for example safety loops. This leads to the conclusion that the use of diagnostic data can increase a plant's safety and reduce unnecessary downtime.

1. Introduction

Many instruments are connected to a hand-held communicator for a short time when they arrive new from the supplier, to setup and calibrate the device. Then they are sent to a lifetime of isolation in the plant, never again exploiting their ability to communicate at a higher level than the simple 4-20 mA representation of their designated process variable. Companies in the processing industry are now seeing significant benefits from a strategic decision to employ HART communications connecting instruments in the field to online asset management systems.

HART communications is a means to manage the instrument's life cycle and to transmit status information to the overlaying safety instrumented system (SIS). SIS do nothing, most of the time. Nonetheless, 100% dependability is expected when something goes wrong in the process. Diagnostics is a crucial means to achieve this goal. If not by the means of diagnostics, how do we know the safety functions will work when needed?

The incorporation of diagnostic information into the safety logics can on the one hand help improve the safety integrity of the safety loop and on the other hand increase the uptime of the plant by uncovering nuisance trip conditions before they affect pant operation. Hence, the here presented approach contributes likewise to plant productivity and safety.

It is commonly assumed that productivity and safety are conflicting requirements, where promoting one will automatically demote the other. This is not necessarily true. The car's airbag is an example where both requirements persist simultaneously – they are both self-evident. Clearly a nuisance trip of an airbag may lead to disaster, as well as its failure to function reliably when needed. Both requirements need to be fulfilled adequately and simultaneously for processing plants just as they are fulfilled for airbags. Modern safety instrumented systems (SIS) can be used to live up to these heightened expectations.

It should be noted that HART is not a safety-rated platform. HART signals should never be substituted for hardwired signals when the hardwired signal is being used to detect a hazardous condition with a SIL rating. HART should only be used for diagnostic purposes.

2. Contribution of diagnostics to device reliability

The tool exSILentia (developed by Exida) is used to model example safety functions. Various options can be selected regarding the diagnostics within the tool. This requires experience and judgement so that all decisions and choices can be justified.

Please cite this article as: Lohmann S., Crosland A., 2016, Modern safety diagnostics, Chemical Engineering Transactions, 48, 613-618
DOI:10.3303/CET1648103

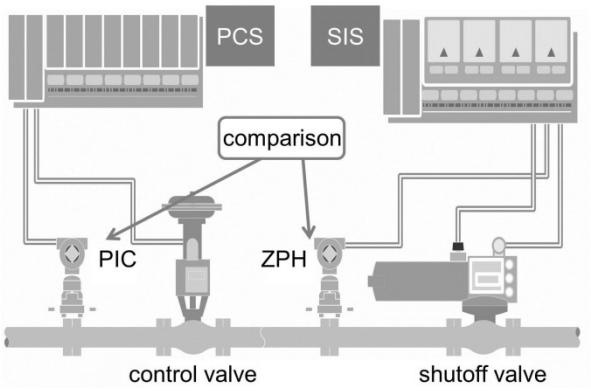

Figure 1: Two examples for the utilization of the HART protocol in safety applications.

Figure 1 illustrates a common setup. There is one transmitter used by the basic process control system (BPCS) as the input to a regulatory control scheme, and a separate transmitter for the safety function. Even if there aren't separate transmitters, other signals may perhaps be correlated with the measured safety parameter.
A change in valve position should cause an expected change in flow rate. External comparison can therefore be used to detect potential failures of the safety function's sensor.
In the analysis, two example safety instrumented functions (SIF) as shown in Figure 2 are employed. Each SIF is analysed first employing external comparison to diagnose failures and the second without external comparison modeling that no diagnostics are used.
Additionally, a diagnostic coverage (DC) factor for the external comparison must be chosen. Assuming that comparison with a similar device in the same location is possible a relatively high diagnostic coverage factor of 90% was allocated. This DC is comparable to the DC for SIL-rated devices (see Table 3).
The first example SIF shown in Figure 2 (left) has a single pressure sensor, which causes two valves to close on demand, isolating the source of excess pressure; the valves are voted in a 1oo2 configuration – either valve closing seals the pipe. The model uses data for generic devices. The proof test intervals (PTI) chosen for the devices are: sensor - 24 months; logic unit – 36 months; valves – 12 months.
The exSILentia tool produces a number of different reports for each SIF, giving details of each analysis and the results. Data from these reports is listed in Table 1.

Table 1: Analysis of sensor diagnostics - obtained with exSILentia.

SIF performance	Diagnostics OFF	Diagnostics ON
Achieved SIL	1	2
PFDavg	1.05E-02	2.91E-03
Achieved RRF	95	343
Contribution to PFDavg: sensor(s)	80.83%	30.57%
Contribution to PFDavg: logic unit	0.20%	0.72%
Contribution to PFDavg: final element(s)	18.97%	68.71%
SIL (PFDavg)	1	2
SIL (Arch. Constraints IEC 61508:2000)	1	2

It can be observed that without diagnostics (column: Diagnostics OFF), the sensor is a major contributor to overall probability of failure on demand (PFDavg), much higher than might be expected. With diagnostics (column: Diagnostics ON) a more balanced picture can be observed with the sensor around 1/3 of the overall total.
To assess the SIL target the design process is briefly summarized in the following. Three design criteria must be fulfilled: I) Systematic integrity: A measure of how well the potential people errors are taken care of in the manufacture of each device. Every certified SIS component is designed with a certain safety integrity level

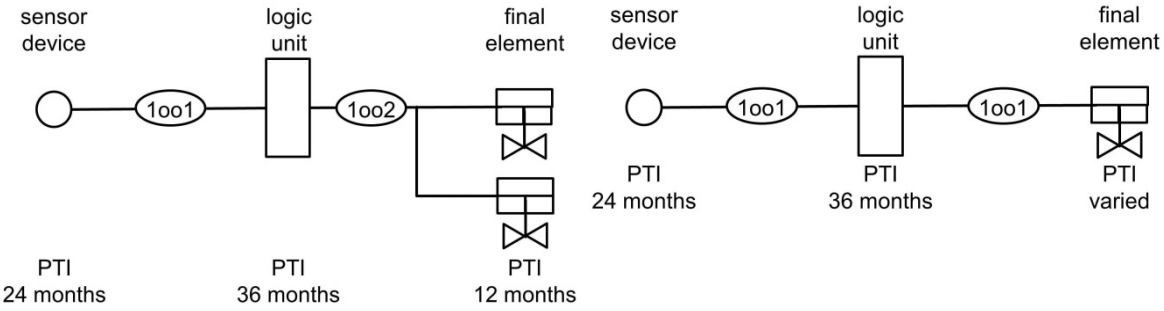

Figure 2: Example safety functions for sensor analysis (left) and valve analysis (right).

in mind. The IEC 61508 standard has rules and requirements for both hardware and software design, and control of the production processes which get increasingly difficult to achieve as the SIL level increases. The standards also present options and requirements for a formal prior use justification, if certified devices are not selected. The systematic integrity of the overall SIF is governed by the lowest systematic integrity level of all components in the SIF; II) Architectural constraints: Applying hardware fault tolerance (HFT) in line with the standards. This is a complex topic and the standards offer many routes to compliance which is not discussed in detail here. However, one common route is to assess the safe failure fraction (SFF) of each device, and as mentioned earlier, diagnostic coverage is an important factor. III) Random failures: the PFDavg figure is evaluated based on dangerous undetected failures (λ_{DU}) of each element and of the complete safety loop.

Table 1 also shows the results of the analysis from exSILentia looking at both PFDavg and Architectural Constraints. The systematic integrity was not evaluated using the tool in this example, since only generic device data was used. It can be seen that without diagnostics, the SIF is only suitable for SIL1. The analysis fails to reach SIL2 on both PFDavg and on Architectural Constraints. Bringing in the diagnostic of an external comparison moves the safety function from SIL1 capable to SIL2 capable, both in terms of PFDavg and in terms of architectural constraints. This is because the increased diagnostic coverage improves also the safe failure fraction, which means that SIL2 can be achieved even with a single device (HFT = 0), according to the IEC 61508 tables (the chosen method).

With the second example SIF shown in Figure 2 (right), the effects of partial stroke testing (PST) on safety integrity level and on required proof test interval (PTI) were modelled.

PTI is a factor in the PFDavg calculation. Testing more often reduces the probability of failure on demand. The problem is, proof testing a safety valve usually causes a process shutdown, since that is what it is designed to do! So operators of continuous processes want to extend the PTI as long as possible. Valves are also often expensive devices to install and maintain, and if the SIL verification analysis determines that a second valve is required to achieve the target SIL Level, this can be unpopular! The options are; more frequent proof testing, or perhaps increased diagnostics.

The same safety function with two different proof test intervals (1 year and 3 years) was analysed, and in each case with and without PST. As the data indicates, the valve is the main contributor to overall PFDavg in this safety function, but to varying degrees.

Table 2: Analysis of valve (final element) diagnostics - obtained with exSILentia.

SIF performance	PST OFF PTI = 12 MM	PST ON PTI = 12 MM	PST OFF PTI = 36 MM	PST ON PTI = 36 MM
Achieved SIL	1	2	1	2
PFDavg	1.81E-02	5.91E-03	3.43E-02	9.84E-03
Achieved RRF	55	169	29	102
Contribution to PFDavg: final element(s)	95%	84%	97%	90%

This time the safety function has a single sensor and a single valve. Once again, generic devices have been used. Table 2 summarises the results of the exSILentia analysis of this safety function with the different proof test intervals for the valve - with and without partial stroke testing. The evaluation shows that with a 1 year PTI, the safety function achieves a risk reduction factor (RRF) of 55, and based on both PFDavg and architectural constraints could only be used in SIL1 applications. However, with PST the safety function becomes suitable for SIL2 with a RRF of 169, due to the increased diagnostics.

Let's assume now that the process operator cannot accept a 1 year proof test interval; 3 years is the minimum time period between planned process shutdowns. SIL1 is still achieved, even without PST but with a much reduced RRF of 29. The range of acceptable risk reduction for a SIL1 SIF is 10 to 100, so this is very low in the range and may not be acceptable if a layers of protection analysis (LOPA) specified a risk reduction target of 60, for example.
With Partial Stroke Testing enabled, the PFDavg is reduced. At the same time the SFF is improved, and the exSILentia tool suggests this SIF could now achieve SIL2 with a 3 year proof test interval. However, with a RRF of 102 it is only just above the SIL2 lower limit. In reality, an experienced assessor is more likely to accept this as a strong SIL1 than as a SIL2 safety function. Nevertheless, if the target was SIL1 with a 3 year proof test interval, this is comfortably achieved, and the proof test interval could perhaps be extended even further.
The use of the exSILentia tool delivers formal proof for the benefits leveraged by diagnostics in safety instrumented systems. Diagnostics make modern safety devices so reliable. Unfortunately, the diagnostic data is very often ignored, when it comes to other applications than reducing the PFDavg for the particulate device. Typically in SIS, the diagnostic data can be transmitted via HART using so-called status bits. The following section focusses on tapping the full potential offered by diagnostics and the resulting gains in productivity and safety.

3. Failures and shutdowns in the chemical industry

The vast majority of safety function failures are field device failures. There are two types of failures: safe failures and dangerous failures. Think of the effects of each type of failure on the process the safety function is designed to protect. Dangerous failures mean that the safety function will fail to achieve the safe state if the hazardous event occurs. So by definition, dangerous failures do not cause a process trip. If the dangerous failure is not detected through diagnostics, then the process could keep running for a prolonged period of time with an important protection layer missing. If diagnostics can detect the dangerous failure, at least then a choice is available on what to do about the situation. This might be a decision made by the process operators in response to an alarm, or might be an automatic action taken by the SIS.
One important concept is this: if the logic solver could be made aware of failures in the field devices or wiring, it could be programmed to take the required action quickly and automatically. The correct action might be to shut down. However, considering that continuous processes spend on average 90% of the time operating normally in steady state, and 50% of process safety incidents occur during the 10% abnormal operation time, such as start-ups, it should be wondered if tripping to the safe state because of a failed instrument is the safest way.
The aging plant or plant in operation poses many challenges. One is the diversity of different causes of failure such as: failure of transmitter electronics, unstable bit in the logic solver electronics, wiring faults, flawed process connection of sensors, blocked air supply, misaligned coupling, mechanical fatigue, actuator wear – to name only a few. One key root cause for failure is certainly "tear and wear" but also the mishaps of continued operation. It may happen that a valve that has just undergone a proof test did not get reassembled or reconnected correctly.
Diagnostics is a suitable means to detect most of these potentially dangerous situations. The typical failure characteristics of a SIL-rated device are shown in Table 3. The failure rate data λ is given in FITS (failures per billion hours). The rate for dangerous and undetected failures λ_{DU} is very low, mostly due to self-diagnostic functions implemented in the transmitter. A safe failure fraction (SFF) of 91 % is reached.

Table 3: Reliability data for an example sensor: Rosemount pressure transmitter 3051.

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
3051 4-20 mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	32	91%

The HART foundation estimates that about 70 % of all field devices installed worldwide are devices with HART capabilities. However, only 10 % of these use their higher functions and are normally reduced to transmitting their 4-20 mA representation of their dedicated process variable. There is a huge potential for improvement, especially considering that this is the installed base and for leveraging benefits only punctual additions to the existing installation need to be made.
Examples for the use of the HART protocol are introduced in the following that help increase plant productivity without compromising safety.

Please refer to Rezabek 2009, for concise information on the latest release of the HART specification. The HART protocol is an open platform and was standardised in 2010 in IEC 62591.

4. Added value through diagnostic data

Two examples shown in Figure 3 are used to illustrate how diagnostic data via HART can be used to improve the plant's productivity and safety.

The first example in Figure 3 (left) is the analogue voting of the measurements of two sensors. Two alternative configurations are common: 1oo2 or 2oo2. For the 2oo2 structure, both sensor readings need to indicate an exceeded threshold, whereas the 1oo2 structure needs only one positive sensor reading to cause the plant to trip. The latter structure employs redundancy and can be considered to be the more reliable option. If one sensor fails the other maintains the plant's safety. In contrast, the 2oo2 structure helps to avoid nuisance trips. If the sensor reading fluctuates in one sensor, yet the other one indicates nominal operating conditions – the plant remains in operation. In practice, a 2oo3 voting is selected to simultaneously fulfil safety and productivity requirements.

Very often the 1oo2 structure is configured such that the plant enters the safe state in the event of a sensor failure – in other words the plant shuts down. Employing diagnostics enables the differentiation between a failed sensor and a sensor that reads an exceeded safety threshold. This simple fact allows for a more elegant solution.

One important principle is necessary to understand that an alternative approach does not jeopardise safety. The principle is about the time it takes until a second failure follows the first. In technical systems the one-failure-assumption is valid, because the occurrence of multiple errors at the same time is highly unlikely. Redundancy in technical systems implies that failures occur independent from each other. In the processing industry the time of occurrence of a second failure, and therefore the entire failure of the example 1oo2 sensor structure, is typically assumed to be 24 to 48 hours. The individual time span needs to be discussed with and confirmed by the respective notified body (e.g.: TÜV, exida).

Because of this valid assumption, the temporary degradation from a 1oo2 to a 1oo1 structure in case of the failure of one sensor is temporarily a safe option. When the HART capable device is transmitting its status to the asset management system, maintenance activities can be planned and executed well before the accepted time to second failure has elapsed.

This means for the first example that the voter degradation maintains the plant safety while increasing the plant's productivity. In case the repairs cannot be carried out during the specified time period, then the plant must be shut down.

The second example in Figure 3 (right) is about detecting failures with the aid of diagnostic data. The safety threshold of a sensor is configured to be at 17 mA. The earth leakage at a junction box causes a decrease of the current by 2 mA. Therefore, if the trip condition of 18 mA is reached the logic unit would still "see" 16 mA and not trip. This is a dangerous undetected failure that may lead to disaster.

The HART protocol allows the transmission of the sensor reading via HART in parallel to the conventional 4-20 mA value. The decisive difference is that the digital information via HART is not affected by the earth leakage current allowing the logic unit to uncover the false reading by comparison before a potentially dangerous situation develops.

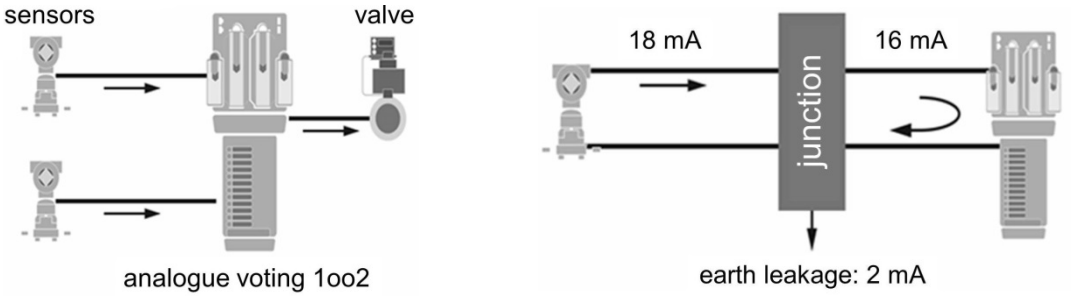

Figure 3: Two examples for the utilization of the HART protocol in safety applications.

Of course, the earth leakage cannot occur suddenly. It is a slowly developing process; non-the-less the safety system can detect those deviations between the digital and the analogue signal using configurable alarm thresholds. Thus, the diagnostic information via HART that is utilised in the logic unit of the SIS is beneficial to the plant's safety.

Studies have shown that operators of oil and gas processes may receive up to 1200 alarms per day. In petrochemical processes, maybe 1500 alarms occur per day and as many as 2000 per day in refineries. This exceeds by far the EEMUA 191 guidelines limit of 144 alarms per day. This circumstance stresses the need to automate safety system reactions where feasible to ease the burden put on operators.
Diagnostic information is indispensable when maintaining the safety integrity of each SIF throughout the safety system. It should not be concluded that diagnostic data is predominantly used for maintenance purposes. In the context of safety systems it is prudent to incorporate the diagnostic information into the safety function's logic to make the safety system react immediately if necessary. The maintenance activities are merely a means to maintain continuous *safety integrity* of every SIF. The goal of employing diagnostic data is to obtain an online assessment of the health of each safety function and to be able to react appropriately as soon as an issue is identified. This will not only increase the overall safety of the plant but will also help avoid unnecessary trips and production losses.

5. Conclusions

The importance of diagnostic functions in field devices to accomplish heightened requirements with respect to device reliability was highlighted in the first section of this paper. To support the argument, an analysis was carried out using the tool exSILentia that yielded a strong influence of diagnostics on safety performance. Then the current situation concerning HART devices, plant operation and root-causes for unplanned plant shutdowns in the processing industry was roughly sketched arguing that HART is a suitable means to incorporate diagnostic data into the assessment and handling of safety functions. Subsequently, examples were used to illustrate the benefits. On the one hand, diagnostics were used to increase the uptime of the plant and on the other hand they were used to increase safety by uncovering a dangerous undetected failure. It was highlighted that maintaining uninterrupted safety integrity of the entire SIS makes it necessary to continuously monitor the health of its field devices.
HART capable devices and their potential for the improvement of the performance of production plants in the processing industry has long time been a very underestimated and misunderstood topic. In the processing industry this potential is slowly beginning to be seized by the operators and owners (CEE 2011). Since the installed base of HART capable devices is that big, the investments necessary to benefit from them is relatively small. Diagnostic information not only helps to increase safety but also to minimise production losses due to unplanned outages.
Diagnostics are essential! Safety systems do nothing, most of the time, so how do we know they will work when needed? Many safety devices have a significant proportion of failure modes which would be dangerous if they were not diagnosed. Modern instruments provide additional information on the state of operation of field devices – seize them!

References

Control Engineering Europe (CEE), 2011, 2010 HART Plant of the Year, controlemgeurope.com, http://www.controlengeurope.com/article/39754/, last visited 09/08/2015.

Engineering Equipment & Materials Users Association (EEMUA), 2013, Publication 191 Alarm systems - a guide to design, management and procurement, www.eemua.org, last visited 09/08/2015.

John Rezabek, 2009, New HART for an old Standard – has HART 7 given this old standby a new lease of life?, CONTROL magazine.