

A MATTER OF HEALTH AND SAFETY

Dr Bert Knegtering, and Elly Funken-van den Blik, Honeywell Safety Solutions, the Netherlands, and Daniel Bolland, ExxonMobil Research & Engineering, USA, examine the importance of health monitoring safety instrumented systems.

Over the past decades, the process industry has made tremendous investments when it comes to the safety of people, protection of the environment, and protection of process equipment. This has seen the implementation of many expensive safeguarding and protection equipment, which needs to be regularly tested and maintained. Despite the best efforts in system design, engineering and construction, ongoing maintenance and testing of the safety instrumented system (SIS) introduces the scope for human error, often causing spurious process trips during testing and leaving systems bypassed (defeated) afterwards.

The safeguarding of equipment must be proven reliable whilst avoiding difficulties such as over engineering, unnecessary redundancy, overly frequent maintenance and testing, and spurious process shutdowns. Only through adequate measurement of the actual reliability performance and health status of the safeguarding equipment can a dedicated reliability assessment, optimisation of design and reduction in testing be achieved.

One of the major weaknesses of safety and reliability assessments is that little or no representative/accurate failure rate data is available. This often results in the use of fixed values obtained from relatively conservative and sometimes misapplied handbooks. The result is the overdesign of systems coupled with too frequent testing of the installed equipment. Overdesign costs money and can result in spurious trips, while frequent testing introduces human error.

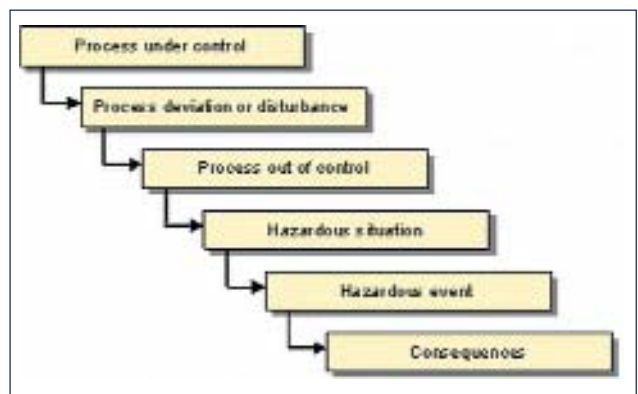


Figure 1. Process hazardous event scenario.

THE PROCESS HAZARDOUS EVENT SCENARIO

If a process is considered under control until a hazardous event with serious consequences occurs, the stages depicted in Figure 1 can be distinguished.

Obviously, the purpose of all safeguarding measures is to prevent or mitigate the impact and consequences of a hazardous event, and thus ensure a safe operating process installation. Therefore, these measures must function properly and be reliable. Adequate definition of safeguarding measures can only be achieved if a full understanding of their design intent is known.

Typical questions that need to be answered are:

- What are the potential hazardous events and their associated risks, and what risk reduction is necessary to achieve a safe process installation?
- How can it be established and confirmed that the safeguarding measures fulfil the required risk reduction?
- What activities must be carried out to guarantee that the safety integrity level (SIL) is maintained during the entire lifetime of the safeguarded process installation?
 - How can it be proven, by proper documentation, that the safety requirements are met continuously?

When it comes to the implementation and operation of SIS, many parameters can influence its performance. For each function implemented in the SIS, the devices



that are needed to fulfil this function can fail in diverse ways. Considering this, some of the questions to be answered are:

- Are all or only a subset of failures essential or dominant?
- Which of them are currently measured?
- Which failures can be detected automatically online?
- Which of them are manually tested e.g. during maintenance and testing?
- Which failures are currently not measured?

Finally, it is important to recognise possible correlations between these parameters (failures). For example, does the detection of a high number of dangerous failures in a particular type of safety related device imply that this device type also suffers from a high number of dangerous undetected failures?

PROCESS PLANT OF THE FUTURE

As a result of SIS standards, the industry is being forced to define safety functions from sensing element to actuating element, and a lot of time and energy is being spent on hazard and risk assessment and validation of the SIS design. However, at the end of the day, when the reliability analysis is performed as part of the validation process, offline (or online) proof tests are often required to confirm that the system is indeed meeting the desired probability to respond on demand.

As traditional reliability data sources are not always considered trustworthy and accurate, the perception of the involved experts often predominates when defining the design of the SIS. Furthermore, processing plants often encompass an overlap of various hazardous areas. In principle, an optimal design would have people absent from these areas, with processes and production controlled from a centralised control room, located at a safe distance.

In an ideal world, the operator or technician should be able to evaluate the performance of safety instrumented functions (SIFs) using data sets (real time or manually collected) that provide performance characteristics of the components of each individual SIF. By doing so, the Probability of Failure on Demand (PFD) can be calculated as a function of time and a continuous assessment of PFD versus required safety integrity can be achieved. Such a tool would allow the easy assessment of a 'safety margin' for individual systems, allowing maintenance or testing to be scheduled only where and when required. This concept requires an accurate failure rate database for devices installed in the plant and a system that is capable of blending historical data with new data, whether this new data is manually or automatically generated. With increased levels of automatic device self validation and diagnostics, links between DCS and SIS logic solvers allowing sensor validations, and automatic partial valve stroke testing systems, these 'plant of the future' type concepts are available today. What is missing is the necessary application suite to allow the integration of such data and the display of such data to operating staff to allow total management of the plant SIS equipment.

URGENT NEEDS FOR THE PROCESS INDUSTRY

In order to optimise the design and operation of SIS, the process industry needs an adequate application/specific health monitoring facility that has the capability of measuring the actual health status, and thus the reliability and safety of the SIS. Benefits include a reduction in testing (and in human errors during testing) and furthermore, by automatically measuring the health status and reliability,

typical trends such as quality problems and wearing out or ageing problems can easily be observed and solved before they grow serious. Additionally, maintenance and testing staff need not be in the field exposed to hazards; time and cost can be saved, and safety risks and spurious process trips can be reduced.

Since the publication of international standards such as IEC 61508 and IEC 61511, many tools and methodologies have been developed and made available for the industry to perform risk assessments and reliability validations. Unfortunately, none of them have ever had the capability of automatically measuring the actual performance of the SIS and optimising the test interval and system design during the system's lifetime.

OBSERVATION AND REGISTRATION IS KEY

A crucial aspect of performing PFD calculations is the availability of representative physical failure data for the safety devices. At present, the majority of end users still use 'old' literature based on handbooks or rely on information obtained from vendors of the safety instrumentation.

Handbooks such as OREDA offer failure rate data typical of environmental circumstances for offshore e.g. in the North Sea. Using these data for onshore applications can result in an overly conservative reliability compared with the user's own experiences. Although these handbooks can be very valuable for their specific application environment, many companies would prefer to have failure rates of their devices for their specific application and environmental conditions.

Furthermore, failure rate data from vendors do not fit the purpose every time. The data is often over optimistic as the failure mode and effect analyses (FMEA) also considers ideal circumstances such as laboratory stress conditions.

For these reasons, end users should focus on the actual failure rates and failure modes of their safety instrumentation. This actual performance is the result of the device/system application conditions and environmental circumstances. Process related stress factors have a significant influence on the measured reliability performance. Depending on installation and environmental circumstances, differences in failure rates can easily vary by orders of magnitude.

By examining device failure data, trends can be observed; failure rates are not fixed values but time dependent (e.g. wear out). As a result of measuring the actual performance, the time until the next test can be assessed; a comparison can be made of the reliability of the devices as provided by different vendors; and design optimisation can be performed. At the same time, the real expected lifespan can be predicted and used to establish the time that is left until the next replacement of safety devices.

These trends in failure rates, based on their specific application and environmental conditions, are not only observed for a complete population of identical devices on a site, but can also enable dedicated analyses to be made for specific devices that perform differently from that population. For example, what ExxonMobil typically calls 'bad actors' can be observed and identified, and treated accordingly e.g. by higher test and maintenance frequencies. On the other hand, typical devices that appear to perform much better than the average population (and than expected), sometimes due to applied higher quality components, can lead to lower test and maintenance activities, thereby improving safety and saving on maintenance cost. More importantly, identification of quality components provides the basis for improvements in SIS design and hence an

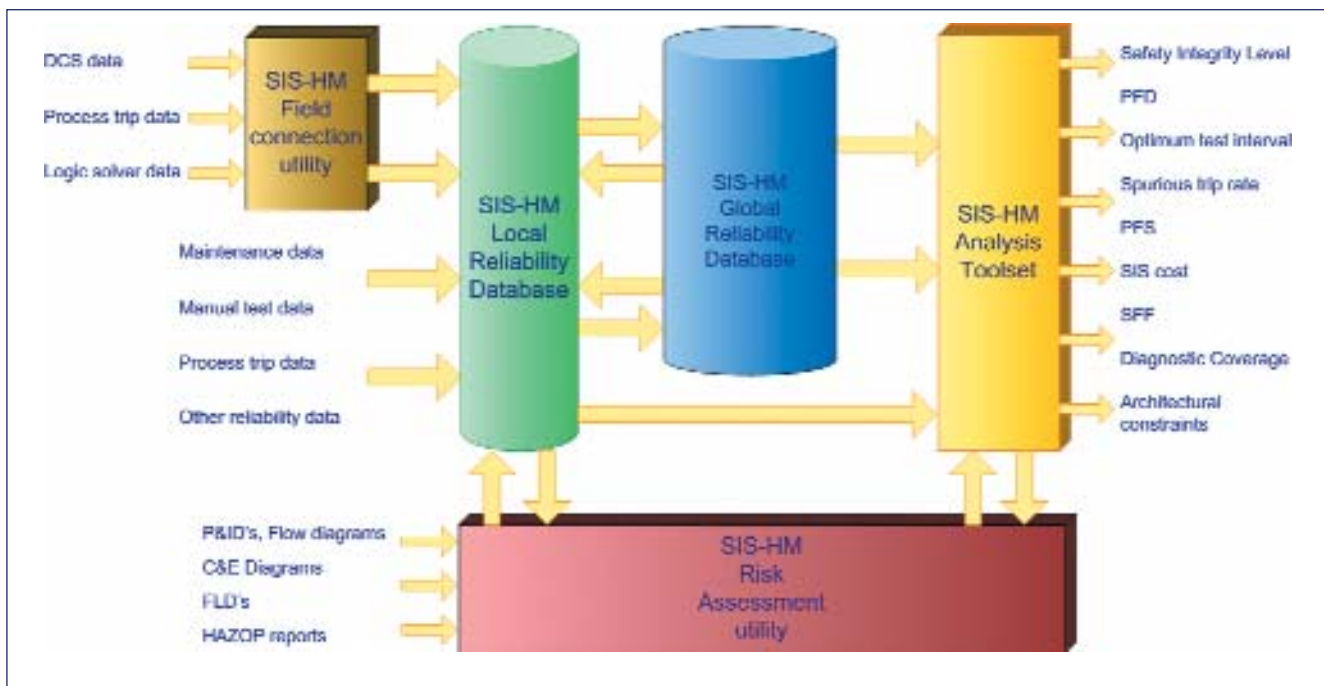


Figure 2. SIS Health Monitoring™: the 'complete picture'.

increase in overall safety. In order to make a plant really safe with the application of SIS, this differentiating approach is absolutely necessary. Bad or weak performing devices form the real bottleneck in the reliability of the SIS.

Finally, by monitoring the health status and safety performance of the site's own safety instrumentation, the 'proven in use' concept of the IEC 61508 and 'prior use' concept of the IEC 61511 can be established.

THE PROJECT

Working in collaboration to share knowledge and experiences with SIS safety and health, ExxonMobil and Honeywell have jointly developed the SIS Health Monitoring™ (SIS-HM™) solution. The aim of the project was to take a step forward in realising fully self operating and self testing safe and reliable SIS installations, consistent with longer term goals related to 'the plant of the future'.

The SIS Health Monitoring™ solution (Figure 2) represents a toolset with a services package that enables the process industry to: automatically measure the actual health status of their safety instruments; analyse their SIS/SIF reliability and safety integrity; optimise test intervals; and reduce spurious process trips. In addition, unexpected trends in time are detected, maintenance and test frequencies automatically indicated, and benchmarking of quality and reliability of various devices in different applications is quickly and easily performed. Similar studies show tremendous savings in the total Capex and Opex of a site's SIS, often representing millions of dollars in investment and support cost (see side bar). As can be seen, substantial savings can be achieved by reducing over engineering, optimising test and maintenance, and reducing spurious trips (thereby increasing process uptime) with no adverse impact on safety.

The SIS-HM™ modular toolset can easily be customised to the specific plant conditions and process demands. Developed in conjunction with maintenance, instrumentation and test engineers at several European manufacturing sites, it is easy to use and integrates seamlessly into the work process. The toolset comprises five modules, which can be connected together or be used as stand alone tools. Each module can work independently

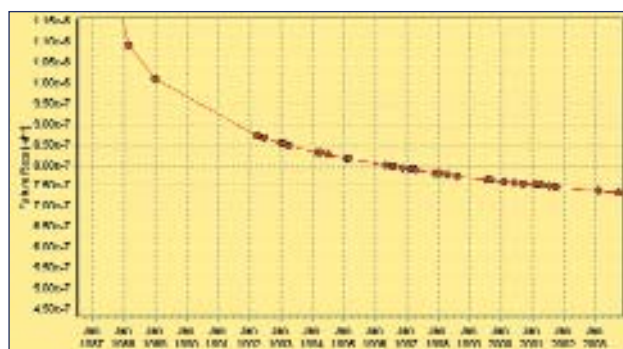


Figure 3. Example of time dependent failure rate as calculated by SIS-HM™.

Illustrative figures on potential savings

- Testing is primary cause for spurious trips¹.
- Unscheduled downtime²:
 - ◆ Cost: US\$ 20 billion, or approximately 5% of total production per year in North America.
 - ◆ largest single factor eroding plant performance.
- Lost performance and expenses:
 - ◆ 3 - 5% lost to asset unavailability and incidents³.
 - ◆ 20% of incidents are caused by maintenance/testing⁴.
 - ◆ 15% of SIS expenses consider maintenance⁵.

and offers significant added values and benefits. These vary from handling SIFs in a structured manner and analysing demands, to optimising safety instrumentation without affecting process safety.

The modules are: the SIS-HM™ Local Reliability Database; the Global Reliability Database; the Analysis Toolset; Field Connection Utility; and the hazard and risk assessment or SIL classification utility. The toolset is generic and can be universally used for any brand of conventional or state of the art instrumentation, making benchmarking available regardless of the type of hardware used.

Using the SIS-HM™ Local Reliability Database, the user can store and handle all information regarding safety instrumentation efficiently, flexibly and in a structured man-

ner. In addition, the information regarding health (failure) events, such as tests, trips or demands, can be input and handled. Based upon the failure behaviour of the instrumentation on the user's site, reliability and safety performance characteristics are determined. This can include 'bad actors', trends, demand rates and application specific, time dependent failure rates (Figure 3).

The SIS-HM™ Field Connection utility facilitates connecting multiple, additional data collectors and generators to the local database via automatic interface modules, such as intelligent instrumentation (e.g. smart transmitters, partial valve stroke testing solutions) or asset management tools.

The SIS-HM™ Global Reliability Database allows a company to use a company wide global database in addition to the local site databases on several sites, to store, handle and process data from multiple local site databases. This enables a larger data collection, data sharing and improved data processing, thereby facilitating benchmarking between sites and between manufacturers, allowing users from local as well as global facilities to obtain data for purchasing and for best practice decision support, and access to company wide data.

The SIS-HM™ Analysis Toolset enables sound and traceable analysis, validation and optimisation of the reliability and SIL behaviour of SIFs. The analysis allows for complex SIS configurations with dependent SIFs. Moreover, maintenance and test policy can be optimised (e.g. by extending the test intervals), thereby saving labour and cost without sacrificing safety.

LIFECYCLE APPROACH

Using online collected, real time data on health events at SIS onsite, the lifecycle safety performance of safety instrumentation can be monitored, analysed and optimised. Data

can be gathered from a wide range of data collectors and data generators such as asset management tools, maintenance management systems, history databases and intelligent instrumentation.

This way, many benefits can be gained from the start for any site, such as:

- A substantial reduction of test resources.
- Minimising people's presence in hazardous areas.
- Reducing spurious trips.
- Preventing over engineering.
- Lowering the cost of unforeseen risks, including insurance premiums, benchmarking of devices and manufacturers.

The SIS-HM™ solution has been successfully implemented at several European sites, providing safety improvement opportunities and substantial savings on maintenance and testing. Moreover, using the site's own data and reliability and safety history, the 'proven in use' concept of the IEC 61508 standard and the 'prior use' concept of the IEC 61511 standard can be claimed.

All together, SIS Health Monitoring provides support in all operational phases of the lifecycle. The result is functional safety based on a robust lifecycle model approach.

REFERENCES

1. ExxonMobil internal memo, proprietary and confidential.
2. CLAYTON, Dave, ARC Insight.
3. Honeywell HiSpec solutions study, internal report, confidential and proprietary.
4. HSE report: Principles for proof testing of safety instrumented systems in the chemical industry.
5. ARC report: Safety and Critical Control System Worldwide Outlook.

