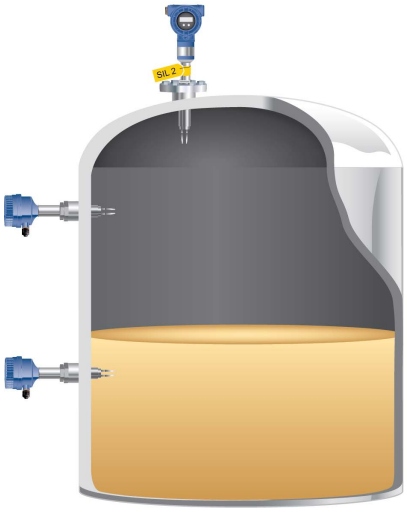
Greater emphasis on reducing dangerous undetected failures helps to improve plant safety

There is a growing opinion that dangerous undetected (DU) failure rates are more relevant than safe failure fraction as a basis for selecting a safety-critical level instrument. Tim Hill, Technical Director at Emerson Automation Solutions, explains how the advanced diagnostics capability of the latest vibrating fork level switches enables them to help improve plant safety by reducing the number of DU failures.

To ensure that industrial processes operate safely and efficiently, it is essential that they are equipped with instruments providing accurate and reliable measurements. Within refineries and petrochemical plants, for example, level monitoring and measurement devices play a critical role in safety applications such as overfill prevention. High-profile incidents such as the Buncefield fire in 2005 have shown that failing to prevent overspills in vessels containing hazardous, flammable or even explosive materials can have devastating consequences for assets, the environment and personnel. It is therefore essential for operators to implement robust Overfill Prevention Systems (OPS) using the most reliable level sensors to minimise risk, meet environmental regulations and improve safety.



An illustration of how vibrating fork technology can be used on a tank, with an overfill switch

Safety instrumented systems and safety integrity level

Worrying about tank overfills is logical because there are hundreds of tank spills of hazardous materials every day (United States Environmental Protection Agency, 2014). However, a properly designed and

implemented OPS helps to reduce their frequency and severity. Safety instrumented systems (SIS) such as OPS are required to meet safety performance targets, and safety integrity level (SIL) is a quantifiable way to establish this. The international SIS standard IEC 61511 defines SIL as the degree of necessary risk reduction for a certain safety function to be implemented by a SIS, to achieve or maintain a safe state for a process, with respect to a specific hazardous event. A function is furthermore defined as a set of instruments intended to detect an imminent accident, decide to take an action and carry out actions as appropriate.

There are many procedures available for the actual determination of a function's SIL, but their common goal is to establish the probability of harm occurring and the severity of that harm. Each safety function is determined to be SIL 1, SIL 2, SIL 3 or SIL 4 - the higher the SIL, the higher the requirements to achieve a tolerable risk - and SIS must be designed using equipment that meets the necessary SIL.

It is important to note that field devices alone are not attributed a SIL rating. It would be wrong, for example, to say that a device is 'SIL 3-rated'. It should instead be stated that the device is 'suitable for use in a SIL 3-rated safety instrumented function'. In other words, the SIL rating applies to the entire loop and not its individual components.

There are two ways to determine the level of SIL system in which a device is suitable for use. The first is FMEDA (Failures Modes, Effects and Diagnostic Analysis) – a systematic analysis technique to determine the device's failure rates, failure modes and diagnostic capabilities. The second method is known as Proven in Use, which uses historical data field to determine whether there are systematic design faults in the device.

Safe failure fraction and dangerous undetected failures

The analyses and data used to determine a SIL rating also helps to establish a product's safe failure fraction (SFF), which is a percentage of its safe failures compared to its total failures. To calculate a device's SFF, it is first necessary to understand that when random hardware failures occur within SIS, they can be categorised in one of four ways: safe undetected (SU), safe detected (SD), dangerous detected (DD), and dangerous undetected (DU).

Safe failures, either detected or undetected, are those which do not affect the safety function of the system. Dangerous failures, meanwhile, pose a significant safety risk and can potentially have catastrophic consequences. If a safety-critical instrument fails but the failure is detected and reported via the device's diagnostic coverage, this enables the system to be brought to a safe state and is classified as DD. Even if a device has a large fraction of dangerous failures, so long as enough of these can be detected and safe action taken, it is still considered a safe device. However, if such a failure occurs without being detected and reported, this can create a critical state and is therefore categorised as DU. The formula for calculating a device's SFF is the sum of its SD, SU and DD, divided by the sum of its SD, SU, DD and DU. This can be displayed as follows (where λ = total failure rate per hour):

λ SU + λ SD + λ DD

λ SU + λ SD + λ DU + λ DD

Recent enhancements in SIS product design have enabled manufacturers to improve their devices' SFF figures. However, because DU is merely one component of SFF, it is possible to achieve an improved SFF figure by reducing the SD, SU and DD elements of the equation, rather than DU. Consequently, there could be a scenario where two different devices have the same SFF figure and SIL rating, but one of them has a much lower DU figure than the other, and is therefore less likely to fail in a dangerous way. Until now, many users have relied on SFF figure and SIL rating as their basis for comparing the reliability of safety-critical level instruments offered by different suppliers. However, there is a growing opinion within safety circles that users ought to look deeper than SFF and SIL, and that DU should be regarded as the more relevant figure, because the most important factor is the likelihood of a device failing in a dangerous way and the system not knowing of the failure.

Vibrating fork level switches

OPS typically consist of a level sensing device, a logic solver and a final control element in the form of actuated valve technology. Within such systems, vibrating fork level switches are often the technology of choice for providing reliable point level detection.

The operating principle of vibrating fork level switches is that of a tuning fork. The switch, comprising a fork with two tines, is oscillated by an internal piezo-electric crystal. The switch is mounted on the side or top of a vessel so that the tines protrude into it. When in air, the tines vibrate at their natural frequency, which is continuously monitored by a detector circuit. When liquid covers the tines, the frequency of oscillation drops and this is detected by the switch electronics, which in turn changes the output state of the switch to operate an alarm, pump or valve. This makes vibrating fork level switches a reliable technology for use in low and high-level alarm applications and overfill prevention.

There are several reasons why vibrating fork level switches are preferred to other technologies - such as float switches, ultrasonic gap switches and capacitance switches - for safety-critical applications such as overfill prevention. A lack of moving parts that can wear or stick makes them less prone to failure and means that they require virtually no maintenance. Their sensing is virtually unaffected by flow, turbulence, bubbles, foam, vibration, solids content, and coating. Their installation is straightforward and there is no need for them to be calibrated, which therefore makes them less prone to human error during commissioning.

Latest technology

The reduction of DUs was a specific aim within the design of the latest vibrating fork switch technology. Advanced diagnostics capability enables these devices' electronic and mechanical health to be monitored continuously, with the result that the number of DUs possible is significantly reduced.

It is important to note that field devices alone are not attributed a SIL rating

These devices have diagnostics that can detect external damage to the forks, internal damage to the sensor, corrosion and over-temperature. Frequency analysis functionality enables emerging conditions such as media build-up which unchecked could lead to fork blockage, or excessive corrosion to be detected over time, enabling preventative maintenance to be carried out before functionality and / or reliability is affected. These devices may also have a new diagnostic tool known as power advisory functionality, which enables operators to identify any potential problems with internal components and circuitry by monitoring the current and voltage drawn over the device's lifetime. Any unusual behaviour which may indicate an emerging issue, such as internal corrosion, can be detected.

Conclusion

Plant managers fear DU failures in safety-critical level instruments, as they can lead to a critical state in a SIS, with potentially catastrophic consequences. The calculation of a device's SFF is used as a means of establishing its suitability for use in an SIS, and end users have traditionally relied on SFF as a basis for selecting instruments. However, opinion is now shifting to the DU figure having more relevance than the SFF in determining product safety. Consequently, the latest vibrating fork level switches have been designed with advanced diagnostics capability, to reduce the number of DU failures and increase plant safety. ■

About the author

Tim Hill (FIMechE) is Engineering Manager - Level Products at Rosemount Measurement, part of Emerson Process Management. He was formerly a project manager at the UK Atomic Energy Authority and before that worked in senior engineering positions for several UK-based companies.