

08 September 2005

Reference: Customer Advisory - 04

Re: Understand the difference between *Continuous Mode* and *Demand Mode* Safety Instrumented Functions.

To Our Customers:

The most recent edition the ANSI/ISA S84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, establishes alternative design procedures for Safety Instrumented Systems (SIS) depending on the expected frequency of a demand condition being placed on a Safety Instrumented Function, or SIF. Designers of Safety Instrumented Systems refer to these different applications as either *Continuous Mode* or *Demand Mode* SIF.

You may be aware that the required performance for a SIF can be classified by the concept of a Safety Integrity Level, or SIL, which is the amount of risk reduction for a SIF. The SIL has a significant impact on the selected design and testing program for a SIF. You may also be familiar with the most-commonly used classification for SIL requirements based on order-of-magnitude categories of average Probability of Failure on Demand, or PFD_{avg} . The following table lists these performance requirements.

Table 1 Safety Integrity Levels – Demand Mode

Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction Factor	Safety Availability
1	10^{-1} to 10^{-2}	10 to 100	90 to 99%
2	10^{-2} to 10^{-3}	100 to 1,000	99 to 99.9%
3	10^{-3} to 10^{-4}	1,000 to 10,000	99.9 to 99.99%

You may not be aware that this table only applies to situations where the expected frequency of a demand condition on the SIF is low compared to the frequency of functional tests of the SIF. We call this situation a *Demand Mode* SIF. When this criterion is satisfied, it is true to say that the probability of uncovering a 'dangerous undetected' or *covert* failure of a SIF component during a functional test of the system is relatively high compared to the probability that this type of failure will be revealed during a hazardous demand condition. The achieved probability of failure on demand is often calculated using the following equation which estimates the probability of this

type of failure over a specified time period – specifically the period of time interval (TI) between functional tests of the SIF.

$$PFD_{AVG} = \frac{\lambda^{DU} TI}{2}$$

Note: this equation does not apply to all SIF architectures and accurately approximates PFD_{avg} only when the calculated value is less than about 0.1.

For example, the frequency of a dangerous undetected for a particular SIF design is estimated to be 0.03 per year (i.e., approximately one chance of a dangerous undetected failure in 33, per year). The planned functional test interval is once every 4 years. PFD_{avg} is calculated as 0.06, which is in the SIL 1 range. If the expected demand rate is once every 10 years, then the result is valid, because the frequency of demands is much less than the interval between functional tests. We would classify this as a demand mode SIF. Note: the frequency of the hazard would be estimated to be 0.1 per year x 0.06 = 0.006 per year (i.e., one chance in 170, per year).

But, what if the expected frequency of a demand condition is twice per year, or once per six months on average? With four year functional testing, the calculated PFD_{avg} remains unchanged at 0.06. But during that four-year period we would about 8 demands to have already occurred. The likelihood of revealing a dangerous undetected failure during a demand condition is “very high”. The likelihood that a dangerous undetected failure would be revealed during a functional test is relatively “low”. As the expected frequency of a demand condition increases compared to the functional test interval, the “value” of functional testing decreases rapidly. In the previous example, if a demand condition could be expected to occur about once every week, then we would reasonably conclude that functional testing at a four year interval would be almost a worthless activity. In this case, the ‘safety’ of this shutdown function is assured only by a sufficiently low likelihood of a SIF failing in a dangerous undetected manner.

This situation is what we call a *Continuous Mode* SIF, because the frequency of demands is so high relative to functional tests that – mathematically speaking – the demands can be considered ‘continuous’. The ISA/IEC standards also refer to this as a Safety Instrumented *Control/Function*. In this case, the only metric that has any bearing on safety performance is the *frequency of a dangerous undetected failure*, or λ^{DU} , expressed in units of failures per year or failures per hour. ISA 84.01-2004 provides the following standard classifications for performance of Continuous Mode SIF, which are based solely on failure frequency.

Table 2 Safety Integrity Levels – Continuous Mode

Safety Integrity Level (SIL)	Dangerous Undetected Failure Frequency λ^{DU} (per hour)	Approximate Dangerous Undetected Failure Frequency λ^{DU} (per year)
1	10^{-5} to 10^{-6}	11 to 110
2	10^{-6} to 10^{-7}	110 to 1,100
3	10^{-7} to 10^{-8}	1,100 to 11,000

Note: the concept of average probability of failure on demand over the functional test interval doesn't make sense for a *Continuous Mode* SIF. Practically speaking, there is no point in calculating PFD_{avg} !

In our previous example, the frequency of a dangerous undetected failure was approximately once in 33 years ($= 3.4 \times 10^{-6}$ per hour). This would still fall into the SIL 1 range of performance based on Continuous Mode SIF classification. However, the frequency of an accident scenario is much higher this time, because the frequency of demands is higher. Because the demands can be considered 'continuous', it the accident would very likely occur with the same frequency as the dangerous undetected failure, or about once in 33 years. This may be unacceptably high based on the company's criteria for tolerable risk, and a higher performance may be required for this SIF, possibly in the SIL 2 range.

If you uncover a situation where a *Continuous Mode* SIF may be required, proceed with caution! It is rarely advisable to design a SIF without relying heavily on the value of functional testing. It is often feasible to use automated diagnostics to 'frequently' test components of the SIF, thereby significantly increasing the frequency of functional testing. This philosophy, which is commonly used in machine guarding applications, can be translated to process industry applications. In a future update of this advisory, Kenexis will provide advice on practical engineering steps for *Continuous Mode* SIF, and making changes that re-classify these applications into a more-desirable *Demand Mode* application.

For more information on demand mode and continuous mode safety instrumented functions or our services, feel free to contact Kevin Mitchell at (614) 451-7031 ext. 2, or kevin.mitchell@kenexis.com.

Keep Safe,

Kevin J. Mitchell
President, Kenexis

Disclaimer:

This customer advisory provides information of a general nature concerning some industry practices involving engineered safeguards. These should not be taken as typical, suggested, or recommended levels of protection. The application of engineered safeguards is highly dependent on process-specific and site-specific factors that have a great deal of influence on the actual degree of hazard control strategy. Neither Kenexis nor its corporate officers make any representations, warranties, or guarantees concerning the content of this document.