HIGH DEMAND AND CONTINUOUS MODE SAFETY FUNCTIONS COMPARED WITH LOW DEMAND MODE

SYSTEMS

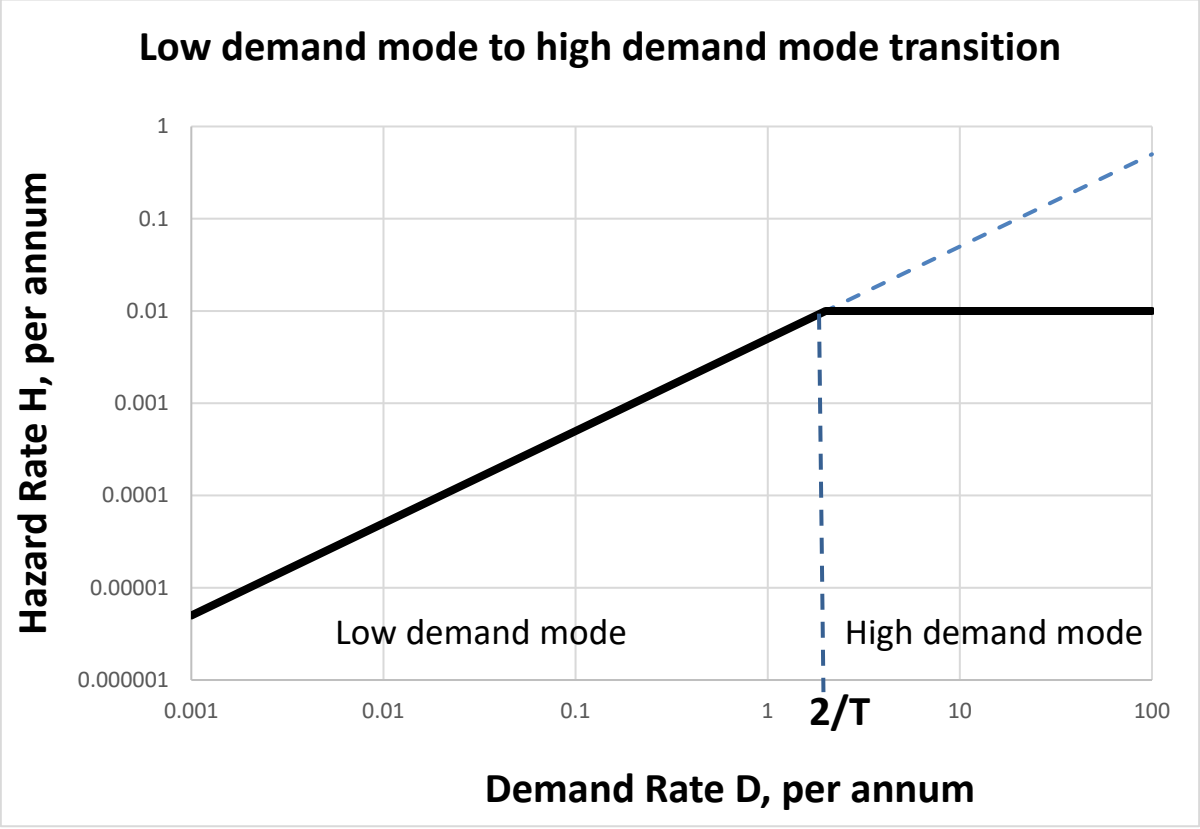
I&E Systems Pty Ltd

ACN 069 813 958

Mirek Generowicz

FS Expert (TÜV Rheinland #183/12)

What is the difference between low demand, high demand and continuous modes of operation in automated safety functions?



I

CONTENTS

Summary **3**

Low demand mode safety functions are common in the process sector 3

High demand or continuous mode safety functions are common in machine safety 3

High demand mode is a limiting case 3

Outline **4**

Introduction – safety function operating modes **6**

Examples of continuous mode compared with demand mode **7**

Hazard rate **8**

Targets for continuous mode or high demand mode safety functions **8**

Demand mode safety function probability of failure **10**

Responses to increasing demand rates in low demand mode **11**

Example of low demand mode with increasing demand rate **13**

Distinguishing between diagnostic tests and proof tests **15**

Responses to decreasing demand rates in high demand mode **15**

Example of high demand mode with decreasing demand rate **16**

Sequence interlocks and permissive functions **17**

Machine safety interlocks 17

Process safety interlocks 17

Process safety interlock example **18**

Company A: Non-safety rated sequence interlock 19

Company B: SIL rated low demand mode function 19

Company C: SIL rated continuous mode function 21

Conclusions **23**

References **24**

Summary

Low demand mode safety functions are common in the process sector

Most safety functions in process industry applications act in a low demand mode. Low demand mode safety functions are characterised by their probability of failure on demand. The mathematical modelling of failure probability in low demand mode assumes that the demand rate is less frequent than the rate of periodic tests.

The demand on any individual safety function is expected to be much less than once per year. It is sufficient for these safety functions to be inspected and tested once per year because the demands are less frequent. Failure of the function does not result in an immediate hazard. The failure is more likely to be revealed in the next test rather than as a failure on demand.

A safety function is described as operating in the high demand mode if demands on the function are more frequent than about once per year. This distinction is based the assumption that low demand mode safety functions are inspected and tested annually. The periodic tests become less effective in revealing failures if the demands on a function are more frequent than the tests. Failures are more likely to be revealed on demand rather than by the periodic test. The mathematical model of failure probability that is used in low demand mode is no longer valid.

Many safety practitioners in process industries are not familiar with the application of high demand mode. They are concerned that it may be more difficult to achieve compliance with safety integrity requirements in a high demand mode. What if the demand rate becomes even more frequent? Do we need to reduce the probability of failure on demand?

High demand or continuous mode safety functions are common in machine safety

Conversely, safety practitioners who deal with machine safety may be concerned about how to allow for demand rates that are less frequent than once per year. In machinery safeguarding applications most safety functions act in a continuous mode or in a high demand mode. The demand on each safety function is expected to be effectively continuous, and at least once per year. These safety functions are designed simply to meet a target for failure rate rather than a target for probability of failure on demand. What if the demand rate is less frequent than once per year? Do we need to estimate the probability of failure on demand instead of using the failure rate as a target?

High demand mode is a limiting case

It turns out that the transition in either direction between high demand mode and low demand mode is simple and straightforward.

High demand mode is the limiting case where the demands occur more frequently than the periodic inspection and testing of the safety function. Further increases in the demand rate become irrelevant. We can model the safety function assuming that hazardous conditions are continuously present. The mathematical treatment is simpler for high demand mode than for low demand mode. We only need to consider the dangerous failure rate of the function rather than having to estimate probability of failure on demand.

The continuous mode or high demand mode is the worst-case scenario. Any function designed to meet the criteria for continuous mode operation will always meet the failure probability criteria for low demand mode.

Outline

Follow the hyperlinks for more information.

Introduction – safety function operating modes

An explanation of continuous, high-demand and low-demand operating modes.

A demand mode function acts to reduce the risk of a hazard that is caused by some other failure.

Failure of a continuous safety function directly causes a hazard, regardless of other failures.

Demand mode safety functions need to be treated in the same way as continuous mode functions if the rate of other failures is more frequent than once per year.

Hazard rate

Demand mode functions act in response to some demand event to prevent hazardous consequences resulting from the event. The rate at which hazardous consequences occur is proportional to the rate at which demands occur on the safety function and proportional to the probability that the function fails on demand.

Dangerous failure of continuous mode functions causes hazardous consequences. The rate at which hazardous consequences occur is simply the rate of dangerous failures in the function itself.

Targets for continuous mode or high demand mode safety functions

The target rate limit for dangerous failure of a continuous mode or high demand mode safety function can be set with reference to the tolerable frequency for the consequences of the related hazardous event.

Credit can be taken for risk reduction provided by other protection methods that can act to reduce risk after the safety function has failed.

Continuous mode functions rely primarily on frequent diagnostic testing to reduce the rate of dangerous failures.

Demand mode safety function probability of failure

The target for low demand mode safety functions is set in terms of the probability that they will fail on demand.

Low demand mode functions reduce risk in proportion to the probability that they will fail on demand If the probability of failure is 0.1, the risk is reduced by a factor of 10.

Low demand mode functions rely on periodic function testing to reduce the probability of failure on demand as well as using frequent diagnostic testing to reduce the rate of dangerous failures.

The probability of failure depends on the interval between periodic function tests and on the rate of undetected dangerous failures in the function.

Responses to increasing demand rates in low demand mode

The estimated probability of failure is based on the assumption that the periodic function tests occur more frequently than the hazardous events that put a demand on the function.

The mathematical model is simply not valid if the demands occur more often than the tests. Period function tests cannot be relied upon to reduce probability of failure in high demand rate applications.

Distinguishing between diagnostic tests and proof tests

Diagnostic tests are sufficiently frequent to be effectively continuous when compared with the hazard rate.

Periodic function testing is not continuous. It is typically conducted annually, in addition to frequent diagnostics. Periodic function testing is effective in reducing probability of failure only if it is more frequent than the rate of demands on the function.

Responses to decreasing demand rates in high demand mode

Treating low demand mode functions in the same way as high demand mode functions is a conservative approach. It does not take any credit for periodic testing in evaluating safety function performance.

A safety function that meets the target set for a high demand rate will always meet the target for any lower demand rate.

Sequence interlocks and permissive functions

Permissive interlock and sequence interlock are terms that may be used to describe functions that keep a machine, a sequence or process in its current safe state. An interlock function may be used to prevent transition to a more hazardous state.

Interlocks are commonly used in machine safeguarding applications.

It might not be immediately obvious how sequence interlocks and permissive functions should be treated in process safety applications.

This section discusses how these functions may be considered either as demand mode or continuous mode safety functions.

Introduction – safety function operating modes

Safety functions are automatic trip functions, controller functions or interlocks that act to reduce risk associated with hazardous equipment.

The 'operating mode' of a safety function describes whether the safety function is designed to act continuously or to act only on demand.

Continuous mode safety functions have a continuous action that ***keeps equipment in a safe state***. **Failure of a continuous mode safety function itself can directly cause a hazardous situation.**

Continuous mode safety functions are characterised by the rate of dangerous and undetected failures per hour or per annum. Failures are classified as dangerous if they increase the risk of the hazard. The rate is represented by the symbol $\boldsymbol{\lambda_{DU}}$.

Demand mode safety functions act only on demand to ***put equipment into a safe state*** in response to a detected hazardous event. **Failure of a demand mode safety function does not itself cause a hazard**.

Demand mode functions act to reduce the risk of a potentially hazardous event that results from some failure in process equipment or in machinery. The safety function action may reduce the likelihood of hazardous consequences occurring or it may reduce the severity of the consequences.

A demand mode safety function is characterised by the average probability that the function will fail to act on demand, abbreviated as $\boldsymbol{PFD_{AVG}}$.

A demand mode safety function may also be characterised by its risk reduction factor, $\boldsymbol{RRF}$, which is simply the reciprocal of its average probability of failure on demand, i.e. $\boldsymbol{RRF = 1/\ PFD_{AVG}}$.

IEC 61511-1 distinguishes between low demand mode, high demand mode and continuous mode. It includes these definitions:

> **3.2.41.1**
> **low demand mode**
> mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year
>
> **3.2.41.2**
> **high demand mode**
> mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year
>
> **3.2.41.3**
> **continuous mode**
> mode of operation where the SIF retains the process in a safe state as part of normal operation

High demand mode functions are considered in the same way as continuous mode safety functions. They are characterised by dangerous undetected failure rate $\boldsymbol{\lambda_{DU}}$.

The purpose of this paper is to explain why high demand mode functions are treated in the same way as continuous functions, and to explain the transition between low demand and high demand.

High demand mode is simply a limiting case. It is the limit that applies when the demand rate is more frequent as periodic test and inspection of the safety function. IEC 61511-1 sets the boundary for the transition between low demand and high demand at one year to simplify the definition. This is because periodic tests are typically scheduled at yearly intervals.

Examples of continuous mode compared with demand mode

The difference between continuous mode and demand mode can be illustrated using the artificial example of interlocks used on hazardous machines.

A machine might be protected by a guard that is held in place by solenoid operated lock. The guard is automatically locked before the machine starts. The guard is held locked while the machine is running. The interlock acts continuously until the machine has stopped. A hazardous situation would result immediately if the lock were to fail and cause the guard to spring open while the machine is running.

This could be classed as a safety function with a continuous mode of operation.

Alternatively (or additionally) the machine might have a trip function that is activated by a limit switch fitted to the guard. The machine is automatically stopped if the guard is opened while the machine is running. The interlock acts only on demand when the guard is moved out of place. Failure of the interlock does not cause an immediate hazard. If the interlock fails a hazardous situation would result only when the operator opens the guard while the machine is running. This could be classed as a safety function with a demand mode of operation. It would be appropriate to class it as a high demand mode if the operator is likely to open the guard more than once per year.

Hazard rate

The objective of a safety system is to limit the rate at which specific hazards occur. Safety system targets are based on levels of risk that are acceptable in a given context, based on current values withing the relevant society. The targets for a hazard may be expressed as a **tolerable frequency** for that hazard.

If we use the term $\boldsymbol{D}$ to represent the rate of demands on a safety function operating in a low demand mode, then the **hazard rate** $\boldsymbol{H}$ can be estimated as:

$$H = D \times PFD_{AVG}$$

The hazard occurs if the demand occurs AND a demand mode safety function fails to act successfully on demand.

The hazard rate can also be expressed in terms of the risk reduction factor for the safety function.

$$H = D \,/\, RRF$$

Failure of a continuous mode function itself directly *causes* hazardous consequences.

The hazard rate is then equal to the rate of **dangerous undetected** failures of the safety function, λ_{DU}:

$$H = \lambda_{DU}$$

In both cases the hazard rate may be reduced by adding other protection methods as well as the safety function.

Targets for continuous mode or high demand mode safety functions

Continuous mode and high demand mode safety functions are relatively easy to model mathematically. The rate of demands on a high demand mode function is irrelevant. The demand on high demand mode safety functions is assumed to be continuous.

Dangerous failures of the safety function are assumed to lead to the hazardous event within a short time.

The performance criterion for the safety function is expressed as a limit on the rate of dangerous undetected failures. The limit is set to ensure that the frequency of hazardous consequences (such as fatality) meets the owner's targets for tolerable risk.

Credit can be taken for risk reduction provided by other protection methods that can act to reduce risk after the safety function has failed.

For example, layer of protection analysis (LOPA) is one of the methods commonly used in determining and allocation risk reduction targets. If a continuous mode or high demand mode function is used then the failure of the function is entered into the LOPA table as the causal event. The failure rate can then be selected to meet the target frequency for the hazardous consequences of the scenario.

The following example uses these abbreviations for probabilities of failure:

λ_{DU}	Dangerous undetected failure rate for the safety function
PFD^{IPL}	The probability that other independent protection layers will fail to prevent the hazard
$PFD^{Process}$	The probability that the process design will ultimately fail to contain the hazard (This is the 'General Process Design' factor in LOPA, refer to IEC 61511-3 clause F.6)

The overall hazard rate $H = \lambda_{DU} \times PFD^{IPL} \times PFD^{Process}$

The target $\lambda_{DU} < \dfrac{\text{Tolerable hazard frequency}}{PFD^{IPL} \times PFD^{Process}}$

The rate of **dangerous detected** failures (represented as λ_{DD}) is not usually of concern provided that there is an immediate corrective response when failures are detected.

It is relatively easy to detect a majority of dangerous failures in machinery applications. Machinery safety functions can be designed in a way that enables automatic diagnostic functions or automatic frequent tests to detect dangerous failures.

Consider a ride-on lawnmower as a simple and contrived example. It might have an interlock that stops the engine if the operator is not sitting on the seat and the park brake is not engaged. A fatality might occur if the operator were to leave the machine unattended with the engine running and if the brakes were not applied.

The tolerable frequency for a fatality is typically set in the range from one in 100,000 years (10^{-5} pa) to one in 10,000 years (10^{-4} pa). That level of risk is at least an order of magnitude lower than the overall risk of unexpected death that people are exposed to from all causes. In this example we set the target at 10^{-4} pa.

We might assume that there is typically less than a 10% chance that the operator could not avoid injury if the machine were to move unexpectedly. We might also assume that there would be less than 10% chance of fatality rather than injury.

The performance target for the safety interlock failure rate λ_{DU} would then be set at

λ_{DU} = 10^{-4} pa / (0.1 x 0.1) = 10^{-2} pa.

That means that the overall dangerous undetected failure rate of the interlock would need to be less than one failure in 100 years.

The safety integrity level (SIL) target for the safety function could be set at SIL 2 because by definition, a SIL 2 safety function operating in a continuous mode has a dangerous undetected failure rate of less than one in 10^6 hours (about 110 years).

It makes no difference how often the operator tries to leave the machine unattended. It could be every day, or it could be once in 10 years. The reason that it makes no difference is that the hazard will arise as soon as the operator next leaves the machine without applying the brake if the interlock has failed.

The target for continuous mode and high demand mode safety functions is based on the worst case, i.e. it assumes a continuous hazard or at least a quasi-continuous hazard.

A hazardous situation can be expected to occur soon after a safety interlock fails so the hazard is treated as being continuous. Periodic testing once a year would not be frequent enough to reduce the risk significantly. In machine safeguarding applications safety function failure rates are limited by using techniques that prevent and/or detect faults in the safety function. Fault detection functions may be automatic or manually initiated. The function tests are relatively frequent, typically at least once per day or once in every cycle of the machine's operation.

Demand mode safety function probability of failure

In process sector applications most safety functions act in a low demand mode. Demand rates are usually much less frequent than once per year.

A dangerous failure in a safety function prevents the function from achieving its purpose of putting equipment into a safe state. Failure of a low demand mode safety function does not result in an immediate hazard. The hazard occurs only after a process disturbance or a process equipment failure causes a demand on the function.

Safety functions operating in low demand mode may be achieved without relying on continuous automatic diagnostic functions because the demands are so infrequent.

It is difficult to achieve continuous diagnostic coverage for devices that are not operated frequently. Most process sector safety functions rely on actuated valves that might be operated only once or twice per year. Jamming or sticking of the valve mechanism might remain unrevealed until the valve is tested or until the valve fails to act on demand.

Infrequent (e.g. annual) periodic testing can be used to reveal dangerous failures in low demand mode safety functions where continuous diagnostics are not practicable. If dangerous undetected failures occur at a reasonably constant rate, then the probability of failure on demand increases in proportion to the failure rate λ_{DU} and the time t since the last periodic test: $PFD \approx \lambda_{DU}.t$

If all dangerous failures can be revealed by periodic tests at time interval T_1, then immediately after a test $PFD \approx 0$. The probability increases linearly with time after the test. Immediately before another test after the time interval T_1, the probability has increased to its maximum:

$$PFD \approx \lambda_{DU} . T_1$$

The average probability on demand over the whole interval T_1 may be estimated as:

$$PFD_{AVG} \approx \frac{\lambda_{DU} . T_1}{2}$$

This simple relationship applies for a single-channel safety function operating in a low demand mode. The basic assumption is that the demands are much less frequent than the tests, so that faults are more likely to be revealed by a test than by a failure on demand.

The probability estimate needs to account for fault tolerance, diagnostics and redundancy in the safety function. The fully detailed equations from comprehensive mathematical models can be much more complicated but cannot usually provide results that are much more accurate than this simplified equation.

The mathematical models are all based on the assumption that failure rates are fixed and constant. In practice equipment failure rates always vary over at least an order of magnitude.

The simple approximation $\lambda_{DU}.T_1$ is sufficiently accurate to illustrate the difference between low demand mode and high demand mode in a single-channel safety function.

The conclusions generally apply equally to more complicated safety function architectures with ‘M out of N’ voting.

Responses to increasing demand rates in low demand mode

The basic process control system is usually the first line of defence in low demand mode process applications. Process alarms might provide the next layer of protection. Credit can only be taken for an alarm if an operator can be expected to respond to the alarm promptly enough to prevent a hazard. Ideally the alarm should be completely independent from the process control loop. It should at least have a separate sensor. Any shared devices or characteristics would need to be taken into account in the probability calculation. For example, if the alarm uses the same type of sensor then common cause failures would limit the risk reduction

Most safety functions are designed to operate as the next line of defence if the basic process control layer has failed and the operator cannot respond effectively to an alarm. The demand rate D on the safety function is then:

Demand rate $D = \quad CF \times PFD^{BPCS} \times PFD^{Alarms}$

CF	Cause frequency, the expected frequency of events that can cause a hazard
PFD^{BPCS}	The probability that the basic process control system will fail to prevent the hazard
PFD^{Alarms}	The probability that the operators will fail to respond successfully to alarms that are independent of the basic process control system

If we use the abbreviation PFD_{AVG}^{SF} for the probability of failure on demand of a safety function, then:

The overall hazard rate $H = \quad D \times PFD_{AVG}^{SF} \times PFD^{IPL} \times PFD^{Process}$

The target for hazard rate H is set to meet the owner's criteria for the tolerable frequency of the consequences expected for each hazardous event.

The target for the PFD_{AVG} of a low demand mode safety function is determined from the tolerable frequency and the demand rate D. Credit can be taken for the probability of failure of other protection layers.

The target $PFD_{AVG} < \dfrac{\text{Tolerable hazard frequency}}{D \times PFD^{IPL} \times PFD^{Process}}$

The overall hazard rate can be limited by improving the performance of the safety function or other protection layers.

The PFD_{AVG} of a safety function can be improved by:

- Reducing λ_{DU}
- Reducing T_1
- Increasing fault tolerance (an architecture with 'M out of N' voting can tolerate N-M faults)
- Reducing the common cause failure fraction β (the β factor represents the proportion of failures in 'M out of N' architectures that can be expected to affect all N channels in a similar way)

High demand mode is the limiting case that occurs when the demand rate D is so frequent that an undetected dangerous failure of the safety function is more likely to be revealed as a failure on demand rather than by testing.

For example, if the test interval T_1 is 1 year and the demand rate D is 100 times per year then the hazard can result soon after the failure of the function because the testing is not sufficiently frequent to reveal the failure.

The approximation $\lambda_{DU}.T_1$ is no longer valid because the demand rate is more frequent than the test rate. The 't' in the relationship $PFD \approx \lambda_{DU}.t$ is now the time since the last demand rather than since the last test.

If the demands occur at rate D, then the next demand occurs at time $t = 1/D$, so $PFD = \lambda_{DU}/D$.

$$PFD = \lambda_{DU}/D < \frac{\text{Tolerable hazard frequency}}{D \times PFD^{IPL} \times PFD^{Process}}$$

Then the demand rate D can be cancelled out of both sides of the relationship:

$$\lambda_{DU} \times PFD^{IPL} \times PFD^{Process} < \text{Tolerable hazard frequency}$$

The hazard rate H for a high demand mode safety function is clearly the same as for a continuous mode safety function.

The overall hazard rate $H = \lambda_{DU} \times PFD^{IPL} \times PFD^{Process}$

The transition from low demand to high demand can be thought of as occurring when the overall hazard rate has increased to the same rate that would be used to set the target for a continuous mode safety function.

For low demand mode: $H = D \times PFD_{AVG}^{SF} \times PFD^{IPL} \times PFD^{Process}$

For continuous mode: $H = \lambda_{DU} \times PFD^{IPL} \times PFD^{Process}$

If these hazard rates are equal, then:

$$D = \lambda_{DU} / PFD_{AVG}^{SF}$$

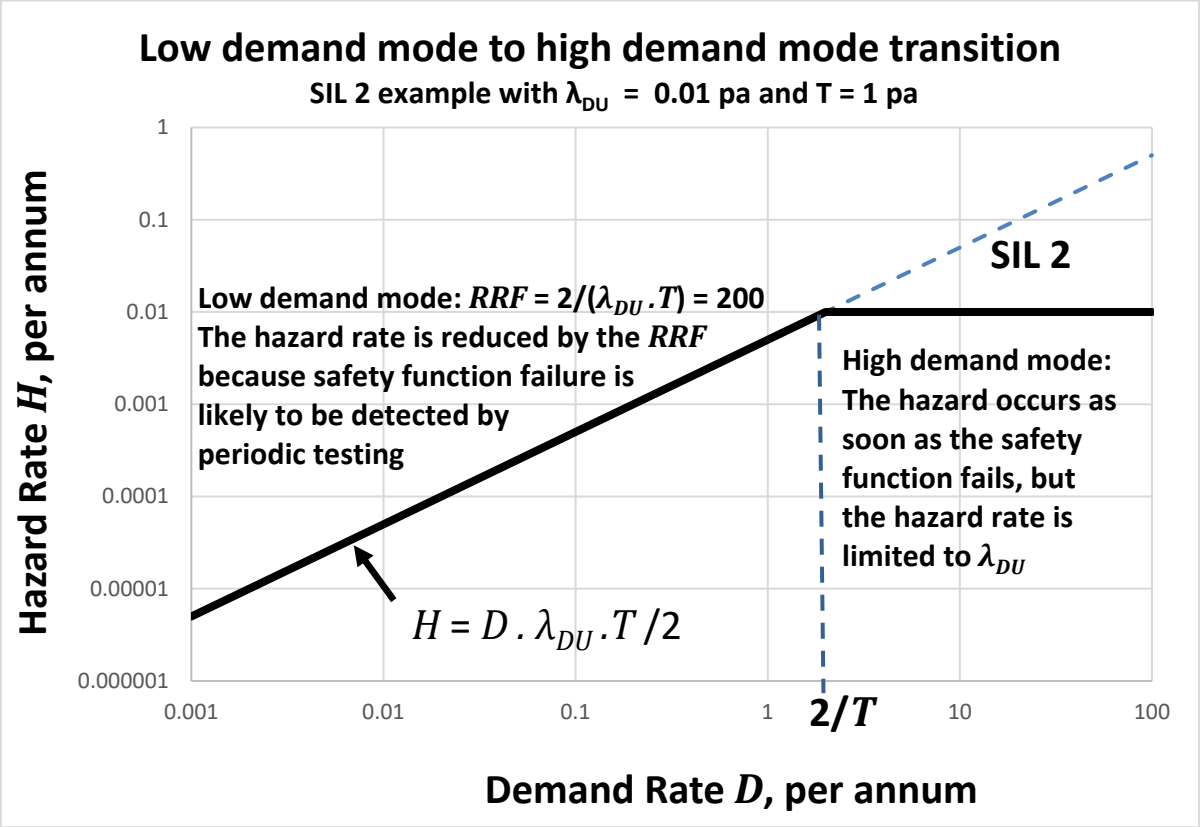
$$D = \lambda_{DU} / (\lambda_{DU} \times T_1 / 2)$$

$$D = 2 / T_1$$

Note that the approximation $\lambda_{DU}.T_1 / 2$ for probability of failure on demand is no longer valid when $D > 1/T_1$, so it is appropriate to consider the transition point from low demand to high demand as being at $D = 1/T_1$ rather than at $2/T_1$.

The definition of high demand mode in IEC 61511-1 is for demand rates > 1 pa. This is based on periodic testing and inspection at annual intervals.

Any further increase in demand rate on the safety function becomes irrelevant. The overall hazard rate is then determined only by the failure rate λ_{DU} of the safety function combined with probability of failure of other protection layers.



Refer to ISA-TR84.00.04-2020 Part 1 Annex I for further explanation.

Example of low demand mode with increasing demand rate

A pump supplies water to cool an exothermic reaction. If the pump fails, the basic process control system will stop the flow of reagents to the reactor. Thermal runaway of the reaction occurs so fast that an operator cannot be expected to respond to an alarm. For this example, we can assume that:

- The power supply to the pump might be interrupted once per year, i.e. 1 pa
- Process control systems typically achieve a probability of failure on demand of around 0.1.
- The probability of the reactor failing catastrophically due to thermal runaway is 0.1
- The probability of catastrophic failure causing a fatality is 0.1
- The maximum tolerable frequency for fatalities is 10^{-4} pa

The fatality rate could be estimated as 1 pa x 10^{-1} x 10^{-1} x 10^{-1} = 10^{-3} pa

The target PFD_{AVG} = 10^{-4} pa / 10^{-3} pa = 10^{-1}

The risk of fatality can be reduced from 10^{-3} pa to below 10^{-4} pa by applying a safety function with $PFD_{AVG} < 10^{-1}$

The demand rate on the safety function is the pump failure rate multiplied by the probability that the process control system will fail in stopping flow of reagents, D = 1 pa x 10^{-1} = 10^{-1} pa.

This would be classed as low demand mode because it is less than 1 pa.

A safety function could be designed with λ_{DU} = 10^{-1} pa and test interval T_1 = 1 year.

The $PFD_{AVG} \approx 10^{-1}$ pa x 1 y /2 ≈ 5 x 10^{-2}

This could be classed as a SIL 1 low demand mode safety function.
The hazard rate would be 1 pa x 5 x 10^{-2} x 10^{-1} x 10^{-1} x 10^{-1} = 5 x 10^{-5} pa.

After several years of operation, the operators might find that power supply is less reliable than expected. For example, the cooling water pump might fail at an average rate of 10 times each year.

The hazard rate has increased to 10 pa x 5 x 10^{-2} x 10^{-1} x 10^{-1} x 10^{-1} = 5 x 10^{-4} pa.

The risk needs to be reduced by at least a factor of 5 if the target for tolerable risk is 10^{-4} pa.

The demand rate on the safety function is now D = 10 pa x 10^{-1} = 1 pa. This is on the borderline between low demand mode and high demand mode.

If the safety function were still to be classed as low demand mode the PFD_{AVG} would need to be reduced by a factor of 5 from 5 x 10^{-2} (SIL 1) to ≤ 10^{-2}, on the borderline between SIL 1 and SIL 2.

The operators have a choice:

- Test the safety function at least 5 times per year (if practicable)

Or

- Reduce the failure rate λ_{DU} of the safety function from 10^{-1} pa to < 2 x 10^{-2} pa, while keeping the periodic tests at 1-year intervals

The problem with this second choice is that the demand rate is now the same as the test frequency. The expression λ_{DU} x T_1 / 2 is not valid as an estimate of average probability of failure on demand if the demands are as frequent as the tests.

Alternatively, the safety function could be reclassified as a high demand mode function. The demands are assumed to be quasi-continuous. The hazard will occur as soon as the safety function fails, so the safety performance depends only on the failure rate of the safety function.

The target is then expressed as limit on failure rate rather than failure on demand.

$$\text{The target } \lambda_{DU} < \frac{\text{Tolerable frequency}}{P(\text{thermal runaway}) \times P(\text{fatality})}$$

$$< \frac{10^{-4} \text{ pa}}{10^{-1} \times 10^{-1}}$$

$$< 10^{-2} \text{ pa}$$

A high demand mode safety function with a failure rate of 10^{-2} pa is at the upper end of the SIL 1 range, close to the border of SIL 1 and SIL 2.

The high demand mode target failure rate of 10^{-2} pa is half the failure rate of 2 x 10^{-2} pa that was sufficient for low demand mode, but in high demand mode the performance target is no longer directly dependent on the test interval nor on the demand rate.

Any further increase in demand rate would not affect the target for a high demand mode function because the target does not depend on demand rate.

Distinguishing between diagnostic tests and proof tests

Theoretically, proof tests could be carried out as frequently as necessary, perhaps once every day.

ISO 13849 does not distinguish between diagnostic tests and infrequent periodic tests. Diagnostic tests on machinery may be initiated automatically or manually.

IEC 62061 allows diagnostic tests to be initiated automatically or manually. It allows for infrequent periodic testing and inspection in addition to frequent diagnostics. The purpose of the infrequent periodic testing and inspection is to find deterioration, faults, and failures that are not revealed by diagnostics, and to verify the diagnostics.

IEC 61511-1 defines diagnostic testing as automatic on-line tests that are frequent in comparison to the process safety time (the time between an incident the causes a hazard and the occurrence of the resulting hazardous consequences). The objective of periodic proof test and inspection is to reveal faults and failures that are not detected by diagnostics.

There essentially two options:

1. If the demand rate is frequent (> 1 pa, or approaching 1 pa), set the safety integrity target in terms of failure rate.
   - Rely on frequent diagnostic testing to reduce the failure rate to meet the target.

2. If the demand rate is infrequent (<< 1 pa, e.g. < 0.1 pa), set the safety integrity target in terms of probability of failure on demand.
   - Use frequent diagnostic testing where practicable to reduce the failure rate.
   - Rely on periodic (typically annual) testing and inspection to meet the PFD target by revealing undetected failures that cannot be detected by diagnostics and may accumulate over time.

There is an underlying requirement here that effective corrective measures are taken when a fault is detected. The response must be fast enough to achieve and maintain process safety, or else the testing and response must be while the equipment is already in a safe state.

Responses to decreasing demand rates in high demand mode

Continuous mode and high demand mode functions are commonly used in machinery protection systems. Safety functions are designed to meet targets for the undetected dangerous failure rate λ_{DU}.

The undetected dangerous failure rate can be managed by using diagnostic coverage, well-tried components, well-tried principles, and fault exclusion techniques.

The final elements used in continuous and high demand applications are generally operated frequently during normal operation. This allows high levels of diagnostic coverage to be achieved through automatically monitoring successful action of the element in each cycle of operation. In machinery applications diagnostic coverage of at least 60% can usually be achieved. It may be feasible to achieve diagnostic coverage > 90%.

Failure of the safety functions will usually immediately lead to a hazardous situation. The overall risk can be reduced by limiting the occupancy (i.e. proportion of time that people are exposed to the risk) and by improving probability that people can avoid harm when the hazard occurs (e.g. provision of guarding and escape paths).

ISO 13849 is intended only to cover continuous and high demand safety functions.

The first edition of IEC 62061 also only covered continuous and high demand safety functions. The second edition released in 2021 introduced the option of low demand mode. It also introduced requirements for periodic testing, but the method of calculation does not change.

The advice in IEC 62061: 2021 is to assume that in low demand mode the demand rate is fixed at 1 pa, and then to treat low demand mode in the same way as high demand mode.

Treating low demand mode functions in the same way as high demand mode functions is a conservative approach. It does not take any credit for periodic testing in evaluating safety function performance.

A safety function that meets the target set for a high demand rate will always meet the target for any lower demand rate.

Example of high demand mode with decreasing demand rate

Consider an example of a machine that could cause a fatality if an operator comes into contact with moving parts. The machine is protected with a trip function that stops the machine if the guarding around the machine is not securely in place. For this example, we can assume that:

- The maximum tolerable frequency for fatalities is 10^{-4} pa
- An operator is near the machine for 10% of the time while it is in operation
- The operator can probably avoid the hazard if the guard is not in place, and the probability of an unavoidable fatality might be less than 0.1
- The operator uses the machine and is potentially exposed to the hazard every day.

The target failure rate λ_{DU} for the safety function could then be set at:

$\lambda_{DU} < 10^{-4}$ pa / (10^{-1} x 10^{-1}) = 10^{-2} pa.

This might be classified as a SIL 2 safety function operating in a high demand mode. A trip function like this might be designed to include an automatic test in every operating cycle of the machine. That would make it relatively easy to achieve the failure rate target.

If the operator were to use the machine less than once per year the function could be classified as low demand mode. The requirements could then be determined on this basis:

- The maximum tolerable frequency for fatalities is 10^{-4} pa
- An operator is near the machine for 10% of the time while it is in operation
- The operator can probably avoid the hazard if the guard is not in place, and the probability of an unavoidable fatality might be less than 0.1
- The demand rate is 1 pa

The target PFD_{AVG} could be set as < 10^{-4} / (10^{-1} x 10^{-1}), i.e. < 10^{-2}

A safety function with λ_{DU} < 2 x 10^{-2} pa and a test interval T_1 = 1 y would meet this target: $PFD_{AVG} \approx$ 2 x 10^{-2} pa x 1 y /2 ≈ 10^{-2}. If the demand rate were reduced to < 0.1 pa then the λ_{DU} target could be increased to < 2 x 10^{-1} pa. The high demand mode λ_{DU} target is always better than needed to meet the requirement for the low demand mode PFD_{AVG} target.

Sequence interlocks and permissive functions

Permissive interlock and sequence interlock are terms that may be used to describe functions that keep a machine, a sequence or process in its current safe state.

An interlock function may be used to prevent transition to a more hazardous state. Interlocks are commonly used in machine safeguarding applications.

Examples of interlocks that prevent action:

- A compressor prime mover is prevented from starting until the lube oil system pressure has been established
- The speed of a robot in a workshop is limited to a safe speed while people are in the vicinity of the moving parts
- The speed of a mobile machine in a stockyard is limited to a safe speed while the machine is close to its operating limits
- A gas-fired appliance start-up sequence is prevented from progressing from pre-purge to the pilot flame ignition phase until the pre-purge has been successfully completed
- The circuit breaker supplying a conveyor drive motor is kept isolated while the machine maintenance mode selector switch is locked in the maintenance position
- A lathe is prevented from starting while the guard in front of the machine is not locked securely in place
- The guard in front of a lathe is held locked in position by solenoid-operated latches while the machine is running. The locks prevent the guard from being removed.
- A process isolation valve cannot be opened unless the pressure across the valve is within safe limits and the upstream flow control valves are closed.

Machines or processes might also have similar interlocks as trip functions that action only in response to a hazard rather than preventing an action that leads to a hazard:

- A compressor prime mover is shut down if the lube oil system pressure has dropped below a safe limit
- A lathe is stopped if the guard in front of the machine is forced open while the machine is running.

Machine safety interlocks

Interlocks are commonly classified as safety functions in machine safeguarding applications.

Both ISO 13849 and IEC 62061 cover interlocks as safety functions. They do not use the term ‘permissive’.

The machinery standards treat demand mode functions and continuous mode functions in the same way.

The distinction does not need to be made between functions that prevent hazards rather than responding to hazards.

The performance targets are always set in terms of the overall dangerous failure rate for the safety function rather than considering probability of failure on demand.

Process safety interlocks

Some risk studies on process sector equipment identify sequence interlocks as safety functions.

Safety integrity targets may be allocated to interlocks. These interlocks are typically seen in the start-up sequences of hazardous equipment such as compressors and gas-fired appliances. Interlocks may be used to protect against potentially hazardous operator actions.

It might not be immediately obvious how sequence interlocks and permissive functions should be treated in process safety applications.

IEC 61511-1 does not specifically discuss interlocks that perform as safety functions. It refers to the term 'permissive' only within safety functions.

ISA-TR84.00.04-2020 Part 1 Annex H states that the term 'permissive' typically refers to subset of a safety function and is not typically synonymous with a safety function.

Interlocks in process sector applications may be treated in three different ways:

- A process may be designed so that its safety does not depend on interlocks that are allocated with safety integrity level targets
- An interlock may be classified as a low demand mode safety function, with the safety integrity level target defined in terms of failure on demand
- An interlock may be classified as a continuous mode safety function, with the safety integrity level target defined in terms of failure rate.

All three approaches may be valid.

Process safety interlock example

Consider an example of a permissive interlock in the start-up sequence of a gas-fired boiler.

The combustion chamber is purged with 5 changes of air volume before the pilot burner can be lit.

The purpose of the purge phase is to make sure that no unburnt gas remains in the combustion chamber. A shutdown purge should remove unburnt gas after a normal shutdown but it is possible for a shutdown purge to fail. Fuel gas may leak into a combustion chamber during maintenance activities if isolation procedures are not implemented effectively.

The boiler manufacturer advises that catastrophic damage might result if the pilot flame were to be ignited while an unburnt gas mixture remains in the combustion chamber. The design of the combustion chamber provides protection against overpressure from most uncontrolled ignition evets. In their assessment around 10% of uncontrolled ignition events would result in catastrophic damage. The damage could result in severe injury or death of people within 10 m of the boiler.

The purge is considered successful if all these conditions are satisfied:

- The main gas block valves are held closed
- The main gas bleed valve is held open
- The ignitor circuit is isolated and earthed
- The fan operates at the expected speed
- The air flow dampers are in the correct positions for purging
- The combustion air flow is within the normal expected range for a total of 15 minutes.

In this example the combustion specialists advise that the purge may fail for these reasons:

- The fan is not running at the correct speed
- The airflow path is blocked
- The air flow dampers are not in the correct positions

Different operators will have different applications, different policies and different practices.

The common requirement is that they need to demonstrate due diligence. They need to keep evidence that shows that they have made reasonable efforts to apply appropriate standards in managing the hazards in the workplace, and they need to monitor the effectiveness of the controls that they implement.

Risk assessment practices and the allocation of risk reduction to safety functions will vary with circumstances.

Company A: Non-safety rated sequence interlock

The members of the risk assessment team at Company A agree that:

- There are several ways of detecting fan failure. It is not plausible that the failure would remain undetected.
- Blockage of the airflow path is possible but unlikely. They agree that the frequency of blockage events would be less than 1 in 100 years.
- It is common that air flow dampers may stick or jam in the wrong position. They agree that over the course of one year 1 in 10 dampers could be expected to jam.
- There is a 10% chance that one or two people will be near the boiler during the start-up.
- For this area of the plant the tolerable fatality frequency is 10^{-4} pa

The team assesses the hazard rate assuming that the most likely cause is that the damper is jammed. The cause frequency is taken to be 10^{-1} pa.

Blow out panels are expected to provide pressure relief in most events. The probability of catastrophic failure is 10^{-1} (i.e. the LOPA 'general process design' factor).

They assume that anybody near the boiler will be killed and that probability of people being in the area is 10^{-1}.

The fatality rate is 10^{-1} pa x 10^{-1} x 10^{-1} = 10^{-3} pa which is a factor of 10 higher than the tolerable frequency of 10^{-4} pa.

Some credit could also be taken for damper position monitoring in the process control system if further risk reduction were necessary.

The team at Company A conclude that the purge sequence interlocks do not require any SIL target. The interlocks can be implemented in the standard burner management system that meets the relevant regulations and codes.

Company A specifies the boiler management system to meet the requirements of NFPA 85, Boiler and Combustion Systems Hazards Code. This standard specifies prescriptive requirements for purging. The interlocks do not need to be allocated with a target for safety integrity level (SIL). NFPA 85 is a prescriptive standard that does not apply functional safety.

Note that NFPA 86 Standard for Ovens and Furnaces specifies that any PLC used for furnace burner management must comply with IEC 61508 and must be capable of at least SIL 2. NFPA 86 specifies prescriptive requirements for purging but does not stipulate any specific SIL requirements for purge interlocks.

Company B: SIL rated low demand mode function

The members of the risk assessment team at Company B agree that:

- There are several ways of detecting fan failure. It is not plausible that the failure would remain undetected.
- Blockage of the airflow path is possible but unlikely. They agree that the frequency of blockage events would be less than 1 in 100 years.
- It is common that air flow dampers may stick or jam in the wrong position. On some occasions the damper blades have become detached, causing the damper to fail completely. They agree that over the course of one year 1 in 10 dampers could be expected to fail in a dangerous way.

- The company policy is that no credit can be taken for limited occupancy. The team assumes that that some people can always be expected to be near the boiler during the start-up.
- For this plant unit the tolerable fatality frequency is 10^{-5} pa. The overall target for the plant is 10^{-4} pa, but there are several other hazardous units in the plant, so a lower target is assigned for each individual equipment unit.

The team again assesses the hazard rate assuming that the most likely cause is that the damper is jammed. Failure would not necessarily lead to a hazard, and most failures would be detected by the process control system.

To be conservative, they assume that the overall frequency of events causing a hazard is 10^{-1} pa.

The probability of catastrophic failure is again taken to be 10^{-1}.

They assume that anybody near the boiler will be killed and that probability of people being in the area is 1.

The fatality rate is 10^{-1} pa x 10^{-1} = 10^{-2} pa which is a factor of 1,000 higher than the tolerable frequency of 10^{-5} pa.

The team at Company B conclude that the purge and pilot ignition sequence interlocks need to be implemented in a SIL-rated safety instrumented system. A risk reduction factor of 1,000 is on the borderline between SIL 2 and SIL 3. According to Company B's policies and standards, the sequence interlock is classified as a SIL 3 safety function. It is deemed to be operating in the low demand mode because the demand rate is in the order of 1 demand in 10 years.

The functional safety engineers might not be sure about how to specify the safety requirements for the interlock function. The action of the function is simply to prevent the start-up sequence form progressing. They decide to call this a 'sensor and logic only' function because it does not seem to depend on any final elements for action.

The safe state is defined as having the gas flow isolated and ignition sources isolated. The main gas block valves are already closed, and the bleed valve is already open. The ignitor circuit is already isolated and earthed. No further action is required, this safety function just needs to keep these final elements in their current state.

The safety function depends on two inductive proximity sensors which sense the damper blade position reaching the opened and closed limits. Sequence progression depends on confirmation that both sensors change state correctly as the damper moves from fully opened to fully closed.

The dampers are also equipped with continuous position transmitters that are monitored by the basic process control system. The team decides not to take credit for diagnostic functions that are in the process control system.

The engineers determine that the only potentially dangerous undetectable failure is for a proximity sensor to be misaligned. They assume that this type of failure would occur at a rate of less than 100 FITS (i.e. a rate of around 10^{-3} pa). Both sensors would have to fail in a similar way at the same time for the failure to be undetectable. They assume a value of 0.1 for the common cause failure fraction β. The rate of concurrent failure of both sensors is in the order of 10^{-4} pa.

The planned interval for inspection and testing is 1 year.

The estimated probability of failure of the sensors is estimated to be in the order of 0.1 x 10^{-3} pa x 1 y/2 ≈ 5 x 10^{-5}.

The probability of failure of the logic solver is taken to be 10^{-6}.

The overall risk reduction achieved is determined to be > 10^4, which exceeds the target of 10^3 by at least an order of magnitude.

Company C: SIL rated continuous mode function

The members of the risk assessment team at Company C agree in general with the assumptions made by Company B.

The Company C team take a different approach in defining the safety function. They specify that the objective of the safety function is to **keep the final elements in the safe state** whenever the boiler is off-line and until the required purge air volume has been measured.

In their interpretation this should be classified as a continuous mode function because it keeps the equipment in a safe state, and failure of the function itself may lead directly to a hazardous situation even if there are no other equipment failures.

Their safety requirements specification specifies that successful purge completion is sensed by:

- Fan blade speed sensor that confirms that the fan is operating at the correct speed
- The air flow is measured as being within +/-10% of the normal value.
- The purge has continued for at least 15 minutes.
- The damper was moved from the low-fire position to the pre-purge position, sensed by change of state in both proximity sensors.

The action is defined in terms of preventing uncommanded operation of the block and bleed valves and the ignitor while the boiler is off-line and until the purge is completed.

The interlock isolates the power to these devices. The power supply voltage and valve positions are monitored so that all dangerous failures are immediately detected.

The safety integrity target is set in terms of dangerous failure rate rather than probability of failure on demand.

The team again assesses the hazard rate assuming that the boiler will typically be off-line for 1 month each year, i.e. about 10% of the time.

The probability of an interlock failure leading to a catastrophic failure the boiler is taken to be 10^{-1}.

They assume that personnel will be near the boiler continuously while it is off line and while it is starting. Anybody near the boiler will be killed if the boiler fails catastrophically.

They choose not to take any risk reduction credit for occupancy, escape paths and guarding.

The tolerable frequency for a fatality is set at 10^{-5} pa.

The target failure rate for the safety interlock is then estimated as < 10^{-5} pa /(10^{-1} x 10^{-1}),

i.e. $\lambda_{DU} < 10^{-3}$ pa

This target is at the lower end of the SIL 3 range. For continuous mode functions the borderline between SIL 2 and SIL 3 is defined as 10^{-7} failures per hour. This corresponds to about 0.9 x 10^{-3} pa, or one failure in around 1,100 years.

The team at Company C decide to classify the interlock as a SIL 3 continuous mode function.

The safety integrity level target is relatively easy to achieve because all dangerous failures of the fan speed sensor and the air flow measurement can be detected by diagnostics in the burner management system. The air flow is directly related to fan speed.

The rate of coincident dangerous failure of the damper proximity sensors is again taken to be in the order of 10^{-4} pa.

All potentially dangerous failures of the final elements are detectable by automatic diagnostics in the burner management system. The block and bleed valves are subject to an automatic leak test each time the boiler is shut down and again each time before the boiler is started. Uncommanded operations of the valves are prevented by design and/or detected by position switches and gas pressure switches.

Conclusions

The target for high demand mode is set in terms of λ_{DU}, the overall rate of dangerous undetected failure. The requirements for high demand mode are easily met if safety functions can be designed to have high levels of diagnostic coverage (e.g. > 90%).

Low demand mode describes the operation of a safety function where the hazardous state occurs infrequently. The demand on the safety function occurs less than once per year. The target for low demand mode is set in terms of PFD_{AVG}, the overall average probability of failure on demand. It may be difficult to achieve diagnostic coverage in low demand mode functions. Annual periodic testing is used to limit PFD_{AVG}.

A safety function designed for high demand mode or continuous mode operation will always meet the requirements for low demand mode operation.

A low demand mode safety function with annual testing should be re-evaluated as high demand mode if the demand rate increases to approach 1 pa. High demand mode will have a more onerous failure rate target, but it will be the limiting case. The failure rate target in high demand mode is about half the rate that could be used for low demand mode. The target remains fixed in high demand mode, regardless of further increases in demand rate.

References

TABLE 1. STANDARDS AND CODES

Number and date	Title
IEC 61511: 2016	Functional safety — Safety instrumented systems for the process industry sector
IEC 62061: 2021	Safety of machinery – Functional safety of safety-related control systems
ISA-TR84.00.04-2020 Part 1	Guidelines for the Implementation of ANSI-ISA-61511-1:2018
ISO 13849-1: 2015	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
ISO 13849-2: 2012	Safety of machinery — Safety-related parts of control systems — Part 2: Validation

TABLE 2. REFERENCE DOCUMENTS

Ref	Title
1	King, A. G ., '*SIL Determination and High Demand Mode*' Presented at the Institution of Chemical Engineers Hazards 24 Symposium No 159, 2014 <https://www.icheme.org/media/8914/xxiv-paper-18.pdf>
2	Hui Jin, Mostia, W. L., and Summers, A., '*High/Continuous Demand Hazardous Scenarios in LOPA*' Presented at AIChE 12 Global Congress on Process Safety, Houston, Texas, 2016 <https://sis-tech.com/wp-content/uploads/2016/07/High_Continuous-Demand-Hazardous-Scenarios-in-LOPA.pdf>
3	Barnard, G., *'Impacts of Demand Rates on SIF/SIS Design and Mechanical Integrity'* aeSolutions Houston, TX < https://www.slideshare.net/GeoffreyBarnardPECFS/barnard-impacts-of-demand-rates >

I&E Systems Pty Ltd gratefully acknowledges contributions to this paper from Harvey Dearden of SISSuite.

