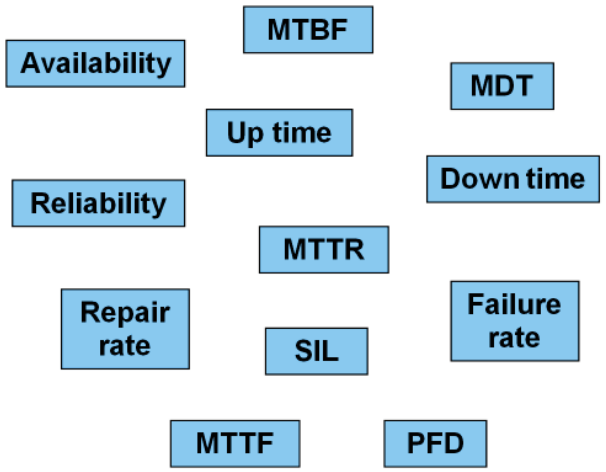
Availability, Reliability, SIL

What's the difference?



We often come across the above terms, and others, when we are talking about equipment and systems. All of them relate in some way to how well something will perform in a particular task; however it is important to use the correct term for the task in hand, otherwise you are likely to end up with the right answer ...but to the wrong question!

Which of these statements is true?

- A 'SIL' certified product is more reliable and will give fewer trips.
- I need 100% availability.
- If the Mean Time To Failure is 100 years, then half of the units will have failed after that time.
- Reliability and safety are the same thing.

Well, none of them are true; read on to find out more.

Reliability

What do we mean by reliability? Reliability is "*The probability that an item will perform a required function, under stated conditions, for a stated period of time*".

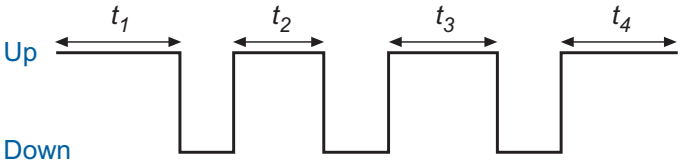
Put more simply, it is "*The probability that an item will work for a stated period of time*".

There are a number of ways of expressing reliability, but one commonly used is the Mean Time Between Failures. Let's examine what this means.

Mean Time Between Failures (MTBF)

MTBF is the mean operating time (up time) between failures of a specified item of equipment or a system.

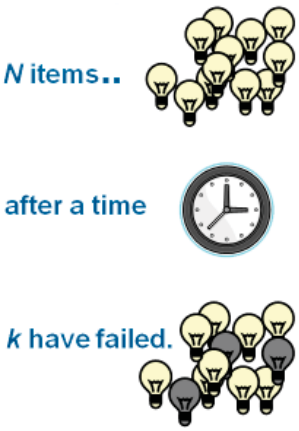
In the diagram, this is the average value of ***t*** over the operating life of the equipment.



MTBF is commonly used to express the overall reliability of items of equipment and systems.

MTBF is the correct term when talking about an item of equipment that is repairable. When we consider items that are not repaired when they fail, then Mean Time To Failure (MTTF) is the more correct term, but it does not much matter as they mean the same thing, Often MTBF is used when talking about non-repairable items too.

Failure rate (λ)



$$\text{Failure rate, } \lambda = \frac{\text{Number of failures}}{\text{Total operating time}} = \frac{k}{T}$$

Failure rate is measured in units of time^{-1}, such as failures per million hours.

Failure rate is often used to express the reliability of simple items and components. It is also frequently used to express the reliablity of particular functions, for example the dangerous failure rate of a safety system.

COOPER Crouse-Hinds

www.mtl-inst.com enquiry@mtl-inst.com

Relationship between MTBF and λ

Since

$$\text{MTBF} = \frac{\text{Total operating time}}{\text{Number of failures}}$$

and

$$\lambda = \frac{\text{Number of failures}}{\text{Total operating time}}$$

It is implied that

$$\text{MTBF} = \frac{1}{\lambda}$$

This is true, but only if the failure rate does not change over time. Usually this is so for simple equipment but not so for redundant[1] systems.

As MTBF and λ are measuring the same thing, why have different terms?

- *MTBF (years, hours) – is most often used to express the overall reliability of equipment.*
- *MTTF (Mean time to failure, years, hours) – more correct for items that are not repaired*
- *λ (hr^{-1}, pmh, FITs) – is convenient to use for components, and it is easy to calculate the MTBF of an item of equipment from the sum of the component λs. It is also commonly used to express the reliability of a particular function, such as a safety function.*

The meaning of MTBF

It is all too easy to assume that MTBF means average life or expected life, or something like that. It does not.

The table shows the percentage of units that will be still working, on average, after a time that is some multiple of the MTBF. For example, after a time equal to the MTBF only 37% of the units will still be working.

If only one unit is being considered, then the table shows the *probability* that the unit will still be working after a given time. After a time equal to the MTBF, the probability that a unit will still be working is just 0.37.

After a time equal to	Percentage of units still working, or the probability that a single unit will still be working
0.01 x MTBF	99%
0.1 x MTBF	90%
0.5 x MTBF	61%
1 x MTBF	37%
2 x MTBF	13%

1 - *A redundant system has two or more parallel paths so that the system continues to operate after the failure of one path.*

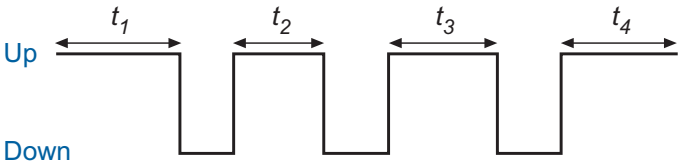
Availability

Availability can be defined as

"The proportion of time for which the equipment is able to perform its function"

Availability is different from reliability in that it takes repair time into account. An item of equipment may not be very reliable, but if it can be repaired quickly when it fails, its availability could be high.

Look again at the diagram we saw earlier:



From this we can see what is meant by Up Time – the time when the equipment is available - and Down Time – the time when the equipment has failed and so is unavailable.

The averages of each of these are:

- Mean Up Time, which we have already seen is known as the MTBF
- Mean Down Time, or MDT

By definition:

$$\text{Availability} = \frac{\text{Up time}}{\text{Total time}}$$

$$= \frac{\text{Mean up time}}{\text{Mean up time + Mean down time}}$$

$$= \frac{\text{MTBF}}{\text{MTBF + MDT}}$$

Sometimes *Mean Time To Repair* (MTTR) is used in this formula instead of MDT. But MTTR may not be the same as MDT because:

- The failure may not be noticed for some time after it has occurred
- It may be decided not to repair the equipment immediately
- The equipment may not be put back in service immediately it is repaired

Whether MDT or MTTR is used, it is important that it reflects the total time for which the equipment is unavailable for service, otherwise the calculated availability will be incorrect.

In the process industries, MTTR is often taken to be 8 hours, the length of an ordinary work shift but in reality the repair time in a particular installation might be different.

Unavailability

Sometimes unavailability can be a useful term:

$$\text{Unavailability} = 1 - \text{availability}$$

$$= 1 - \frac{\text{MTBF}}{\text{MTBF} + \text{MDT}}$$

$$= \frac{\lambda\,\text{MDT}}{1 + \lambda\,\text{MDT}}$$

$$= \lambda\,\text{MDT}$$

What is PFD?

PFD means *probability of failure on demand*. Safety systems are often designed to be working in the background, monitoring a process, but not doing anything until a safety limit is exceeded when they must take some action to keep the process safe. These safety systems are often known as *emergency shut down* (ESD) systems.

PFD is the *unavailability of a safety function*. If a demand to act occurs after a time, what is the probability that the safety function has already failed? As you might expect, the formula for PFD looks very similar to the formula above for general unavailability:

$$\text{PFDavg} \approx \lambda_{DU}\,\text{MDT}$$

PFD_{avg} means the *average probability of failure on demand*, which is really the correct term to use, since the probability does change over time – the probability of your system having failed will depend on how long ago you tested it.

Note that we talk about λ_{DU} here, the *failure rate of dangerous undetected failures*. We are not counting any failures that are deemed to be 'safe', perhaps because they cause the process to shut down, only those failures which remain hidden but will defeat the operation of the safety function when it is called upon.

This is important, as it warns us not to assume that a safety-related product is generally more reliable than a general purpose product. A safety-related product is designed to have a particularly low rate of failure of the safety function, but its total failure rate (or, equivalently, its MTBF) may not be very impressive.

So, what is the MDT for a safety function? By definition, a dangerous undetected failure will not be apparent until either a demand comes along or it is revealed by a *proof test*.

Suppose we proof test our safety function every year or two, say every T_1 hours. The safety function is equally likely to fail at any time between one proof test and the next, so, on average it is down for T_1 / 2 hours.

From this we get the simplest form of PFD calculation for safety functions:

$$\text{PFDavg} \approx \tfrac{1}{2}\,\lambda_{DU}\,T_1$$

What is SIL?

SIL is one of the most misused terms in the field of reliability. 'SIL' is often used to imply that a product has better quality, higher reliability, or some other desirable feature. It does not.

SIL means *safety integrity level*, a number between 1 and 4. It is used to describe the degree of safety protection needed by a process and consequently the safety reliability of the safety system necessary to achieve that protection. SIL1 is the lowest level of safety protection and SIL4 the highest.

Many products are described as 'SIL' rated, implying that they are suitable for use in safety systems. Whether this is really true depends on a lot of detail, which is beyond the scope of this article. But remember that even when a product genuinely complies with 'SIL' requirements, that is only telling you that it will do a certain job in a safety system. Its safety reliability may be high, but its general reliability may not be, as we noted in the previous section.

Useful to remember

- *An item is highly reliable if it works for a long time without failing.*
- *An item is highly available if it does not fail very often and, when it does, it can be quickly returned to service.*
- *A system is considered to be safe, if it is reliable in performing its safety function. The system may fail much more frequently in modes that are not considered to be dangerous.*
- *Consequently, a safety system may be less reliable in total (lower MTBF) than a non-safety system performing a similar function.*
- *'SIL' is not a guarantee of quality or reliability, except in a defined safety context.*
- *MTBF is a measure of reliability, but it does not mean the expected life, the useful life, or the average life.*
- *Calculations of reliability and failure rate of redundant systems are complex and often counter-intuitive.*