# Benefits and issues related to redundancy

**Alan Blight**
**GE Fanuc Automation Solutions SA**
**GE Fanuc Automation Solutions SA (UK Branch)**
**Tove Valley Business Park**
**Old Tiffield Road**
**Towcester**
**NN12 6PF**
**UK**
**alan.blight@gefanuc.com**

***Abstract: This presentation examines the concepts of reliability, availability and integrity, and expalins how redundancy affects them. It is designed to assist automation engineers in understanding the benefits and constraints of redundancy.***

## 1 Reliability

Reliability is not an exact science; it is based on probability and assumptions.

So no matter how impressive the statistics, engineers must remember that they are not a guarantee but an indication of probability.

### 1.1 Causes of failure

Failure may be due to several causes as shown in Figure 1 below:

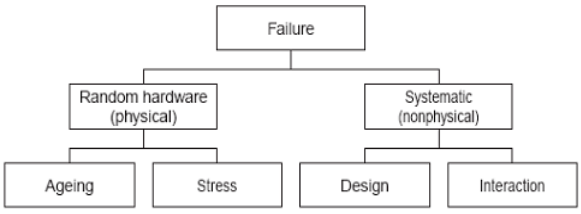


Figure 1 – Causes of failure

We will concentrate on random hardware failures for electronic components

Manufacturers will supply MTTF (Mean Time To Fail) data for their products but sensible engineers will examine the origins of that data. For example:

- Is it based on theoretical calculation, data from comparable known systems or actual failure data such as bench testing or field returns?
- Does it assume continuous operation or has the operating period been modified (eg no weekends) to extend the MTTF?
- Is there any data on how the product fails?

From the MTTF the failure rate can be calculated as

$$\text{Failure rate } (\lambda) = 1/\text{MTTF} \qquad (1)$$

The units will be the same at those for the MTTF, so if the MTTF is quoted in hours then the failure rate is calculated in failures per hour. Sometimes a universal unit called the FIT is used:

$$1 \text{ FIT} = 1 \text{ failure per } 10^9 \text{ hours} \qquad (2)$$

Most components follow the "Bathtub" model of failure where a high infant mortality (usually detected by the manufacturer's quality testing) is followed by a relatively constant random failure

rate over the useful life of the element (providing it is operated within the manufacturers specification) before failure rates increase again at the end of life.

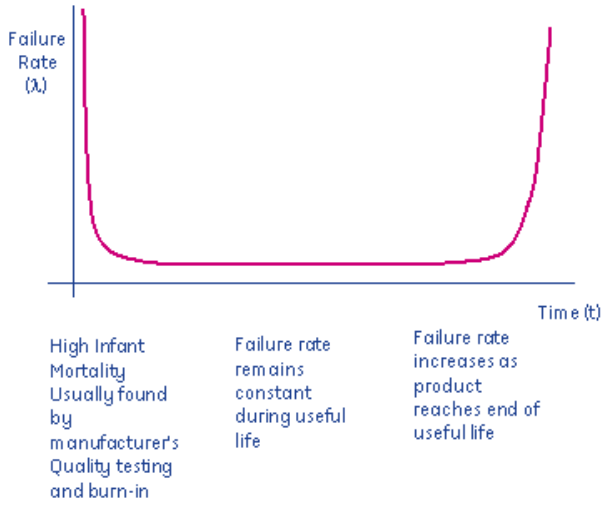


Figure 2 – Bathtub model of failure rates

Notice that by assuming the probability of failure for a functioning element on any given day is independent of how long it has already been functioning. We are assuming that elements don't "wear-out" (nor do they improve) over time. This characteristic is fairly accurate for many kinds of electronic devices with essentially random failure modes. However, in each application it's important to evaluate whether the devices in question really do have constant failure rates. Note that this is not the only model for failure probability, and other models (such as Weibull) may be found especially for mechanical components.

If the failure rate is constant then the density function follows an exponential decay. This can be explained in non-mathematical terms – if we start with 1000 healthy elements in circulation and the probability of failure is a constant 0.1 (ie 1 in 10) failures per year then after year 1 we can expect to loose 100 leaving 900 remaining. After year 2 we can expect to loose 90 leaving 810 in circulation. After year 3 we can expect to loose 81… and so on.

So the failure density follows the curve below, and is modelled by the function

$$f(t) = \lambda \exp^{-\lambda t} \qquad (3)$$

as shown in Figure 3 below

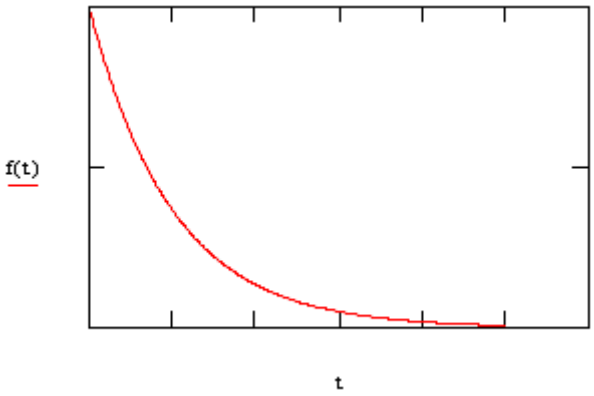


Figure 3 – Failure density for a constant failure rate

The probability of an element failing over a specific time interval is the integral (area under the curve) of the above function between those times. If we assume that the lifetime starts with t=0 and ends at t=t, the probability of failure is

$$PF = 1 - \exp^{-\lambda t.} \qquad (4)$$

Put another way, the probability of the element NOT failing (ie the reliability) of an element from t=0 to t=t is expressed as

$$R(t) = e^{-\lambda t}. \qquad (5)$$

Once a MTBF is calculated, what is the probability that any one particular element will be operational at time equal to the MTBF? We have the following equation:

$$R(t) = e^{-t/MTBF}.$$

But when t = MTBF

$$R(t) = e^{-1} = 0.3677$$

This tells us that the probability that any one particular element will survive to its calculated MTBF is only 36.8%.

Example: A component is required to run for 2 years.Two manufacturers offer to supply the component. The cheapest quotes a MTTF of 3 years for his component. The other component is more expensive but has a MTTF of 12 years

Reliability for the cheap component = $e^{-2/3}$ = 0.513 (Ie the chance of failure of this component in 2 years is about 50%)

Reliability for expensive component = $e^{-2/12}$ = 0.846 (ie the chance of failure of this component in 2 years is about 15%)

So, providing the element fits this reliability model, the engineer can make an educated choice about the best option, although note that choosing the more expensive component does not guarantee a longer lifetime, it merely increases the probability.

### *1.2 Redundancy and reliability*

So will redundancy increase the reliability?

If we have a dual redundant system with two identical elements then in order for the process to fail, both elements need to have failed.

The probability of failure = $(1- \exp^{-\lambda t})^2$ (6)

giving the failure density shown in Figure4 below:

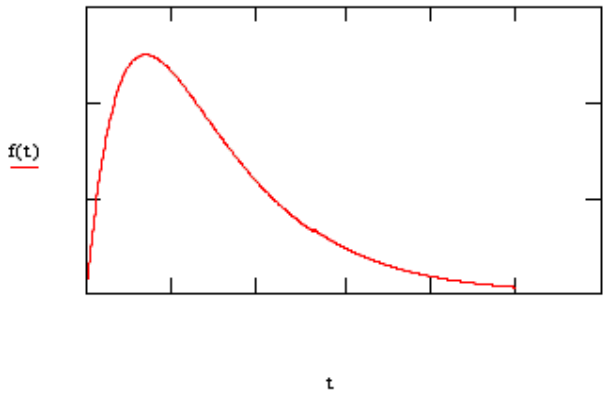


Figure 4 – Failure density for a duplex element with identical failure rates

Initially the probability of both elements failing failure is very low so it performs better than a simplex element, but as time progresses the performance degrades because both elements still have the same MTTF so it is unlikely that either or them will last significantly longer than the other.

In fact for a duplex system:

$$\text{MTTF} = \frac{3}{2\lambda} \quad (7)$$

For a triplex system:

$$\text{MTTF} = \frac{11}{6\lambda} \quad (8)$$

Based upon the assumption that the MTTF for a system with n identical parallel paths is

$$\text{MTTF} = \frac{1}{\lambda}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}.....+\frac{1}{n}\right) \quad (9)$$

So redundancy will not offer a dramatic improvement in reliability.

## 2 Availability

Availability (or uptime) is the probability that the system is actually running (or operational) at any given moment in time. It is NOT the same as reliability. When a component fails it is unavailable until it is repaired or replaced. Therefore we need to quantify the Mean Time to Repair (MTTR)

$$\text{System availability} = \frac{MTTF}{MTTF + MTTR} \quad (10)$$

(Note – the MTTR must be realistic)

To give a perspective on availability in relation to downtime, consider the table below.

| Availability | Downtime |
|---|---|
| 90% | 36.5 days/year |
| 99% | 3.65 days/year |
| 99.9% | 8.76 hours/year |
| 99.99% | 52 minutes/year |
| 99.999% | 5 minutes/year |
| 99.9999% | 31 seconds/year |

### *2.1 Redundancy and Availability*

If we consider two identical components in parallel, each with an availability of $A_s$ as shown in Figure 5 below:

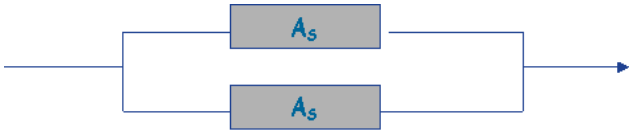


Figure 5 – Duplex Element

For a simplex system

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

For a duplex system =

$$\text{Unavailability} = (1-A_S)^2$$

(ASSUMING IDENTICAL SYSTEMS)

For a parallel system shown above

$$\text{Availability} = 1 - (1 - A_S)^2 \qquad (11)$$

If we take a system with a MTTF of 1000 hours and a MTTR of 8 hours, the simplex system will be unavailable for about 3.5 DAYS per year. The duplex system will be unavailable for about 30 MINUTES per year.

Therefore redundancy can make a very significant improvement to availability, providing the MTTR is short in relation to the MTTF.

However there is one further complication. Some causes of failure may be common to both elements (for example two elements fed from the same power source). So the system is represented by Figure 6 below:

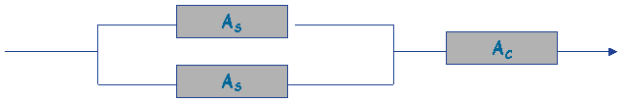


Figure 6 – Duplex Element with common cause failure component

In this case the common cause failure acts as a simplex element so we need to evaluate the fraction of common cause failures (β)

## 3 Integrity

Integrity is the probability that a system will perform a given function when called upon to do so. This is particularly important if the function is safety-related so IEC61508 bands the probability in a series of Safety Integrity Levels (SILs).

IEC61508 gives guidance on integrity throughout the lifetime of the system (called the safety lifecycle) from design to decommissioning.

In fact statistics from the UK Health & Safety executive (Figure 7) show that well over half the causes of accidents are designed into the system before it is ever operational.

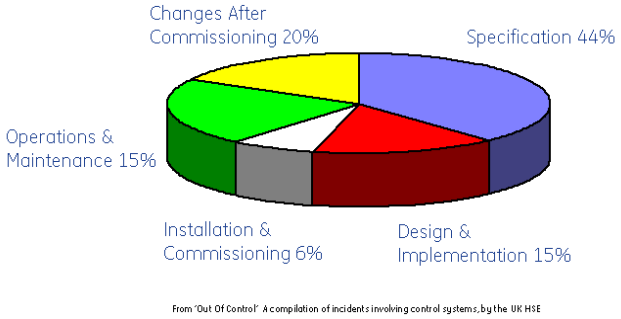


Figure 7 – Causes of incidents involving control systems

Therefore when designing a safety instrumented system (SIS) it is very important to try to predict causes of accidents and to design methods to prevent them.

IEC61508 adopts a risk-based analysis where the hazards associated with the process are identified, their risk of causing harm assessed, and if the risk is intolerable measures are implemented to reduce the risk.

One of these measures may be to introduce a control function, which is a SIS would be called a Safety Function.

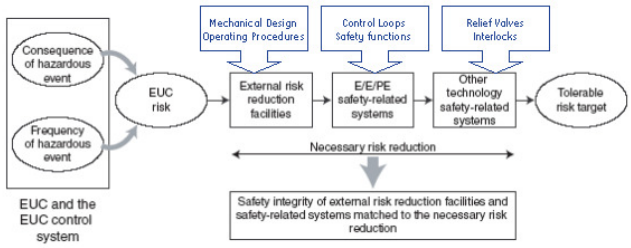


Figure 8 – Measures to reduce risk

As Figure 8 shows, the control system is just one of a number of possible measures to reduce risk.

The integrity is defined differently depending on whether the safety function is demanded rarely (such as a ESD or Fire & Gas system) or frequently such as in a burner management system. In Low Demand Mode, the frequency of demands for operation is no greater than one per year and no greater than twice the proof test frequency). All other systems are classified as High Demand mode.

For low demand systems the integrity is specified as the Average Probability of a failure on demand ( $PFD_{AVG}$ )

For high demand systems it is specified as the average probability of a dangerous failure per hour ( PFH )

Figure 9 below shows how the SIL is related to the probability of failure:

| Probability of failure | | |
|---|---|---|
| **Safety Integrity Level (SIL)** | **Mode of operation – on demand** (average probability of failure to perform its design function upon demand) | **Mode of operation – continous** (probability of dangerous failure per hour) |
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | $\geq 10^{-6}$ to $< 10^{-7}$ |

Figure 9 – Safety Integrity Levels

Typically safety functions are layered to provide a progressive response to an incident as shown in Figure 10 below

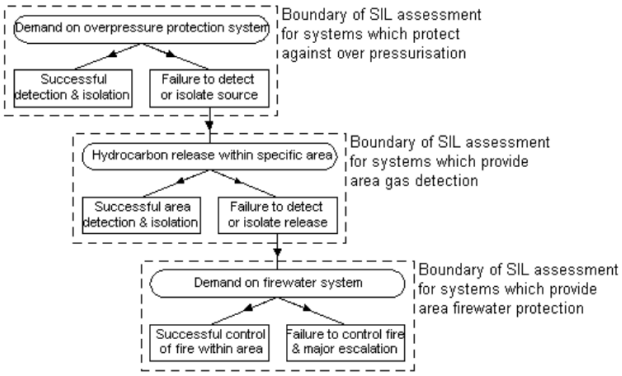


Figure 10 – Layered Safety Functions

In order for the control system to perform its function it must be available but although any component failure is undesirable, the way in which a component fails can have significant consequences.

Take a relay, for example. It can fail in one of two ways; either on or off. If the relay is connected to a fire warning siren the failure mode has different consequences.

If it fails ON the siren sounds even though there may not be a fire. This is inconvenient but not dangerous – this is known as a Safe Failure.

On the other hand, if it fails OFF the alarm will not be able to sound when there is a fire so the workers will be unaware of the danger – this is known as a Dangerous Failure.

If there is a requirement to test the siren every shift then the failure will soon be detected and can be repaired. However if the siren is only tested once every year then the failure could remain undetected for up to a year. So Diagnostic Coverage (which may be a function of the control system, such as monitoring for open or short circuits) is important in order to detect dangerous failures.

A relay is a relatively simple component with two failure modes but for more complex components the failure modes need to be analysed and categorised into safe and dangerous failures as shown in Figure 11. Typically this is done by Failure Mode, Effects and Diagnostic Analysis (FMEDA)

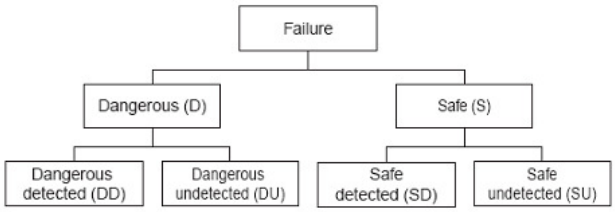


Figure 11 – Failure Modes

From this we get the Safe Failure Fraction (SFF)

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \qquad (12)$$

The point here is that failures themselves are not the problem; it is undetected dangerous failures that compromise safety.

### *3.1 Redundancy and Integrity*

For this reason, in addition to demonstrating an acceptable probability of failure, for SIL compliance we must also demonstrate an acceptable SFF. IEC61508 categorises components into two classes:

For type A subsystems it is considered that all possible failure modes can be determined for all elements. Typically this would be a simple field device.

For type B subsystems it is considered that it is not possible to completely determine the behaviour under fault conditions. Typically this would be a PLC. Most automation components are type B.

For a Type B subsystem:

To meet SIL 2 a simplex element must have a SFF of >90%

To meet SIL3 a simplex element must have a SFF of >99%

If this cannot be met by a simplex element, redundancy is required to introduce fault tolerance into the system so that another element can perform the safety function. Figure 12 shows the level of hardware fault tolerance required to meet a particular SIL

**Type B subsystems definition:**
Failure mode of at least one constituent component is not well defined, or
The behaviour of the subsystem under fault conditions cannot be completely determined, or
There is insufficient dependable data from field experience to support the claimed failure rates for detected and undetected dangerous failures

| Safe Failure Fraction | Hardware Fault Tolerance (N) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60% | Not allowed | SIL 1 | SIL 2 |
| 60% - <90% | SIL 1 | SIL 2 | SIL 3 |
| 90% - <99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

Figure 12 – Hardware Fault Tolerance against SFF

Therefore redundancy may be required to improve the integrity of a system

### *3.2 Proof testing*

The only way in which an element can really be shown to work is a proof test. Since these affect the operation of the plant they are generally carried out infrequently, although some techniques (such a s partial stroke testing of valves) offer an intermediate choice.

We have already seen that the probability of failure for an element with a constant failure rate (if we assume that the lifetime starts with t=0 and ends at t=t) = 1- exp $^{-\lambda t.}$ (4)

For a fully effective proof test we can assume that the system is fully functional with no failures so we can assign this as t=0

If we let t = the proof test period then the probability of failure during that time depends upon the proof test period, so shortening the proof test period can improve the integrity if a system.

This is reflected in the calculations in IEC61508 where different failure rates and proof test intervals are tabulated. Note that this assumption depends upon the fact that the proof test detects all failure which may be in the system. An imperfect proof test will alter the probability of failure.

Finally it must be remembered that a safety loop consists of several components – typically the sensor, input channel, logic solver, output channel and actuator.

The integrity requirement relates to the whole loop so poor performance of any one component can degrade the integrity of the loop. Typically the sensor and actuator are outside the scope of the control system vendor, so if the control system is just within the integrity limits required it might be difficult to achieve the integrity for the whole loop when the sensor and actuator are taken into account.

### *3.3 Redundancy architectures and integrity*

Where there are redundant components, there will be multiple versions of the same parameter. Therefore some voting strategy must be introduced to arbitrate if the different components produce different results.

These voting strategies are typically majority decisions. For example a 1 out of 2 (1oo2) strategy requires either one of two channels to execute a function whereas a 2oo3 strategy

requires two channels to agree before a function is executed (a single channel cannot execute a function)

In a failsafe strategy, any single failure will result in the plant assuming a safe state.

However in a fail safe and fault tolerant strategy if a channel fails the system will continue to operate using a degraded voting strategy. This is illustrated below in Figure 13:

| Fault-free system | Degradation 1 | Degradation 2 | Degradation 3 | System structure |
|---|---|---|---|---|
| 2oo4 | 1oo2 | Shutdown | | Safety related and fault tolerant |
| 1oo3 | Shutdown | | | Safety related |
| 2oo3 | 1oo2 | 1oo1* | Shutdown | Safety related and fault tolerant<br>*with time restriction |
| 2oo3 | 1oo2 | Shutdown | | Safety related and fault tolerant |
| 1oo2D | 1oo1D | Shutdown | | Safety related and fault tolerant with time restriction |
| 1oo2 | Shutdown | | | Safety related |
| 2oo2 | 1oo1 | Shutdown | | Safety related and fault tolerant |
| 1oo1 | Shutdown | | | Safety related |

Part 4 of the IEC 61508 gives the defintion of
**MooN :** M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)
**MooND :** M out of N channel architecture with diagnostic

Figure 13 – Degradation of a Redundnat System

### *3.4 Redundant Control Systems*

Redundant control systems operate differently depending on whether the aim is to improve integrity or availability.

In a high integrity system each element operates independently and the results are compared. If there are discrepancies the safest option is chosen. Additional elements may be added to improve the fault tolerance.

A high availability system operates in the same manner as a simplex system with the redundant component acting as a standby. In the event of failure of the active element the standby element takes over. Normally the redundancy is limited to the controller (primarily to maintain SCADA visibility) and there is no voting. The IO needs to be accessible to both controllers; normally this is simplex because redundant IO will need a voting strategy to deal with discrepancies.

Redundancy controllers may be synchronous or asynchronous. The term “Bumpless Transfer” is often used when specifying hot standby systems; this means that there will never be a change in state of IO as a result of control shifting from one controller to the other. The only way in which this can be guaranteed is if both controllers contain the same data 100% of the time and for this to be achieved the controllers must be synchronised – ie scan at the same time and exchange data during the scan.

This requires expensive hardware and usually an asynchronous system will suffice. This consists of two controllers scanning independently and exchanging data. In this system the redundancy is handled by software, and there will be a finite (but small) time lag between the data being sent from the active controller and being written in the backup controller. The latency depends on the amount of data, the speed of transmission, and the rate at which the controllers send and receive data (usually once per scan).

For many systems this latency can be made acceptably small so the cost benefit (in terms of the improved availability is well worth the expenditure over the lifetime of a plant.

### *3.5 Dont forget the SCADA*

When dealing with redundant controllers it is important to choose a SCADA with redundant drivers so that it can follow the active controller