TECHNICAL PAGES

Inductive Encoders

Celera
MOTION
A Novanta Company

Position Sensors for Safety Applications

TN-1518 | 191013

INTRODUCTION

Position sensors are a core element in modern control systems . In many cases, if a position sensor fails there is no implication for safety, whereas in other cases the consequences could be catastrophic. This paper outlines the design techniques that engineers should adopt with regards to position sensors to ensure safe and reliable equipment operation.

TERMINOLOGY

Firstly, we should define some terminology. For clarity and brevity, we will be using the term 'position sensor' to cover devices such as encoders, transducers and transmitters that measure angle, linear displacement, angular or linear speed and correspondingly output an electrical signal. Such devices can take a variety of formats such as potentiometers, resolvers, optical and inductive encoders.

In particular, 'failure' needs to be considered carefully. For the purposes of this paper, we consider three types of failure:

1. No output – the sensor stops reporting its output signal either permanently or intermittently
2. Incorrect output with error flag – output from sensor is incorrect but this is flagged by the sensor
3. Incorrect output with no error flag – sensor outputs an apparently correct reading but is actually reporting incorrect position.

Case #3 is typically the most serious type of failure.

Other useful terms are 'safety relevant' and 'safety critical'. These terms are often mistakenly used interchangeably by those unskilled in the art. Safety relevant generally refers to an instance where position sensor failure may have some safety implications whereas safety critical generally means that failure has significant safety implications. 'Intrinsic safety' is yet another term but it is not especially relevant to this discussion as it refers to sensors which operate in potentially hazardous or explosive environments. Intrinsically safe sensors prevent ignition in such atmospheres through various techniques such as encapsulation, sensor packaging, limiting the amount of stored energy etc.

SAFETY RELATED APPLICATIONS

When designing any position sensor into a safety related application it is useful to think in terms of a spectrum ranging from zero safety relevance to safety critical. As the degree of safety relevance increases, the most appropriate sensor arrangement changes. It is also worthy of note that as the safety relevance increases, generally the cost of the most appropriate solution also increases.

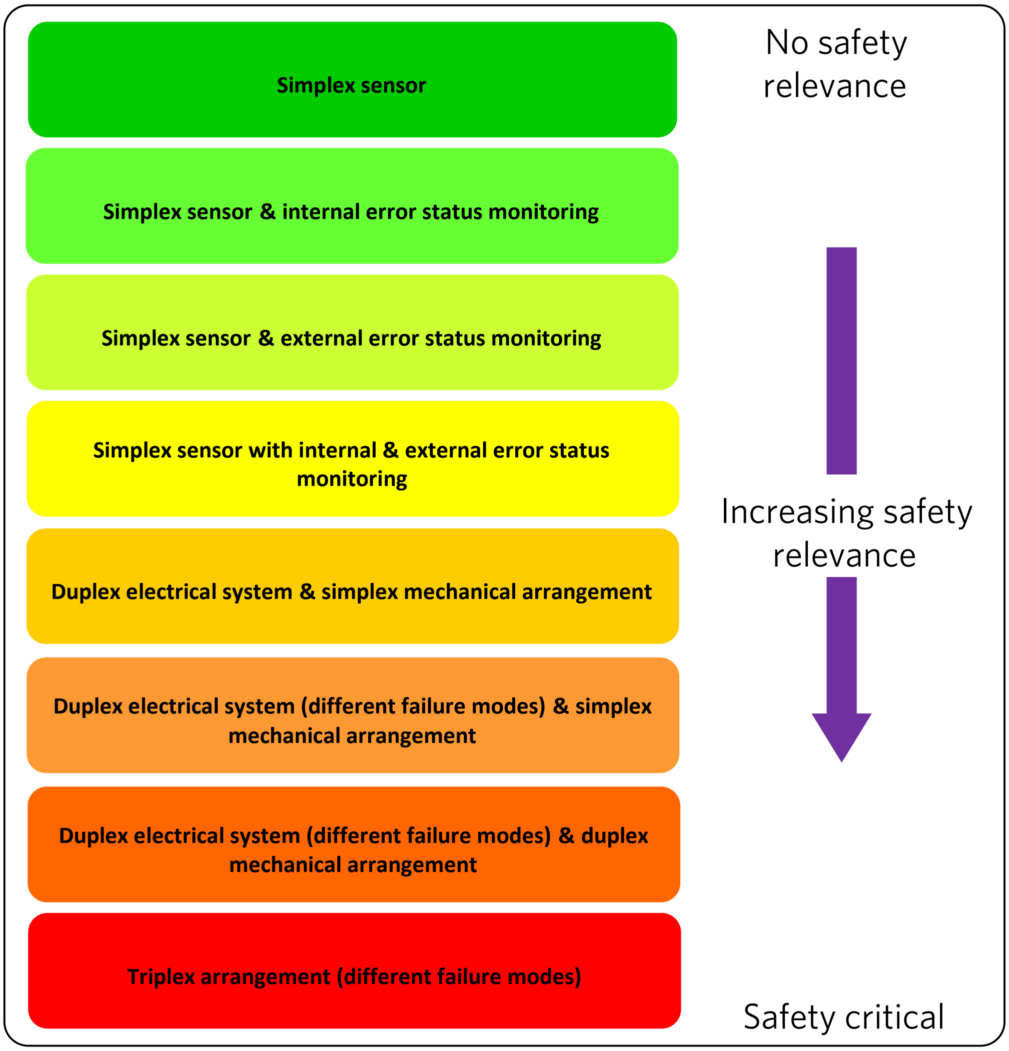
Simplex sensor
Simplex sensor & internal error status monitoring
Simplex sensor & external error status monitoring
Simplex sensor with internal & external error status monitoring
Duplex electrical system & simplex mechanical arrangement
Duplex electrical system (different failure modes) & simplex mechanical arrangement
Duplex electrical system (different failure modes) & duplex mechanical arrangement
Triplex arrangement (different failure modes)
No safety relevance
Increasing safety relevance
Safety critical

Figure 1. A spectrum of design approaches for position sensors as safety demands increase

An application with zero safety relevance is pretty straightforward. If we take the example of the potentiometer which controls the volume of a domestic radio then its failure typically results in only a minor inconvenience and there is no need for the potentiometer's performance to be monitored.

As safety relevance increases, the first step in the engineer's armory is to employ a sensor which can carry out some self-diagnostics often referred to as Built-In–Test or BIT. If the sensor fails one or more of its internal diagnostic tests, the sensor outputs an error flag instead of or as well as its output signal. Such error flags can take a variety of forms. For example, with an analogue sensor with a 0.5 to 10V output then the output can be reduced to <0.5V as an error signal. Similarly, devices such as modern inductive encoders (or 'Incoders') with digital outputs like SSI or SPI, can be configured so their communication protocol carries an error flag if necessary. Examples of built-in-tests include internal watchdog timer, internal flash data memory check or a timeout for receipt of a clock signal. Such sensors can continue to operate but the output contains a caveat which tells the host system "I'm giving you this data but watch out - it may be wrong". The receipt of such a flag by the host system should then be used to trigger going to a fail-safe state. A sensor which outputs its own error flag is said to be internally referenced.

As safety relevance increases further, sensors should be referenced externally and, in turn, both internally and externally. We can illustrate with an example of a microwave satellite communications antenna on a ship. Such antennas are typically required to move within a (software) defined arc so that on-board personnel or other equipment are not affected by the microwave energy. The failure of a position sensor on one of the antenna's axes can potentially lead to unsafe conditions. Such antennas are typically driven in azimuth and elevation axes by electric motors driving through a gearbox. The angle of the gearbox output shaft is typically measured by an absolute angle encoder whose failure can be internally monitored by the sensor itself and referenced by an internally generated error flag. Additionally, the output from a resolver or encoder on the motor's shaft (input to the gearbox) can be counted by the host system and used as a rough guide to the approximate angle of the antenna axis. Should the two measurements differ outside of expected bands then the microwave energy may be halted as the fail-safe condition.

The next step along the safety spectrum is to use redundant or duplex arrangements whereby two sensors are used to measure the same parameter - such as the rotation angle of a shaft. The safety of such arrangements can be increased further by using different types or constructions of sensor so that their failure modes differ.

An example of a duplex (electrically redundant) sensor is shown below in which the first sensor is shown on the inner ring and the second is shown on the outer ring. Whilst both sensors have a common mechanical housing, each operates electrically independently. Each has its own set of 10 built-in-tests and corresponding error flagging functionality. The inner and outer devices differ by virtue of different numbers of winding pitches on inner and outer rings and their electronics may also be chosen to be different – for example

- with an inner device outputting 0-10V and the outer device outputting a digital signal in SSI or similar format.
- with the inner device set with its zero position at 12 o'clock and the outer device with its zero position at 6 o'clock
- with an inner device outputting an incremental measurement (such as A/B pulses) and the outer device outputting an absolute digital signal such as SSI so that the inner may be used to check against the outer and vice versa.

Such differentiation in the sensor's design further helps mitigate against common failure modes and is one of the reasons why such devices are increasingly chosen for demanding, hi-rel applications.

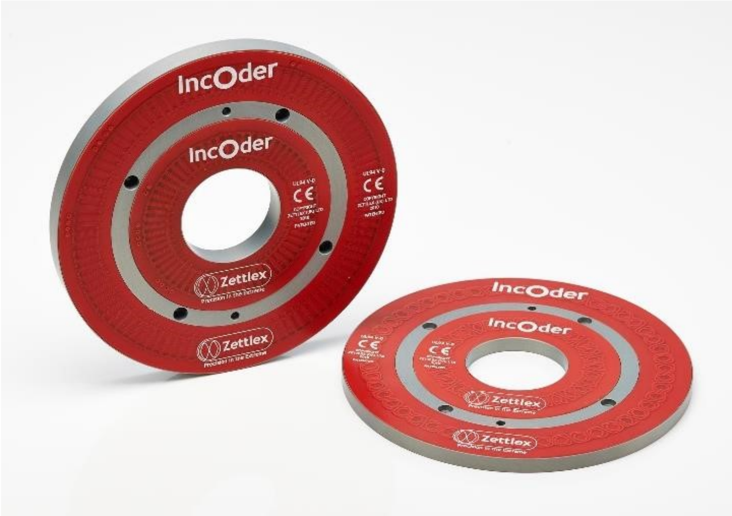

Figure 2. An example of an electrically redundant or duplex sensor

Many safety requirements can be met using electrically redundant sensor arrangements. Higher safety demands might also require mechanical redundancy - for example using two sets of mechanical components, again preferably arranged such that their failure modes differ.

A common adage in safety related system design is that when two sensors measure the same parameter, then if one of the sensors gives an incorrect output it may not be obvious which one is wrong. Simply put, they do not agree. Accordingly, the host system should be engineered such that it continues to operate only if the two sensors agree within reasonable bounds. If they do not agree the system should revert to its fail-safe state (or possibly reduced performance state).

Of course, whenever safety is a concern, it is an absolute must that highly robust and reliable sensors are selected. Non-contact, inductive sensors are an extremely reliable form of measurement device as they are not subject to failure modes caused by wear, dirt, condensation etc. Nevertheless, no matter how reliable, every sensor has a finite mean-time between failure. It should also be the case that the host control system should be arranged so that, as far as practical, reasonableness tests can be employed.

These tests may include for example:

- out of bounds measurements – if position measurements in a range of 1-1000units is expected and a measurement of 7000units is received it can be used as an error flag
- impossible steps in position or speed – if a system operates normally in arrange of say 0-60 rpm and a speed of 120rpm is shown then an error should be flagged
- cross referenced motions – for example if the angular motion of two mating gears is sensed – one which rotates clockwise causing the second to rotate anti-clockwise, then if both are sensed to be rotating clockwise an error should be flagged. Similarly, if their speeds do not vary in accordance with their gear ratio an error can be flagged.
- out of bounds energy consumption – for example an unduly high supply current to a sensor.

Notably, when MTBF data is aggregated, duplex arrangements are less reliable than simplex systems because of the inherently greater electrical and mechanical complexity. The most demanding applications – notably in aerospace, military and oil and gas applications - might also require that the host system continues to operate in the case of sensor failure. In such instances it may be the case that a triplex arrangement is required whereby the host system is configured so that a voting arrangement can instigated. In other words, at least two of the three sensors must agree within reasonable bounds for the equipment to operate (possibly at a reduced performance level). At an extreme all three sensors should differ such that all three do not have common failure modes and, as far as practical, the system should include some elements of mechanical redundancy.