Essential Concepts of Intrinsic Safety

Sean Costall, Sr. Certifications Engineer
Spark Institute, Calgary, AB, Canada

Updated: Originally written in 2016, this information remains as relevant as ever for 2025 and beyond. See our new white paper about the new 7th Edition of IEC 60079-11, coming soon to a theater near you!

Abstract

Intrinsically safe (I.S.) design is a particularly challenging form of engineering. It involves concepts that are outside the norm for ordinary design work. This guide will explain some of the essential concepts of I.S. design, which must be considered in order to achieve I.S. certification.

Limiting Energy

The first essential concept is that of *energy limitation*. I.S. devices are designed such that the total amount of energy available in the apparatus is simply not enough to ignite an explosive atmosphere. The energy can be *electrical* (in the form of a spark) or *thermal* (in the form of a hot surface).

This concept leads to several fundamental limitations in I.S. design. As energy must be limited, all potential sources of energy must be considered and appropriately limited to safe levels.

However, except for very simple apparatus, all electrical and electronic devices must contain energy to operate. This represents a fundamental contradiction. It is the role of the designer to find an appropriate compromise design, which is often challenging.

Energy limitations are best addressed from the very beginning of the design. If not, the situation becomes similar to converting a production-line family sedan into a high-performance stock car: it is possible, but also very difficult, expensive, and time-consuming.

One solution is to locate only very simple apparatus, such as thermocouples, inside the hazardous area. Another is to limit the total energy in the entire design. The most appropriate approach is dictated by the design requirements.

The design margin for electronic designs that are both operable and safe is often narrow, and can be difficult to find. There are few, if any, reliable references that can provide guidance; those that do exist are difficult to interpret. Designers must always be cautious about relying on theoretical predictions for allowable energy.

Faults

A second essential concept is that of *faults* and fault tolerance. Designers are often concerned with reliability, but the approaches taken to ensure safety in intrinsically safe design differ markedly from conventional measures of reliability.

Typical reliability metrics rely on analysis of the probability of failure, and lead to metrics such as estimated working life. I.S. design, however, does not concern itself with these types of measures.

Instead, I.S. designs are analyzed based on the premise that circuit faults are a certainty. Moreover, the premise is extended to assume that a nearly unlimited number of simultaneous faults can occur at the same time. The probability of failure is irrelevant and is not considered.

Such outlandish assumptions regarding failure may seem unreasonable, but they are not. In the field of hazard and risk analysis, it is not always enough to say that something is simply unlikely to happen; devastating consequences demand extra caution. Circuit faults are therefore considered inevitable in order to evaluate the possible effects.

Different levels of certification provide for different levels of fault tolerance, which are denoted by letters. 'A' level, or top-grade designs – designated type 'ia' intrinsically safe – are the most stringent, and are currently the only designs allowed in the most hazardous areas (Zone 0).

This is followed by 'B' level (type 'ib'), which is allowed in Zone 1 areas. Lastly, 'C' level designs (type 'ic') are specifically intended only for the least risky (Zone 2) areas.

Fault tolerance is also related to energy limitation. With failures being guaranteed, the circuit designer will likely find that the total energy in the circuit under "fault conditions" is much higher than in a 'normal' situation. This makes the task of limiting the total energy even more difficult.

Fortunately, the situation is usually not hopeless, so long as it is addressed early in the design process. The number of potential circuit failures can be reduced by following specific design criteria laid out in the I.S. standards. These rules provide the designer a measure of control to make the design both practical and safe.

The Worst-Case Scenario

This leads us to the final concept, that of the *worst case*. This concept makes the task of analyzing complex designs manageable, by reducing the possible number of scenarios that must be considered.

I.S. designs are always considered from a worst-case perspective in order to achieve maximum safety in their intended application. Of course, this again makes the designers' task more difficult.

Note that the worst case may not actually be the situation with the maximum number of circuit failures (known as 'faults'). In some cases, a single fault results in a worse situation than multiple faults. Generally, however, the worst case occurs at the maximum number of allowable faults.

The worst case is also inherently linked to the ideas of energy limitation. Generally, the worst possible energy case for any design occurs when all sources of energy available in the entire circuit are added up. This is because the design cannot physically exceed this total.

With appropriate design techniques, it is possible to either limit this total energy, segregate circuits into independent blocks that are isolated from each other, or both, thus allowing the design to stay within the permitted energy limits. There are, of course, specific criteria that must be followed to achieve this.

Even with this worst case analysis, there is a measure of uncertainty – designs can never be analyzed perfectly. To account for this, various margins of safety are routinely applied to account for any unanticipated effects.

Summary

The limit on allowable energy is the core of intrinsically safe design, and its biggest challenge. It is the single biggest obstacle to achieving a working design; it is also the single biggest reason why designs fail to meet I.S. requirements.

Fault requirements and worst case analysis both work against the designer, making retroactive changes extremely difficult. Addressing energy limitations, circuit fault requirements and worst case analysis from the very beginning of the design is the best approach for maximizing the possibility of success.