[1]Less Than Severe Worst Case Accidents

Gary A. Sanders, Mgr., 12332; SNL; Albuquerque, N.M.

Abstract

Many systems can provide tremendous benefit if operating correctly, produce only an inconvenience if they fail to operate, but have extreme consequences if they are only partially disabled such that they operate erratically or prematurely. In order to assure safety, systems are often tested against the most severe environments and accidents that are considered possible to ensure either safe operation or safe failure. However, it is often the less severe environments which result in the "worst case accident" since these are the conditions in which part of the system may be exposed or rendered unpredictable prior to total system failure. Some examples of less severe mechanical, thermal, and electrical environments which may actually be worst case are described as cautions for others in industries with high consequence operations or products.

Introduction

For many industries and products, safety is paramount and an assured, safe response in an accident is a key requirement during design, development and testing. A common approach to meeting this objective is to survey the industry historical experience for the most severe accidents, compile a data base of the worst case environments, and then test or model the design in the most severe accident environments to characterize the response. The argument is that, clearly, if the design can be shown to be safe in the most severe accident environment, then the problem is declared "bounded", the "envelope has been characterized" and any less severe environment is considered less threatening and - indeed - safe. A car, for example, which is designed to withstand an impact of 30 miles per hour into a wall would also be considered safe for lesser speed impacts if all other conditions remain the same.

While many systems depend upon survivability to ensure that the system can respond safely, there are many high-tech examples of systems such as medical lasers for surgery or computer controlled systems which may have high consequences if they operate in an unpredictable manner. For these systems, complete, safe, inoperable failure is more desirable than a system which is only partially disabled or intact and operating in an

[1] This work was supported by the United States Department of Energy under Contraact DE-AC04-94AL85000.

unpredictable manner - or which is normally contained or protected but is left partially exposed in an accident. Weapon systems, by their very nature, are designed to create some form of destruction under controlled conditions. As such, they certainly share this perspective of having potentially dire consequences if they prematurely operate. Bombs, for example, are designed to remain safe until a detonation is specifically intended in normal environments. As long as the weapon systems are unarmed and they remain intact to prevent any electrical stimuli from reaching their detonators, they are generally considered safe. In an accident, bombs which use insensitive high explosives are an example of systems where total system disintegration actually results in a nuclear detonation-safe response, while partial damage may leave a highly hazardous situation. For this reason, and to illustrate the points in this paper, high explosive bombs will be used as the prime example.

Mechanical

In mechanical environments, the integrity of containment is often the first example of a safety requirement. For bombs, the high explosive is often contained in an outer high strength casing to protect it from various forms of energy stimuli which could initiate it - primarily electrical energy. Many modern bombs use high strength metallic casings to form a Faraday cage to protect against alternating and direct current electrical systems, nearby and direct strength lightning strikes, and electromagnetic energy. It is readily apparent that as long as the casing is well designed and intact, the explosive is considered safe from electrical detonation. At very low impact velocities or crush loads, the casing will likely remain intact and ensure safe containment. At extremely high velocities, the weapon system, the associated electronics, and the insensitive high explosives are often pulverized into rubble and no longer operable as a bomb. However, for some range of intermediate velocities, the bomb casing may be breached yet leave an intact arming and firing system which is no longer entirely protected from subsequent electrical stimuli. Similarly, the crush environments that crush the weapon flat will yield an irreversibly inoperable system, while lesser crush loads may simply crack a bulkhead and allow electrical energy or conductive material to penetrate.

Wiring and printed circuit boards may similarly be effected by mechanical environments. In normal environments, wire insulation, printed circuit physical separation, and open switches may all provide low volta ge isolation from critical circuits. Again, very high energy mechanical environments will crush the circuitry into dust and render it safe. Lower energy environments may strip the insulation off the wires, move circuits closer together, dislodge piece parts and cause random shorts across circuits, close switches that are normally open, or in other ways reorient the electrical system. The mechanical damage may also cause damage to internal power supplies such as cracking a battery and allowing the electrolyte to flow into the cells and generate unwanted energy. This electrical energy could be coupled into the normal circuitry, or the mechanical damage may have crushed wires or caused shorts that couple the energy to other circuits.

Penetration of the system by puncture probes may also defeat the containment integrity, cause shorting of electrical circuits, allow water penetration that leads to shorts, provide a conductive pathway for electrical threats or even act as an antennae to attract and conduct lightning energy into the system.

Thermal

A severe fire will ultimately burn everything to slag and ashes and render a system safe while lesser thermal environments may create many of the same concerns as mechanical environments in that they may cause partial breach of a protective container while leaving the internal system intact and operable. Insulation may be melted and allow shorting, organic materials may become carbonized and create electrically conductive pathways, and solder may melt and open some circuits while flowing to complete other circuits. The electrolyte in batteries can expand due to heating, rupture burst discs, flow into the cells and produce power.

There are many examples of thermal responses which are actually reversible up to final destruction. Resistors can heat up and fail to operate, but when cooled can function again. High explosives can become heated and actually become more sensitive to mechanical shock initiation while heated or after recooling. Organic materials may have a high electrical resistivity at benign temperature, undergo a resistance drop as the temperature rises and then, if the temperature decreases prior to carbonization, the resistance is recovered as cooling occurs.

There are also examples of thermal activated safing devices which have interesting responses in less than severe environments. Explosive charges have been incorporated into circuits to explosively open the circuit in a fire. Some of these can be desensitized when subjected to heat transients below their initiation threshold so that they don't work later. Thermal fuses, often made with a solder plug which melts at nominal temperature thus allowing a spring to open the circuit have been known to open predictably, then melt further and the molten metal flows back together at higher temperatures prior to final destruction. Thermal batteries can be heated and produce voltage, and later be reheated and again produce energy.

While a full raging propellant fire of near 5000 degrees Fahrenheit will quickly destroy virtually every system, a slow cook fuel fire can allow slow carbonization, pressure buildup, and material interactions. One such interaction occurs between aluminum and steel. Steel normally melts at roughly 1850 degrees F, but when the lower melting aluminum comes into contact with the steel, the materials interact and the steel melts at about 1000 degrees F.

Electrical

Many systems are designed to withstand energy from an inadvertent lightning strike since the enormous amount of energy available is almost certainly the most severe case. The 1 percentile lightning strike is generally characterized as one with 200 kAmps and 400 kAmp/microsecond rate of rise to peak current. When such a pulse is put across a detonator input/output leads, the inductance of the cable often causes an arc across the input-to-output without effecting the detonator. Lowering the pulse to 20 kAmps, however, can actually prevent the current from taking the shortest distance air arc path to ground, and instead travel down the length of the detonator and fire the system. For the metallic Faraday cage casings mentioned earlier, it is often not the 200 kAmp peak current stroke that endangers the system, but the 700 amp continuing current between return strokes which can arc weld a hole through extremely thick metals.

Even much lower energy electrical faults can generate system failures. A circuit designed to carry one amp can be threatened by a fault that applies ten amps for several seconds causing insulation charring, circuit board charring, solder melting and splattering, and wiring shorts. Many of these faults may only be exhibited in certain orientations since the charring, loose wire, or melted solder may physically move if you simply tilt the board to another position.

Conclusions

For systems where faulty operation can have high consequences, total system failure in an irreversibly, inoperable, safe condition is often preferable to partial system failure in an unpredictable manner. As such, the design requirements that the system must be safe in the most severe accident environments is certainly important. However, many systems can easily be shown to be completely demolished in extreme impact, crush, thermal or electrical transients. Far lesser environments can often produce system faults which may only exist for the period of the exposure, they may cause continuous yet unpredictable faults long after the initial exposure, or they may actually desensitize the safing features and prevent safe responses in subsequent events. For these types of systems, the full range of environments must be characterized and considered to assure safe responses, rather than focusing simply on the most severe threats.

Biography

Gary A. Sanders, Mgr.
Sandia National Laboratories
Org. 12332, MS0492
P. O. Box 5800
Albuquerque, NM 87115 USA

Gary Sanders has nuclear and mechanical engineering degrees from Pennsylvania State University and over fifteen years of nuclear reactor and weapon safety experience. He is the manager of the Sandia System Surety Assessment Department.