**Gary Weidner, Product Safety Consultant**

# Hazard-Based Safety Engineering

## A process based presentation of Safety Principles

The term "Hazard Based Safety Engineering," or HSBE, emerged a few years ago at Agilent Technologies (then a part of Hewlett Packard) during development of an in-house product safety seminar. That seminar has matured into a two day UL seminar which presents safety in the context of "applying engineering fundamentals to the design and analysis of provably safe products." This article reviews the motivation for the HSBE approach and gives an overview of a curriculum that has been successful in presenting it.

HSBE instructors setting up electrical leakage demonstration. Students experienced low-level, controlled shocks. There's no teacher like experience!

Historically, product safety has sometimes been seen as an add-on to the design process. All too often, the product designers would work within a minimum set of safety guidelines and call in the safety staff for detailed compliance shortly before production was scheduled to commence. In today's world, that approach is inefficient. The proliferation of new and complex products, combined with increased regulatory and liability concerns, make product safety engineering more important than ever.

Early integration of safety compliance concerns into the product design cycle yields obvious benefits in the areas of time and cost. Time is money. There are immense pressures to shorten the "time to market"; redesigns due to safety compliance concerns can slow product introduction and increase cost.

Another area of concern is, or course, legal liability. Application of product safety standards through certification is a start, but is no longer a complete safety net against liability actions. A plaintiff's attorney in a product liability suit will certainly assert that a manufacturer should have foreseen a hazard, regardless of whether the language in a standard used for certifying the product addresses it.

With these considerations in mind, it is easy to see why the role of the safety engineer is both evolving and expanding. A professional example recognizing this reality is the recent creation of the IEEE Product Safety Engineering Society.

Industry is ahead of academia in addressing these issues. Engineering schools rarely teach even the basics of product safety engineering. An engineering course in that subject would likely relate safety measurements to the physical principles involved—which is the HSBE approach. With that in mind, let's examine the main topics in the HSBE seminar curriculum.

### Overview and Basic Principles

Most product safety education is devoted to the detailed requirements of particular standards. The HSBE approach is different. HSBE is an engineering process. The seminar described in this article combines lectures, visuals, and hands-on experiments along with problem-solving examples. It starts off with basic engineering principles, and then relates them to the hazards electrical products present.

Laws, regulations, liability concerns, and third-party certification all have the objective of injury prevention. The waters can get muddied when the focus is on addressing the effects of injury rather than focusing on the causes and anticipating them. The Hazards Based Safety Engineering approach brings the focus back to engineering principles that fulfill the "prevent injury" objective.

The seminar continues to lay its foundations by asking what "safety" and "hazard" really mean. The process oriented premise of HSBE is this: Any product that causes injury does so through the transfer of some energy to or from a body part as depicted by the HSBE three-block model shown in Figure 1. The energy may be thermal, or electrical, or may even be kinetic, involving the transfer of a mass of material.

At first glance the three-block model looks overly simplistic. However, its power in helping to quantify hazardous situations should not be underestimated. If we can quantify the energy source, the transfer mechanism, and the effect (e.g., the human body's susceptibility) we can predict whether or not injury will occur. To set the stage, the seminar introduces a number of common products, such as power tools, heaters, and appliances.

The last foundation topic is fault tree analysis. This concept is based on the U. S. Nuclear Regulatory Commission Fault Tree Handbook. The energy transfer model for injury is developed into the "HSBE standard injury fault tree" and employed throughout the course.

### Application To Thermal Hazards

Burns from contact with hot surfaces is a major product safety concern. Protecting personnel against burns involves understanding and controlling the mechanisms of heat production, storage, and transfer. Understanding heat storage involves a discussion of heat generation, thermal capacity, thermal resistance, and heat transfer. Information is presented on pain and burn thresholds as a function of exposure time and energy absorption rate.

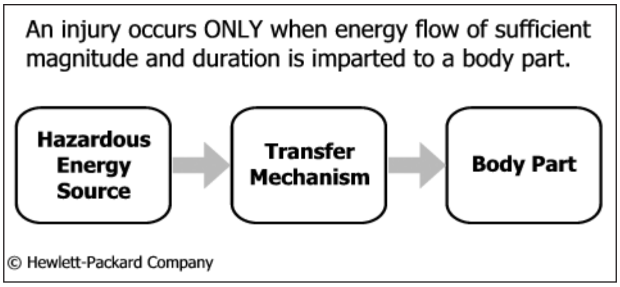


**Figure 1: The HBSE three-block energy transfer model for injury**

How hot is a watt? After some calculations for what will happen to a finger in contact with a 1 $cm^2$ hot spot, the class is exposed to a number of "hands on" thermal demonstrations. A number of materials maintained at the same temperature but with different thermal conductivities are presented for the class to touch.

The accumulated information on heat transfer and burn injury is organized into a burn injury "fault tree" which makes clear the relationships between conditions, causes, effects, and safeguarding mechanisms.

### HSBE And Electrical Shock

Electric shock is the next topic to be explored. The understanding of shock hazards begins with an understanding of how electricity affects the body's nerves, muscles, and electro-chemical system. The levels of electric shock are explained in detail, progressing from the threshold of sensation, through the level of involuntary reaction, to the "can't let go" level, and finally to the levels that produce cardiac fibrillation and cardiac and respiratory arrest. These physiological reactions are related to the stimulus in terms of voltage, current, frequency, and exposure time.

Given an electrical source, the resulting current will be related to the source's voltage and frequency by the impedance of the load. Unfortunately, when electrical shock is at issue, the impedance involved is that of the human body. Its impedance is a complex function, but data is available on its variation with voltage frequency, and the upper and lower limits that will be found from person to person.

Again, since experience is the best teacher, a controlled leakage demonstration is presented. Volunteers can have their hands exposed to modest levels of AC current. A video is then presented which shows the effects when a brave subject is exposed to considerably higher current levels, such as 12 mA, through his arm.

On the basis of the foregoing presentation, a model and fault tree for electric shock injury is developed. These tools are used to determine applicable safeguards. In the shock source/body load model, the variable parameters include voltage and current limitation, isolation, and protective grounding. Solid and air insulation are also treated in detail, along with their typical implementation and a discussion of insulation failure modes.

A more detailed discussion of these topics follows. For example, the issue of equipotential bonding, which is used to shunt fault energy to ground, is more complex than it might appear at first. That is why the National Electrical Code devotes 26 pages to it!

Insulation is presented in terms of basic, supplemental, and reinforced types. The issue of what makes supplemental insulation work is addressed in detail. Philosophically, it is a secondary layer or level of insulation added to a basic level, but it can come in a number of different forms. It might take the form of an insulating enclosure, an isolation transformer, an additional layer, or an extra-robust, "reinforced insulation". These are all presented and related to an electrical hazards fault tree.

### Understanding Fire Hazards

Product-related fires are always unintentional. However, an HSBE basics-first approach focuses on the combustion process itself before addressing the faults that may cause it. Combustion requires an ignition source, fuel, and oxygen. The manner of provision of fuel may not be obvious—for example, under heat, many plastics decompose in a process known as pyrolysis (literally, "fire splitting") to yield combustible gases and other flammable byproducts. The details of ignition are discussed, as are the types of flame and combustion.

Once the mechanism of fire generation and maintenance is understood, the process of safeguarding against it can be discussed. The likelihood of ignition can be reduced by managing the sources of heat, the way heat couples to potential fuel materials, and by the selection of less flammable materials.



Heat sources may be managed by controlling temperature, power dissipation, power density, and the duration of possible fault conditions. Reducing the cross-sectional area of the thermal pathway between source and fuel reduces the likelihood of ignition by controlling the coupling between heat sources and flammable material. Fuel management choices are somewhat limited to the selection of materials that are flame-retardant or have a high volatilization temperature. Heat sinking can also play a part by diverting heat from the flammable material.

Two additional fire safety measures involve the enclosure: containment and oxygen regulation. A fire-containing enclosure prevents or slows the escape of flames from the enclosure until the fuel is depleted. An oxygen-regulating enclosure prevents or slows air replacement, starving the fire. There is a tradeoff in the decision whether to provide more openings to vent heat buildup and reduce the chance of fire, versus using fewer openings, to contain the fire and reduce the airflow.

### Enter Safety Testing

The last module of the course discusses safety testing. Philosophically, HSBE unites with the safety process in a simple two-step process:

- First, test (or examine) to confirm the existence of hazardous energy sources
- Next, test to determine the effectiveness of protective safeguards

While this is a logical pair of ideas, in practice, considerable thought may be needed to decide what kind of testing should be done. That is where specific product safety standards come into play, and the motivation for their requirements. Remember that safety testing is performed on all products, whether intentionally by the manufacturer, or unintentionally by the end user.

### Conclusion

The seminar closes with a look at larger issues. Is the information used in the HSBE modeling process relevant to the product and its anticipated environment? In the real world, most things are variable. Manufacturing variations will affect both energy sources and safeguards. People will vary in their susceptibilities to hazards. To identify the hazards and their levels, we have to think beyond product specifics.

Another theme is the wider emergence of the HBSE philosophy in the product safety arena. Standards can be developed and viewed either as a recipe of design details or the logical outcome of a hazard-based performance analysis. This philosophy has taken root in Europe. For example, the Machinery Directive's Essential Requirements contain a risk and fault tree analysis. In electronics IEC Technical Committee TC 108, which is concerned with the safety of audio/video, information technology and communications equipment has a group working on a hazard-based assessment standard.

The purpose of HBSE based analysis is not to provide a magic "silver bullet" prescription for safety. What it does provide is a philosophy and set of tools for designing safety into products. ■

### About The Author

*Gary Weidner is an independent product safety certification consultant specializing in advice on meeting requirements of cleaning equipment standards. He may be reached at: gweidner@mchsi.com.*