NELSON & ASSOCIATES

3131 EAST 29TH STREET, SUITE E, BRYAN, TEXAS 77802

979/774-7755 info@hazardcontrol.com FAX: 979/774-0559

CORE PRINCIPLES OF SAFETY ENGINEERING AND THE CARDINAL RULES OF HAZARD CONTROL

Safety engineering, like any applied science, is based upon fundamental principles and rules of practice. Safety engineering involves the (a) **identification**, (b) **evaluation**, and (c) **control** of hazards in man-machine systems (products, machines, equipment, or facilities) that contain a potential to cause injury to people or damage to property.

A REALISTIC VIEW OF THE TERM "ACCIDENT"

Safety engineers recognize that accidents are typically dynamic events involving a combination of causative factors. *The term "accident" means a dynamic, multi-causal event that begins with the activation of a pre-existing hazard which then flows through its host system in a logical sequence of events, factors, and circumstances to produce a final loss event* (often including personal injury of the system operator).

IMPORTANT FOUNDATIONAL CONCEPTS

System Life Cycle

The concept of "system life cycle" recognizes that every system (product, machine, facility, etc.) has a "life cycle" which begins in the (a) "concept or definition" stage before proceeding through the successive stages of (b) system "design and development," (c) "production, manufacture, construction, or fabrication," followed by (d) system "distribution" before arriving at the (e) system "operation or deployment" stage, which after a period of time, is inevitably followed by (f) the "termination, retirement, recycle, or disposal" stage.

The Accident Process

Effective safety engineering and safety management must also take into account what has come to be known as "the accident process." This concept recognizes the fact that although personal injury or system damage may take place at a moment in time, the foreseeable causative factors that ultimately produce such injury or damage are typically set into motion, and could have been controlled or prevented, at an early stage in the system life cycle.

That is, this concept recognizes that foreseeable causes of accidents are typically set into motion well in advance of the injury or damage occurrence itself. A key element in the accident process is the concept of cause "foreseeability." A foreseeable cause is called a "proximate cause."

Producing vs. Proximate Cause

According to the safety engineering literature (having its counterpart in law), a **"**producing cause" means a cause which, in a natural and continuous sequence or chain of subsequent producing causes, produces an event, and without which the event (accident/injury) would not have occurred.

Some producing causes of accidents, through the use of reasonable and prudent methods of prediction, can be reasonably foreseen or anticipated before they actually produce an accident/injury event. Such a producing cause may further be identified as a "proximate cause."

That is, **a proximate cause** is a producing cause that **is reasonably foreseeable** (or should be reasonably anticipated) by a person exercising ordinary care to discover and control such causes before they produce accident events.

There can also be a hierarchy of proximate causes. One or more proximate causes might logically be viewed as a primary, dominant, or **root** proximate cause; that is, a proximate cause that necessarily sets all following causes in motion. These root proximate causes are typically created during the early stages of the system life cycle and should be the primary targets for elimination or control at that time.

FORESEEABLE VS. UNFORESEEABLE ACCIDENTS

Until an adequate accident causation analysis has been conducted, it is unwise to conclude that its causative factors were unforeseeable. Therefore, one might define the following two types of "accidents:"

Type I Accident

A Type I Accident might be considered an undesired and unforeseen event that results in an unacceptable system loss, which could have been foreseen and prevented through the prior application of recognized principles and methods of system hazard identification, evaluation, and control.

Type II Accident

A Type II Accident might then be defined as an undesired and unforeseen event that results in an unacceptable loss, which could **not** have been foreseen and prevented through the application of recognized principles and methods of system hazard identification, evaluation and control.

Obviously, Type I accident events should not be called "accidents" at all in the traditional sense, but rather, such an event should more realistically be called a "foreseeable loss event."

UNSAFE ACTS VS. UNSAFE CONDITIONS

Unfortunately, when discussing the causative factors of accidents, many people cling to the traditional over-simplified labels that have divided such factors into "unsafe acts" and "unsafe conditions." In balance, this dichotomy approach has proven harmful to the effective control of accidents.

Many otherwise sincere individuals have mistakenly believed or assumed that these factors are subject to equal control and that only one or the other of the two need be of major concern in the prevention of accidents. Typically, such focus has been on "unsafe acts," as the majority of practitioners do not possess the expertise to evaluate the technical issues involved, or do not recognize with what relative ease and positive effect unsafe conditions can be controlled.

The term "unsafe act" may also contain an unwarranted implication of *blame* or *fault* (rather than a genuine lack of knowledge or training). During the investigation of accidents, such an inordinate focus on "unsafe acts" will typically stifle the effective control of accidents, as the investigation is typically ended when the first immediate cause is identified (unsurprisingly some action or inaction on the part of the accident victim). As a result, potentially more important root causes related to system design are overlooked.

Herein, the term "unsafe condition" is retained, but the term "unsafe act" is rejected as historically leading to error or incomplete cause analysis.

Rather, inappropriate human actions or inactions of persons that contribute to accidents (resulting from error or human nature associated with the common relevant human factor capabilities and limitations of men and women) are called "unsafe actions," defined as unsafe system use methods and procedures, without any initial implication of fault or blame.

Hazard Control:
Engineering vs. Work Methods

Given the initial proposition that accidents can be prevented by either controlling the design of a system's hardware, or by controlling the actions or behavior of system operators – that is, by controlling the design of the product, machine, or facility (the *machine* or environment), or by controlling the actions of operators or users of such systems (the *man* or human factor), the question then becomes:

If the goal is the effective prevention of accidents (personal injury), should one give initial primary attention to the identification and control of potential unsafe physical conditions (hazardous system hardware components), or the identification and control of potential unsafe actions (unsafe work methods and system use procedures)?

In essence, this question is asking: Are hazardous product, machine, and facility components, **or** the hazardous actions or behaviors of people, more easily or effectively (a) ***identified***, (b) ***evaluated***, and (c) ***controlled?*** (See Appendix for a discussion of this issue.)

BASICS OF SAFETY ENGINEERING
STEP #1: HAZARD IDENTIFICATION

The first step in safety engineering is "hazard identification." A hazard is anything that has the potential to cause harm when combined with some initiating stimulus.

Many system safety techniques have been pioneered to aid in the identification of potential system hazards. None is more basic than "energy analysis." Here, potential hazards associated with various physical systems and their associated operation, including common industrial and consumer related activities, can be identified (for later evaluation and control) by first recognizing that system and product "hazards" are directly related to various common forms of "energy." That is, system component or operator "damage" or "injury" cannot occur without the presence of some form of hazardous "energy."

"Hazard identification" in reality can be viewed as "energy identification," recognizing that an unanticipated undesirable release or exchange of energy in a system is absolutely necessary to cause an "accident" and subsequent system damage or operator injury. Therefore, an "accident" can now be seen as "an undesired and unexpected, or at least untimely release, exchange, or action of energy, resulting, or having the potential to result in damage or injury." This approach simplifies the task of hazard identification as it allows the identification of hazards by means of a finite set of search paths, recognizing that the common forms of energy that produce the vast majority of accidents can be placed into only ten descriptive categories.

The goal of this first step in the hazard control process is to prepare a list of potential hazards (energies) in the system under study. No attempt is made at this stage to prioritize potential hazards or to determine the degree of danger associated with them – that will come later. At this first stage, one is merely taking "inventory" of potential hazards (potential hazardous energies). A practical list of hazardous energy types to be identified might include:

Mechanical Energy Hazards

Mechanical energy hazards involve system hardware components that cut, crush, bend, shear, pinch, wrap, pull, and puncture. Such hazards are associated with components that move in circular, transverse (single direction), or reciprocating ("back and forth") motion. Traditionally, such hazards found in typical industrial machinery have been associated with the terms "power transmission apparatus," "functional components," and the "point of operation."

Electrical Energy Hazards

Electrical energy hazards have traditionally been divided by the general public into the categories of low voltage electrical hazards (below 440 volts) and high voltage electrical hazards (greater than 440 volts).

Chemical Energy Hazards

Chemical energy hazards involve substances that are corrosive, toxic, flammable, or reactive, to include chemical explosives.

Kinetic (Impact) Energy Hazards

Kinetic energy hazards involve "things in motion" and "impact," and are associated with the collision of objects in relative motion to each other. This would include impact of objects moving toward each other, impact of a moving object against a stationary object, falling objects, flying objects, and flying particles.

Potential (Stored) Energy Hazards

Potential energy hazards involve "stored energy." This includes things that are under pressure, tension, or compression; or things that attract or repulse one another. Potential energy hazards involve things that are "susceptible to sudden unexpected movement." Hazards associated with gravity are included in this category and pertain to potential falling objects or persons. This category also includes the forces of gravity transferred biomechanically to the human body during manual lifting.

Thermal Energy Hazards

Thermal energy hazards involve things that are associated with extreme or excessive heat, extreme cold, sources of flame ignition, flame propagation, and heat related explosions.

Acoustic Energy Hazards

Acoustic energy hazards involve excessive noise and vibrations.

Radiant Energy Hazards

Radiant energy hazards involve the relatively short wavelength energy forms within the electromagnetic spectrum to include the harmful characteristics of visible, infrared, microwave, ultra-violet, x-ray, and ionizing radiation.

Atmospheric/Geological/Oceanographic Hazards

These hazards are associated with atmospheric weather situations such as excessive wind and storm conditions, destructive geological events such as instabilities of the earth's surface (rock or mud slides and earthquakes), and oceanographic currents and wave action, etc.

Biological Hazards

These hazards are associated with poisonous plants, dangerous animals, biting or poisonous insects, and disease carrying bacteria, etc.

Systematic Inventory of Potential Hazards

To develop a list of potential system hazards, one should consider each form of energy in turn. First, list each particular type of energy contained in the system under study, and then describe the various reasonably foreseeable circumstances under which it might become a proximate cause of an undesirable event. Here, full use of the published literature, accident statistics, system operator experience, scientific and engineering probability forecasting, system safety techniques (such as Preliminary Hazard Analysis, Fault Tree Analysis, Hazard Mode and Effects Analysis, and What-If Analysis), as well as team brainstorming are brought to bear on the question of how each form of energy might cause an undesirable event.

Prerequisite to such an identification of all system hazards is a thorough understanding of the system under study related to its general and specific intended purpose and all reasonably anticipated conditions of use.

Specifically, one must thoroughly understand (a) the engineering design of the system, including all physical hardware components - their functions, material properties, operating characteristics, and relationships or interfaces with other system components, (b) the intended uses as well as the reasonably anticipated *misuses* of the system, (c) the specific (demographic and human factor) characteristics of intended system users,

taking into account such things as their educational levels, their range of knowledge and skill, and their physical, physiological, psychological, and cultural capabilities, expectancies, and limitations, and (d) the general characteristics of the physical and administrative environment in which the system will be operated. That is, one must have a thorough understanding of the man/ machine/ task/ environment elements of the system and their interactions.

BASICS OF SAFETY ENGINEERING
STEP #2: HAZARD EVALUATION

The evaluation stage of the safety engineering process has as its goal the prioritizing or ordering of the list of potential system condition or physical state hazards, or potential system personnel of human factors compiled in Step #1.

The mere presence of a **potential hazard** tells us nothing about its potential danger. To know the danger related to a particular hazard, one must first examine associated **risk factors**.

Risk can be measured as the product of three components: (a) the probability that an injury or damage producing mishap will occur during any one exposure to the hazard; (b) the likely severity or degree of injury or damage that will likely result should a mishap occur; and (c) the estimated number of times a person or persons will likely be exposed to the hazard over a specific period of time. That is…

(1) H x R = D, and since

(2) R = P x S x E, then

(3) H (P x S x E) = D

where:

H= Hazard	P = Probability
R = Risk	S = Severity
D = Danger	E = Exposure

In the evaluation of mishap **probability**, consideration should be given to historical incident data and reasonable methods of prediction.

Use of this equation must take into account that an accident event having a remote probability of occurrence during any single exposure, or during any finite period of exposure to a particular hazard, **IS CERTAIN TO OCCUR** if exposure to that hazard is allowed to be **repeated** over a longer period of time. Therefore, a long term or large sample view should be taken for proper evaluation.

Determination of potential **severity** should center on the most likely resulting injury or damage as well as the most severe potential outcome. Severity becomes the controlling factor when severe injury or death is a likely possibility among the several plausible outcomes. That is, even when other risk factors indicate a low probability of mishap over time, if severe injury or death may occur as a result of mishap, the risk associated with such hazards must be considered as being "unacceptable," and strict attention given to the control of such hazards and related mishaps.

Exposure evaluation should consider the typical life expectancy of the system containing a particular hazard, the number of systems in use, and the number of individuals who will be exposed to these systems over time.

Acceptable vs. Unacceptable Risk

This step in the hazard evaluation process will ultimately serve to divide the list of potential hazards into a group of "acceptable" hazards and a group of "unacceptable" hazards. Acceptable hazards are those associated with acceptable risk factors; unacceptable hazards are those associated with unacceptable risk factors.

An "**acceptable risk**" can be thought of as a risk that a group of rational, well-informed, ethical individuals would deem acceptable to expose themselves to in order to acquire the clear benefits of such exposure. An "**unacceptable risk**" can be thought of as a risk that a group of rational, well-informed, ethical individuals would deem unacceptable to expose themselves to in order to acquire the exposure benefits.

Hazards associated with an acceptable risk are traditionally called "safe," while hazards associated with an unacceptable risk are traditionally called "unsafe." Therefore, what is called "safe" does contain elements of risk that are judged to be "acceptable." Once again, the mere presence of a hazard does not automatically mean that the hazard is associated with any real danger. It must first be measured as being unacceptable.

The result of this evaluation process will be the compiling of a list of hazards (or risks and dangers) that are considered unacceptable. These unacceptable hazards (rendering the system within which they exist "unreasonably dangerous") are then carried to the third stage of the safety engineering process, called "hazard control."

BASICS OF SAFETY ENGINEERING
STEP #3: HAZARD CONTROL

The primary purpose of engineering and the design of products and facilities is the physical "control" of various materials and processes to produce a specific benefit. The central purpose of safety engineering is the control of system "hazards" which may cause system damage, system user injury, or otherwise decrease system benefits. Current and historic safety engineering references have advocated a specific order or priority in which hazards are best controlled.

For decades, it has been well established by the authoritative safety literature (as well as by logic and sound engineering practice) that, in the order of preference and effectiveness, regardless of the system being examined, hazards are first to be controlled through (a) "hazard removal," followed by (b) the use of "physical safeguards," and then, after all reasonable opportunities have been exhausted related to hazard removal and safeguarding, (c) remaining hazards are to be controlled through the development and use of adequate warnings and instructions (to include prescribed work methods and procedures).

Listed in order of preference and effectiveness, these control methods may be called the " cardinal rules of safe design," or the "cardinal rules of hazard control."

Cardinal Rule #1

The first cardinal rule of hazard control (safe design) is "hazard elimination" or "*inherent safety*." That is, if practical, control (eliminate or minimize) potential hazards by designing them out of products and facilities "on the drawing board." This is accomplished through the use of such interrelated techniques as hazard **removal**, hazard **substitution**, hazard **attenuation**, and/or hazard **isolation** through the use of the principles and techniques of system and product safety engineering, system and product safety management, and human factors engineering, beginning with the concept and initial planning stages of the system design process.

Cardinal Rule #2

The second cardinal rule of hazard control (safe design) is the minimization of system hazards through the use of add-on **safety devices** or **safety features** engineered or designed into products or facilities, also "on the drawing board," to prevent the exposure of product or facility users to inherent potential hazards or dangerous combinations of hazards; called "*extrinsic safety*." A sample of such devices would include shields or barriers that guard or enclose hazards, component interlocks, pressure relief valves, stairway handrails, adequate lighting, and passive vehicle occupant restraint and crashworthiness systems.

Passive vs. Active Hazard Controls

A principle that applies equally to the first two cardinal rules of safe design is that of "passive vs. active" hazard control. Simply, a **passive** control is a control that works without requiring the continuous or periodic involvement or action of system users. An **active** control, in contrast, requires the system operator or user to "do something" before system use, continuously or periodically during system operation in order for the control to work and avoid injury. Passive controls are "automatic" controls, whereas active controls can be thought of as "manual" controls. Passive controls are unquestionably more effective than active controls.

Cardinal Rule #3

The third cardinal rule of hazard control (safe design) is the control of hazards through the development of warnings and instructions; that is, through the development and effective communication of safe system use (and maintenance) methods and procedures that first **warn** persons of the associated system dangers that may potentially be encountered under reasonably foreseeable conditions of system use, misuse, or service, and then **instruct** them regarding the precise steps that must be followed to cope with or avoid such dangers. This third approach must only be used after all reasonably feasible design and safeguarding opportunities (first and second rule applications) have been exhausted.

Further, it must be recognized that the (attempted) control of system hazards through the use of warnings and instructions, the least effective method of hazard control, requires the development of a variety of state-of-the-art communication methods and materials to assure that such warnings and instructions are received and understood by system users.

Among other things, the methods and materials used to communicate required safe use or operating methods and procedures must give adequate attention to the nature and potential severity of the hazards involved, as well as reasonably anticipated user capabilities and limitations (human factors).

Briefly stated, the cardinal rules of hazard controls involve system design, the use of physical safeguards, and user training. It must further be thoroughly understood that **no warning or safe procedure can equal or replace an effective safety device, and no safety device can equal or replace the elimination of a hazard on the drawing board.**

Appendix

Behavioral Human Factor Causes vs. Physical Condition Causes of Accident Events

Are hazardous product, machine, and facility components, **or** the hazardous actions or behaviors of people, more easily or effectively (a) ***identified***, (b) ***evaluated***, and (c) ***controlled?***

Question #1 – Within any man-machine system, are potential **unsafe conditions** (unsafe system hardware components) **or** potential **unsafe actions** (unsafe system use methods and procedures) **easier to IDENTIFY?** That is, how many potential unsafe system hardware conditions can be reasonably foreseen *as compared with* reasonably foreseeable potential unsafe actions (unsafe system use methods and procedures) or human error factors associated with system operation?

Answer – In most systems, the set of potential unsafe condition hazards is typically fewer in number (more finite) than the set of potential human errors or potential deviations from prescribed safe system use methods or procedures resulting from fatigue, distraction, and various hardwired (intrinsic and relatively unmodifiable) human factor capabilities and limitations).

Logically, one must choose to analyze and control the finite over the comparatively infinite. That is, **potential unsafe system condition hazards** are potentially **easier to identify**. It follows then that it is more effective to give one's initial primary attention to "the *machine"* rather than to "the *man*."

Question #2 – Are **potential unsafe conditions** (unsafe system hardware components) **or potential unsafe behaviors** (unsafe system use methods and procedures) **easier to EVALUATE?** That is, are the **probabilities** (and related injury *severities*) associated with foreseeable exposures to potential system unsafe condition hazards and resulting loss events **easier to calculate or estimate** than similar determinations of probability associated with potential unsafe actions or human error factors related to system operation?

Answer – In most situations, it is typically easier, **more predictable**, and **more accurate** to **calculate or estimate** the **failure rates** (accident probabilities and severities) associated with **hardware** system hazards (defects/wear/failures) than it is to predict the multitude of potential human errors or deviations from prescribed safe system use methods or procedures. Once again, this indicates that it is more effective to give primary attention to "the *machine*" rather than to "the *man*."

Question #3 – Are **potential unsafe conditions** (unsafe system hardware components) or **potential unsafe behaviors** (unsafe system use methods and procedures) **easier to CONTROL?** That is, if the ultimate goal is overall "hazard control," are hazardous physical conditions of hardware systems, or potential human error and deviations from prescribed safe system use methods or procedures, more susceptible to effective, positive, and more permanent control?

Answer – As verified by the authoritative safety literature for the past several decades, **engineering controls** (the removal or physical safeguarding of potential hazardous product, machine, or facility system components) are **universally recognized as being more effective** and long lasting than behavioral or administrative controls.

For the third time, this recognized hierarchy dictates that, at the earliest stage in a system's life cycle that potential system hardware hazards can be foreseen, primary attention should be given to the elimination or engineering control of hazards.

A "bonus" advantage of controlling physical system condition hazards in the early stages of a systems life cycle is the safe system design "on the drawing board" can automatically eliminate the potential effect of later "operator errors." The fact that operator errors are typically the result of system design errors is exemplified in the safety and human factors engineering proverb: "***How a system, product, or facility is designed will dictate how it can and will be used***."

CAUTION: The fact that control of system hazards and resulting potential personal injury to system operators and users is recognized as first involving attention to designing *hazards out*, and designing *safety into* various product, machine, and facility systems, should not detract from the **vital importance** of giving paramount attention to the use of **adequate warnings and instructions** and the development and effective communication of **safe system operating methods and procedures** to system users ***at the proper time*** in the system design process.

In every hardware system, not only must human factors be considered early in the design process to learn how people might be exposed to system hazards, so that these hazards can be removed or minimized in the design process, **residual hazards** that cannot be designed out of such systems through engineering means **must be given proper attention** in the form of **adequate warnings and instructions**, and in many situations, required **formal training** (and subsequent supervision). If the training becomes complex, a **formal certification** program must be developed.