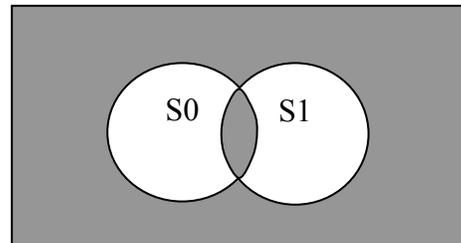


# Chapter 1 Markov

## Markov Analysis

In this section we will talk briefly about markov chain analysis of probability states.

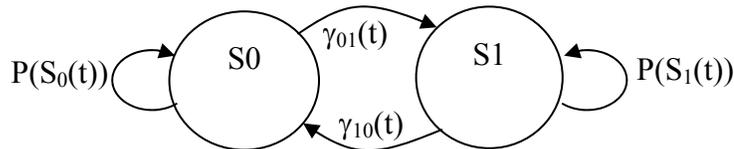
Figure 1 shows a Venn diagram of two probability sets plus all probabilities that are not contained in either set. Each set represents the probability that our system is in a given state. The shaded intersection is interpreted as no members of S0 are contained in S1 and visa-versa. Also, there are no states outside S0 and S1, they are complete. However, it is possible to instantaneously flip between the states.



In a markov diagram, circles represent mutually exclusive states that the system can attain, denoted S0, S1, S2...Sn  
 Arrows represent the transitions out-of or in-to a state.

The probability of being in a state is equal to 1 minus the probability of the sum of all exits from the state.

$$P(S_n(t)) = 1 - \sum_{n=0}^m \gamma_{nm}(t) \tag{1.1}$$

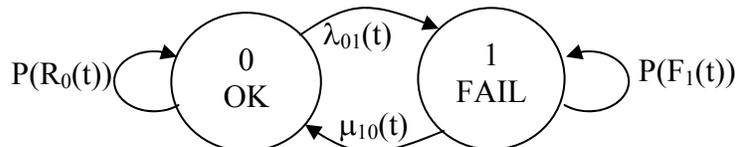


In the diagram above, the probability of being in state S0 at time t is:

$$P(S_0(t)) = 1 - \gamma_{01}(t)$$

In reliability analysis, states represent success and failure states of a system. Transitions from a lower to a higher state are failure probabilities  $\lambda(t)\Delta t$ , and transitions from higher to lower states are considered repair rates,  $\mu(t)$ .

With that in mind the figure can be redrawn as a reliability model where S0 is the fully operational state and S1 is a failed state:



The English interpretation of this diagram is:

Given the system starts in state 0;

The probability of transitioning to the failed state is the failure rate multiplied by the time interval  $\lambda(t)\Delta t$ . Therefore the probability of not transitioning is  $1-\lambda(t)\Delta t$ .

Once the system has transitioned to state 1, the probability of transitioning back to state S0 is the probability that it will be repaired within  $\Delta t$ , repair rate  $\mu_{10}(t) \Delta t$ . Therefore the probability of staying in state S1 is  $1-\mu_{10}(t) \Delta t$ .

Reminder: when  $\lambda(t)\Delta t \ll 1$ ,  
 $1 - e^{-\lambda(t)\Delta t} \approx \lambda t$

In order to solve markov chains it is necessary to use linear algebra to solve for the probability of being in any state at time t. Using this method it is possible to do two things:

1. Solve for the limiting, steady state probabilities for each state; and
2. Create a model that gives probability of failure as a function of time.

We start with the probabilities of being in a state or transition at any time t. This is the transition matrix. It describes the probability of transitioning from one state to another. The matrix is constructed by inserting the probability of the transition from row number to column number. The matrix diagonal () is the probability of being in a state. All others are transition from one state to another.

$$\begin{bmatrix} P_{1 \rightarrow 1} & P_{1 \rightarrow 2} & P_{1 \rightarrow 3} & P_{1 \rightarrow n} \\ P_{2 \rightarrow 1} & P_{2 \rightarrow 2} & P_{2 \rightarrow 3} & P_{2 \rightarrow n} \\ P_{3 \rightarrow 1} & P_{3 \rightarrow 2} & P_{3 \rightarrow 3} & P_{3 \rightarrow n} \\ P_{n \rightarrow 1} & P_{n \rightarrow 2} & P_{n \rightarrow 3} & P_{n \rightarrow n} \end{bmatrix}$$

Next we give starting conditions. This is the S matrix. If the system starts out fully repaired and perfectly operable, the starting matrix is:

$$S = [1 \quad 0 \quad 0 \quad 0_n]$$

When we multiply the transition matrix by the starting matrix we get the matrix at t+dt.

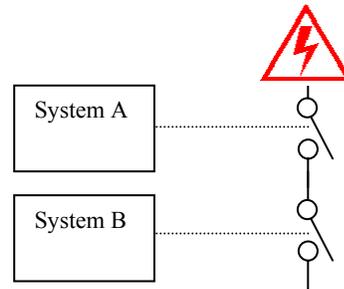
Transition Matrix

$$P = \begin{bmatrix} P(S_0) & \lambda_{01} & \dots & \lambda_{0n} \\ \mu_{10} & P(S_1) & & \\ \dots & & \dots & \\ \mu_{m0} & & & P(S_n) \end{bmatrix} \tag{1.2}$$

note that the sum of any row must add up to 1.

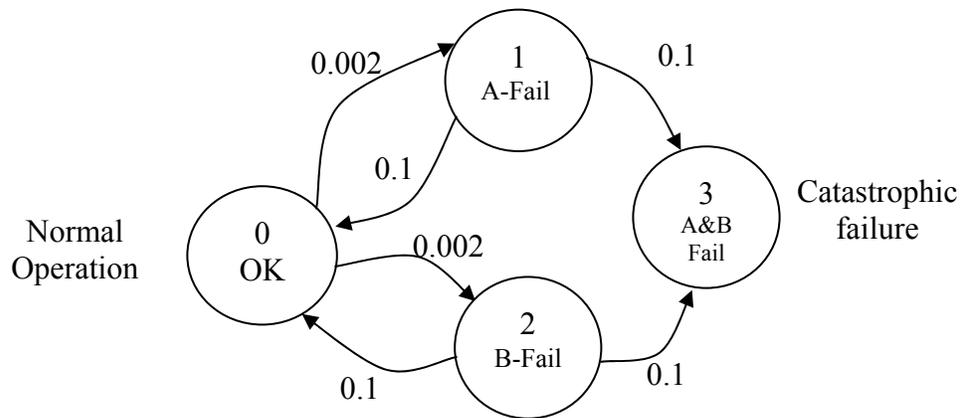
Example (Based on Goble Example 8-6, pp 171)  
 The independent and redundant safety system in figure has four operating states.

- All Systems operational
- System A failed but System B Operational
- System B failed but System A Operational
- And both systems failed.



Repair of the safety function is possible in the partially failed states. It is in the last state that the safety function is lost and an unmitigated accident is possible. At that point it is assumed that repair is not possible.

The markov model for this system is given below.



The transition matrix for the model is given below:

$$P = \begin{bmatrix} 0.996 & 0.002 & 0.002 & 0 \\ 0.1 & 0.899 & 0 & 0.001 \\ 0.1 & 0 & 0.899 & 0.001 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S^1 = S^0 \times P = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.996 & 0.002 & 0.002 & 0 \\ 0.1 & 0.899 & 0 & 0.001 \\ 0.1 & 0 & 0.899 & 0.001 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Algebraic method of finding limited state probability

$$\begin{pmatrix} a_{11} & K & a_{1k} \\ M & O & M \\ a_{j1} & L & a_{jk} \end{pmatrix} = \begin{pmatrix} b_{11} & K & b_{1k} \\ M & O & M \\ b_{j1} & L & b_{jk} \end{pmatrix} \begin{pmatrix} c_{11} & K & c_{1k} \\ M & O & M \\ c_{j1} & L & c_{jk} \end{pmatrix}$$

$$a_{ij} = \sum_{k=1}^n b_{jk} c_{kj}$$

i is row and j is column

$$\begin{bmatrix} S_1^L & S_2^L \end{bmatrix} = \begin{bmatrix} S_1^{L-1} & S_2^{L-1} \end{bmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{bmatrix} S_1^L & S_2^L \end{bmatrix} = \begin{bmatrix} S_1^{L-1} & S_2^{L-1} \end{bmatrix}$$

$$S_1^L = aS_1^{L-1} + cS_2^{L-1}$$

$$S_2^L = bS_1^{L-1} + dS_2^{L-1}$$

$$S_1^L = \frac{cS_2^{L-1}}{(1-a)}.or.S_2^{L-1} = \frac{S_1^L(1-a)}{(1-c)}$$

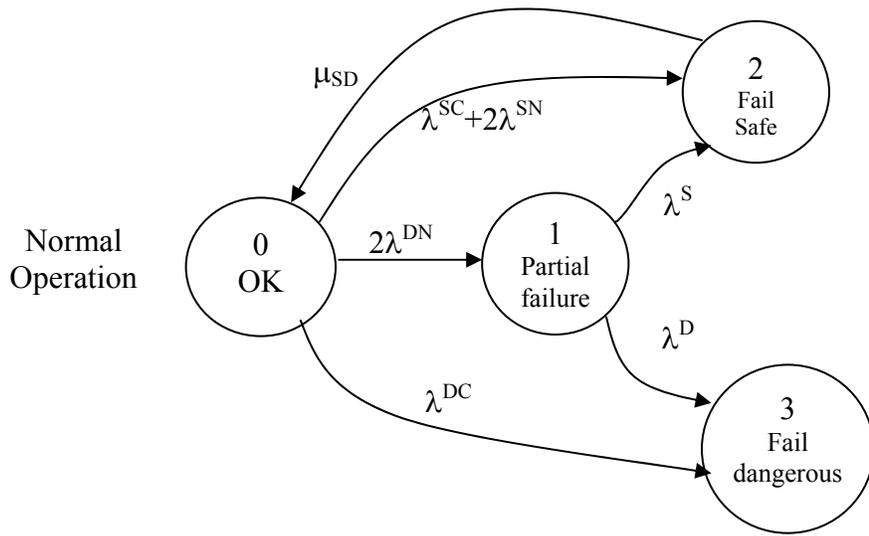
$$S_2^L = \frac{S_1^L(1-d)}{b}.or.S_1^L = \frac{bS_2^L}{(1-d)}$$

$$S_1 + S_2 = 1$$

$$S_1 + S_1 \frac{(1-a)}{c} = 1$$

$$S_1 = \frac{c}{c + (1-a)}$$

$$S_2 = 1 - S_1$$



- $\lambda^{SN} = (1-\beta) \lambda^S$  Normal (non-common cause) safe failure
- $\lambda^{SC} = \beta \lambda^S$  Common cause safe failure rate
- $\lambda^{DN} = (1-\beta) \lambda^D$  Normal (non-common cause) Dangerous failure
- $\lambda^{DC} = \beta \lambda^D$  Common cause Dangerous failure rate

[Goble pp 290]

$$P = \begin{bmatrix} 1 - (\lambda^{SC} + 2\lambda^{SN} + \lambda^{DC} + 2\lambda^{DN}) & 2\lambda^{DN} & \lambda^{SC} + 2\lambda^{SN} & \lambda^{DC} \\ 0 & 1 - (\lambda^S + \lambda^D) & \lambda^S & \lambda^D \\ \mu_{SD} & 0 & 1 - \mu_{SD} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} .99981 & 0.00009 & 0.000095 & 0.000005 \\ 0 & 0.9999 & 0.00005 & 0.00005 \\ 0.041667 & 0 & 1 - \mu_{SD} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



# Chapter 1 Reliability Models

## Introduction

In this chapter we will look at some of the most common methods of evaluation of reliability in safety systems.

In the last chapter we learned about generalized probability distribution functions (pdf) and cumulative distribution functions (CDF). In this chapter we will attach some meaning to these terms in the context of safety systems.

The pdf  $f(t)$  will be used to define the probability of failure of a system **at time  $t$** . The CDF  $F(t)$  will be used to define the probability of failure over time period  $\Delta t$ .

Therefore the CDF  $F(t) = \int_0^t f(t)dt$

Conversely the pdf  $f(t) = \frac{dF(t)}{dt}$

As we shall see, definition of success and failure are important to construction of accurate models.

$$\begin{aligned} P(\text{success}) + P(\text{failure}) &= 1 \\ P(\text{failure}) &= 1 - P(\text{success}) \end{aligned} \tag{1.1}$$

In safety systems we are concerned with the probability of success, i.e. the probability that the system will work as intended, and the probability of failure, the probability that the system will not function at the time that there is a demand placed on the system.

**Reliability  $R(t)$**  – the probability that a system will operate over a designated time period. Unless otherwise noted, the starting time is 0.

$$R(t) = 1 - F(t)$$

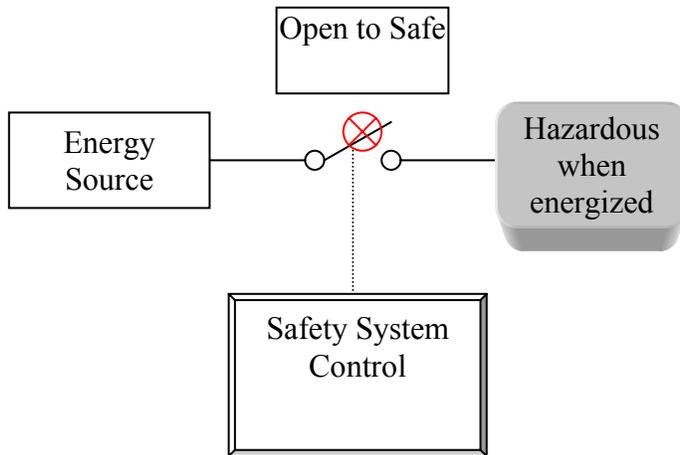
**Reliability is the probability of success**

**Unreliability  $F(t)$**  = Probability of failure over a designated time period.

$$F(t) = 1 - R(t)$$

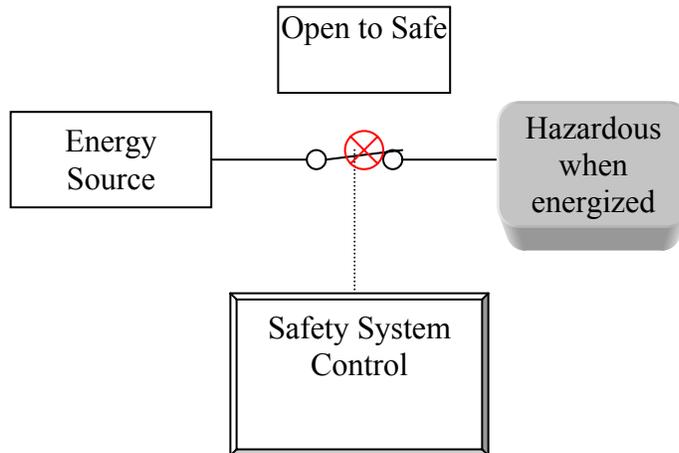
**Unreliability is the probability of failure**

In safety systems,  $F(t)$  is the probability that a system will fail during a designated mission time. In safety systems, the failure mode is very important. For example a switch that fails open, thus cutting off energy to a hazardous device, is failed but **failed-safe**. This type of failure is termed fail-to-safe.



Switch failed to safe.

Of greater concern is the switch that fails closed and is unable to transition to the open or safe state, even when commanded to do so by the safety system. This is termed **fail-to-danger** or **PFD**.



Switch failed dangerous.

Of the failure modes of the system, there is a subset of probabilities that a system will fail-to-safe (pfs) or fail-to-danger (pfd) at a given time  $t$ .

$$pfs(t) = f(t)_{safe} \quad (1.2)$$

$$pfd(t) = f(t)_{dangerous} \quad (1.3)$$

! Don't confuse this with pdf=probability distribution function !

The complementary cumulative probability of safe or dangerous failure over time is the **PFD** and **PFS**. Note that it is the average PFD that is used in the definition of SIL levels for safety systems.

$$PFD(t) = F(t) - PFS(t) \quad (1.4)$$

**Risk reduction factor RRF** is the amount of risk mitigation required from the safety system. It is equal to  $1/PFD_{avg}$ .

**Failure Rate  $\lambda(t)$**  (in some places called hazard rate): A measure of the instantaneous rate at which components fail.

$$\lambda(t) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)} \quad (1.5)$$

Note that items that are given as “rates per unit time” are sometimes just referred to as the “frequency” of the item. e.g  $\lambda(t)$  = failure rate or frequency of failure.

$$\lambda(t) = \frac{\#units\ failed\ over\ time\ t\ at\ time\ t}{Total\ \#units} \quad (1.6)$$

Note that  $\lambda(t)$  can be divided into safe failure rates and dangerous failure rates.

$$\lambda(t) = \lambda^D(t) + \lambda^S(t) \quad (1.7)$$

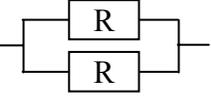
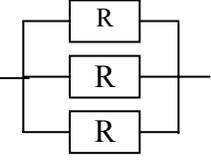
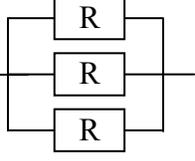
**Mean Time to Failure (MTTF)**. By definition MTTF is the measure of the mean of a CDF with respect to time. The mean value of a probability function is given by

$$\hat{u} \cong \int_{-\infty}^{\infty} xf(x)dx \quad (1.8)$$

$$MTTF = \int_0^{\infty} R(t)dt \quad (1.9)$$

For a constant failure rate, the MTTF is the time that one would expect that 63.2% ( $1 - e^{-1}$ ) of a given number of components would have failed.

**Availability  $A(t)$**  – the probability that a system is successful at time  $t$  *assuming that a hazard can be present at time  $t$ .*

Configuration	Reliability for Constant Failure Rate $\lambda(t) = \lambda$	PFDavg Approximation	General System Reliability	MTTF (assumes repair time $\ll$ MTTF)
Single 	$e^{-\lambda t}$	$\frac{\lambda^{DU} \cdot TI}{2}$	$R_i$	$\frac{1}{\lambda}$
Series 	$e^{-(\lambda_1 + \lambda_2)t}$	$\frac{\lambda^{DU} \cdot TI}{2}$	$\prod_{i=1}^n R_i$	$\frac{1}{\sum_{i=1}^n \lambda_i}$
Parallel 	$e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$	$\frac{(\lambda^{DU} \cdot TI)^2}{3}$	$1 - \prod_{i=1}^n (1 - R_i)$	$\frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{(\lambda_1 + \lambda_2)}$  if $\lambda_1 = \lambda_2$ then MTTF = $\frac{3}{2\lambda}$
1/3 voting 	$3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$	$\frac{(\lambda^{DU} \cdot TI)^3}{4}$	$1 - \prod_{i=1}^n (1 - R_i)$	$\frac{11}{6\lambda}$
2/3 voting 	$3e^{-2\lambda t} - 2e^{-3\lambda t}$	$(\lambda^{DU} \cdot TI)^2$	$1 - \sum_{i=0}^{m-1} \binom{n}{i} R^i (1-R)^{n-1}$	$\frac{5}{6\lambda}$
m/n voting	$\sum_{i=m}^n \binom{n}{i} e^{-i\lambda t} (1 - e^{-\lambda t})^{n-1}$	$\frac{n! (\lambda^{DU} \cdot TI)^{n-m}}{(m-1)!(n-m+1)!(n-m+2)}$	$1 - \sum_{i=0}^{m-1} \binom{n}{i} R^i (1-R)^{n-1}$	$\frac{1}{\lambda} \sum_{i=m}^n \frac{1}{i}, 1 \leq m \leq n$

## 1oo2 Redundancy

For a 1oo2 system:

PFD average is approximately (Goble pp 274)

$$PFD_{avg}(t) = \frac{1}{TI} \int_0^{TI} (\lambda^D t') dt' \quad (1.10)$$

$$PFD_{avg} = \frac{(\lambda^D \cdot TI)^2}{3} \quad (1.11)$$

If common cause failure modes are added

The full block diagram, including common cause and systematic errors is:

$$PFD_{avg} = \left[ ((1-\beta)\lambda^{DU})^2 \frac{TI^2}{3} \right] + [(1-\beta)\lambda^{DU}\lambda^{DD} \cdot MTTR \cdot TI] + \left[ \beta\lambda^{DU} \frac{TI}{2} \right] + \left[ \lambda^D \frac{TI}{2} \right] \quad (1.12)$$

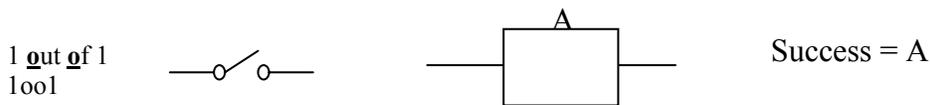
For the purposes of the models given in the next section:

### Fail Safe

Open/Isolated/Unenergized

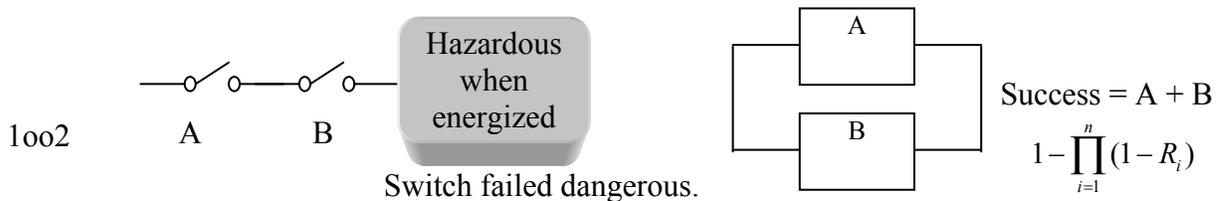
### Fail Unsafe

Closed/Connected/Energized



$$(1.13)$$

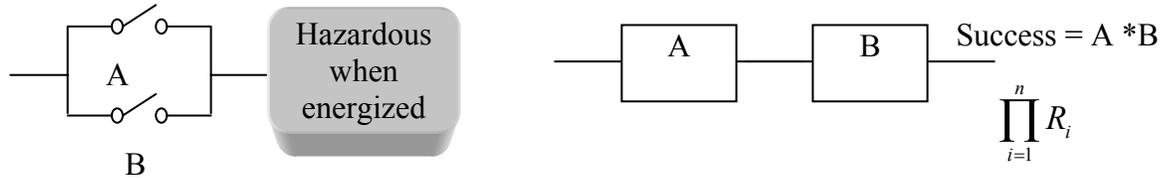
$$(1.14)$$



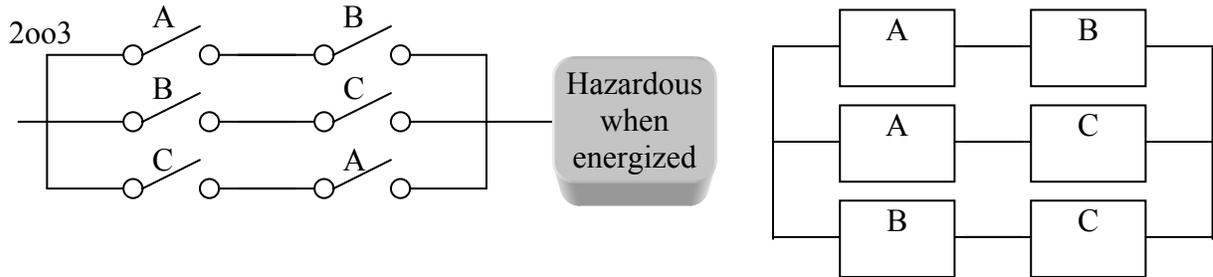
$$MTTF_{1oo1} = \frac{1}{\lambda^S + \lambda^D}$$

In the redundant system above, success is defined as either switch A opening **OR** switch B opening.

2002



In the system above, success requires both switch A opening **AND** switch B opening. This type of configuration is not typical in accelerator safety systems.



Control can be by:

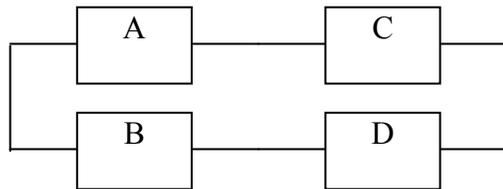
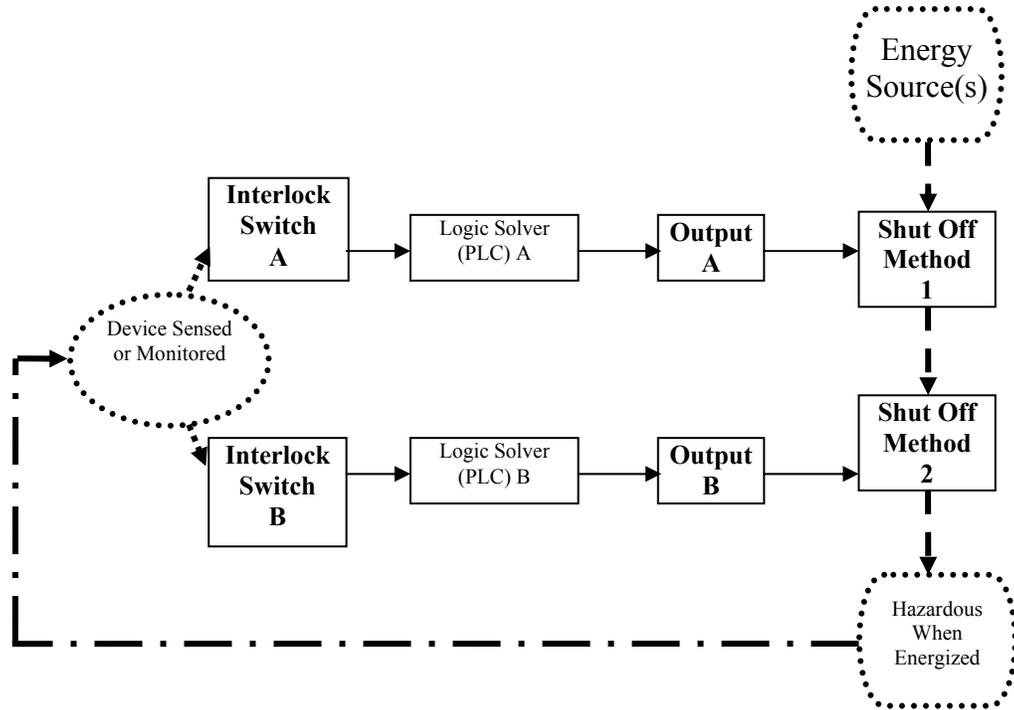
Direct – direct shut off of energy source

Isolation- isolate energy source from hazardous location

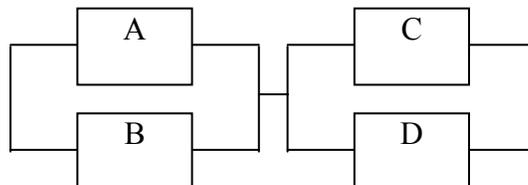
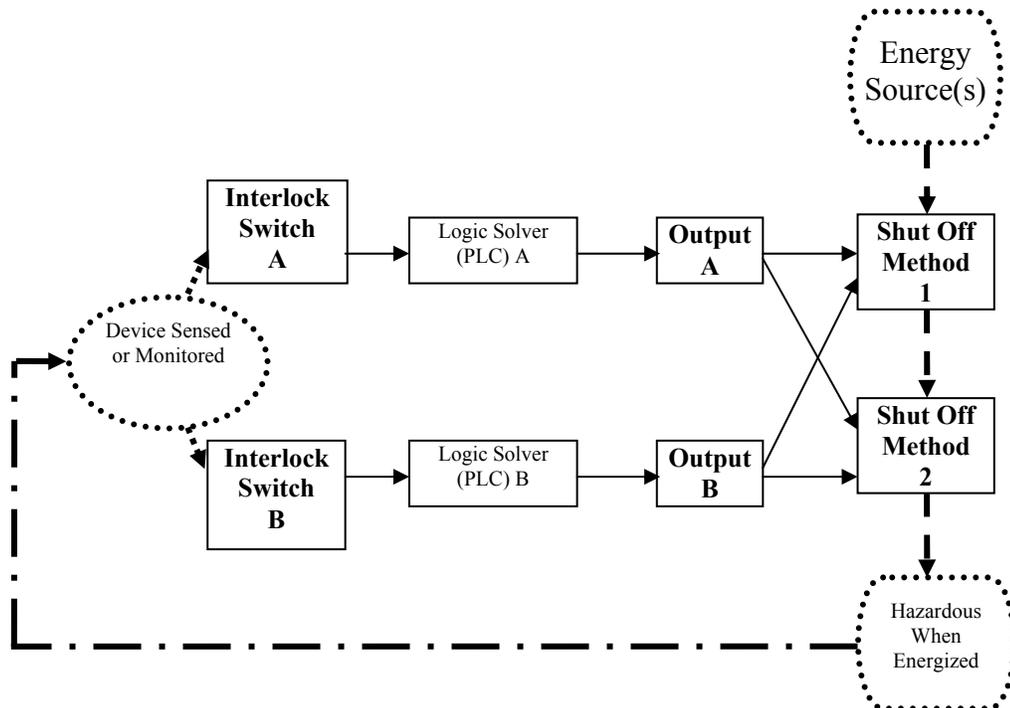
Containment- keep hazardous energy within a barrier

Redirection – shunt energy to alternate, safe, location

Typical redundant safety system architecture



State	Combination	System Status
0	ABCD	OK
1	<del>A</del> BCD	OK
2	A <del>B</del> CD	OK
3	AB <del>C</del> D	Failed
4	AB <del>C</del> D	OK
5	A <del>B</del> CD	OK
6	A <del>B</del> CD	Failed
7	A <del>B</del> CD	Failed
8	<del>A</del> BCD	OK
9	<del>A</del> BCD	Failed
10	<del>A</del> BCD	OK
11	<del>A</del> BCD	Failed
12	<del>A</del> BCD	Failed
13	<del>A</del> BCD	Failed
14	<del>A</del> BCD	Failed
15	<del>A</del> BCD	Failed





## **Chapter 1 Reliability Statistics**

*“There are three kinds of lies: lies, damned lies and statistics.”  
Benjamin Disraeli (unconfirmed) (1804–1881), British statesman, author.*

*“Like dreams, statistics are a form of wish fulfillment.”  
Jean Baudrillard (b. 1929), French semiologist. *Cool Memories*, ch. 4 (1987,  
trans. 1990).*

### **Where are we going with this and why is it important?**

In this section we are going to relate general statistical theory to specific formulas for calculating reliability. Later in the book we are going to use this foundation for many of the safety system analysis tools. We will simplify some of the material presented here based on assumptions. Also, terms like “Mutually exclusive” have an important meaning when doing things like performing a fault tree analysis.

### **Introduction**

This chapter gives a short introduction to statistics used in safety system reliability analysis. It is not intended to be thorough or generally applicable outside the context of safety systems. One should consult the references for a more thorough treatment of statistics and reliability statistics in particular.

The two quotes at the start of this chapter illustrate that statistics, taken out of context or given incomplete treatment, can lead to unacceptable results. In the world of safety systems, incomplete statistics can lead to under design or over design of safety functions. The former case could lead to accidents, the latter to unacceptable system availability or difficulty in operations.

Safety system design and evaluation involves estimation of both the probable and the possible. Conversely, the compliments of these are the improbable and the (nearly) impossible. Each of these concepts is aided by the use of statistical models to project outcomes of unmitigated and then mitigated risk, the safety system being one form of mitigation.

### **Probability**

A probability is a measure of the chance of the possible outcomes for an event at a given point. The bounds of probability are between zero – not possible, and one – absolute. The sum of all possible outcomes must add up to one. Another way of looking at it is that all possible outcomes must be accounted for. A coin has two sides. We may only be interested in “heads”, in our application, but “tails” is the other possible outcome. (This gets us back to the idea of inferred outcomes. We still must account for the fact that the “tails” side exists.) Together the probability of flipping heads and the probability of flipping tails must add up to 1.

Note that probability can only give an insight to the chance of a future event. Once an event has been observed, the probability of a given outcome is unity. For safety systems that may mean the beginning of an incident investigation!

Probability functions describe the chance of a given outcome at a particular point in time. There are two types of probability functions considered here, the discrete probability and the continuous probability. We generally use continuous probability functions to describe the chance of failure of one or more system components. For example, a safety computer has a probability of failure measured in failures per billion hours, termed FITS. A place where we may use discrete probabilities would be to calculate the chance that two out of three safety computers will fail when the accelerator is operating.

$P(x)$  is the probability of a discrete outcome and  $f(x)$  is the probability density of a continuous function.

$$\sum_{i=1}^n P(x_i) = 1 \quad (1.1)$$

for discrete outcomes.

$$\int_{-\infty}^{\infty} f(x)dx = 1 \quad (1.2)$$

for continuously variable outcomes.

Both are read as “the sum total of the probabilities all possible outcomes must add up to 1.”

An example of a discrete outcome would be a die toss. There are only six faces on the die. Your chance of getting any one number is 1 in 6 for each toss. An example of a continuous function would be the chance of your car breaking down tomorrow.

Reliability (R) is defined as the *probability that a system will achieve a desired result over a given mission time*. As we will see later, the “desired result” may take on different meanings for a safety system. For example, if a safety system fails safe, the system has achieved the desired result. To the accelerator operator, the safety system has shut down the accelerator – not a desired result in their mind. Put another way, reliability is the probability that a safety function will NOT fail in an unsafe manner over a given time period. In recent treatments this is termed *safety reliability* in order to point out the distinction. This is a book on safety systems so we will interpret reliability and safety reliability to mean the same thing.

In safety systems we are usually interested in the question “what is the probability that a safety system will fail during a specific period of time.” In that case we are interested in the cumulative probability of failure or success over a given time interval.

$$F(t) = \int_{t_1}^{t_2} f(t)dt \quad (1.3)$$

$$R(t) = \int_{t_1}^{t_2} [1 - f(t)]dt \quad (1.4)$$

For accelerators, we are interested in two time ranges – the probability of system failure between certification intervals, and the average probability of failure over the life of the system. For most practical applications  $t_1=0$  and  $t_2=t$ .

### Failure or Hazard Rate

One of the most quoted (and misunderstood) parameters in reliability nomenclature is the failure rate  $\lambda(t)$  and this is one place where the system safety and process safety literature differ in treatment of the subject. In reliability engineering texts, it is assumed that if the safety system fails, there is by definition a hazard and the hazard rate  $h(t)=\lambda(t)$ . In the IEC61508 standards and similar recent treatments mainly from the process industries, failure rates are broken down in to safe failure rates and dangerous failure rates. It is presumed that safe failures will not present a hazard while dangerous (fail-unsafe) failures will.

$$\lambda(t) = \lambda^S(t) + \lambda^D(t)$$

Failure rate is defined as *the probability of failure per unit interval given that the system or component has not failed yet*. Of course, the most commonly used interval is time. However failure rate may be expressed in failure per lot, per demand, per meter, per phase of the moon and so on.

Since the failure rate is probability per unit time, the probability of failure can be expressed as  $\lambda(t)$  multiplied by a time interval,  $\Delta t$ .

It is easy to see why the aerospace industry may automatically consider a system failure a hazard. A failure, even a “fail-safe” failure in an aircraft could result in loss of the aircraft and everyone on board. Accelerators have the luxury of being able to shut down in the fail-safe mode without endangering people. This may not be the case for equipment. A beam loss event with a multi-megawatt beam can do considerable damage.

A general discrete expression for failure rate is<sup>1</sup>  $\lambda(\Delta t) = \frac{N_t - N_{t+\Delta t}}{N_t \Delta t}$  where

$N_t$  = initial number of units at time  $t$

$N_{t+\Delta t}$  = number of units surviving after time  $\Delta t$

Normally a constant failure rate is assumed and this is simplified to

$$\lambda = \frac{\text{Number of failed units}}{\text{Total number of units}} \cdot \frac{1}{\text{hours in operation}}$$

Example: An accelerator has 50 door interlock switches that were installed 18 years ago. Over that time period, 6 switches have failed unsafe. What is the unsafe failure rate?

$$\lambda^D = \frac{6}{50} \cdot \frac{1}{18 \cdot 8760} = 7.6 \times 10^{-7} \text{ h}^{-1}$$

A more precise expression for  $\lambda(t)$  is the probability of failure at time  $t$  with respect to the probability of survival over a given time interval. As the limit of the time interval approaches zero, the expression becomes:

$$h(t) = \lambda(t) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)} \quad (1.5)$$

This is termed the instantaneous failure rate.

Note that for the exponential distribution the hazard rate is constant:

$$f(t) = \lambda e^{-\lambda t} \quad (1.6)$$

$$F(t) = \int_0^t f(t) dt = \int_0^t \lambda e^{-\lambda t} dt \quad (1.7)$$

$$F(t) = \frac{-\lambda}{\lambda} e^{-\lambda t} = -e^{-\lambda t} \Big|_0^t = e^0 - e^{-\lambda t} = 1 - e^{-\lambda t}$$

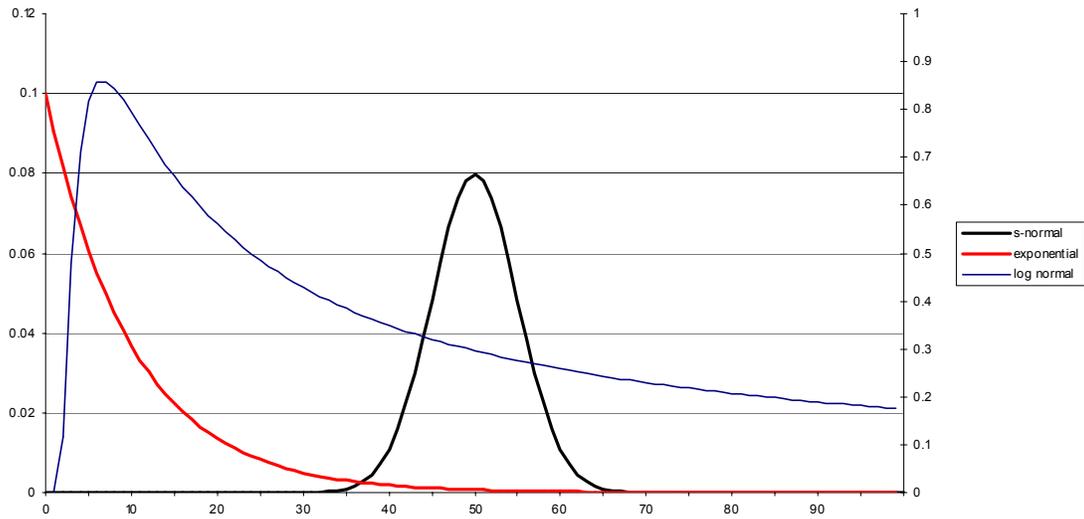
$$R(t) = 1 - F(t) = e^{-\lambda t} \quad (1.8)$$

for the normal distribution

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{\lambda t}}{e^{\lambda t}} = \lambda \quad (1.9)$$

That is, for the exponential distribution, failure rate is not a function of time. This is the most commonly used definition of failure rate. This is also the definition that will be used throughout this book unless otherwise noted. Why? Because it is an expression of failure rate as a function of time that can be easily measured and inserted in to time based reliability models such as the Markov.

pdf functions

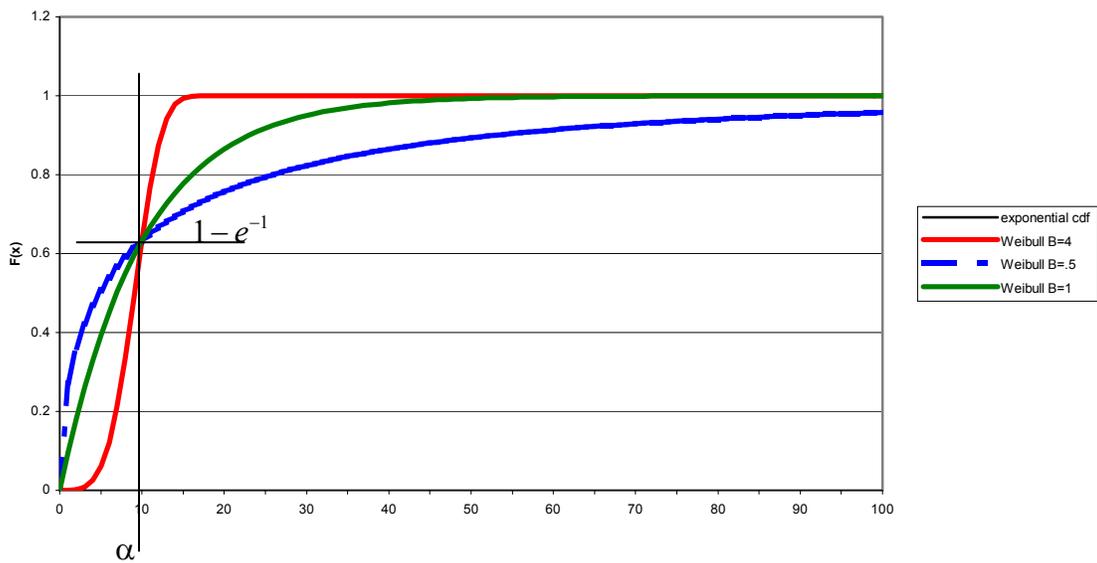


Other

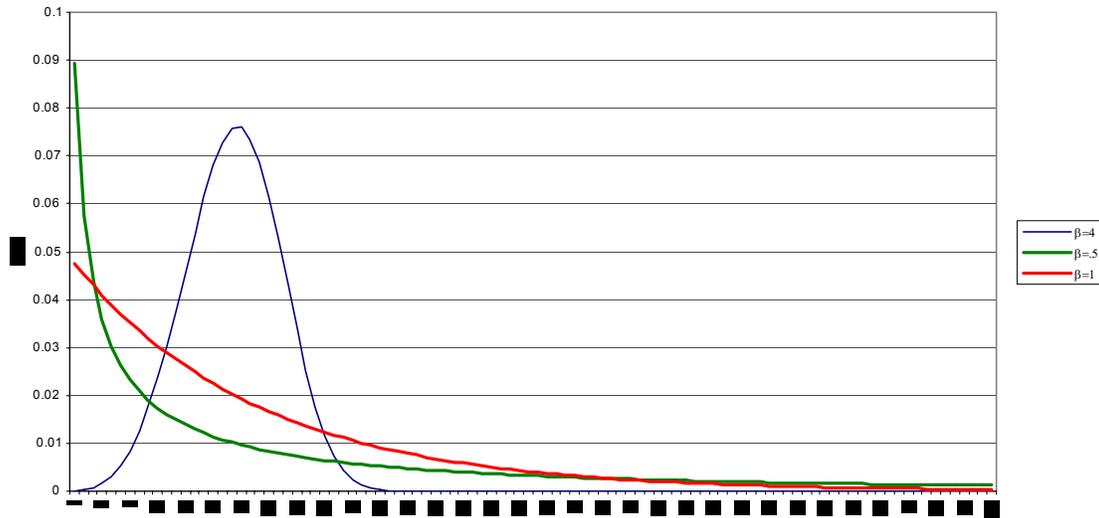
The cumulative hazard function H(t) is:

$$H(t) = \int_0^t h(t)dt = \int_0^t \frac{f(t)}{1-F(t)} dt \quad (1.10)$$

Cumulative Distribution Functions



Weibull pdf



## Discrete Statistics

Binomial Distribution [*Rheja, O'Connor*]

The binomial distribution applies to systems where there are mutually exclusive outcomes, e.g. failed or not failed. It can be used to estimate the reliability of redundant or fault tolerant systems.

$$f(x) = \binom{n}{x} R^x (1-R)^{n-x} \quad (1.11)$$

where

$$\binom{n}{x} \rightarrow \frac{n!}{x!(n-x)!}$$

This is the probability that, out of n units, there will be x good ones and n-x bad ones when the probability of having a good unit is R and the probability of having a bad unit is R-1. Note that for binomial distribution, x is an integer.

The mean and standard deviation of the binomial distribution are:

$$\mu = nR \quad (1.12)$$

$$\sigma = \sqrt{nR(1-R)} \quad (1.13)$$

The cumulative distribution function for a binomial distribution is the sum of success states:

$$R(s) = \sum_{i=m}^n \binom{n}{m} R^i (1-R)^{n-i} \quad (1.14)$$

where m is the number of success states out of n total states.

*Example.*

*A safety function uses triplicate sensors. At least 2 of the sensors must be operable for the system to continue to function over the mission time of the system. Each sensor has a calculated reliability of 0.99 over the mission time. What is the probability of system success?*

*Solution: The system will be successful if at least 2 out of the three sensors are operating, i.e. the success states are 2 out of 3 or 3 out of 3. From equation (1.14), the probability of success over the mission time is:*

$$\begin{aligned} R(r) &= \binom{3}{2} (.99)^2 (.01)^{3-2} + \binom{3}{3} (.99)^3 (.01)^{3-3} \\ &= \frac{3!}{2!1!} (.99)^2 (.01)^1 + \frac{3!}{3!0!} (.99)^3 (.01)^0 \\ &= 3(.99)^2 (.01) + 1(.99)^3 (1) \\ &= 0.999702 \end{aligned}$$

	pdf	CDF Failure	Hazard Rate
s-normal	$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right]$	$F(x) = 1 - \left(\frac{1}{\sigma\sqrt{2\pi}} \int_x^{\infty} \exp\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right] dx\right)$	$\frac{f(t)}{R(t)}$
log-normal	$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{\ln x - \mu}{\sigma}\right)^2\right]$	$F(x) = 1 - \left(\frac{1}{\sigma\sqrt{2\pi}} \int_x^{\infty} \frac{1}{x} \exp\left[-\frac{1}{2}\left(\frac{\ln x - \mu}{\sigma}\right)^2\right] dx\right)$	$\frac{f(t)}{R(t)}$
exponential	$f(x) = \lambda e^{-\lambda x}$	$F(x) = 1 - e^{-\lambda x}$	$\lambda$
Weibull	$f(x) = \frac{\beta(x-\gamma)^{\beta-1}}{\alpha^\beta} \exp\left[-\left(\frac{x-\gamma}{\alpha}\right)^\beta\right]$	$F(x) = 1 - \exp\left[-\left(\frac{x}{\alpha}\right)^\beta\right]$	$\frac{\beta}{\alpha^\beta} t^{\beta-1}$

Table x. Common continuous probability functions

<sup>1</sup> Rheja pp14

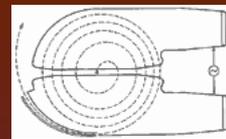


# Introduction to System Safety in Research Accelerators

Safety Systems

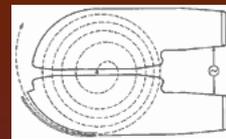
USPAS

June 2004



# Outline

- ❖ Logistics
- ❖ Course Overview
- ❖ Course Outline
- ❖ Accelerator Basics



# Logistics

## Class hours

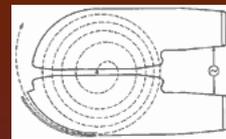
Morning 9-10:45

Break 10:45-11:00

Computer 11-12 (Tue-Thurs)

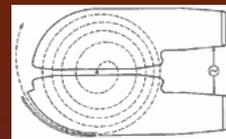
Lunch 12-1:30

Afternoon 1:30-4:30



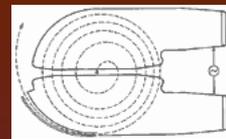
# Material

“Reliability, Maintainability, and Risk”, David Smith  
Handouts



# Homework

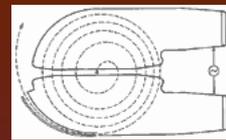
Selected exercises from Smith  
Handouts



# Course Outline

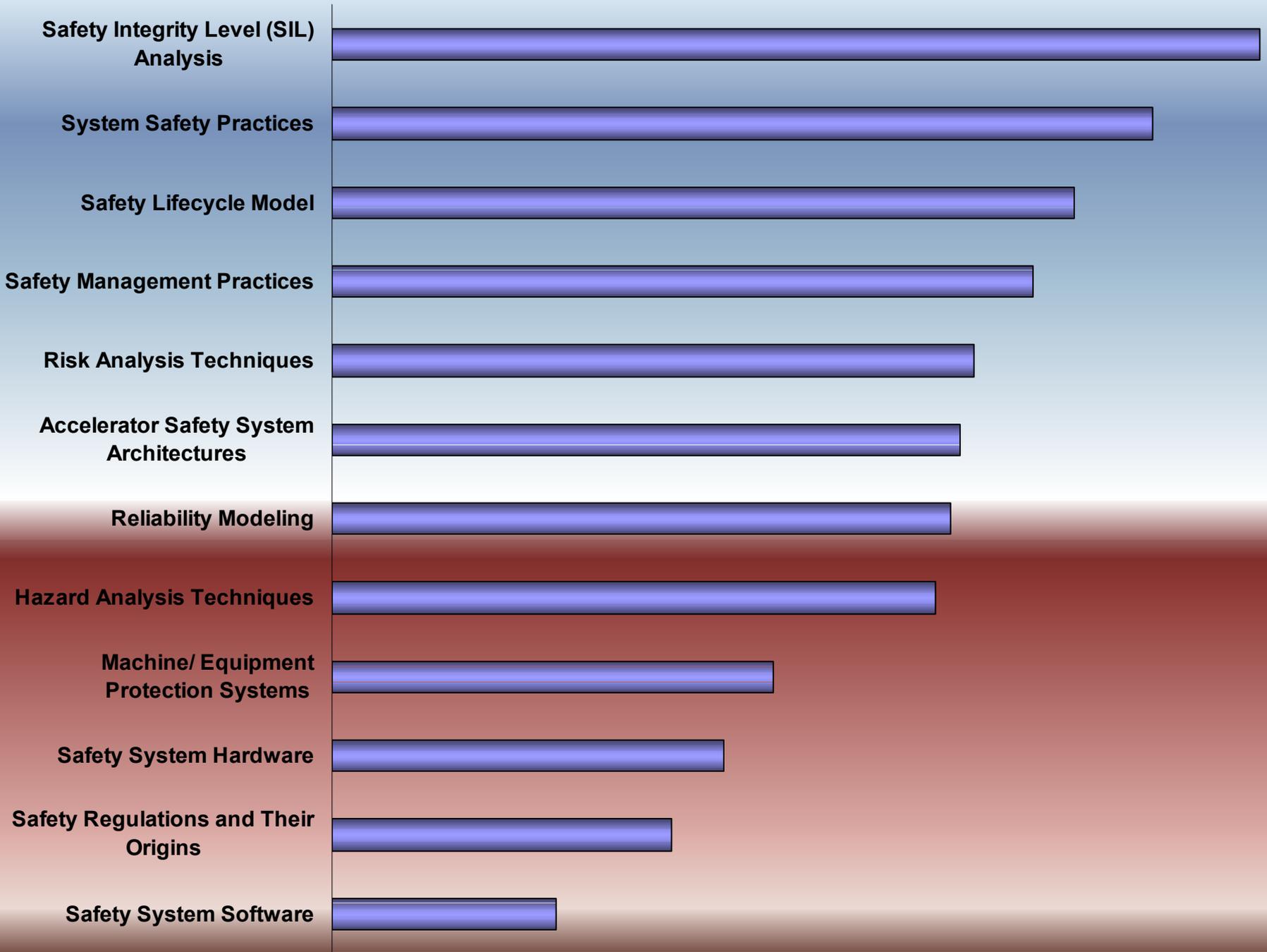
## Intent:

It is the intent of this class to communicate a basic knowledge about safety systems used at accelerator labs. One should leave the class knowing the basic steps required for the development of a safety system and the system plan. The class is intended not only to teach basic technical skills such as reliability evaluation but also a greater context in which safety systems are developed. To that end, the class includes a significant amount of material on system safety programs, accelerator regulatory requirements, and what is considered good practice among accelerator management and safety professionals.



# Scope

- ❖ This class is intended to address hazards associated with operation of particle accelerator systems. It does not specifically address normal industrial hazards common to all workplaces.



**Safety Integrity Level (SIL) Analysis**

**System Safety Practices**

**Safety Lifecycle Model**

**Safety Management Practices**

**Risk Analysis Techniques**

**Accelerator Safety System Architectures**

**Reliability Modeling**

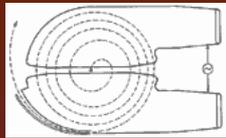
**Hazard Analysis Techniques**

**Machine/ Equipment Protection Systems**

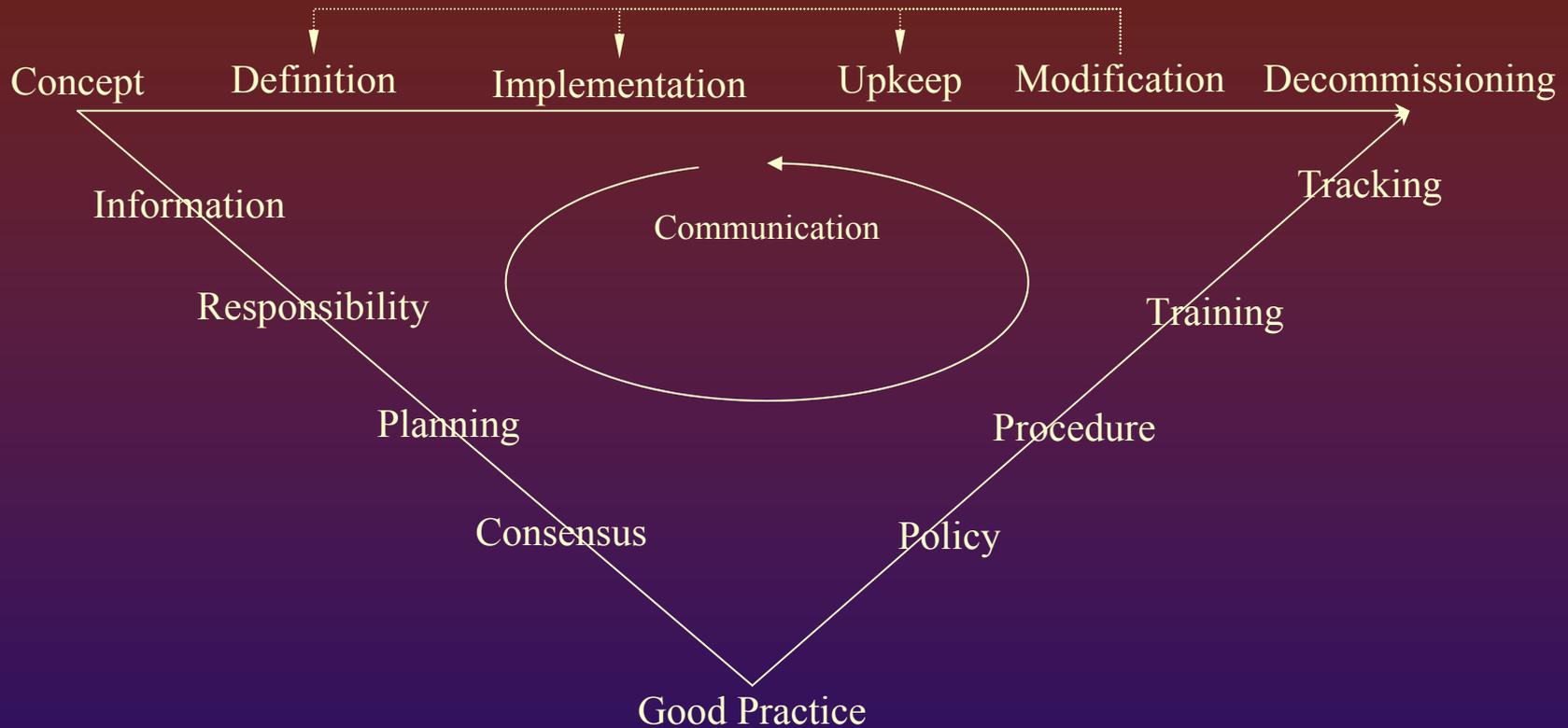
**Safety System Hardware**

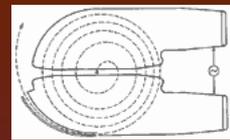
**Safety Regulations and Their Origins**

**Safety System Software**



# Foundations of Good Practice

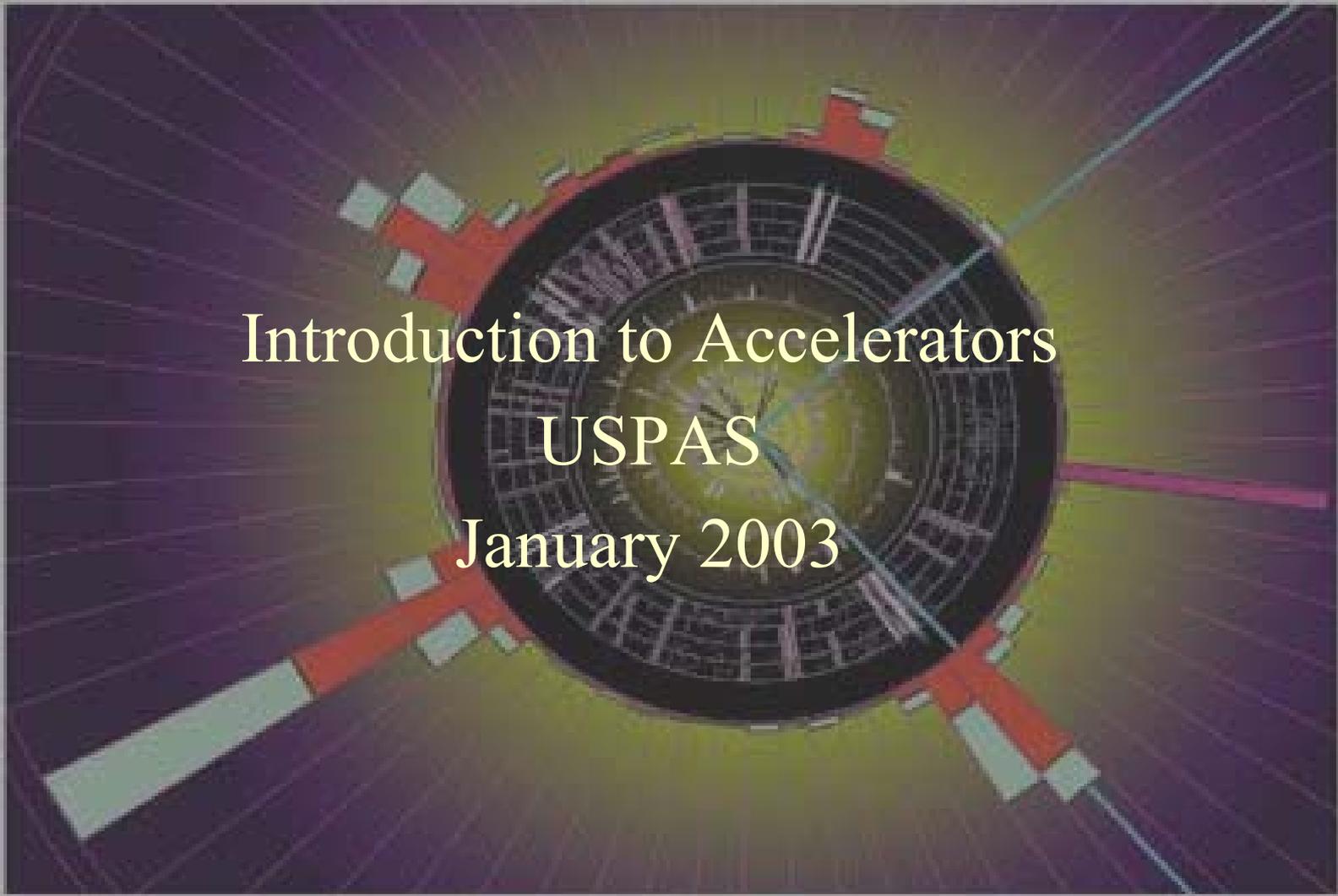




# Context

- ❖ One of the most important concepts to understand in working with safety systems is context.
  - ❖ Physical Environment
  - ❖ Regulatory Environment
  - ❖ Risk Environment
  - ❖ Management Structure
  - ❖ Resource Environment
- ❖ Without understanding the proper context of a safety system, tacit assumptions are made that could lead to undesired system behavior or worse.

# Introduction to System Safety in Research Accelerators



Introduction to Accelerators  
USPAS  
January 2003

# Accelerators

## 1934 Patent for the cyclotron awarded to E.O. Lawrence

Feb. 20, 1934.

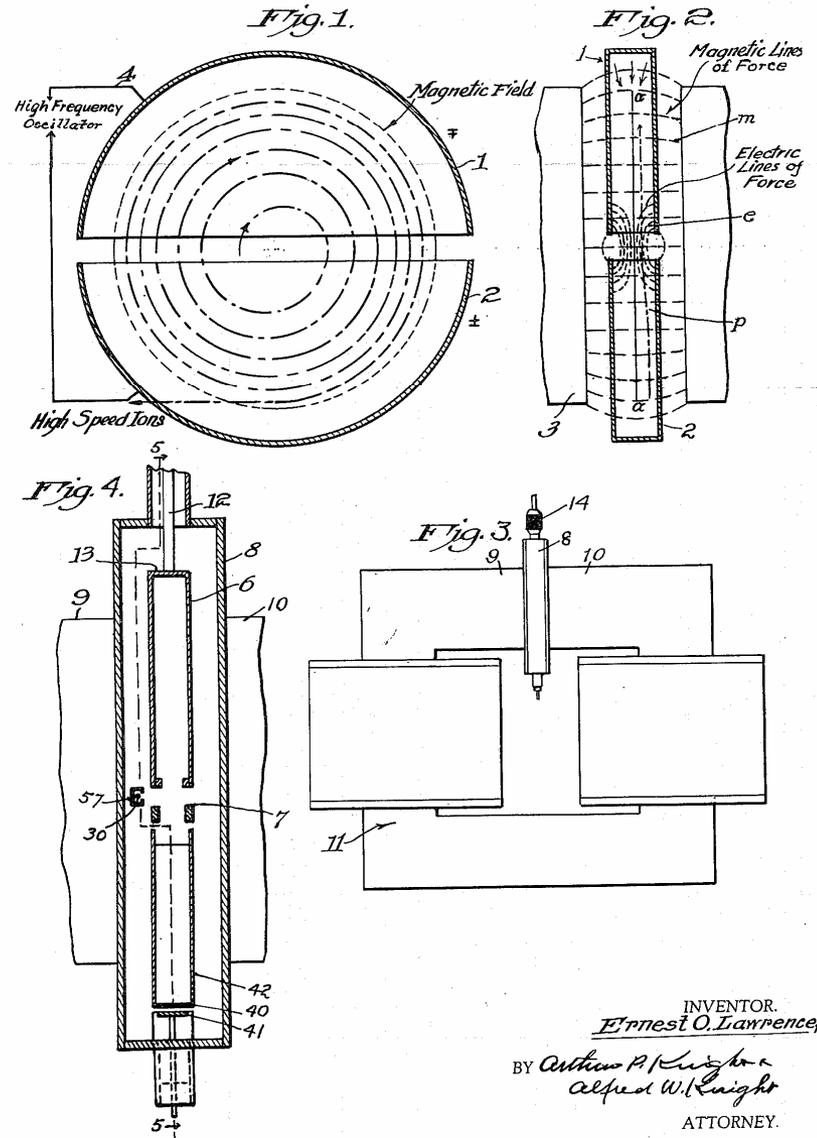
E. O. LAWRENCE

1,948,384

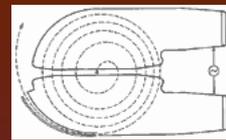
METHOD AND APPARATUS FOR THE ACCELERATION OF IONS

Filed Jan. 26, 1932

2 Sheets-Sheet 1



INVENTOR.  
*Ernest O. Lawrence*  
BY *Arthur P. Knight*  
*Alfred W. Knight*  
ATTORNEY.



# Accelerator Basics

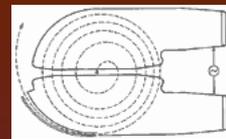
- ❖ Accelerators are used to transfer kinetic energy to charged particles.

$$\Delta E = qV$$

where

$$\Delta E = E_T - E_{rest}$$

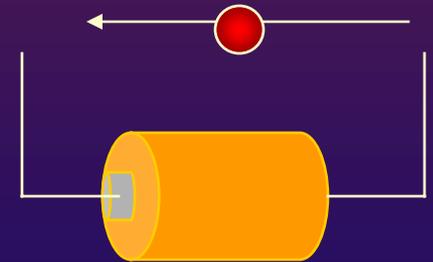
- ❖ The energetic particles are used to transfer energy and momentum to nuclei in order to generate a myriad of ionizing radiation byproducts.

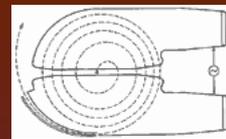


# The eV

Energy equivalent to that gained by an electron passing through a potential difference of one volt.

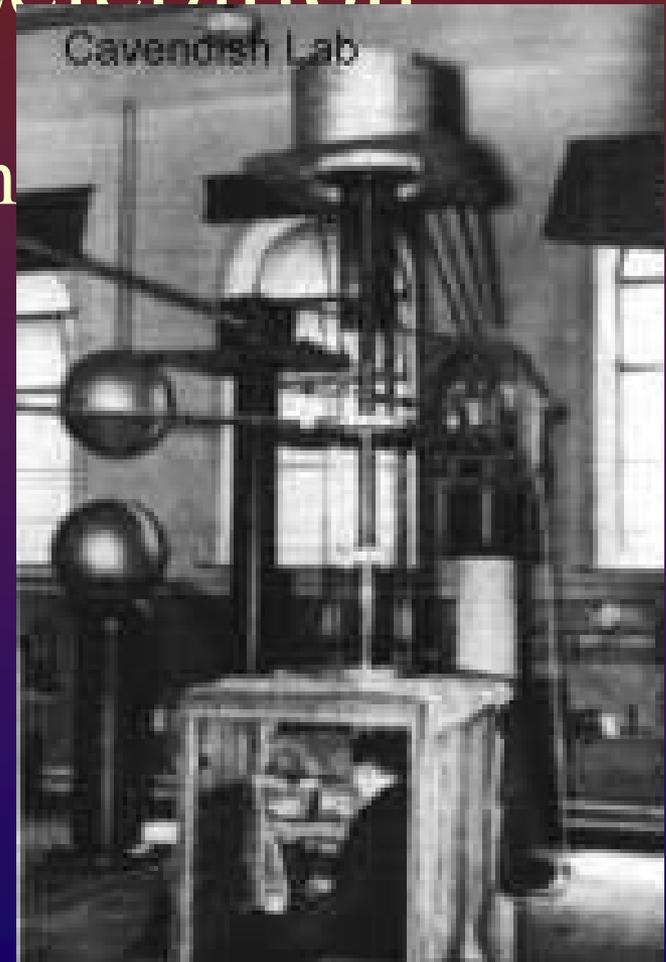
$$\begin{aligned} 1\text{eV} &= 1.602 \times 10^{-19} \text{ Joule } \left( \frac{\text{kg} \cdot \text{m}^2}{\text{s}^2} \right) \\ &= 1.602 \times 10^{-12} \text{ ergs} \\ &= 4.451 \times 10^{-26} \text{ kilowatt-hour} \end{aligned}$$

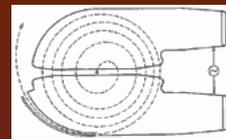




# Electrostatic Acceleration

1932 photo of Cockcroft-Walton  
Accelerator.





# Energy Gain as $v \Rightarrow c$

$$E = mc^2$$

$$m = \frac{E}{c^2}$$

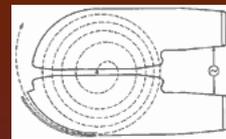
$$m = \frac{m_0}{\sqrt{1 - \left(\frac{v}{c}\right)^2}}$$

$$\beta = \frac{v}{c}$$

$$\gamma = \frac{1}{\sqrt{1 - \beta^2}}$$

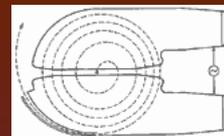
$$E = \gamma mc^2$$

# Types of Accelerators



Type \ Use	Collider	Fixed Target	Synchrotron Light	Free Electron Laser
Cyclotron				
Betatron				
Synchrotron				
Linac				
Recirculating Linac				

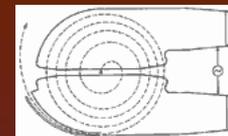
# Accelerator Inventory



World wide inventory of accelerators, in total 15,000. The data have been collected by W. Scarf and W. Wieszczycka (See U. Amaldi Europhysics News, June 31, 2000)

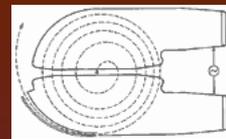
Category	Number
Ion implanters and surface modifications	7,000
Accelerators in industry	1,500
Accelerators in non-nuclear research	1,000
Radiotherapy	5,000
Medical isotopes production	200
Hadron therapy	20
Synchrotron radiation sources	70
Nuclear and particle physics research	110

From Sven Kullander, Nobel e-museum, First published August 28, 2001  
<http://www.nobel.se/physics/articles/kullander/>



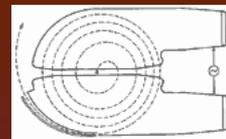
# Accelerated Particles

Particle	Symbol	Charge	Rest Mass, MeV	Spin
Electron/ Positron	$e^-, e^+$	-1,+1	0.511	$1/2$
Proton/Anit- Proton	$P, \bar{P}$	+1,-1	938	$1/2$
Heavy Ion	Atomic Symbol, Number	Varied	$\sim 939 * \text{Atomic}$ number	$1/2$
Muon (not yet built)	$\mu$	-1	106	$1/2$



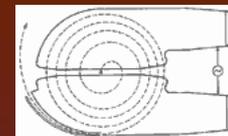
# Secondary Particle Beams

Particle	Symbol	
Photon	$\gamma$	FEL, Synchrotron Light, x $\rightarrow$ far gamma
Neutron	$n$	Slow- irradiation Fast – therapy, spallation
neutrino	$\nu$	Standard model
muon	$\mu^{+/-}$	Standard model
$\pi$ -meson	$\pi^{+/-}$	Muon source, Therapy

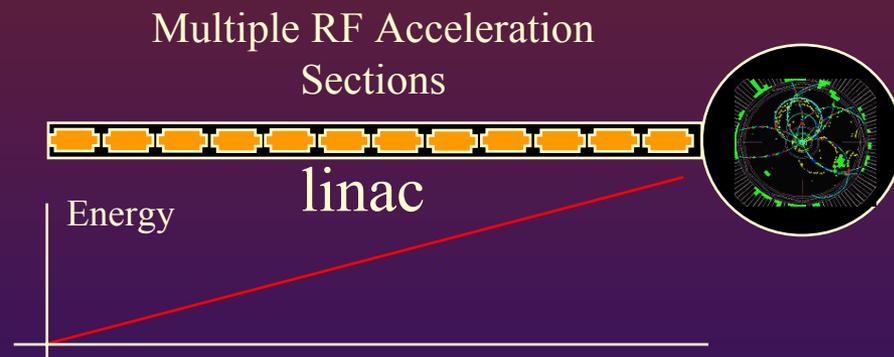
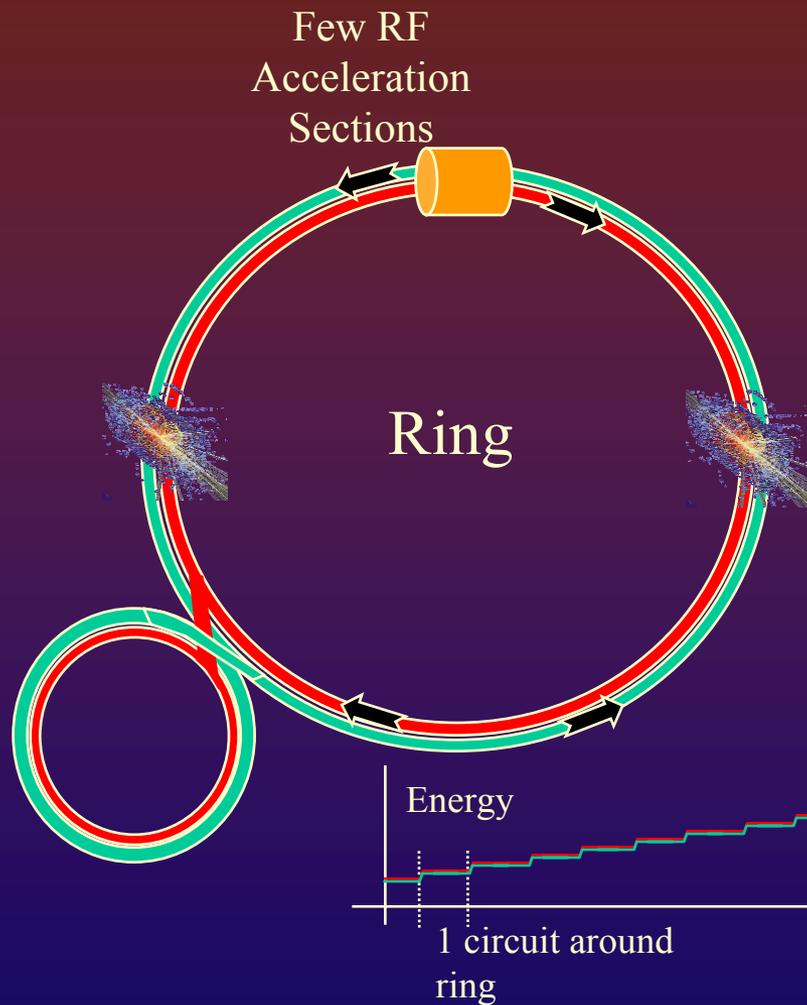


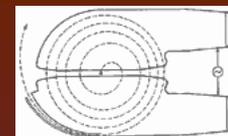
# Common Accelerator Facility Units

- ❖ Source
  - ❖ Generates primary beam
  - ❖ Establishes timing structure
  - ❖ keV-MeV Energies
- ❖ Linear Accelerator (linac)
  - ❖ Many accelerator sections
  - ❖ Few magnetic steering sections
  - ❖ keV – 50GeV+
- ❖ Ring Accelerator
  - ❖ Few acceleration sections
  - ❖ Many magnetic steering sections
  - ❖ MeV-1TeV+
- ❖ Accumulator/Storage Ring
  - ❖ Accumulation of exotic particles
  - ❖ Particle storage
- ❖ Interaction Region
  - ❖ Target area
  - ❖ Collider area

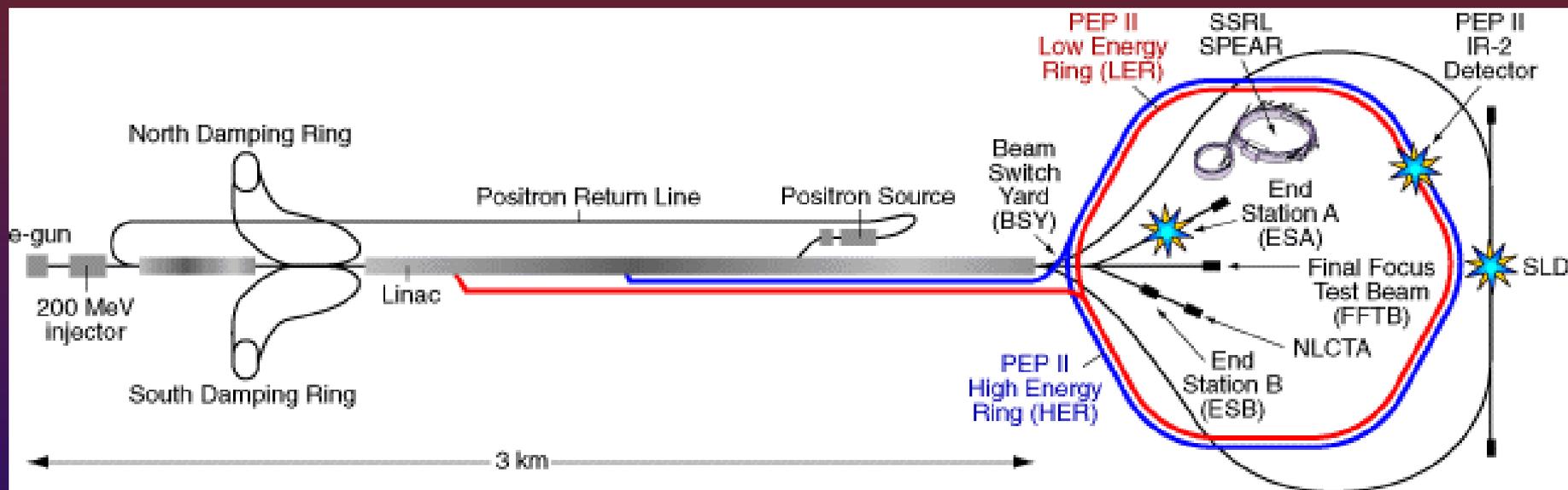


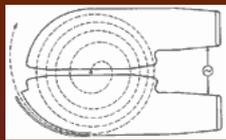
# Ring vs. linac





# SLAC



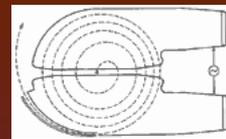


# Fermi



© K Mahoney/S. Prior  
2002-2004

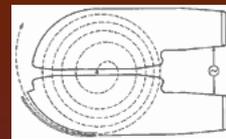
USPAS  
June, 2004



# CERN

CERN aerial  
photo showing  
27 km tunnel.



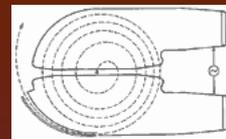


# APS

Advanced Photon  
Source, Aurora, IL.

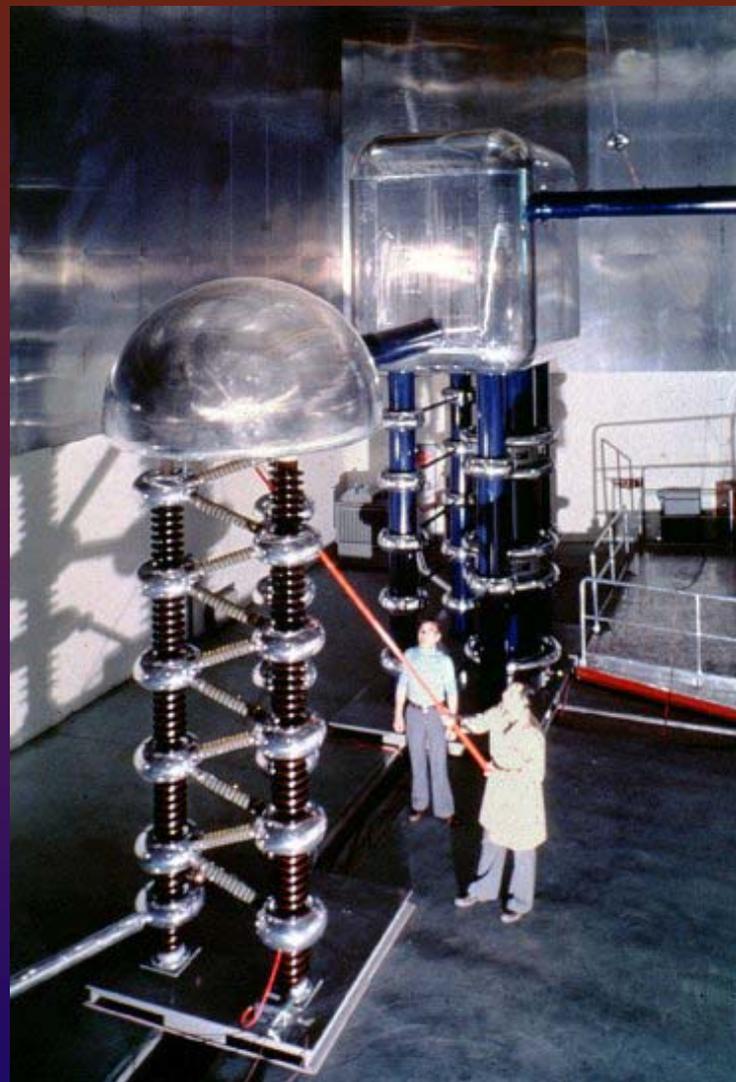
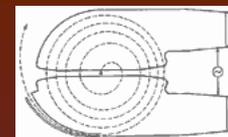
Positron beam  
generates X-ray light  
as it circulates around  
the beam line.





# Basic Accelerator Systems

- ❖ Source
- ❖ Acceleration
- ❖ Beam Containment and Transport
- ❖ Beam Interaction and Dissipation



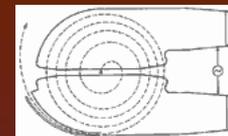
CERN 750keV Proton Source

© K Mahoney/S. Prior  
2002-2004

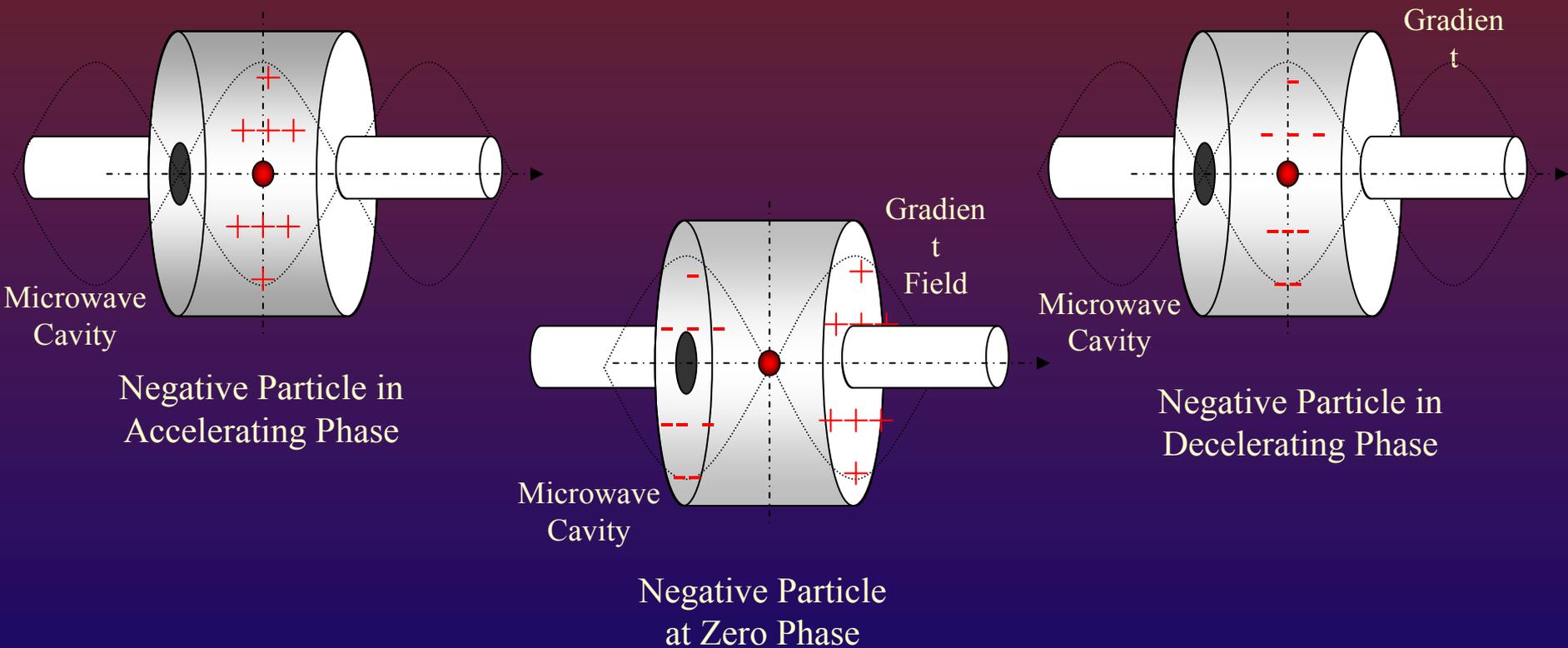


JLab 100keV Electron Source

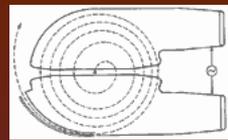
USPAS  
June, 2004



# RF Acceleration

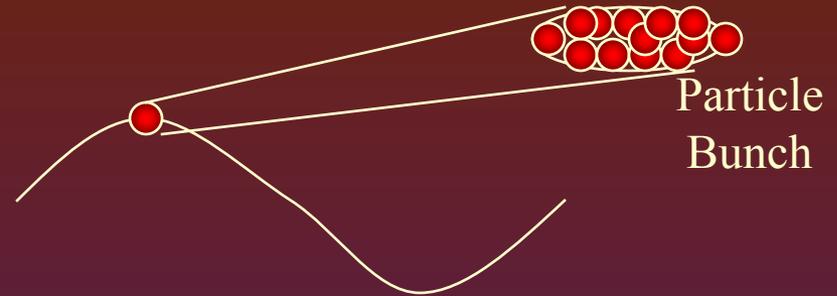


# RF Acceleration



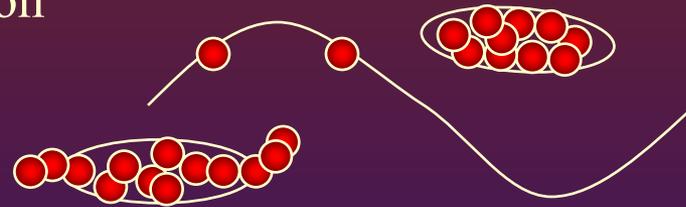
- ❖ On Accelerating Crest

- ❖ Max Acceleration



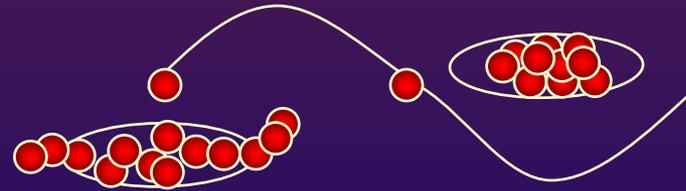
- ❖ Off Crest

- ❖ Different head-tail acceleration but still net acceleration
- ❖ Bunching
- ❖ Focusing



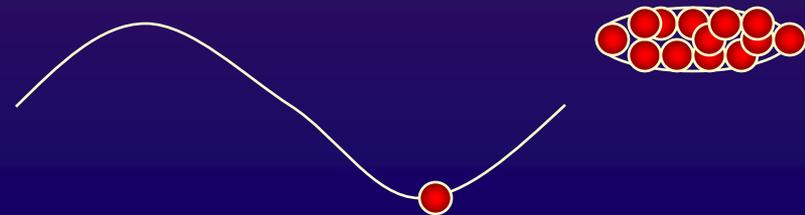
- ❖ Zero Crossing

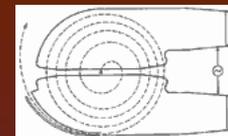
- ❖ Bunching
- ❖ Make up Lost Energy



- ❖ On Decelerating Crest

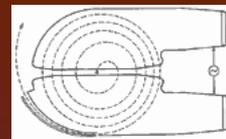
- ❖ Energy Recovery





# RHIC RF Cavities





# Field Emission and Multipacting

- ❖ Electrons are stripped off of cavity walls and accelerated within the cavity
- ❖ Can be accelerated into beam line (Dark Current)
- ❖ Source of radiation without beam

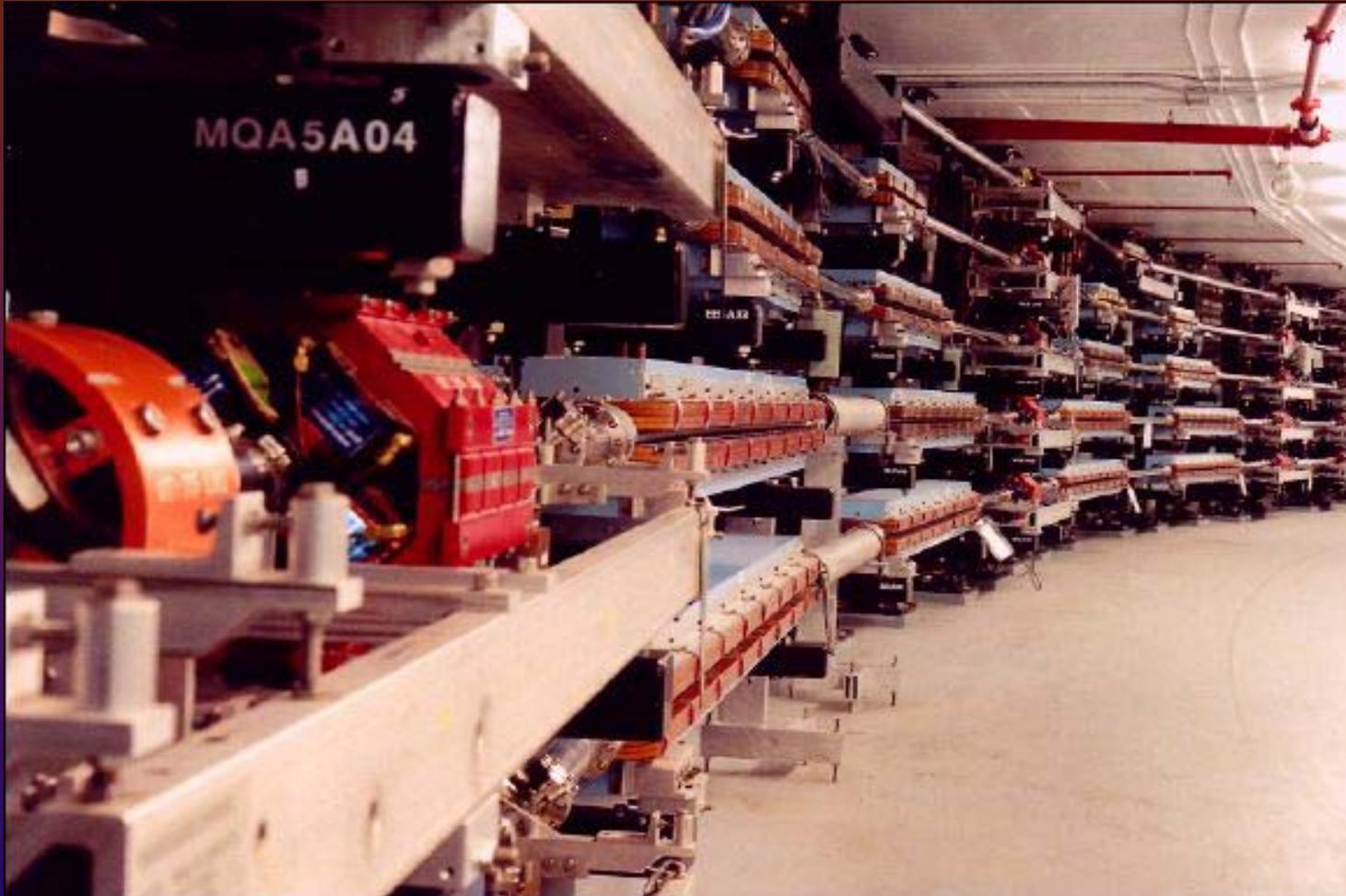
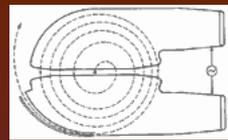
## Field emission

Electrons emitted from surface irregularity

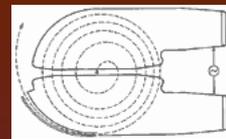
## Multipacting

Electrons stripped off cavity material and impact adjacent walls in resonance with RF frequency

# Beam Transport



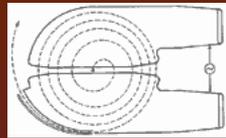
Jefferson Lab magnetic beam transport system showing dipoles (blue), quadrupole (red), and sextupole (orange) magnets.



# Supporting Accelerator Systems

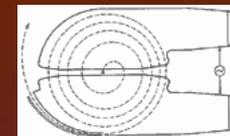
- ❖ Timing and Control
- ❖ Diagnostic
- ❖ Shielding
- ❖ Safety Systems
  - ❖ Access Control
  - ❖ Safety Interlock Systems
  - ❖ Alarm and Warning Systems

# What's Ahead?

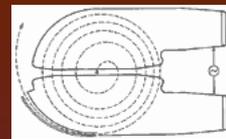


- ❖ High Power Photon Sources
- ❖ TESLA
- ❖ Neutrino factory
- ❖ CLIC
- ❖ ELIC/eRHIC
- ❖ LHC
- ❖ NLC
- ❖ Plasma/Laser Fusion
- ❖ JLab 12GeV
- ❖ Meson Scattering
- ❖ RIA
- ❖ Muon Collider

# Special Safety Concerns for Accelerators

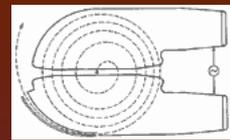


- ❖ Beam Production (Source)
  - ❖ Prompt ionizing radiation
    - ❖ Beam
    - ❖ Field Emission
    - ❖ Dark Current
    - ❖ Beam scraping
  - ❖ Laser systems, e.g photocathode
  - ❖ High Voltage
- ❖ Acceleration
  - ❖ Prompt ionizing radiation
    - ❖ Dark Current
    - ❖ Multipacting
    - ❖ Field Emission
    - ❖ Beam Scraping
  - ❖ Electromagnetic Radiation
  - ❖ High Voltage
  - ❖ Cryogenic Vessel
- ❖ Beam Transport
  - ❖ Prompt ionizing radiation
    - ❖ Beam Scraping
  - ❖ High Voltage
  - ❖ High Current
  - ❖ Laser Systems
  - ❖ Cryogenic Systems
  - ❖ Vacuum implosion
- ❖ Beam Interaction Area
  - ❖ Prompt ionizing radiation
  - ❖ High Voltage
  - ❖ High Current
  - ❖ Cryogenic Systems
  - ❖ Explosive Gas
  - ❖ Lasers
  - ❖ Vacuum implosion



# Context

- ❖ In order to implement effective safety systems for accelerators, one must understand the context in which the system operates.
- ❖ This includes statutory, regulatory, and site specific requirements.
- ❖ It also includes a basic understanding of the equipment interfaced to the system.



- ❖ Ill defined requirements lead to:
  - ❖ Outright failure
  - ❖ Work arounds that are not as thoroughly evaluated as the original design
  - ❖ “complex” solutions; especially when using computer based systems
- ❖ One of the major causes of ill defined requirements is misinterpretation or misuse (or no reference to) regulatory requirements.

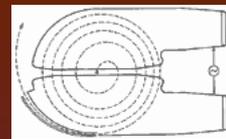


# Speaking Safety

Safety Systems

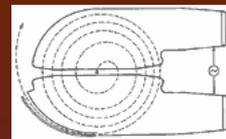
USPAS

June 2004



# Outline

- ❖ Overview of Safety
- ❖ Definitions
  
- ❖ Objective
  - ❖ Communicate the nomenclature and context for terms used in this class.

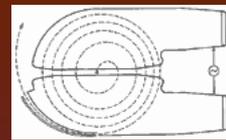


# System Safety

## What is System Safety?

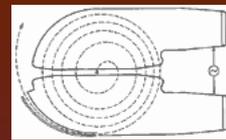
System safety is the practice of proactive hazard management.

It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from conception to decommissioning.



# System Safety

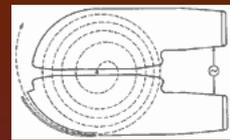
- ❖ System Safety is a holistic approach to critical systems' management.
- ❖ Safety related systems must be evaluated and designed in the context for which they are to be applied.
- ❖ This includes foreseeable changes and upgrades over the life of the system.



# System Safety

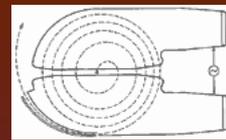
## From N. Leveson, “Safeware”

- ❖ *System safety emphasizes building in safety, not adding it to a completed design.*
- ❖ *System safety deals with systems as a whole rather than with subsystems or components.*
- ❖ *System safety takes a larger view of hazards than just failures.*
- ❖ *System safety emphasizes analysis rather than past experience or standards.*
- ❖ *System safety emphasizes qualitative rather than quantitative approaches.*
- ❖ *System safety recognizes the importance of tradeoffs and conflicts in system design.*
- ❖ *System safety is more than just system engineering*



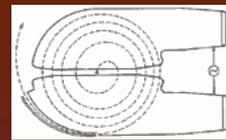
# Systems Safety

- ❖ Original safety models used the fail and fix method.
- ❖ Design a product to the best practices (usually over design), wait until it fails, fix the cause of the failure, and continue.
- ❖ Quite often ‘improvements’ were introduced that made the actual incremental improvement questionable.
- ❖ Coupled with this was an acceptance of some accidents as inevitable. In addition, the consequence of accidents involved a few individuals at most.



# System Safety

- ❖ Greater consequences from failure.
  - ❖ Technology allows concentration of great amounts of energy in small areas. This energy, if not controlled, can lead to more catastrophic accidents.
- ❖ Greater dissemination of information
  - ❖ People saw pictures of the Hiroshima, Nagasaki atomic bombs, Apollo 1 fire, Bhopal...etc.
  - ❖ Intolerance for poor living and working conditions at the beginning of 20<sup>th</sup> century eventually spilled over into intolerance for being placed in danger in the name of “progress”.



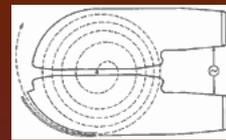
# What is a Safety System?

A Safety System is an engineered system that reduces the risk of harm to people, equipment, or the environment that may arise from the operation of a process or equipment.

## General Attributes of a Safety System:

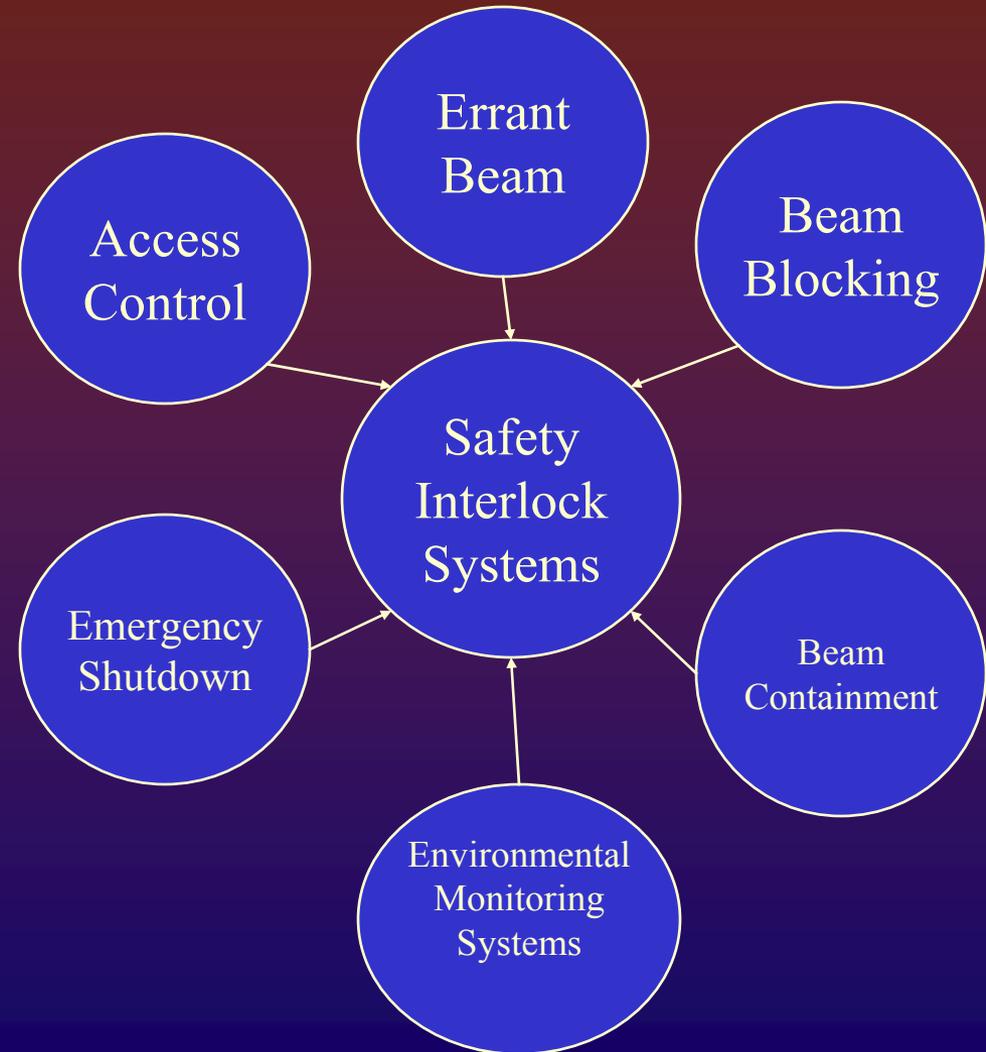
- ❖ Autonomous – acts on it's own to achieve a safe state
- ❖ Requires kinetic energy external to the process (although fails-safe)
- ❖ Sensor  $\Rightarrow$  Logic  $\Rightarrow$  Final Control Element
- ❖ Independently verifiable safety function

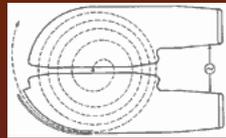
# What is a Safety System for Accelerators?



## ❖ Typical elements

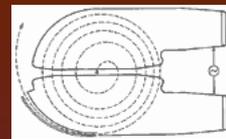
- ❖ Access Control
- ❖ Safety Interlock Systems
- ❖ Emergency shut down systems
- ❖ Errant beam detection
- ❖ Beam Containment
- ❖ Environmental monitoring systems
  - ❖ Radiation monitoring
  - ❖ Oxygen monitoring
  - ❖ Chemical agent monitoring
  - ❖ Explosive gas monitoring
  - ❖ Laser/RF Monitoring





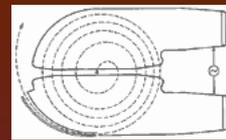
# Harm

- ❖ Damage to people, the environment, or property.
  - ❖ Intentional
  - ❖ Accidental
  - ❖ Negligent



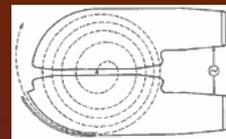
# Safety

- ❖ Freedom from harm or potential harm



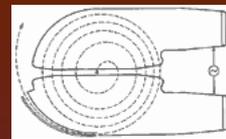
# Accident/Mishap

- ❖ An event that results in a definable level of harm or loss.
  - ❖ Minor
  - ❖ Severe
  - ❖ Catastrophic
- ❖ Due to an unmitigated release of hazardous energy.
- ❖ Requires both uncontrolled energy and exposure to the harmful effects of the energy.



# Hazard

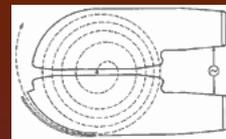
- ❖ A state or set of conditions of a system within a given environment that will lead to an accident.
- ❖ Usually involves potential energy.



# Risk

- ❖ A measure of the combination of hazard severity, likelihood, exposure, and opportunity that could lead to an accident.

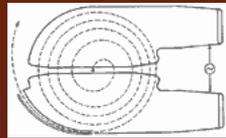




# Concrete Risk

- ❖ Risk of harm to people
- ❖ Risk of harm to the environment
- ❖ Risk of harm to equipment

# Objective vs. Perceived Risk (especially radiation)



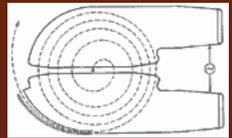
What weight has perception?

Most individual risks feed into a larger concern ...

Q.) Where does perception have an impact?

A.) Institutional risk.

# Perceived Risk

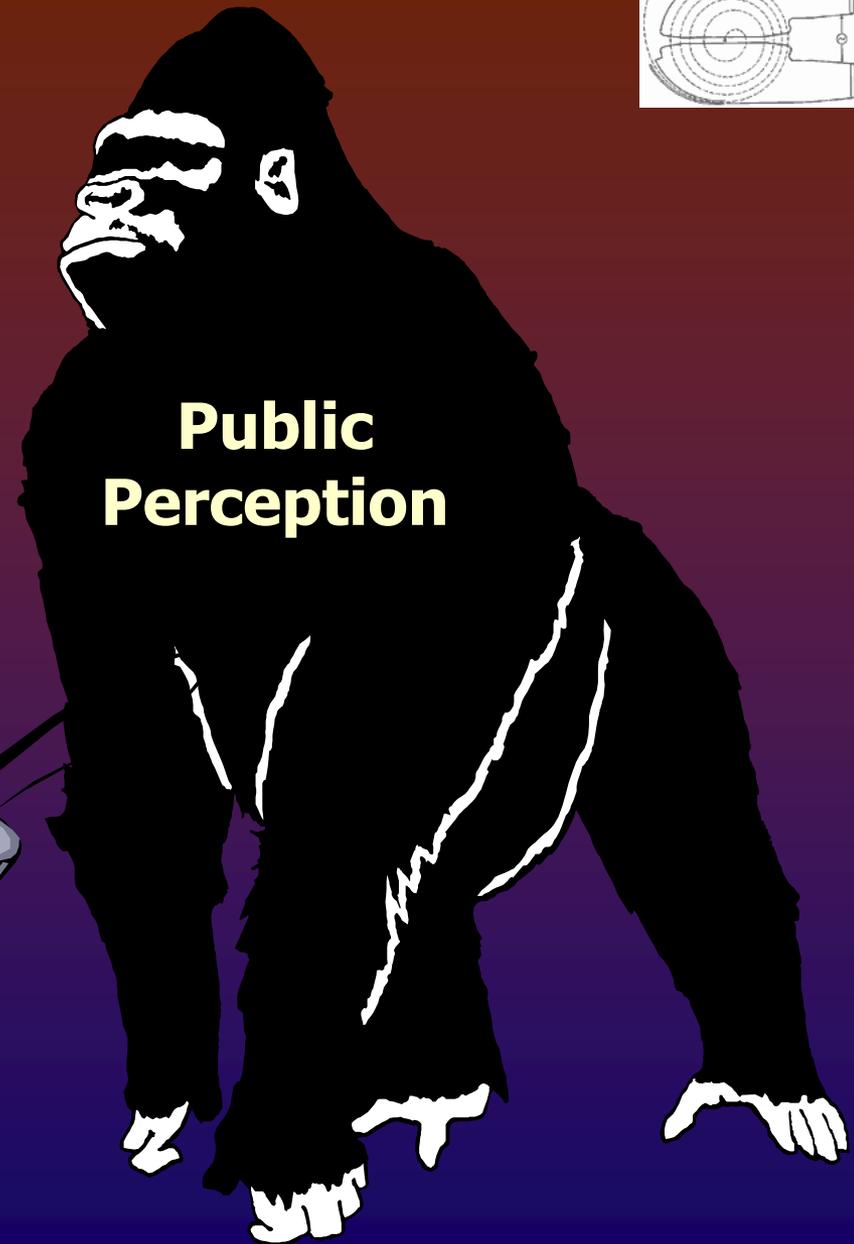


Sometimes  
Perceived Risk is  
the dominating  
factor in a risk  
assessment

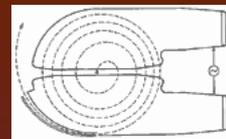


**RISK**

**Safety  
Professional**



**Public  
Perception**



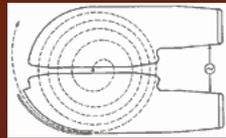
# Esoteric Risk

Schedule Risk

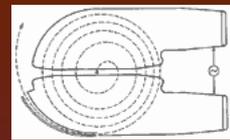
Institutional Risk

Risk to mission

Risk of public perception

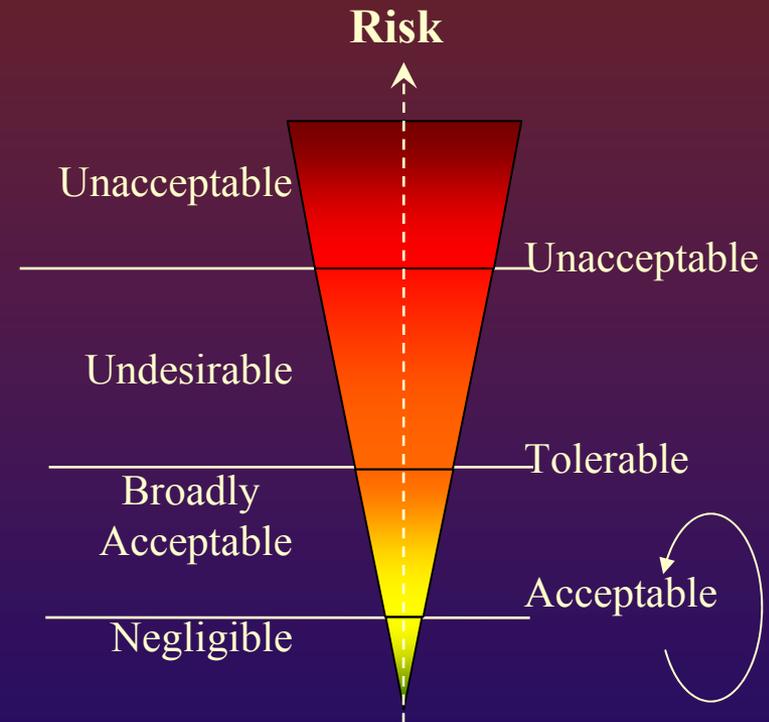


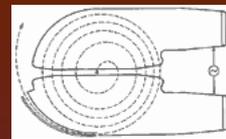
For practical purposes most risk can be associated with institutional risk. Therefore management is ultimately responsible for making an informed decision about how much risk they are willing to accept.



# Approaches to safety system risk management

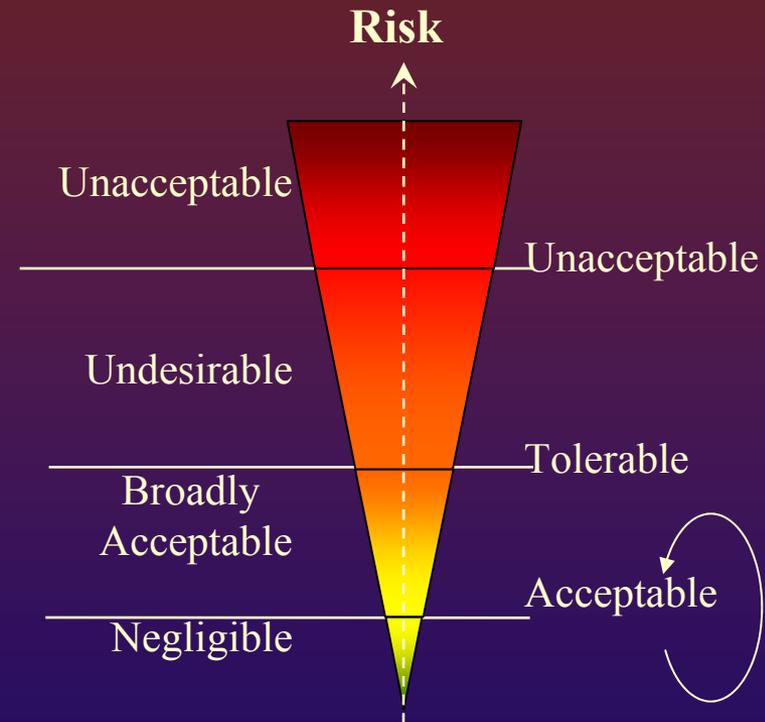
- ❖ **ALARP**
- ❖ **System Safety (e.g. MIL 882D)**
- ❖ **Regulation**
- ❖ **SIL**



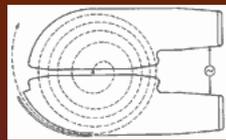


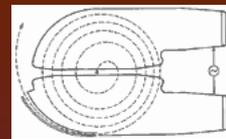
# Risk Reduction

The purpose of safety programs is to identify risk and design methods to reduce the risk to the acceptable region over the life of the facility or system.



# Methods of Mitigation





# Reliability

*The probability that a piece of equipment will perform it's intended function satisfactorily for a prescribed time and under stipulated environmental conditions.*

## Elements of reliability:

### Equipment

The thing that enables a hazard to occur

### Probability

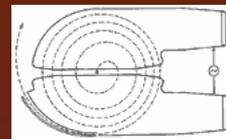
Equipment will eventually fail, it's a matter of how and when

### Time

When

### Environment

Assumptions as to the operating conditions of the equipment

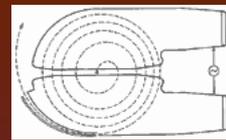


# Reliability

**Safety Reliability** - The probability that a piece of equipment will perform the intended safety function over a given time period.

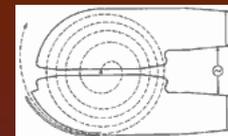
**Safety Availability** – the probability that a piece of equipment is able to perform the intended safety function when the hazard can be present.

$$SA = 1 - PFD$$



# Safety Integrity Level

- ❖ Applies a range to the average probability of fail dangerously ( $PFD_{avg}$ ) of a safety instrumented function.
- ❖ Each level covers 2 orders of magnitude



## DEMAND MODE OF OPERATION

Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10,000$ to $\leq 100,000$
3	$\geq 10^{-4}$ to $<10^{-3}$	$>1000$ to $\leq 10,000$
2	$\geq 10^{-3}$ to $<10^{-2}$	$>100$ to $\leq 1000$
1	$\geq 10^{-2}$ to $<10^{-1}$	$>10$ to $\leq 100$

## CONTINUOUS MODE OF OPERATION

Safety Integrity Level (SIL)	Frequency of Dangerous Failures Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

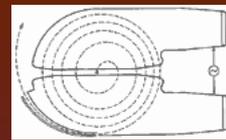


# Standards and Competency

Safety Systems

USPAS

June 2004



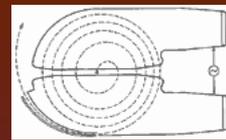
# Outline



- ❖ Standards and Competency

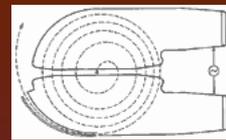
- ❖ Objective

- ❖ Communicate the requirements for technical competency in safety system management and engineering.



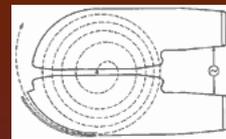
# In a nutshell...

- ❖ Accelerators have hazards that are potentially lethal to people and harmful to unique, expensive equipment as well as the environment
- ❖ Management assumes the responsibility for safe and productive accelerator operations – this is a public trust
- ❖ By proxy, the public relies on competent personnel to evaluate, quantify, and manage risk
  - ❖ Failure to meet this trust can result in harsh consequences
    - ❖ Human Loss
    - ❖ Financial Loss
    - ❖ Valuable Scientific Research Loss
    - ❖ In worst cases – criminal or civil prosecution
- ❖ Standards attempt to capture recognized accepted good practice.
- ❖ To be competent, one must have a proven understanding of the standards and the implications of decisions that affect safety.



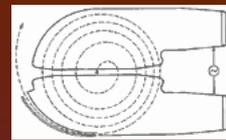
# Four Approaches to Safety Systems

- ❖ System Safety (882/FAA/NASA)
- ❖ IEC and SILs
- ❖ Machine Safety
- ❖ Nuclear/Radiation Safety



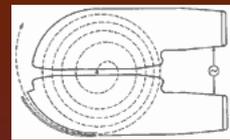
# Types of Standards

- ❖ Consensus Standards
- ❖ Performance Based Standards
- ❖ Proscriptive Standards
  
- ❖ Normative Information (Shall, Must, Comply...)
- ❖ Informative Information (Guidance, Reports,...)



# Competency Requirements

- ❖ Applicable education and training
- ❖ Demonstrated ability to apply education and training
  - ❖ Peer Recommendation
  - ❖ Successfully pass examination(s)
  - ❖ Ability to determine appropriate techniques
- ❖ Continuing education and professional growth
  - ❖ “Maintenance” points



# IEC61508

## Functional safety of electrical/electronic/programmable electronic safety related systems –

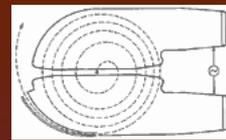
### Management Responsibilities

Managers shall...specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety. In particular, the following should be considered:

6.2.1 h) the procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:

- the training of staff in diagnosing and repairing faults and in system testing;
- the training of operations staff;
- the retraining of staff at periodic intervals;

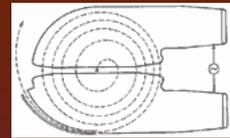
# Examples from IEC61508



The following factors should be considered when assessing the competence of persons to carry out their duties:

- a) engineering knowledge appropriate to the application area;
- b) engineering knowledge appropriate to the technology (for example electrical, electronic, programmable electronic, software engineering);
- c) safety engineering knowledge appropriate to the technology;
- d) knowledge of the legal and safety regulatory framework;
- e) the consequences in the event of failure of the E/E/PE safety-related systems; the greater the consequences, the more rigorous should be the specification and assessment of competence;
- f) the safety integrity levels of the E/E/PE safety-related systems; the higher the safety integrity levels, the more rigorous should be the specification and assessment of competence;
- g) the novelty of the design, design procedures or application; the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be;
- h) previous experience and its relevance to the specific duties to be performed and the technology being employed; the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken;
- i) relevance of qualifications to specific duties to be performed.

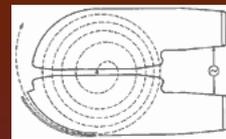
# Examples from IEC61511



**5.2.2.2** Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

NOTE As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

- a) engineering knowledge, training and experience appropriate to the process application;
- b) engineering knowledge, training and experience appropriate to the applicable technology used (for example, electrical, electronic or programmable electronic);
- c) engineering knowledge, training and experience appropriate to the sensors and final elements;
- d) safety engineering knowledge (for example, process safety analysis);
- e) knowledge of the legal and safety regulatory requirements;
- f) adequate management and leadership skills appropriate to their role in safety life-cycle activities;
- g) understanding of the potential consequence of an event;
- h) the safety integrity level of the safety instrumented functions;
- i) the novelty and complexity of the application and the technology.



# Example Certifications

## ◆ BCSP

### ◆ ANSI/ISO 17024 Accredited

(Accredited Personnel Certification Programs)

### ◆ System Safety Specialty Examination (being phased out)

◆ For US Navy and other DOD offices as requested

## ◆ Certified Functional Safety Expert (CFSE)

### ◆ Process Industry

### ◆ Safety Hardware Development

### ◆ Safety Software Development

### ◆ Safety of Machinery

# Introduction to System Safety

Sandra L. Prior, REM, CHMM

System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

# System Safety History

- System safety (SS) movement began in 1940s
  - Amos L. Wood, 14<sup>th</sup> Annual Meeting of the Institute of Aeronautical Sciences in January 1946
- USAF an early leader
- Air Force-Industry partnership began as early as 1954
- Early 60s, small group of managers, scientists, & engineers implemented SS in aerospace program
- In 1962, the System Safety Society was organized; professional organization in 1972

# What is System Safety?

System safety is the practice of proactive hazard management. It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from conception to decommissioning.

# USAF System Safety Definition

## **Air Force System Safety Handbook:**

“The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle.”

# FAA System Safety Definition

## **FAA System Safety Handbook:**

“The application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity.”

# System Safety Principles

- Safety must be designed in.
- Inherent safety requires both engineering and management techniques to control the hazards.
- Safety requirements must be consistent with other program or design requirements.

# System Safety Goal

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures.

**Question- Where do you find the DOE system safety program defined?**

# DOE Safety Management System Policy 450.4

“The Department and Contractors must systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the workers, and the environment.”

# Step 1: Define Objectives

- Typically documented in
  - Business Plan
  - Operating Specifications
- In what DOE document(s) might you find this type of information?

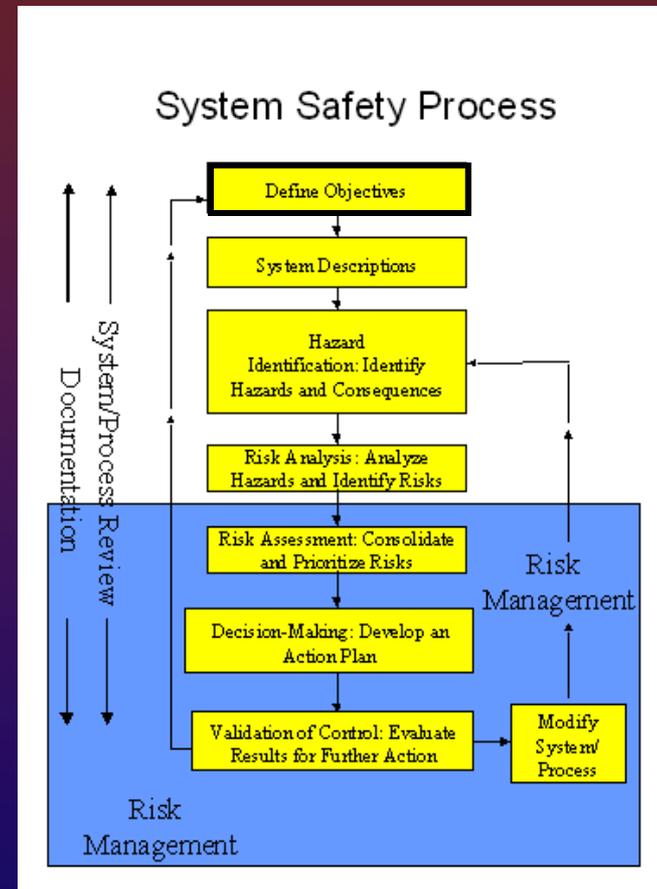


Diagram taken from FAA web site at  
<http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm>

“There are no "safety problems" in system planning or design. There are only engineering and/or management problems that, if left unresolved, may lead to accidents.”

FAA System Safety Handbook

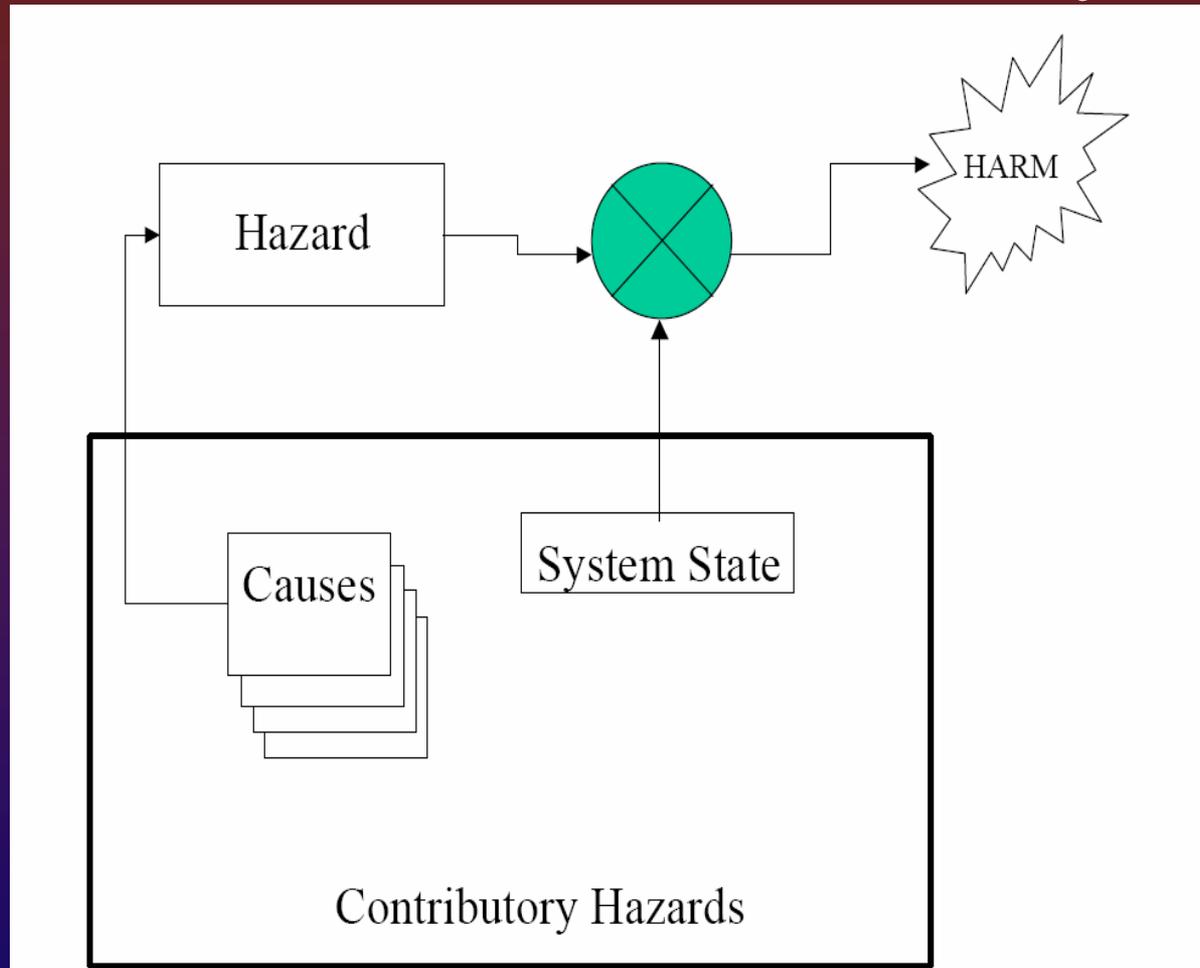


# System Description (continued)

- **The object of a good system definition is to:**
  - ✓ **set limits for the following steps in the process**
  - ✓ **reduce complex systems into manageable parts.**



# Hazard Analysis



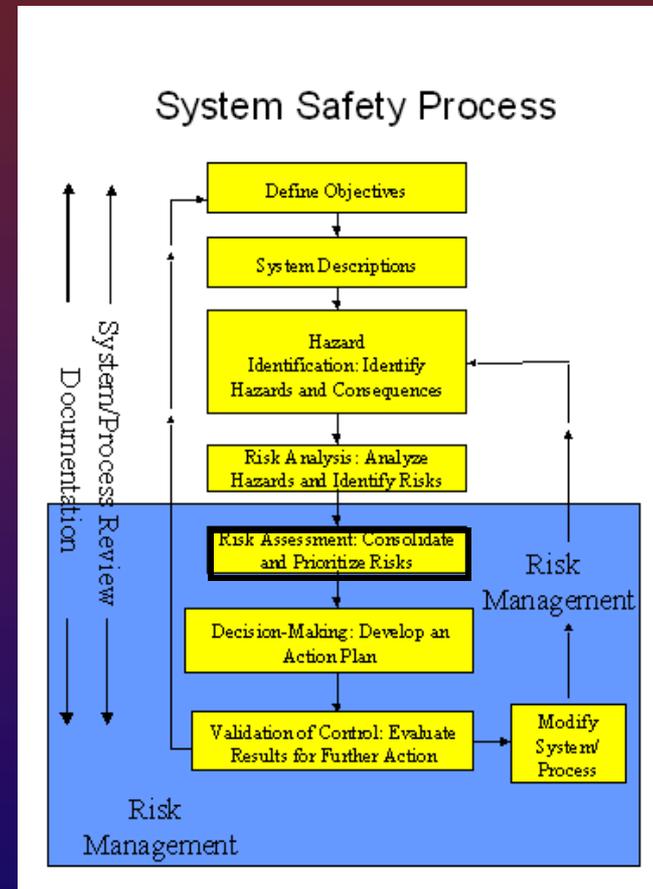
**Analysis should be:**

- ✓ **Comprehensive**
- ✓ **Methodical**
- ✓ **Disciplined**



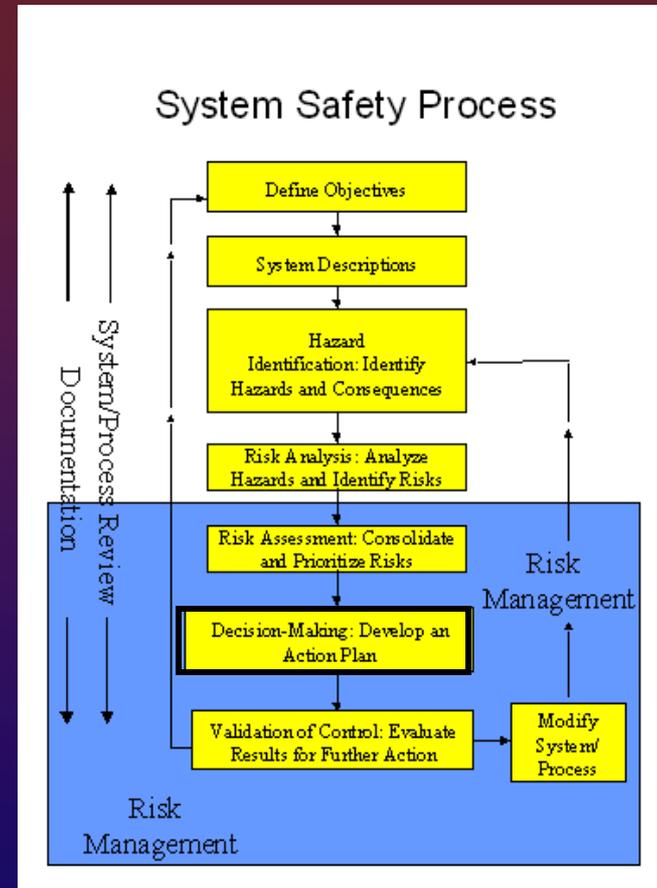
# Step 5: Risk Assessment

- Combine impacts of risk elements
- Compare impacts against acceptability criteria
- May consolidate risks into sets for joint mitigation and decision making



# Step 6: Decision Making

- Begins with
  - Management decision
  - Resources allocation
  - prioritized task list
- Most crucial step in process
- Decide how to address each risk
  - Safety Order of Precedence



# Safety Order of Precedence

- Design engineering approach:
  - Design for minimum risk
  - Design to reduce hazards
  - Incorporate safety devices
  - Provide warning devices
  - Develop procedures and training
- Alternative action plans
- Final result -written assessment document

# Effective Safety Risk Management Decisions

- Assign qualified, competent personnel
- Authority commensurate w/ responsibility
- Define, document, & track all known hazards as program policy
- Include safety risk assessment in program reviews
  - Risk acceptability
  - Risk responsibility
  - Decision milestones



# DOE Accelerator Readiness Review (ARR)

- Required by DOE Order 420.2A, para 4.d –  
“Accelerator Readiness Reviews. Accelerator Readiness Reviews (ARRs) must be performed prior to approval for commissioning and routine operation and as directed by the Cognizant Secretarial Officer/NNSA Deputy Administrator or a field element manager/NNSA field manager.”

# DOE Accelerator Readiness Review (ARR)

(FEL-ARR) Status - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://mis/fel/> Go Links »

Help - Search

Maintained by: [ingapps@llab.org](mailto:ingapps@llab.org)  
system ERD

[NEW! FEL Readiness Plan](#)

### Upgrade FEL Readiness Status

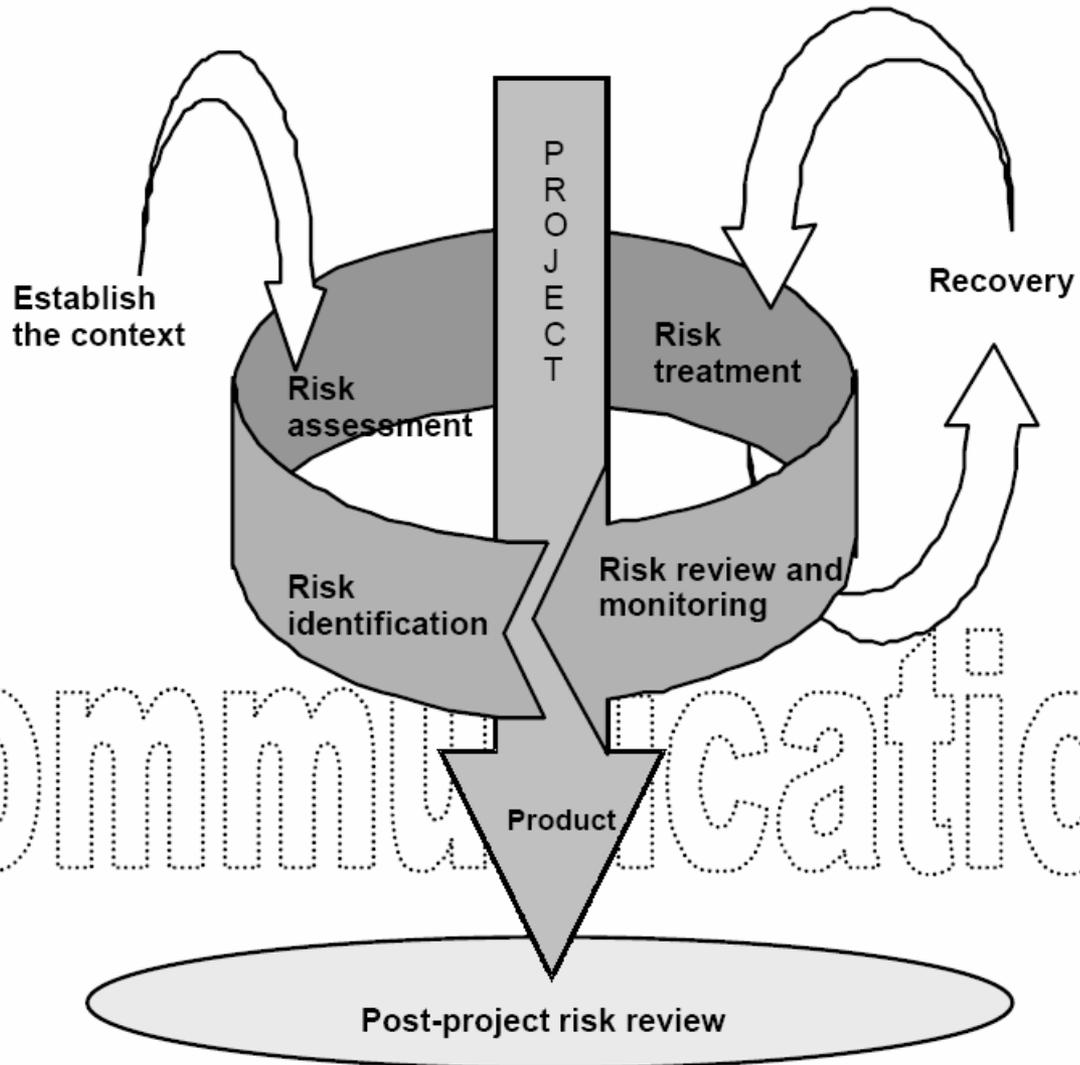
ARR Stage ▶ FEL Sub-System (Mgr) ▼	Major Design			Detail Specifications			Fabrication			Testing			Integrated			READY		
	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c
Project Mgmt (Dylla)	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c
Facility (Neil)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Beam Physics (Douglas)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Injector (Dylla)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
SRF (Preble)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
RF (Walker)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Cryogenics (Arenius)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Instrumentation (Jordan)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
e <sup>-</sup> Beam Transport (Biallas)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Wiggler (Benson)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Optics (Shinn)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Laser Safety (Benson)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Personnel Safety (Mahoney)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
RadCon (May)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c

<b>System last updated:</b> 18-NOV-03 @ 09:29 AM	<b>Key:</b>	<b>Color Key:</b>	<b>Other Links:</b>
	a: equipment	Green: completed and ready	<a href="#">FEL Logbook</a>
	b: personnel	Blue: on schedule and no issues	<a href="#">BAIR Web Home</a>
	c: procedures	Yellow: behind schedule but no issues	<a href="#">FEL Project Mgmt Tools</a>
	n/a: not applicable	Red: unresolved issues or critical path work behind schedule	<a href="#">OPS-PR Query</a>

Logged in as: prior



# Project Success



# Summary

- System Safety is a process that guides you into developing a context for your safety system design.
- The System Safety process requires you to document this context.
- Once your context has been established, you can then develop your safety system within that context.

# Regulatory Requirements

Sandra L. Prior, REM, CHMM  
System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School  
June 28 – July 2, 2004

# Branches of Federal Government

– Legislative

– Executive

– Judicial

# Legislative Branch

- Enacts laws
- Defines agency's regulatory authority
- Defines agency responsibilities
- Tells how agency will perform administrative functions and carry out enforcement activities

# Executive Branch

- Headed by the President
- Regulatory agencies are located here
  - Independent
    - Ex. EPA
  - Cabinet appointed
    - Ex. Secretary of Labor
  - Develop regulations and program guidance
  - Carry out enforcement actions
  - US Occupational Safety & Health Review Commission: <http://www.oshrc.gov/index.html>

# Judicial Branch

- Laws are interpreted and enforced
- Civil and criminal cases are tried for violations
- Conduct law reviews
- Review regulatory agency actions

The Federal Government can  
take no action on any issue  
without a law that allows it to act.

# Interpreting the Requirements

- Individual Acts are enacted by Congress
  - May refer to short portions or a broader law that was enacted at some period of time
  - May be an original act that created an entirely new regulatory area
  - May be an act that amends an existing law (most common)
  - Body of standing law, or *statutes*

# Statutes

- Compiled in two ways
  - Publish separate major laws
    - *As amended*
  - Publish in the United States Code
    - Compilation of law/statutes w/ amendments current up to date of Code publication
    - Organized in *Titles*

# Regulations

- Outline specific procedures for the administration and enforcement of laws.
- *Rules* and *Regulations* are synonymous
- Compiled in the **Code of Federal Regulations (CFR)**
- Regulations have the *force of law*

# Rulemaking

- Many technical details are determined during the regulatory development process
- We have numerous opportunities to comment on technical details during the rulemaking process
- Can track rulemaking process via *Federal Register*

# Typical Rulemaking Process

- Congress enacts law permitting or requiring agency to develop regulations
- Agency develops schedule, effectively puts parties on notice of impending process.
- Agency establishes **docket**
- Agency develops internal regulatory concept

# Typical Rulemaking Process

- Agency develops proposed regulation
  - Published in *Federal Register*
  - Preamble – important part
    - *The preamble contains the agency's interpretation of how the regulation will work and is a potential source for any future questions and/or interpretation.*
- Public Hearing – if necessary
- Revise or publish in final form

# Challenging The Rules

- Final rule may undergo legal review
  - Agency did not follow administrative procedure requirements or specific requirements in enabling legislation or the agency's own internal rules
  - Based upon erroneous science or economic analysis

# Enforcement

- Two kinds of enforcement
  - Administrative: covers all enforcement actions taken by an agency
    - Inspection/administrative review resulting in a violation
    - Official Notice of Violation (NOV)
    - Consent Order
  - Judicial: occurs when the agency takes a case to the courthouse for lawsuit or criminal prosecution.

# Summary of Roles

**Congress** – enacts legislation to create regulatory agencies and give them authority to regulate in specific subject areas.

**Regulatory Agencies** – develop regulations that describe detailed requirements of regulatory programs, and enforce these programs.

**Courts** – determine if a regulated entity is civilly or criminally liable for violating laws and regulations; rule on constitutionality of laws and agency conformance to laws and regulations.

# How Do You “Navigate” Through Requirements?

- Define your legal scope
  - Federal
  - State
  - Government-owned, contractor-operated
  - Public
  - Private
  - International

# How Do You “Navigate” Through Requirements?

- Define your operational scope
  - What requirements apply to safety systems?
    - Very little legal requirements
    - Must identify standards of good practice for guidance
  - What requirements affect my safety system?
    - Environment w/in which the system resides
    - Also must address requirements applicable to hazards the system is designed to mitigate

# Conflicts – How Do You Resolve Them?

- Order of precedence
- Examine governing requirement document
  - Scope/applicability
    - CFR – read the Preamble
    - Contracts
  - Provisions for exceptions
    - Waiver
    - Exemption
    - Equivalency

# Pedigree of a Requirement

Public Law/Act

Federal Regulation

State/Local Regulations

Contract Requirements

Organization Policy

Work Procedures

# How Do You Stay Current?

- CFRs are the body of standing law
  - Updated annually
  - Consult the *Federal Register*
  - Internet access: Government Printing Office; OSHA, EPA, USC, state DEQ & OSHA
- Consensus Standards
  - Professional organization membership
  - Journals, newsletters
  - Networking
- Organizational guidance
  - Internal policies/procedures under documents control

# WORK SMART STANDARDS (WSS)

## DOE-HDBK-1148-2002

“The Department has deliberately adopted a standards-based approach to safety management that is intended to allow for good judgment in work design and resource allocation.”

# DOE Work Smart Standards

- Necessary Standards
  - Legal requirements that must be met
- Sufficient External Standards
  - External guidelines that establish good practice
    - Consensus standards
    - DOE Handbooks, Guides, & Manuals
- Sufficient Internal Standards
  - ES&H Manual
  - Safety System User Manual

# Questions?

# Application of Standards to Accelerator Safety Systems

Sandra L. Prior, REM, CHMM  
System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School  
June 28 – July 2, 2004

# Why Do I Have to Have a Safety System?

- ❖ Legal requirements
- ❖ Good Business practices
- ❖ Liability reduction
- ❖ Competition for resources
- ❖ Mission accomplishment

# Aren't Administrative Controls Good Enough?

- ❖ Not as effective as engineering controls
- ❖ Criticized as means of spreading exposures rather than eliminating or reducing them
- ❖ Depend upon continual human intervention
- ❖ Difficult to implement and maintain
- ❖ May be more expensive over the long term

# What Are The Hazards Associated With Accelerators?

- ❖ Prompt Ionizing Radiation
- ❖ Residual Ionizing Radiation
- ❖ Oxygen Deficiency
- ❖ Fire/Explosive (Hazardous Classified) Areas
- ❖ Laser Radiation
- ❖ Other Non-Ionizing EM Radiation
- ❖ Open Machinery
- ❖ Exposed Electrical Equipment
- ❖ Chemical Processes
- ❖ Biological Research Facilities

# Who Has Legal Authority Over Accelerators?

- ❖ OSHA covers all radiation sources not regulated by A.E.C.
  - Examples of non-A.E.C. regulated radiation sources include X-ray equipment, accelerators, accelerator-produced materials, electron microscopes, betatrons, and some naturally occurring radioactive materials.

# Accelerator System Design and Implementation

- Very little specific requirements on accelerators exist in law/regulations
  - 10 CFR 835
  - 29 CFR 1910.1096
  - 29 CFR 1910, Subpart S
- OSHA's Process Safety Standard, 29 CFR 1910.119, contains some guidance but is not applicable to accelerators
- Must defer to consensus standards for guidance

# OSHA General Duty Clause (GDC)

Section 5 of the OSH Act or the "General Duty Clause" which states:

A. Each Employer:

- 1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or likely to cause death or serious physical harm to his employees;
- 2) shall comply with occupational safety and health standards promulgated under this Act.

# OSHA General Duty Clause (GDC)

Section 5 of the OSH Act or the "General Duty Clause" which states:

B. Each employee shall comply with occupational safety and health standards and all rules, regulations and orders issued pursuant to this Act which are applicable to his own actions and conduct.

# OSHA GDC Criteria

- ❖ The employer failed to keep the work place free of a hazard to which employees of that employer were exposed.
- ❖ The hazard is (or should have been) recognized by the employer.
- ❖ The hazard is causing or was likely to cause death or other serious physical harm.
- ❖ There is a feasible and useful method to correct the hazard.

# Why Consensus Standards?

- ❖ Establish a context where ideas and solutions can be exchanged
- ❖ Focused on quality outcomes
- ❖ Part of an overall risk management plan
- ❖ Provide you a sound basis for your documented justification



# Types of Standards

## ❖ Implementation Prescriptive

- ❖ Nuclear Industry
- ❖ Air Craft
- ❖ Space

## ❖ Consensus

- ❖ Process Industries
- ❖ Manufacturing Industries
- ❖ Research and Development

# Public Law 104-113

National Technology Transfer and  
Advancement Act of 1995 [Public Law (PL) 104-113]

*“Federal Participation in the Development and Use of Voluntary Standards...”*

*“PL 104-113 is a true shift in the paradigm for many Federal agencies regarding the conduct of their technical standards activities. Where DOE, in its continued transition to a "work smart", standards-based operating culture, identifies the need for new or revised technical standards, PL 104-113 compels us to focus all technical standards development efforts deemed necessary toward voluntary standards in lieu of DOE technical standards. “*

*Assistant Secretary for EH*

# Consensus Standards

- Both National and International
- Voluntary
- May become regulatory when:
  - Referenced in law/regulation
  - Incorporated into agreements
  - May reference entire document or only portions
- May become an implied requirement

# How Do I Determine What Consensus Standards To Follow?

- ❖ Identify standards that are applicable to a wide group of users.
- ❖ Identify standards that add value to the organization and tasks at hand.
- ❖ Identify standards that are not obsolete the day they are published.
- ❖ The trick then is to translate these standards into commitments that are not overly prescriptive.



# Possible Accelerator Safety System Standards

ANSI/ISA S84, Application of Safety Instrumented Systems for the Process Industries

IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511, Functional safety – Safety instrumented systems for the process industry sector

MIL-STD-882D, Standard Practice for System Safety

IEC 62198, Project Risk Management

IEC 61131-3, Programming Industrial Automation Systems

# Possible Accelerator Safety System Standards (continued)

IEC 1025, Fault Tree Analysis NCRP 88, Radiation Alarms and Access Control Systems

ISO 9001:2000, Quality Management Systems

ISO 14001, Environmental Management Systems

ISO 18001, Occupational Health & Safety Management Systems

# ANSI/ISA S84.01

- ❖ Consensus Standard
- ❖ Designed to meet Needs of Process Industry, e.g. 10CFR1910.119
- ❖ Wide Body of Experience
  - Equipment Manufacturers
  - System Integrators
  - Reliability Engineers
  - Academia
- ❖ Deals mostly with the programmable section of the safety system

# S84 Key Points

- ❖ Requires Hazard Identification and Classification
- ❖ Safety Requirements Specification
  - ❖ Identify Safety Functions
  - ❖ Identify Required SIL for Safety Systems
  - ❖ Identify Safe State
- ❖ Safety Implementation
- ❖ Evaluation of Proposed Design
- ❖ Management of Change Plan

# S84 and OSHA

March 31, 2000 - "As S84.01 is a national consensus standard, OSHA considers it to be a recognized and generally accepted good engineering practice for SIS (Safety Instrumented Systems),"

Richard E. Fairfax, Director, Directorate of Compliance Program Assistance for OSHA

Refers to S84 in the context of requirements of 10CFR1910.119 Hazardous Chemical Controls

# ISA-TR84.02

- Guidance to S84 for determining safety integrity level (SIL) of a safety system
- Gives Three methods for calculating SIL
  - Simplified Equations (Block Diagram)
  - Fault Tree
  - Markov Model
- Part 5 gives methods for calculation of PFD of logic solver using Markov models.

# IEC61508

- ❖ Umbrella Standard intended to cover all industrial safety system applications –E/E/PE
- ❖ Meant as starting point for sector standards
- ❖ Very detailed, almost prescriptive
- ❖ Defines key numerical risk reduction criteria
- ❖ Intended for manufacturers

# IEC61508

## ❖ 7 Parts

- ❖ Part 1 General Requirements
- ❖ Part 2 Systems Requirements
- ❖ Part 3 Software Requirements
- ❖ Part 4 Definitions
- ❖ Part 5 SIL Evaluation methods
- ❖ Part 6 Guidelines on applying parts 1 and 2
- ❖ Part 7 Overview of techniques

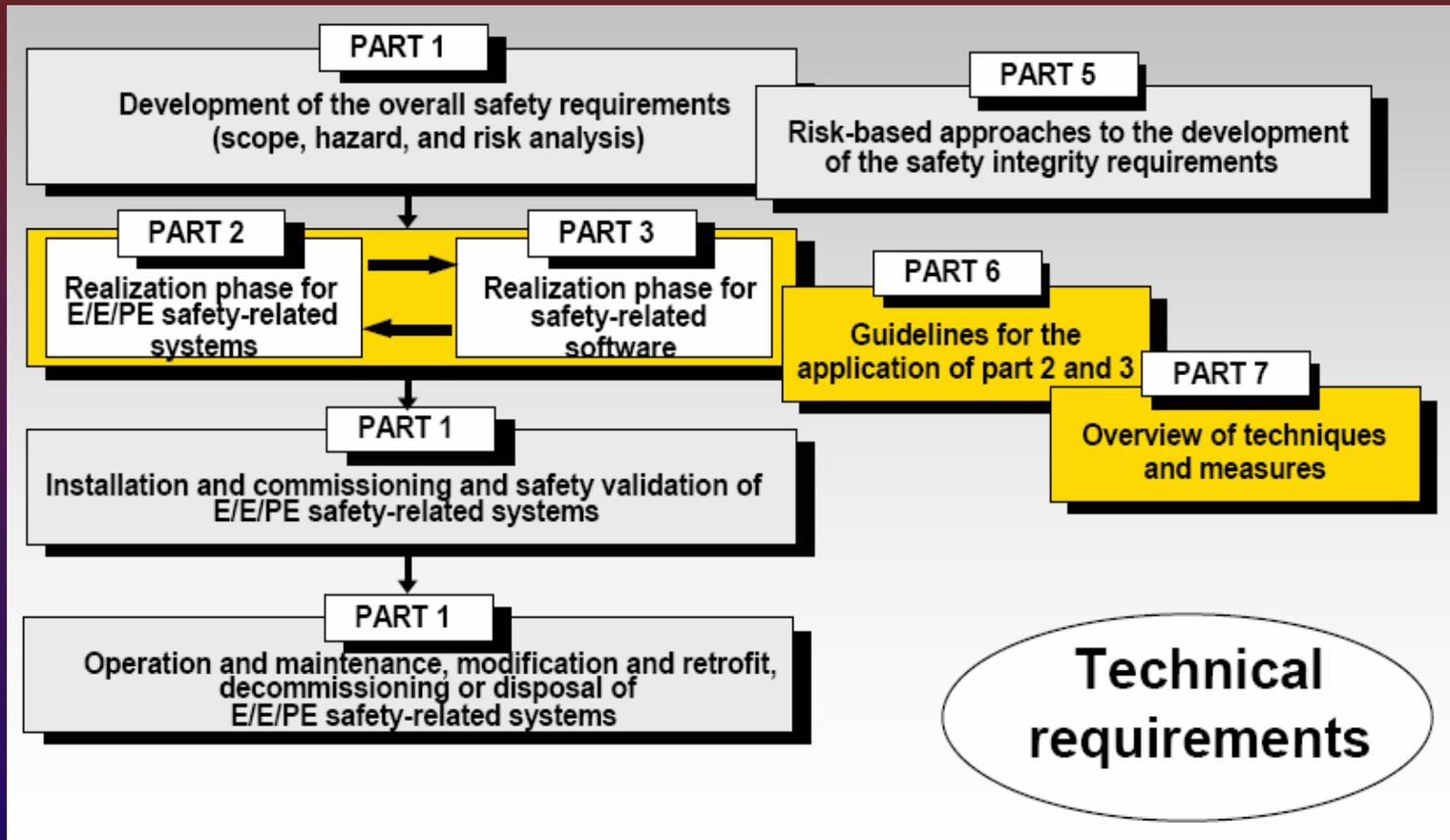


Normative



Informative

# IEC 61508 – Functions of Parts 1-7



Exida's *Introduction to IEC 61508*, <http://www.exida.com/training/>

# ‘In Country’ Clause

IEC61508 Part 1.4...

“In the USA and Canada, until the proposed sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC61508.”

# IEC61511

- ❖ IEC revision of process sector standards, e.g. ANSI/ISAS84.01
- ❖ Released in February 2003
- ❖ 3 Parts
  - ❖ Part 1 General Requirements
  - ❖ Part 2 Guidelines for application
  - ❖ Part 3 Guidelines for Hazard and Risk Analysis

# Software

## ❖ Languages

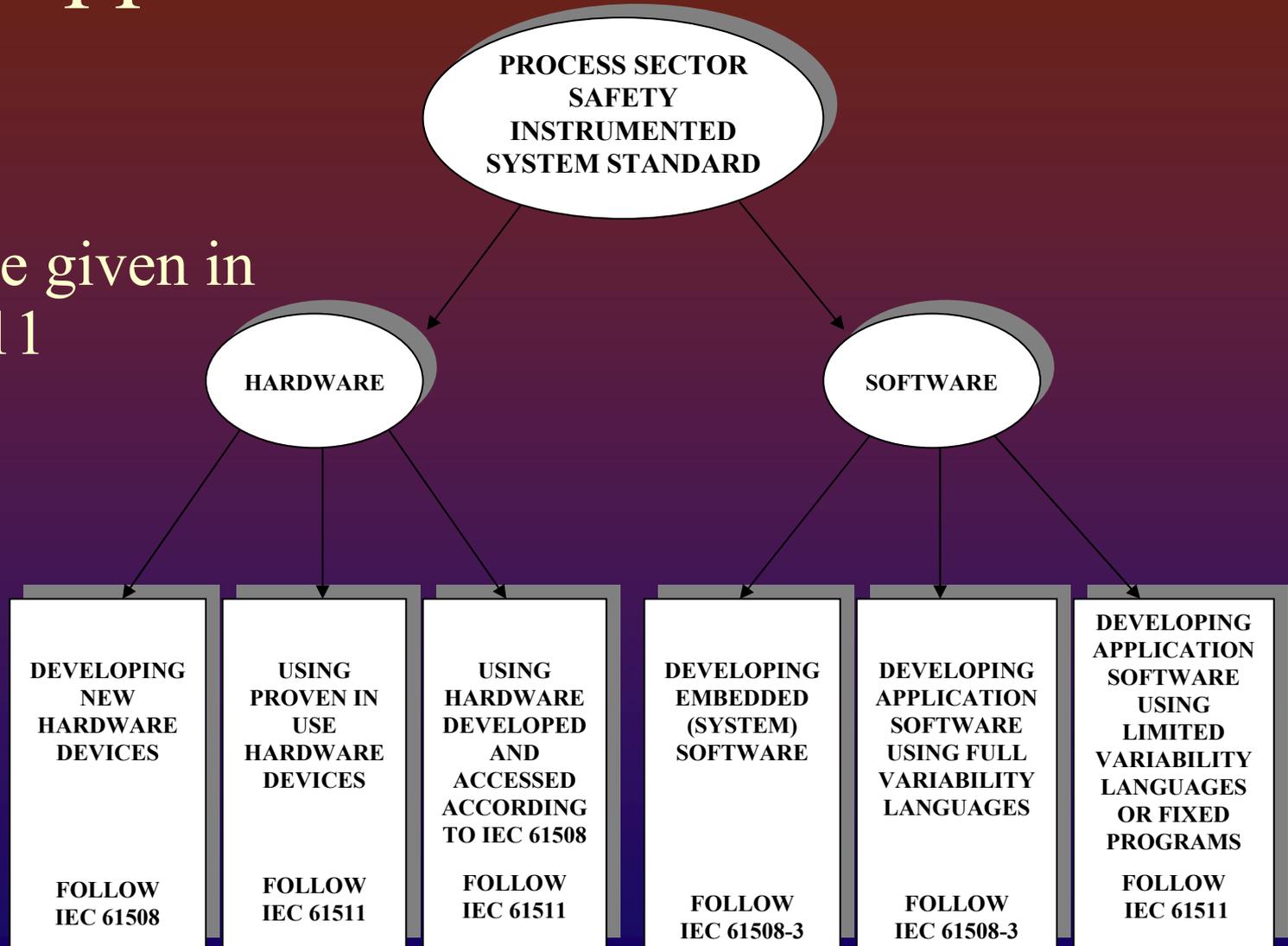
- ❖ IEC61131-3 Defines PLC programming Languages

## ❖ Applications

- ❖ Software application development is left to “Good Practice”
- ❖ A good start is in IEC 61508 and 61511
- ❖ IEC880 (Software for Computers in the Safety Systems of Nuclear Power Stations) is a good reference

# Application of IEC Standards

Guidance given in  
IEC61511



# Basis for OSHA/NRC Evaluation

- ❖ Safety program conforms to accepted “good practice”
- ❖ Personnel are recognized as “competent” in their field
- ❖ Safety programs are well documented
  - ❖ Hazard/Risk Analyses
  - ❖ Design & design basis
  - ❖ Testing/Certification
  - ❖ Procedures
  - ❖ Training
  - ❖ Corrective Action

# What is Your Legal Basis?

California

Illinois

New Mexico

Tennessee

New York

Utah

Brazil

DOE

# Lifecycle Management

Sandra L. Prior, REM, CHMM  
System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

# Outline

- ❖ Overview of Safety Lifecycle

- ❖ Objective

- ❖ Introduce the concept of a safety lifecycle and the applicability and context in safety systems.

# Lifecycle Management

- ❖ A risk based management plan for a system or subsystem from conception to decommissioning.

(and recommissioning)

# ISA 84.01 Definition

# IEC 61508 Definition

## **Safety Lifecycle (IEC 61508)**

*necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.*

# IEC 61511 Definition

## **Safety Lifecycle (IEC 61511)**

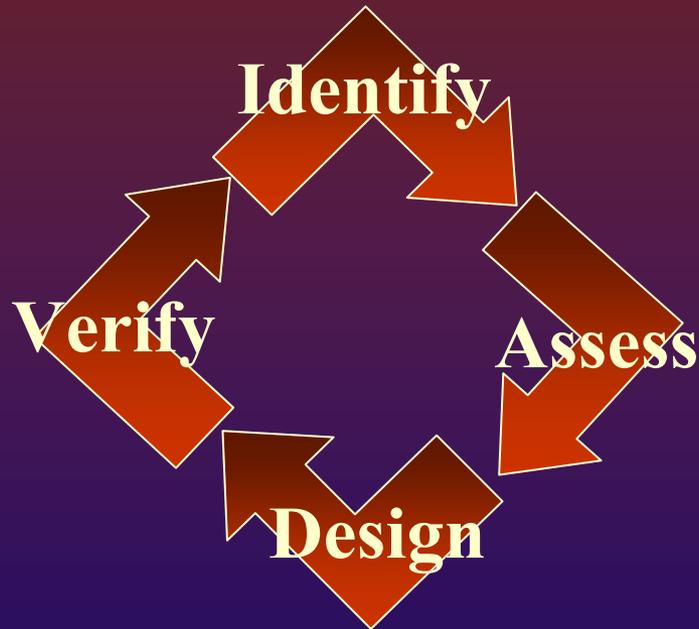
*necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use*

# MIL-STD-882d Definition

*‘Life cycle. All phases of the system's life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.’*

MIL-STD-882d

# Safety Lifecycle Approach



The safety lifecycle approach, as described in ISA 84.01, IEC 61511, and IEC 61508:

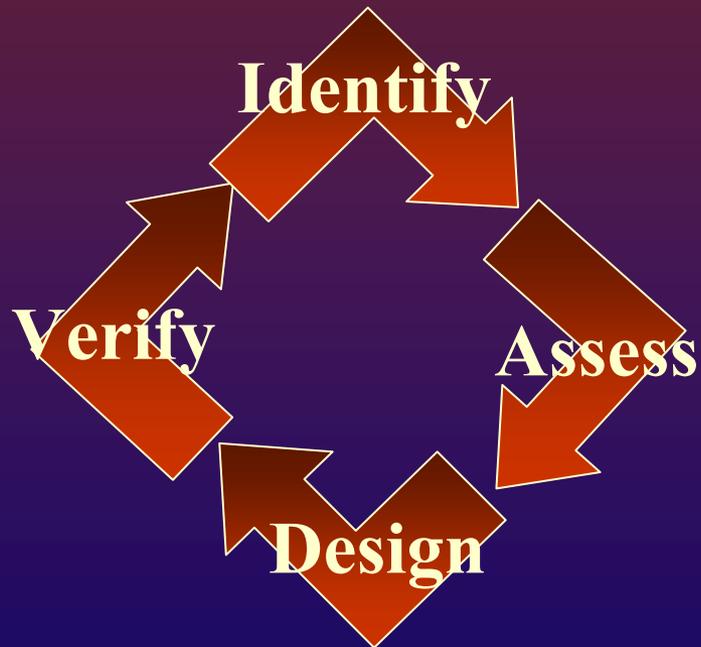
- ✓ utilizes common sense
- ✓ is a closed loop process
- ✓ Is continuous/has no end

# Quality Systems Approach



# ISO & IEC Comparison

IEC Model



ISO Model

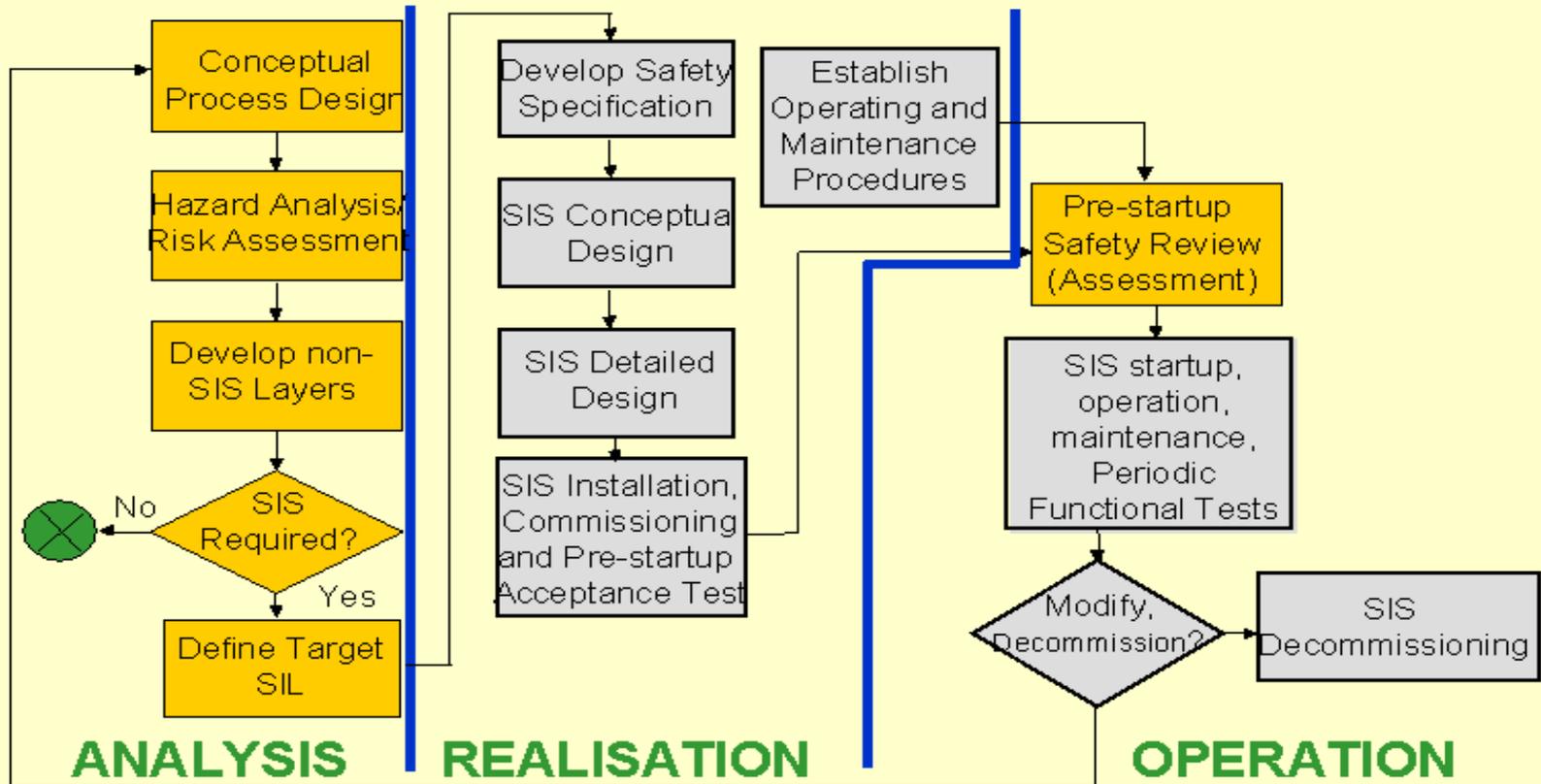


# Safety Lifecycle Model

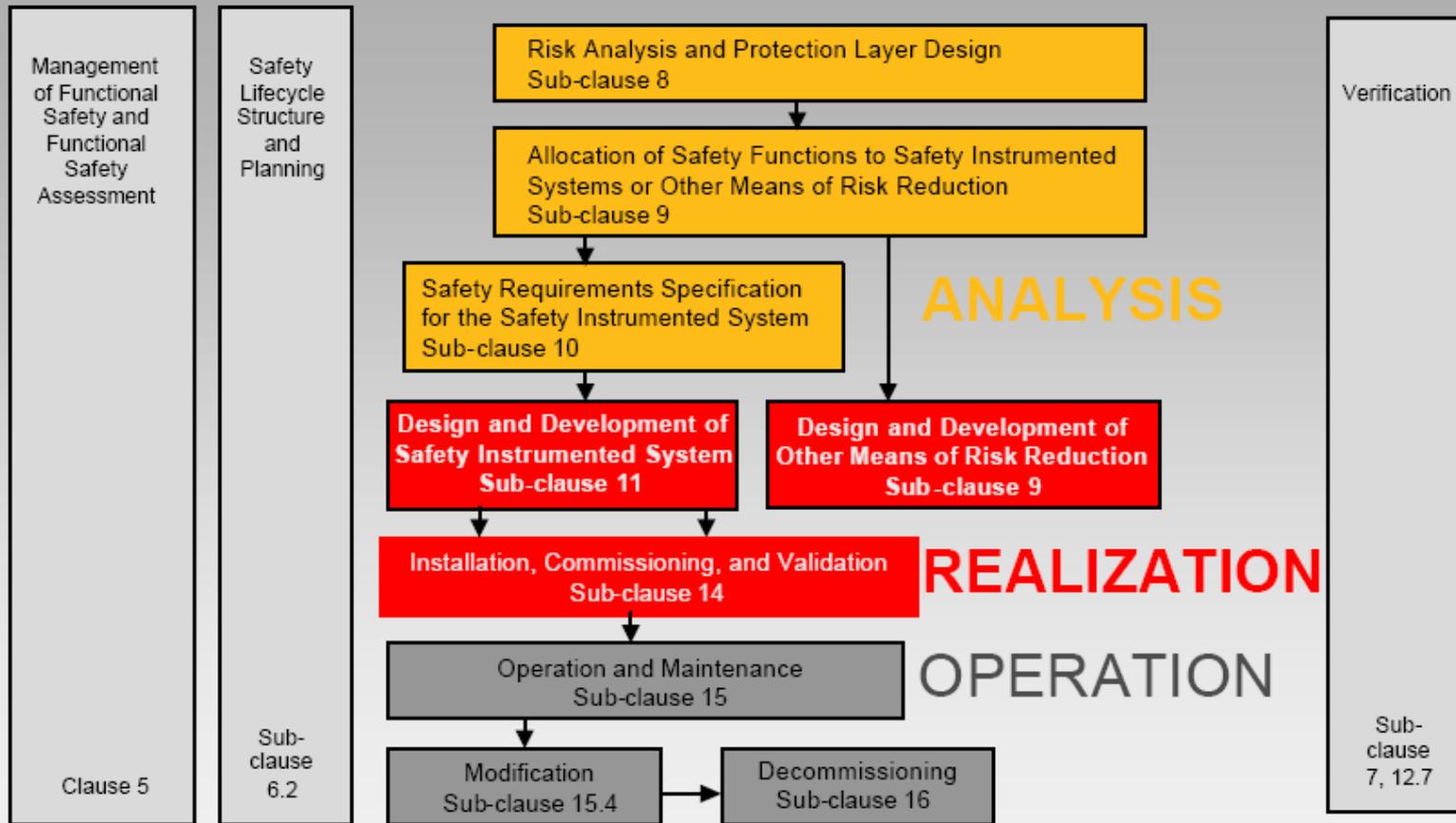
## ❖ Divided into three phases

- Analysis Phase - the problem is identified and assessed
- Realization Phase – the problem is solved and verified
- Operational Phase – the solution is put into use

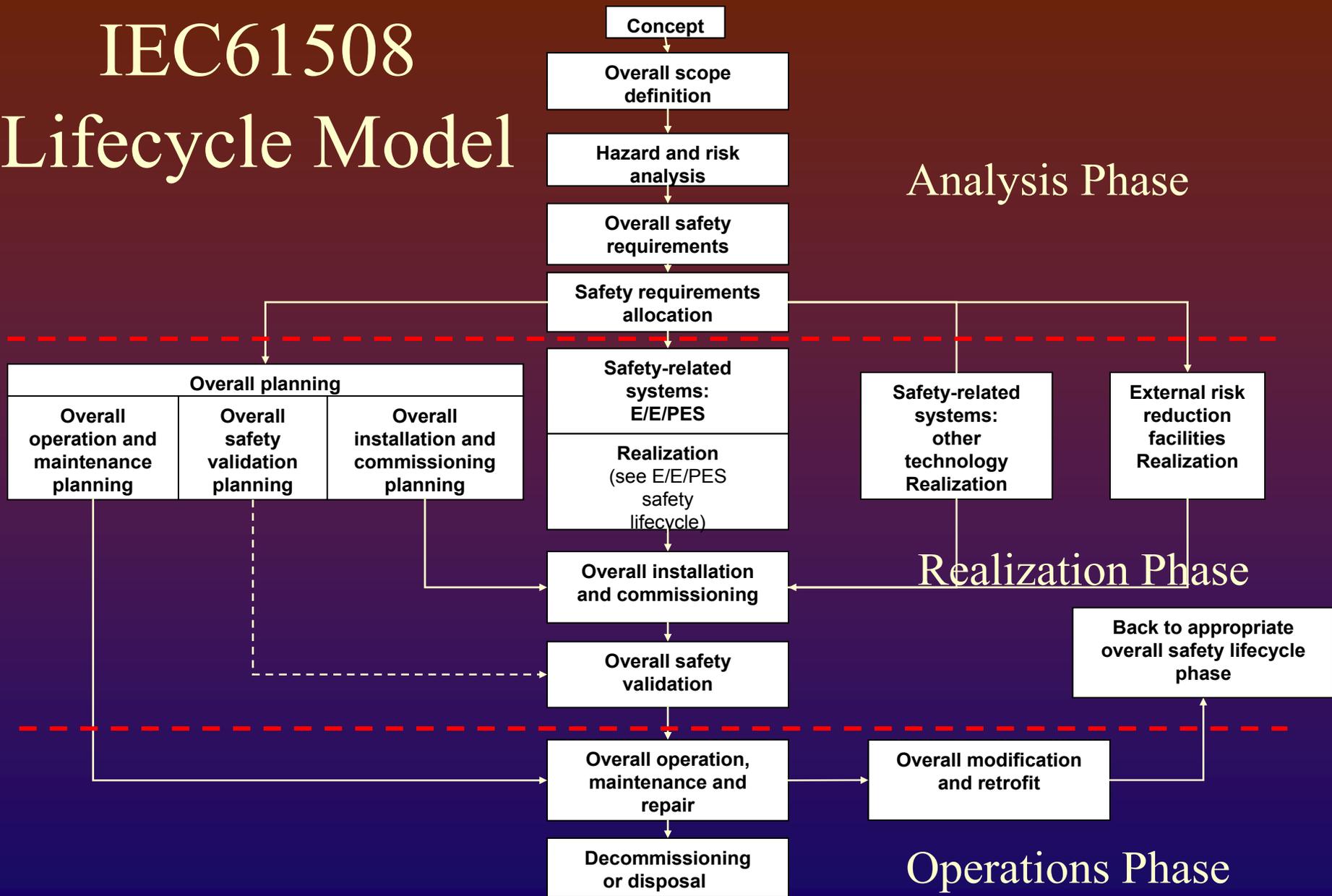
# ISA 84.01 Safety Lifecycle



# IEC 61511 Safety Life Cycle



# IEC61508 Lifecycle Model



# Analysis Phase

## ❖ Concept

- ❖ Develop an understanding of the equipment under control & its environment (physical & legal)
- ❖ Determine likely hazard sources
- ❖ Collect info on determined hazards (toxicity, explosion)
- ❖ Hazard interaction with other equipment

## ❖ Scope Definition

- ❖ Determine process/system boundaries
- ❖ Determine the scope of hazards

# Analysis Phase

## ❖ Scope Definition

- ❖ Determine the physical equipment to be included in hazard/risk analysis
- ❖ Determine the subsystems associated w/ the hazards
- ❖ Determine what external events will be included
- ❖ Determine types of accident-initiating events

# Analysis Phase (continued)

## ❖ Hazard & Risk Analysis

- Develop hazards list & events
  - Includes fault conditions & misuse
  - Abnormal & infrequent operation modes
- Determine event sequences
- Determine the likelihood & consequences for each event
- Evaluate the risk

# Analysis Phase (continued)

- ❖ Overall Safety Requirements
  - ❖ Specify necessary safety functions
    - ❖ Functions will not be defined in technology-specific terms
  - ❖ Determine necessary risk reduction
    - ❖ Qualitative or quantitative
  - ❖ Determine safety integrity requirement for each safety function
    - ❖ This is an interim stage toward determining SILs

# Analysis Phase (continued)

- ❖ Safety Requirements Allocation
  - ❖ Specify safety-related systems to be used
    - ❖ External risk reduction facilities
    - ❖ E/E/PE safety-related systems
    - ❖ Other technology safety-related systems
  - ❖ Allocate safety integrity level to each E/E/PE safety-related system
    - ❖ Done after taking into account risk reductions from external risk facilities and other technology safety-related systems
  - ❖ Ends with a Safety Requirements Specification document

# Realization Phase

- ❖ Technology & Architecture selections
- ❖ Determine test philosophy
- ❖ Perform reliability and safety evaluation to determine if you met your target SIL requirement
- ❖ Develop SIS conceptual design
- ❖ Prepare detailed design document (wiring diagrams; installation plans, etc.)
- ❖ Install system, commission, & perform acceptance testing

# Operations Phase

## ❖ Design Validation

- ✓ Does the system solve the problems identified during the hazard analysis?
- ✓ Have all necessary design steps been carried out successfully?
- ✓ Has the design met the target SIL for each safety instrumented function?
- ✓ Have the maintenance procedures been created and verified?
- ✓ Is there a management of change procedure in place?
- ✓ Are operators and maintenance personnel qualified and trained?

# Operations Phase

- ❖ Yes? - May proceed with operations
- ❖ Lifecycle continues with evaluations of system modifications and decommissioning activities
- ❖ Validation reviews the safety lifecycle activities and ensures that all steps were carried and documentation is in place

# Summary

- ❖ The safety lifecycle was created to
  - ❖ help safety instrumented system designers build safer systems
  - ❖ help create more cost effective systems
- ❖ Various lifecycle models exist but contain similar steps
- ❖ Documentation at every step is key to managing your system effectively

# Introduction to System Safety

Sandra L. Prior, REM, CHMM

System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

# System Safety History

- System safety (SS) movement began in 1940s
  - Amos L. Wood, 14<sup>th</sup> Annual Meeting of the Institute of Aeronautical Sciences in January 1946
- USAF an early leader
- Air Force-Industry partnership began as early as 1954
- Early 60s, small group of managers, scientists, & engineers implemented SS in aerospace program
- In 1962, the System Safety Society was organized; professional organization in 1972

# What is System Safety?

System safety is the practice of proactive hazard management. It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from conception to decommissioning.

# USAF System Safety Definition

## **Air Force System Safety Handbook:**

“The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle.”

# FAA System Safety Definition

## **FAA System Safety Handbook:**

“The application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity.”

# System Safety Principles

- Safety must be designed in.
- Inherent safety requires both engineering and management techniques to control the hazards.
- Safety requirements must be consistent with other program or design requirements.

# System Safety Goal

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures.

**Question- Where do you find the DOE system safety program defined?**

# DOE Safety Management System Policy 450.4

“The Department and Contractors must systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the workers, and the environment.”

# Step 1: Define Objectives

- Typically documented in
  - Business Plan
  - Operating Specifications
- In what DOE document(s) might you find this type of information?

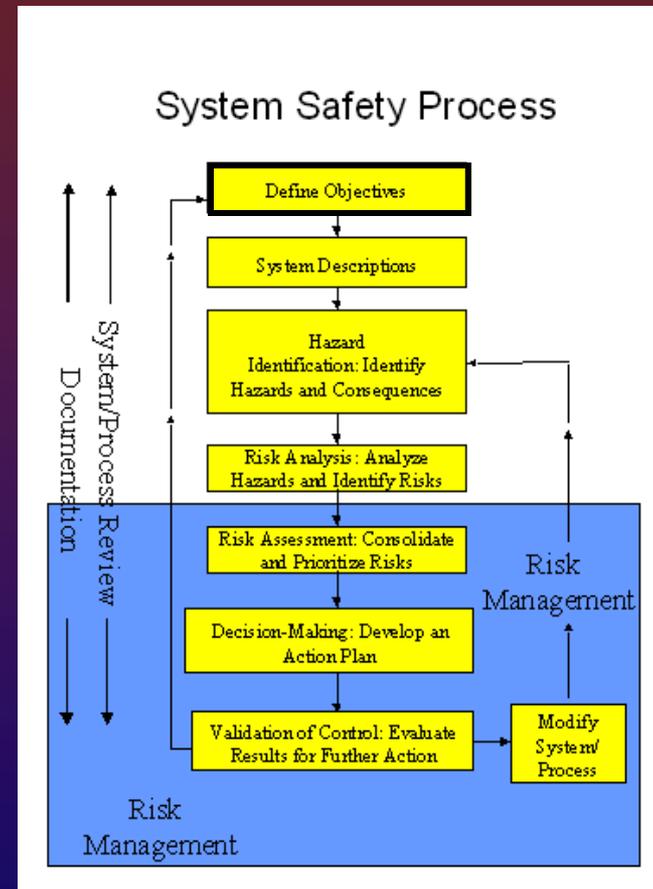


Diagram taken from FAA web site at  
<http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm>

“There are no "safety problems" in system planning or design. There are only engineering and/or management problems that, if left unresolved, may lead to accidents.”

FAA System Safety Handbook

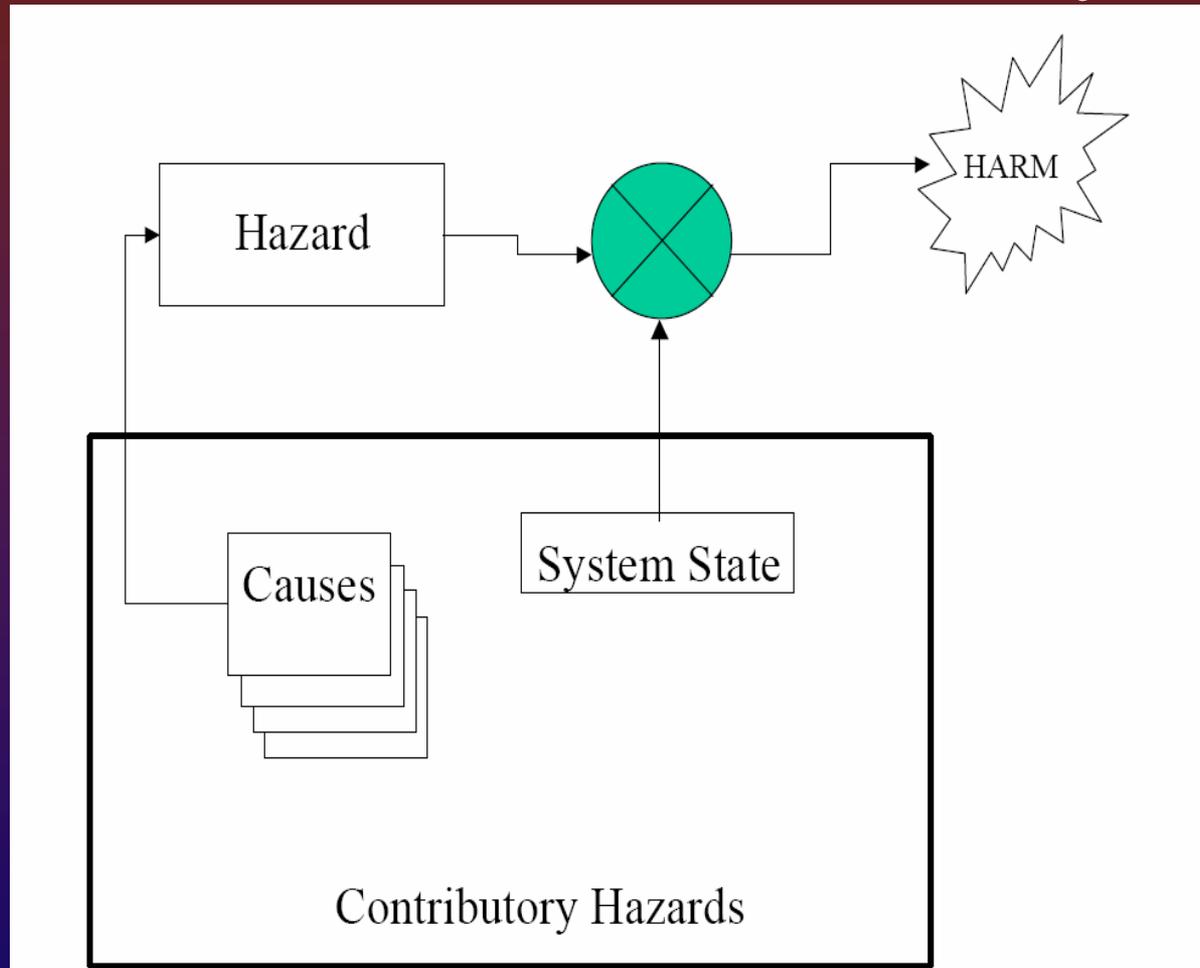


# System Description (continued)

- **The object of a good system definition is to:**
  - ✓ **set limits for the following steps in the process**
  - ✓ **reduce complex systems into manageable parts.**



# Hazard Analysis



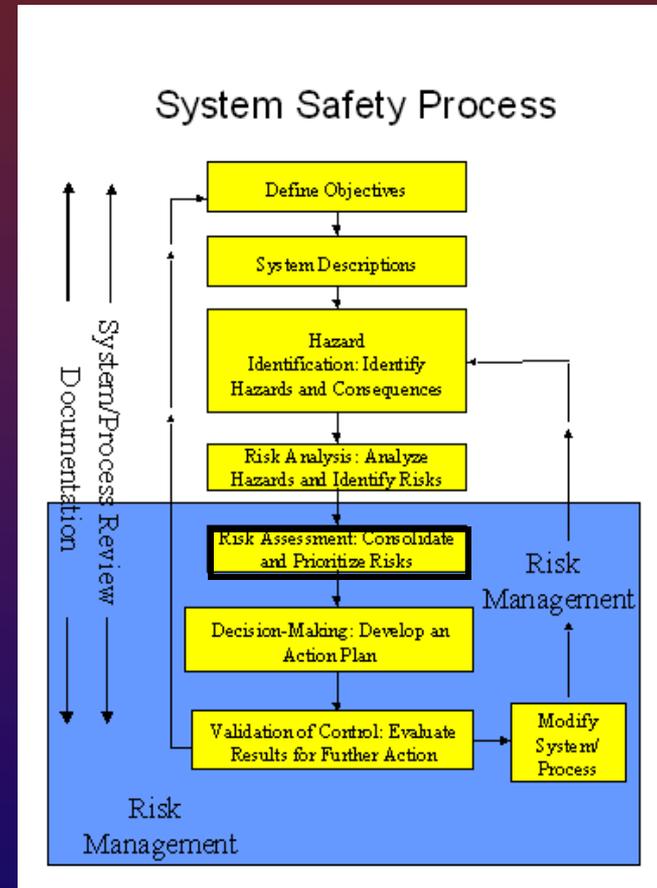
**Analysis should be:**

- ✓ **Comprehensive**
- ✓ **Methodical**
- ✓ **Disciplined**



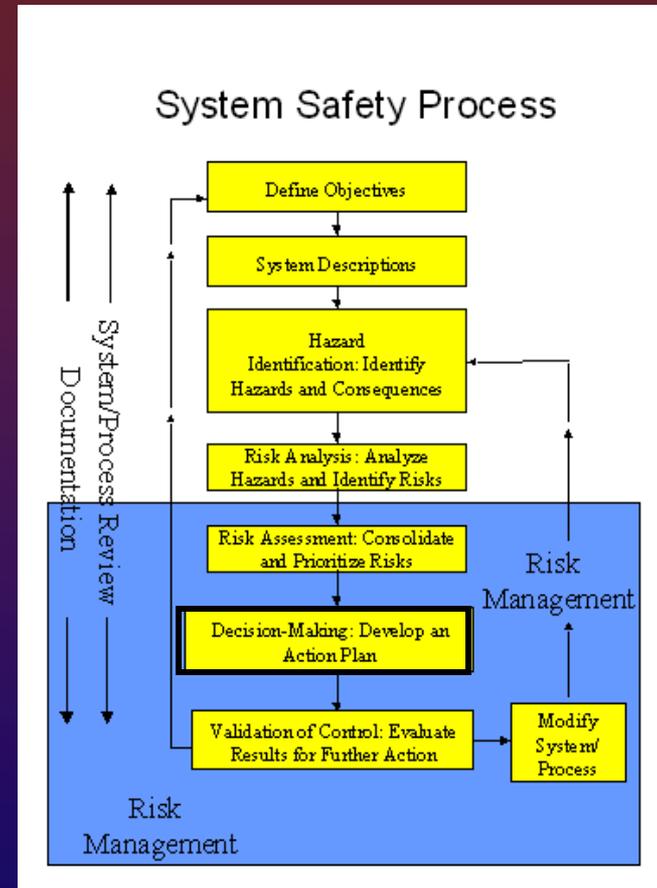
# Step 5: Risk Assessment

- Combine impacts of risk elements
- Compare impacts against acceptability criteria
- May consolidate risks into sets for joint mitigation and decision making



# Step 6: Decision Making

- Begins with
  - Management decision
  - Resources allocation
  - prioritized task list
- Most crucial step in process
- Decide how to address each risk
  - Safety Order of Precedence



# Safety Order of Precedence

- Design engineering approach:
  - Design for minimum risk
  - Design to reduce hazards
  - Incorporate safety devices
  - Provide warning devices
  - Develop procedures and training
- Alternative action plans
- Final result -written assessment document

# Effective Safety Risk Management Decisions

- Assign qualified, competent personnel
- Authority commensurate w/ responsibility
- Define, document, & track all known hazards as program policy
- Include safety risk assessment in program reviews
  - Risk acceptability
  - Risk responsibility
  - Decision milestones



# DOE Accelerator Readiness Review (ARR)

- Required by DOE Order 420.2A, para 4.d –  
“Accelerator Readiness Reviews. Accelerator Readiness Reviews (ARRs) must be performed prior to approval for commissioning and routine operation and as directed by the Cognizant Secretarial Officer/NNSA Deputy Administrator or a field element manager/NNSA field manager.”

# DOE Accelerator Readiness Review (ARR)

(FEL-ARR) Status - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://mis/fel/> Go Links »

Help - Search

Maintained by: [ingapps@llab.org](mailto:ingapps@llab.org)  
system ERD

[NEW! FEL Readiness Plan](#)

### Upgrade FEL Readiness Status

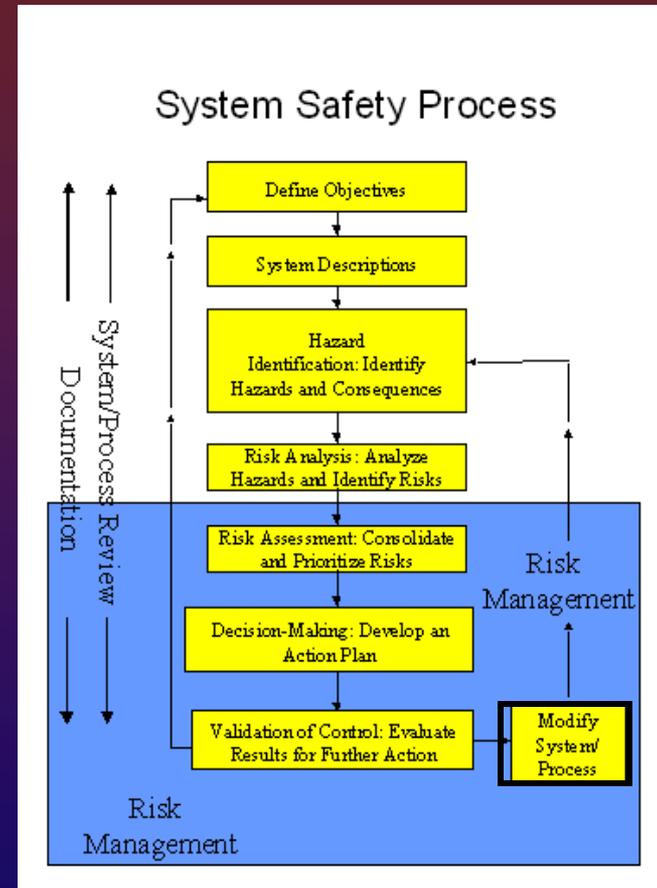
ARR Stage ▶ FEL Sub-System (Mgr) ▼	Major Design			Detail Specifications			Fabrication			Testing			Integrated			READY		
	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c
Project Mgmt (Dylla)	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c	n/a	b	c
Facility (Neil)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Beam Physics (Douglas)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Injector (Dylla)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
SRF (Preble)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
RF (Walker)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Cryogenics (Arenius)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Instrumentation (Jordan)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
e <sup>-</sup> Beam Transport (Biallas)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Wiggler (Benson)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Optics (Shinn)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Laser Safety (Benson)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
Personnel Safety (Mahoney)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
RadCon (May)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c

<b>System last updated:</b> 18-NOV-03 @ 09:29 AM	<b>Key:</b>	<b>Color Key:</b>	<b>Other Links:</b>
	a: equipment	Green: completed and ready	<a href="#">FEL Logbook</a>
	b: personnel	Blue: on schedule and no issues	<a href="#">BAIR Web Home</a>
	c: procedures	Yellow: behind schedule but no issues	<a href="#">FEL Project Mgmt Tools</a>
	n/a: not applicable	Red: unresolved issues or critical path work behind schedule	<a href="#">OPS-PR Query</a>

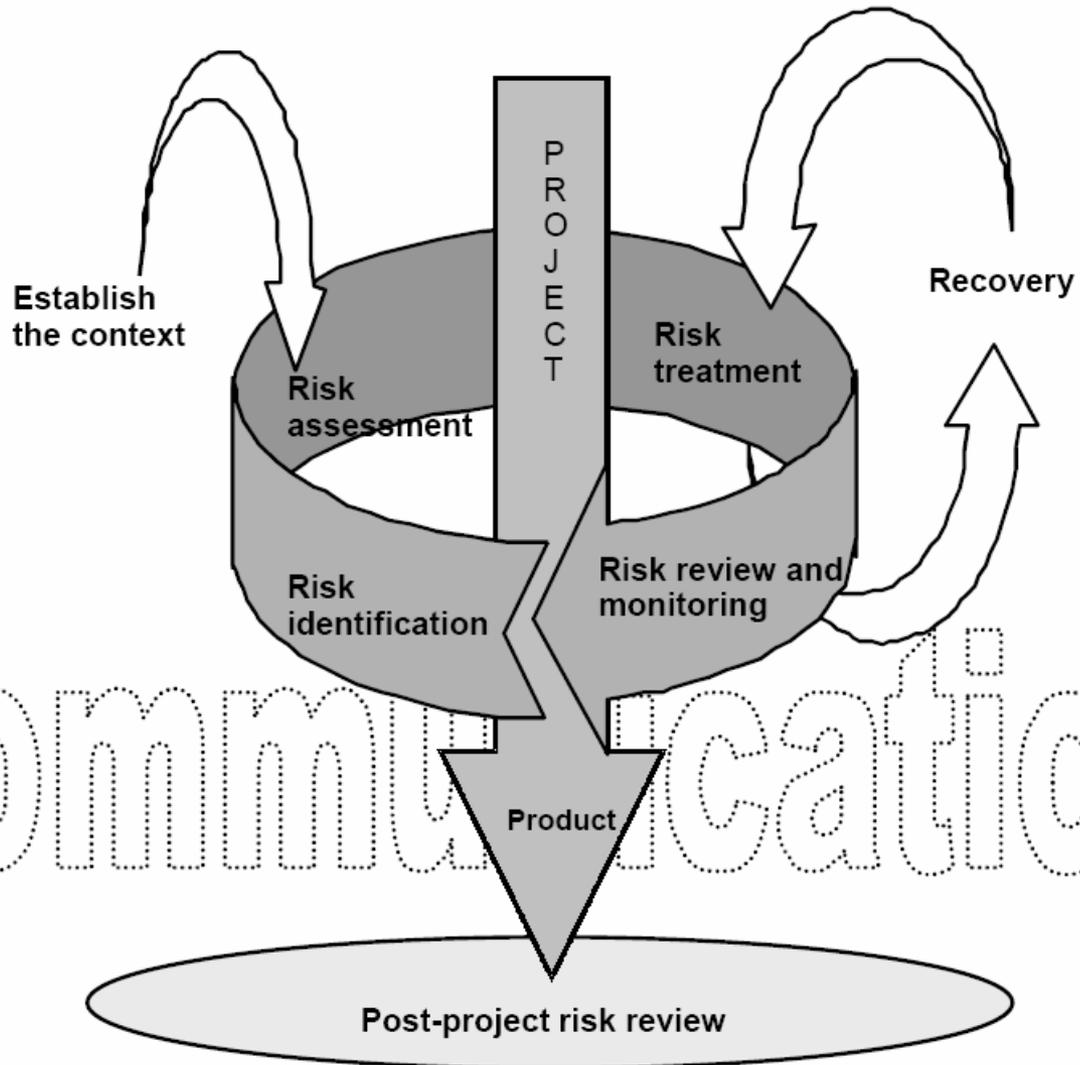
Logged in as: prior

# Step 8: Modify System/Process

- Modify if needed
- Why?
  - Risk status changes
  - Mitigation results are unacceptable
  - Addressed wrong hazard
  - System/process undergoes change
- Re-enter process at the hazard ID step



# Project Success



# Summary

- System Safety is a process that guides you into developing a context for your safety system design.
- The System Safety process requires you to document this context.
- Once your context has been established, you can then develop your safety system within that context.

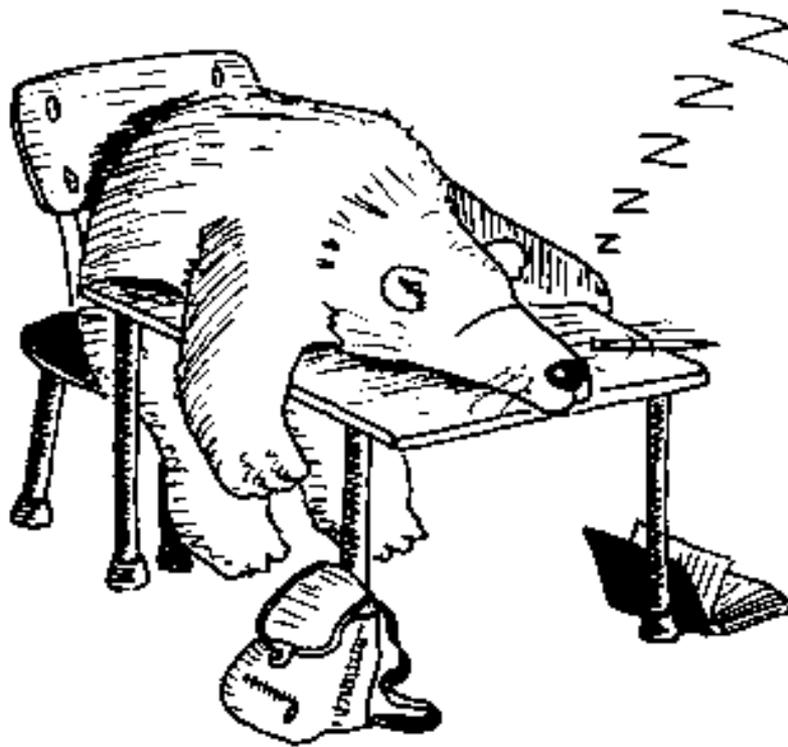


# Introduction to Safety Systems in Research Accelerators

Hazard Assessment and Risk  
Analysis

USPAS

June, 2004



Eventually Randolph was forced to leave University due to his tendency to hibernate through lectures.

© Uwe Oehler, Driguana@chembio.uoguelph.ca

# Most encountered words from senior management?

“I do not want any surprises”



Hazard and risk analysis are a means to that end...

# Hazard Analysis

- ❖ Hazard analysis uncovers and identifies hazards that exist in the workplace, generally focusing on a particular activity, project, or system.
- ❖ Basic information for risk based decisions
- ❖ Develop a means to:
  - ❖ Communicate
  - ❖ Track
  - ❖ Quantify
  - ❖ Allocate mitigation measures
  - ❖ Verify effectiveness
- ❖ Hazard analysis can also be referred to as *hazard recognition*, based upon the above definition.

# Anticipate

Hazard assessment of a proposed facility or system should occur before design criteria or other, less formal work-description documents are drafted, ideally even before initial concepts are finalized.

# Definitions

- ❖ Hazard – *a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).*
- ❖ Hazard Level – *the combination of severity and likelihood of occurrence*

# Definitions - continued

- ❖ Accident – *an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.*
- ❖ Mishap – *Department of Defense term for **accident** which is defined as an unwanted or uncontrolled release of energy or a toxic exposure.*
- ❖ Near miss/incident – *an event that involves no loss (or only minor loss) but with the potential for loss under different circumstances.*

# Definitions - continued

- ❖ *Safety – freedom from accidents or losses*
- ❖ *Reliability – the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time under stipulated environmental conditions.*
- ❖ *Error – a design flaw or deviation from a desired or intended state.*

# Definitions - continued

- ❖ Severity of occurrence – *the worst possible accident that could result from the hazard given the environment in its most unfavorable state.*
- ❖ Probability, or likelihood of occurrence – *may be specified either quantitatively or qualitatively.*
- ❖ Mishap probability – *is the probability that a mishap will occur during the planned life expectancy of the system. [MIL-STD-882D]*

# Definitions - continued

- ❖ Risk – *is the hazard level combined with (1) the likelihood of the hazard leading to an accident (sometimes called danger) and (2) hazard exposure or duration (sometimes called latency).*
  - ❖ Correct way to combine all elements of risk is unknown
  - ❖ Parameter values of each function are also unknown
  - ❖ No agreement on how to combine probability, severity and non-probabilistic factors
  - ❖ Comparison of catastrophic but unlikely events with likely but less serious events is unknown
  - ❖ Must involve qualitative judgment and personal values

# Definitions - continued

- ❖ Hazard Analysis – *the identification of hazards and the assessment of hazard level.*
- ❖ Risk Analysis – *includes hazard analysis plus the addition of identification and assessment of environmental conditions along with exposure or duration.*
  - ❖ Often used interchangeably with hazard analysis
  - ❖ Reliability often used incorrectly as a measure of risk

# The Risk Components

**RISK**

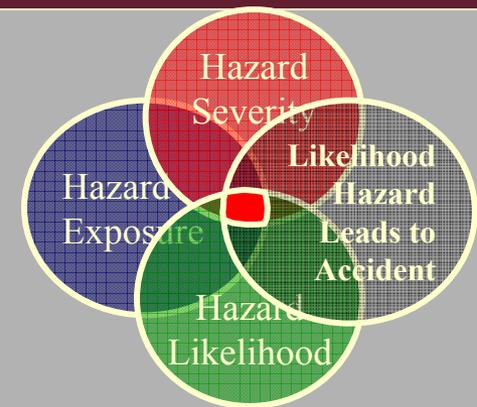
**Hazard Level**

Hazard  
severity

Likelihood of  
hazard occurring

Hazard  
exposure

Likelihood of  
hazard leading  
to an accident



# Factors Affecting Risk Components

- ❖ Introduction of new hazards
- ❖ Lessons learned that are passed down through codes and standards of practice for known hazards
- ❖ New engineering specializations and technologies for which codes & standards have not been developed.
- ❖ Older, simpler technologies are replaced w/ newer, more complex technologies.

# Factors Affecting Risk Components

- ❖ Redundancy may increase complexity
- ❖ Increasing complexity of hazards
- ❖ Exposure
- ❖ Energy
- ❖ Automation
- ❖ Centralization
- ❖ Scale
- ❖ Pace of technological change in the system

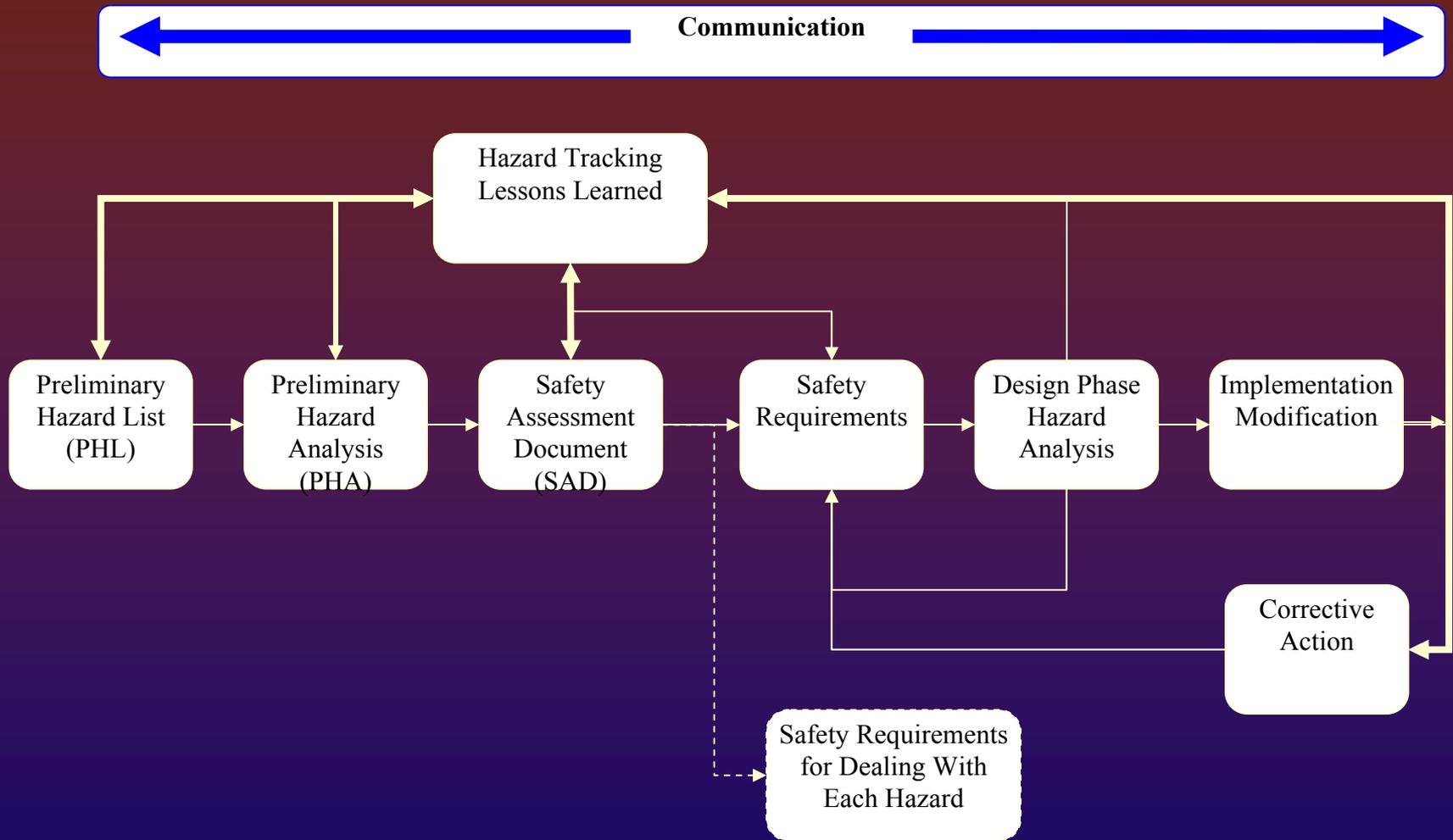
# Hazard Assessment: Identification

- ❖ Identify hazards and the possible accidents that might result from each hazard.
  - ❖ Process should be systematic
  - ❖ Entail detailed analysis of system hardware and software
  - ❖ Evaluate environment in which it will exist
  - ❖ Include intended use or application

# Hazard Identification Processes

- ❖ Preliminary Hazard Assessment (PHA)
- ❖ Preliminary Safety Assessment Review (PSAR)
- ❖ Preliminary Safety Assessment Document (PSAD)

# Hazard Management Lifecycle



# Hazard Identification Sources

- ❖ Sources of information
  - ❖ Historical hazard and mishap data
    - ❖ Accidents
    - ❖ Occurrence events
  - ❖ Lessons learned from other systems
  - ❖ Hazards that occur over the lifetime of the system
    - ❖ Mean time to failure of system components

# PHL Form

Hazard And Risk Analysis  
Revision A. June 2004

Page 1 of 3

Title:		ASIS PHL Example		Hazard Analysis Worksheet					<table border="1"> <tr> <td>To be completed during PHL</td> </tr> <tr> <td>To be completed during PHA</td> </tr> <tr> <td>To be completed during Final HA</td> </tr> </table>			To be completed during PHL	To be completed during PHA	To be completed during Final HA
To be completed during PHL														
To be completed during PHA														
To be completed during Final HA														
Date:		PHL4/20/04 PHA FHA												
Evaluator:		K. Mahoney												
Facility:		USPAS-A-TRON		Location: Univ. Wisc. Madison										
Purpose:		Preliminary Hazard Li		Risk Analysis					Risk Mitigation					
Reviewed/Comments	Hazard Tracking Number	Hazard Description	Hazard Type	Hazard Target	Exposure	Severity	Likelihood	Risk Code	Hazard Controls	Control Method	Control Risk Reduction			
<input type="checkbox"/>	1-1	Prompt ionizing radiation in beam enclosure due to source other than beam.	Radiological	Employee										
<input type="checkbox"/>	2-1	Exposed energized electrical bus on dipole magnets in beam enclosure.	Electrical	Employee										
<input type="checkbox"/>	3-1	Oxygen deficient environment due to helium leak	ODH	Employee										
<input type="checkbox"/>	4-1	Microwave radiation in excess of 5mW/cm2 due to open waveguide.	Electromagnet	Employee										
<input type="checkbox"/>	5-1	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Employee										
<input type="checkbox"/>	5-2	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Equipment										

PHL Approved: \_\_\_\_\_

Date: \_\_\_\_\_

# Hazard/Risk Assessment

- ❖ Having identified the hazards, one must assess the risks by considering the severity and likelihood of bad outcomes. If the risks are not sufficiently low, then additional controls or alternate methods must be applied.
- ❖ Risk increases if either likelihood or severity [*magnitude of loss*] increases provided the other component does not decrease proportionally.

# Tailoring Your Risk Definition

- ❖ No task is completely without risk.
- ❖ Must develop tailored risk matrix, based upon acceptable risk, in order to identify what is considered *sufficiently low*
- ❖ Must define “*acceptable risk*”

# Risk Class

- ❖ Example Risk Classification (IEC61508-5)

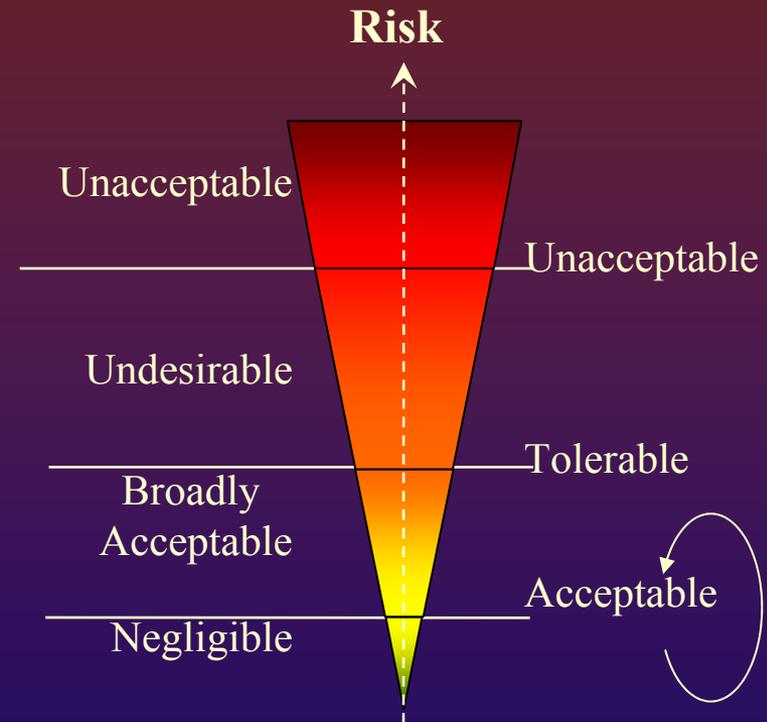
  - I Unacceptable

  - II Undesirable

  - III Action Recommended (ALARP)

  - IV Broadly Acceptable

- ❖ Classifications are developed inside the organization and approved by senior management



# Acceptable Risk

- ❖ What is it?
  - ❖ The threshold level below which risk will be tolerated
- ❖ To whom is the risk posed?
  - ❖ Generally the risk is posed to those who are not defining it
- ❖ By whom is it judged acceptable?
  - ❖ Senior management based upon input from technical experts

# Risk Assessment: Severity

- ❖ Evaluate the severity, or consequences, of each possible accident and rank order them by severity of the outcome.
  - ❖ Determine the potential negative impact of each hazard scenario on
    - ❖ Personnel
    - ❖ Equipment
    - ❖ Operations
    - ❖ Public
    - ❖ Environment
    - ❖ The system itself

# Risk Assessment: Likelihood

- ❖ Likelihood, or Probability, assignment
  - ❖ Qualitative
  - ❖ Quantitative
- ❖ Estimate the probability of each possible accident.
  - ❖ Past history of accidents/incidents
  - ❖ Industry benchmarks

# Likelihood/Probability Definition

- ❖ Can be defined in terms of occurrences per
  - ❖ Units of time
  - ❖ Events
  - ❖ Population
  - ❖ Items
  - ❖ Activity

# Risk Assessment Tools

- ❖ To determine what actions to take to eliminate or control a hazard, a system of determining the level of risk is needed.
- ❖ Risk tool should enable you to properly understand the level of risk involved relative to what it will cost in schedule and mitigation \$\$

# Risk Tool Development

- ❖ In early design stages, severity consideration is all that's needed since you should first try to eliminate the hazards by design
- ❖ When all hazards cannot be eliminated, probability factors become important
- ❖ General risk assessment tools are available however it's best if you use tools tailored to your individual program

# Simple Probability Functions

$$P(\text{Event})=P(\text{Hazard})*P(\text{Severity})*P(\text{Likelihood})*P(\text{Exposure})$$

# The Risk/Hazard Matrix (RHM)

- ❖ Allows you to assign a risk value to each hazard scenario
- ❖ Can rank order hazard scenarios
- ❖ Identify potential mitigation alternatives
- ❖ Evaluate alternatives in terms of risk reduction (use your matrix)
- ❖ Prioritize mitigation tasks

# Risk Matrix

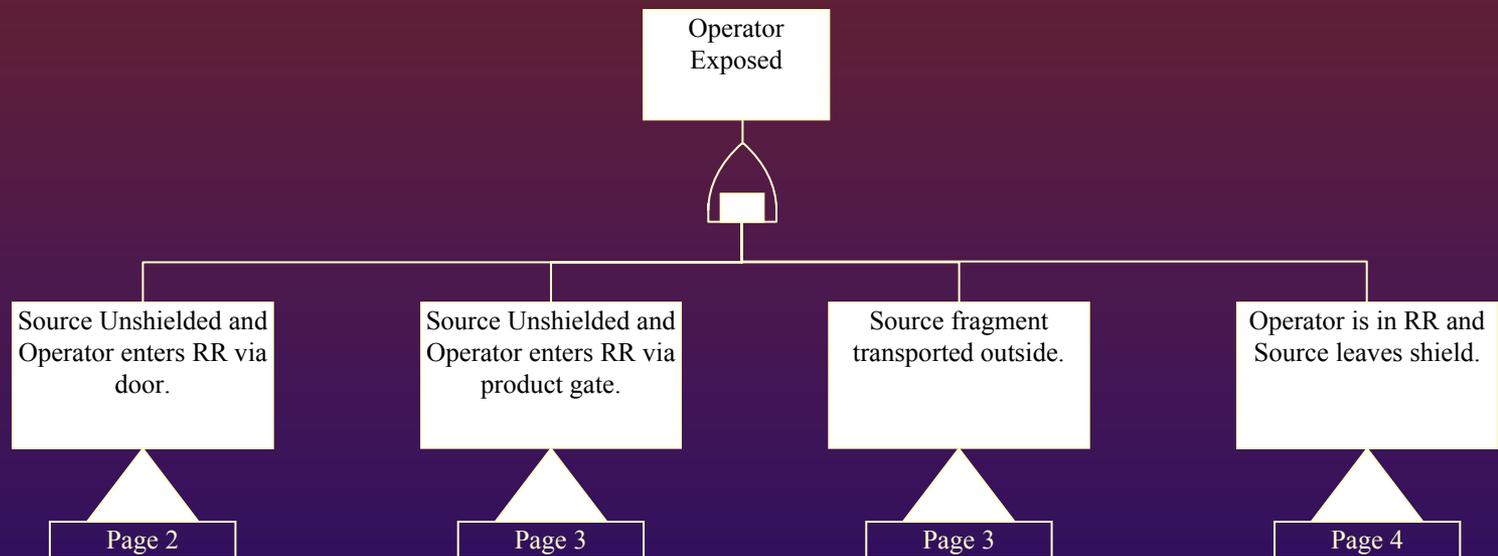
<b>Frequent</b>	I	I	I	II
<b>Probable</b>	I	I	II	III
<b>Occasional</b>	I	II	III	III
<b>Remote</b>	II	III	III	IV
<b>Improbable</b>	III	III	IV	IV
<b>Incredible</b>	IV	IV	IV	IV
<b>Frequency</b>	<b>Catastrophic</b>	<b>Critical</b>	<b>Marginal</b>	<b>Negligible</b>
	<b>Consequence</b>			

	A	B	C	D	E	F	G
1	Today's Date	6/29/2004					
2							
3	Project	USPAS					
4	Evaluator	K. Mahoney					
5	Date	6/22/2004					
6	Hazard	Shock from Energized Magnets					
7	Constraint 1	50-250VDC					
8	Constraint 2	<5mA					
9							
10	Likelihood						
11	Consequence						
12							
13							User Defined Ra
14	<b>Risk Matrix</b>		<b>Color code</b>	<b>Intolerable</b>		0	4
15				<b>Undesirable</b>		4	5
16				<b>Tolerable</b>		5	7
17				<b>Acceptable</b>		7	>
18	User Defined Likelihood						
19	Immanent	<b>0 Frequent</b>		3	2	1	0
20	1day-1year	<b>1 Probable</b>		4	3	2	1
21	1-10 years	<b>2 Occasional</b>		5	4	3	2
22	Over life of facility	<b>3 Remote</b>		6	5	4	3
23	100-1000 years	<b>4 Unlikely</b>		7	6	5	4
24	>1000 years	<b>5 Impossible</b>		8	7	6	5
25				<b>3</b>	<b>2</b>	<b>1</b>	<b>0</b>
26			<b>Consequences</b>	<b>Minimal</b>	<b>Marginal</b>	<b>Critical</b>	<b>Catastrophic</b>
27				<b>First Aid</b>	<b>&lt; 5 Lost Work Days</b>	<b>&gt; 5 lost work days</b>	<b>Death or Disability</b>

# Fault Tree Analysis (FTA)

- ❖ Widely used in aerospace, electronics and nuclear industries
- ❖ Primarily a means for analyzing causes of hazards, not identifying hazards
- ❖ Top-down search method, with the top event having been foreseen
- ❖ Four basic steps: (1) system definition; (2) fault tree construction; (3) qualitative analysis; and (4) quantitative analysis

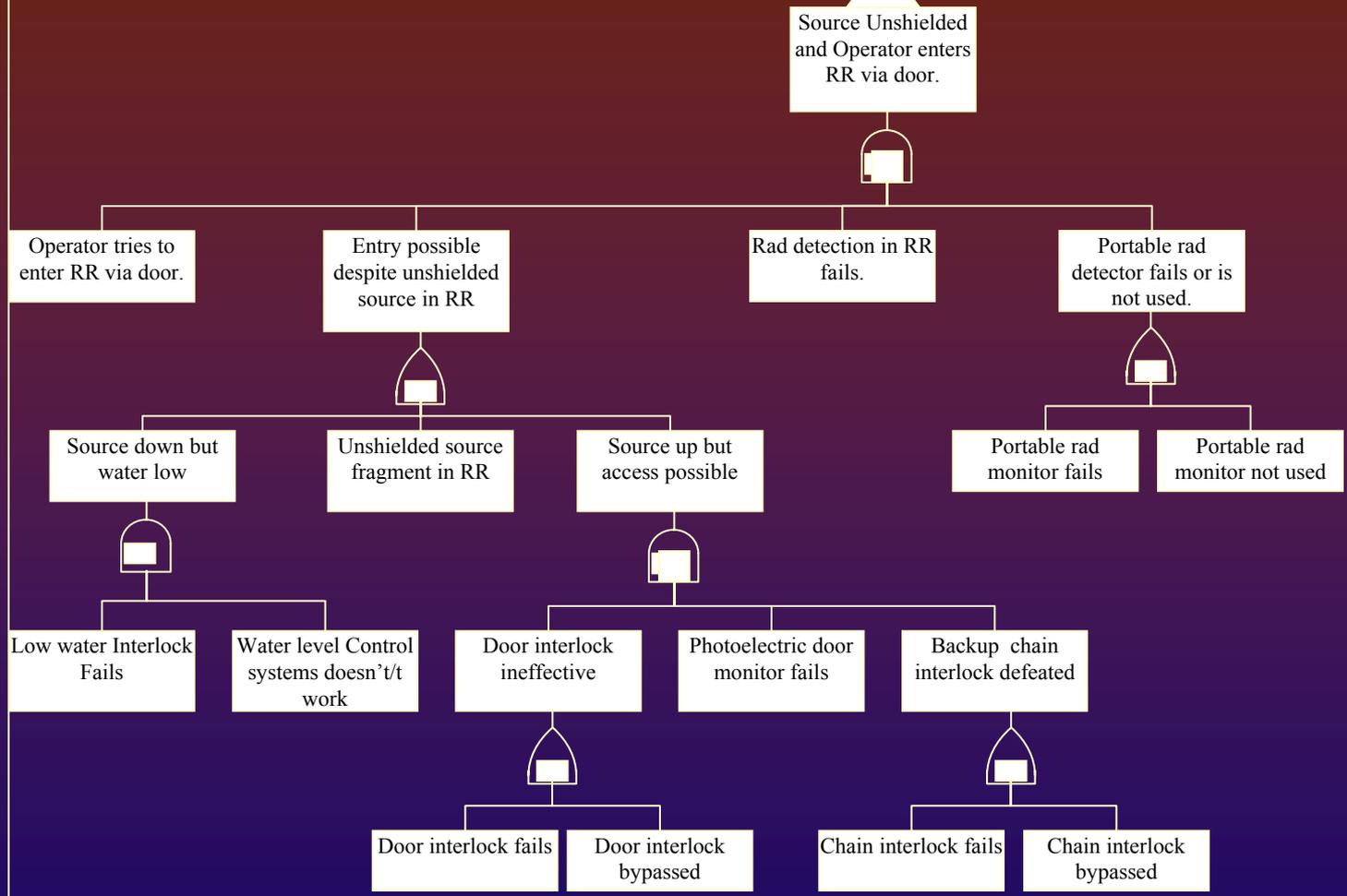
# Qualitative Fault Tree



# Qualitative Fault Tree

PAGE 2

Page 1

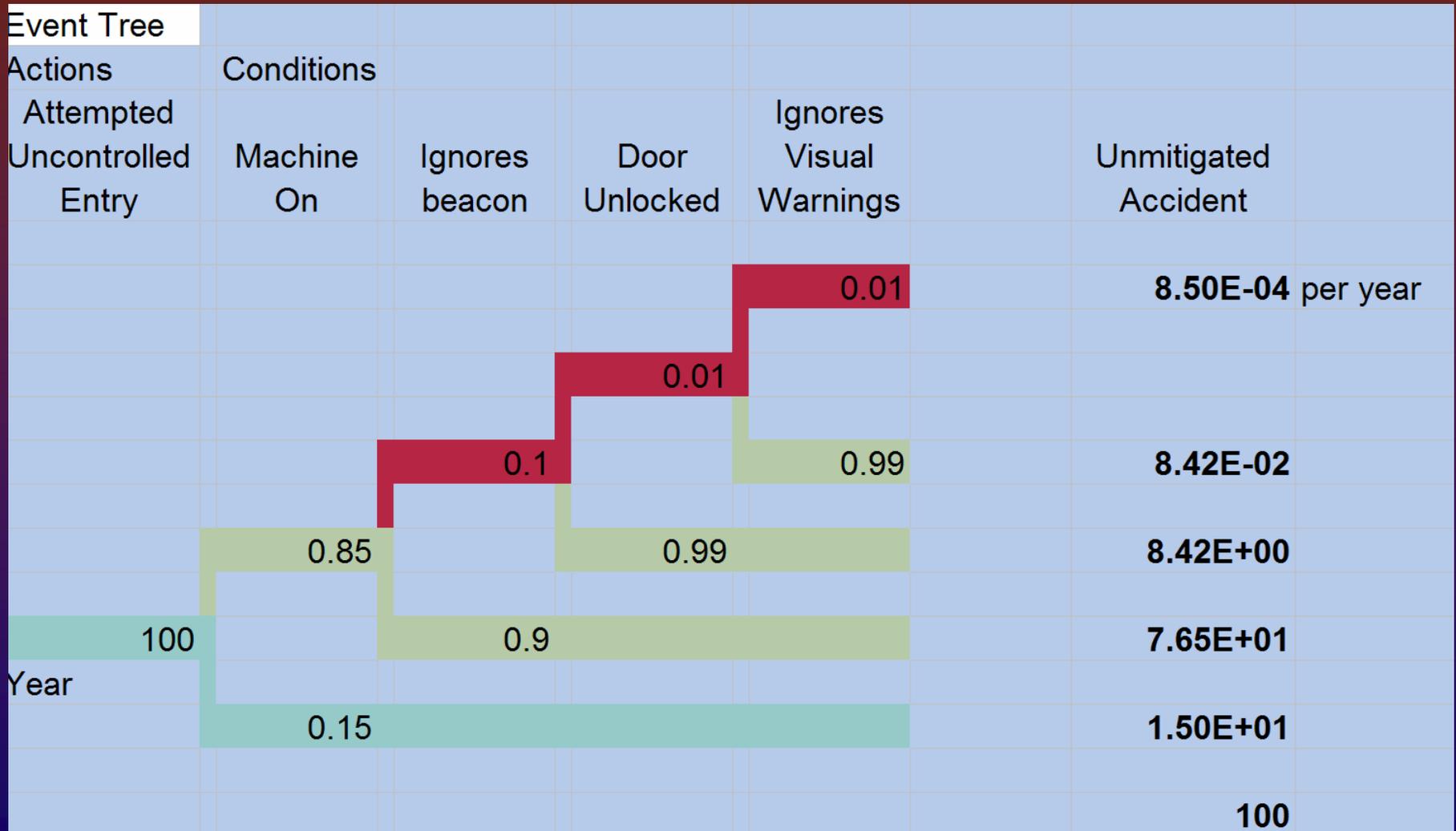


From ICRP Publication 76 pp34

# Event Tree Analysis (ETA)

- ❖ An adaptation of general decision tree whereby a problem is broken up into smaller parts to which the FTA is then applied.
- ❖ Uses forward search to identify possible outcomes of an event
- ❖ Principally used in nuclear power plants
- ❖ Drawn from left to right
- ❖ Based upon a binary state system [success or failure]
- ❖ Tend to be quite large

# Example Event Tree



# Failure Modes & Effects Analysis (FMEA)

- ❖ Form of reliability analysis
- ❖ Emphasizes successful functioning rather than hazards & risk
- ❖ Uses forward search based upon chain-of-events model
- ❖ All significant failure modes must be known in advance
- ❖ Doesn't consider effects of multiple failures (except for subsequent effects it might produce)

# Failure Modes & Effects Analysis (FMEA)

- ❖ Analyzes single failure modes
  - ❖ Determines effects on all other system components and on overall system
  - ❖ Probabilities and seriousness of each failure mode's results are calculated
  - ❖ Critical effects are added to get failure probability for entire system
- ❖ Failures rates predicted from generic rates developed from experience over time

# Failure Modes & Effects Analysis (FMEA) - Uses

- ❖ Identify redundancy and fail-safe design requirements
- ❖ Single-point failure modes
- ❖ Inspection points
- ❖ Spare parts requirements
- ❖ Strength of technique is completeness but it is also time consuming

# Hazard & Operability Analysis (HAZOP)

- ❖ Primarily used by the chemical industry
- ❖ Focuses on safety & efficient operations
- ❖ Assumes accidents are caused by deviations from design or operating intent
- ❖ Systematic, qualitative technique
- ❖ Able to identify “unreviewed” safety issues
- ❖ It is labor-intensive

# Layer of Protection Analysis (LOPA)

- ❖ Used to more realistically assign risk reduction factors to non-safety system functions
  - ❖ Operator Response
  - ❖ Dedicated Control System safety functions

# Hazards Control Precedence

- ❖ The accepted precedence for dealing with hazards is:
  - Eliminate the hazard (the most effective method but oftentimes incompatible with the mission objective)
  - Reduce the hazard in a manner that prevents or minimizes conditions that could lead to unacceptable risk

# Hazard Elimination

- ❖ Eliminate hazards through design selection
  - ❖ Process change
  - ❖ Material substitution
- ❖ Reduce hazards by using
  - ❖ safety features or devices
  - ❖ detection and warning systems
  - ❖ procedures and training (may involve use of personal protective equipment)

# Classes of Hazard Controls

- ❖ Engineering - methods of controlling employee exposures by modifying the source or inherent design of the process or work configuration
- ❖ Administrative – Procedural controls which depend upon employee awareness and compliance for their effectiveness
- ❖ Personal Protective Equipment (least preferred)

# Two Types of Controls

- ❖ Active Controls - require some action to prevent or mitigate the hazard.
  - ❖ Safety interlock system
  - ❖ Access control system
- ❖ Passive Controls - relies on basic physical principles to prevent/minimize a hazard's effects
  - ❖ Shielding
  - ❖ Labyrinths
  - ❖ Barriers – locked doors & enclosed fencing
  - ❖ Distance

# Hazard Controls Verification

- ❖ Verify effectiveness of controls through
  - ✓ Analysis – design reviews, computer modeling
  - ✓ Testing – commissioning activities, system certification/functional testing, readiness reviews
  - ✓ Inspection
- ❖ Look for new hazards during testing that may have been overlooked

# Residual Risk

- ❖ The risk that remains after all planned risk management measures have been implemented:
  - ❖ Must be documented along with reasons why it exists
  - ❖ Must be reviewed and accepted by management
  - ❖ Management review must be documented
  - ❖ Generally managed by administrative controls

# Documentation

- ❖ Records of hazard reviews should be incorporated into the overall project design documentation.
  - ❖ It preserves your methods and rationale so that you are able to undertake a comparable review more efficiently in the future.
  - ❖ It provides a defensible basis for your system during a permitting or agency review.
  - ❖ It augments the customary discipline found in good engineering and architectural design practices.

# Tracking Systems

- ❖ System performance over its life cycle
  - ❖ System failures and corrective actions
  - ❖ Maintenance and certification tests
  - ❖ Inspection findings
  - ❖ Change control
    - ❖ Modifications
    - ❖ Upgrades
    - ❖ System “add-ons”

# Communicate!

- ❖ Managers
- ❖ System managers
- ❖ System integrators
- ❖ System support staff
- ❖ System operators
- ❖ EH&S staff
- ❖ Affected workers



# Introduction to Safety Systems in Research Accelerators

SIL Selection

USPAS

June, 2004

# Outline

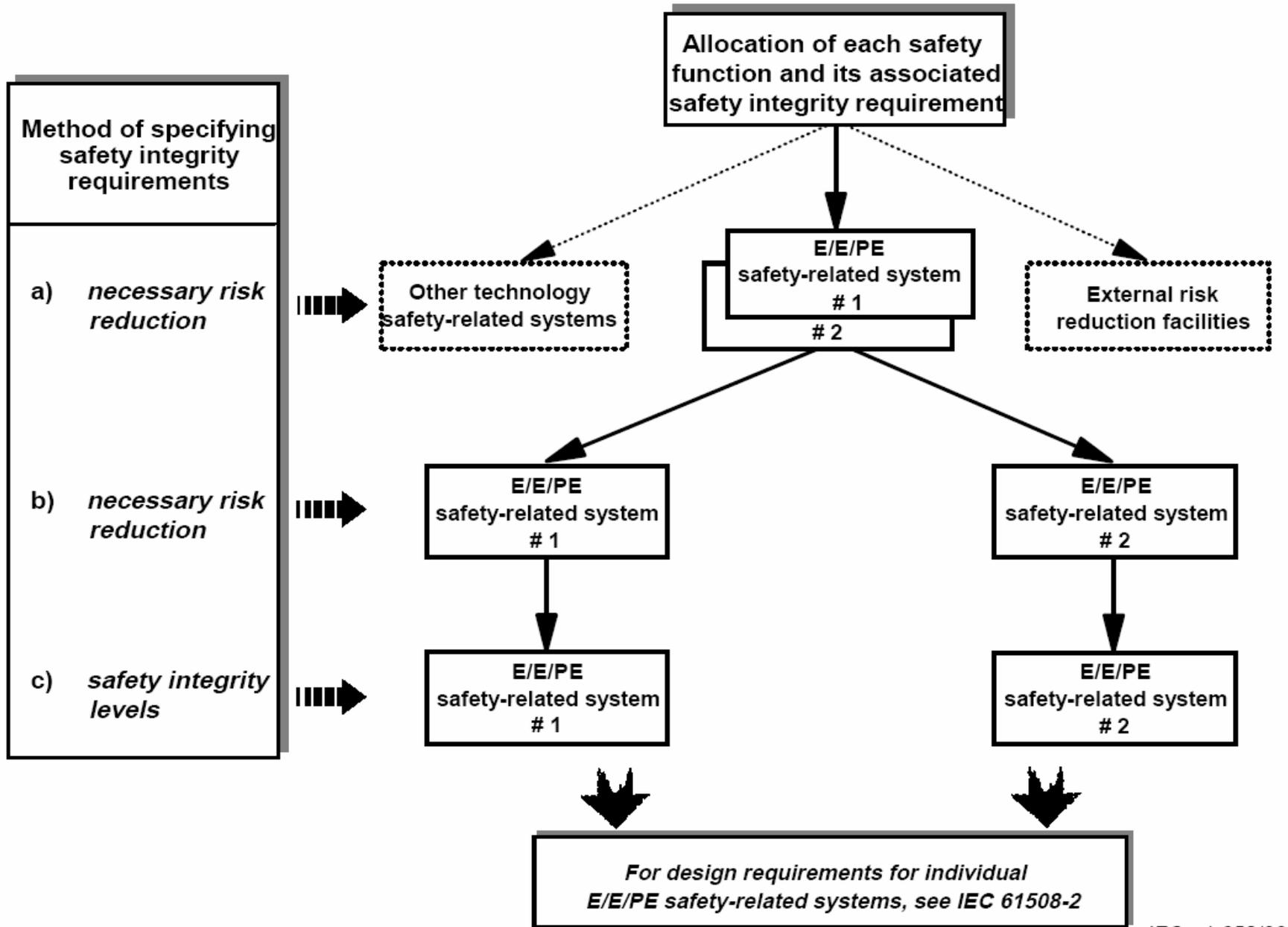
- ❖ **Review of SIL Allocation**
- ❖ **SIL Selection Tools**

# Review of SIL Allocation

- ❖ Allocation of safety functions to specific protection layers for the purpose of prevention, control or mitigation of hazards from the accelerator and its associated equipment;
- ❖ The allocation of risk reduction targets to safety instrumented functions.

# Guide Lines for Determining Necessary Risk Reduction

- ❖ Guidelines from the appropriate safety regulatory authority;
- ❖ Discussions and agreements with the different parties involved in the application;
- ❖ Industry standards and guidelines;
- ❖ International discussions and agreements; the role of national and international standards are becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- ❖ The best independent industrial, expert and scientific advice from advisory bodies;
- ❖ Legal requirements, both general and those directly relevant to the specific application.





# SIL Ranges

## DEMAND MODE OF OPERATION

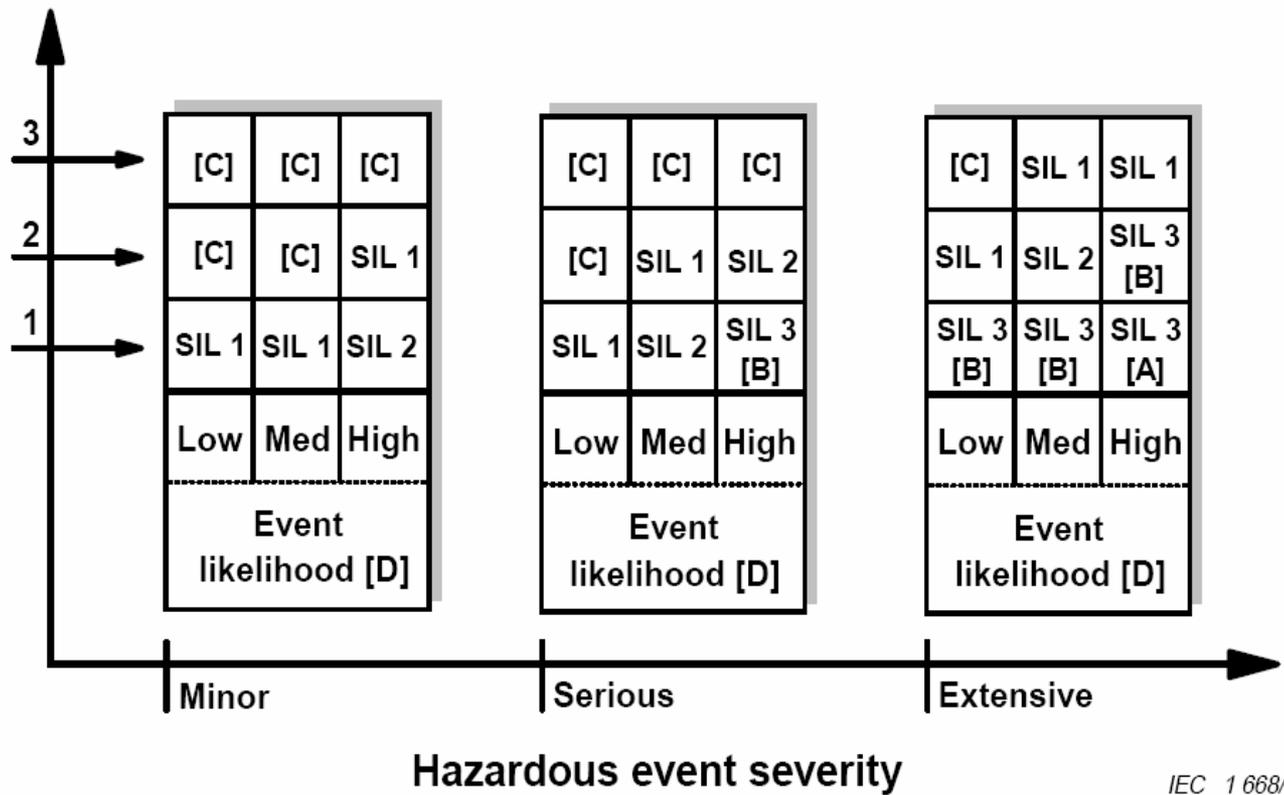
Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10,000$ to $\leq 100,000$
3	$\geq 10^{-4}$ to $<10^{-3}$	$>1000$ to $\leq 10,000$
2	$\geq 10^{-3}$ to $<10^{-2}$	$>100$ to $\leq 1000$
1	$\geq 10^{-2}$ to $<10^{-1}$	$>10$ to $\leq 100$

## CONTINUOUS MODE OF OPERATION

Safety Integrity Level (SIL)	Frequency of Dangerous Failures Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

# Risk Matrix Approach

Number of independant SRSs and external risk reduction facilities [E]  
 (including the E/E/PE SRS being classified)



IEC 1 668/98

# Risk Matrix

- Risk matrix set up for hazard type

External Risk Reduction	0					
Other Technology Based Systems	0					
SIL	0					
Risk Matrix	Color code	Intolerable		0	4	User Defined Range
		Undesirable		4	5	
		Tolerable		5	7	
		Acceptable		7	>	
User Defined Likelihood						
Immanent	0 Frequent	3	2	1	0	
1day-1year	1 Probable	4	3	2	1	
1-10 years	2 Occasional	5	4	3	2	
Over life of facility	3 Remote	6	5	4	3	
100-1000 years	4 Unlikely	7	6	5	4	
>1000 years	5 Impossible	8	7	6	5	
		3	2	1	0	
	Consequences	Minimal	Marginal	Critical	Catastrophic	
		First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

# Risk Matrix

- External Risk Reduction and Other Methods Evaluated

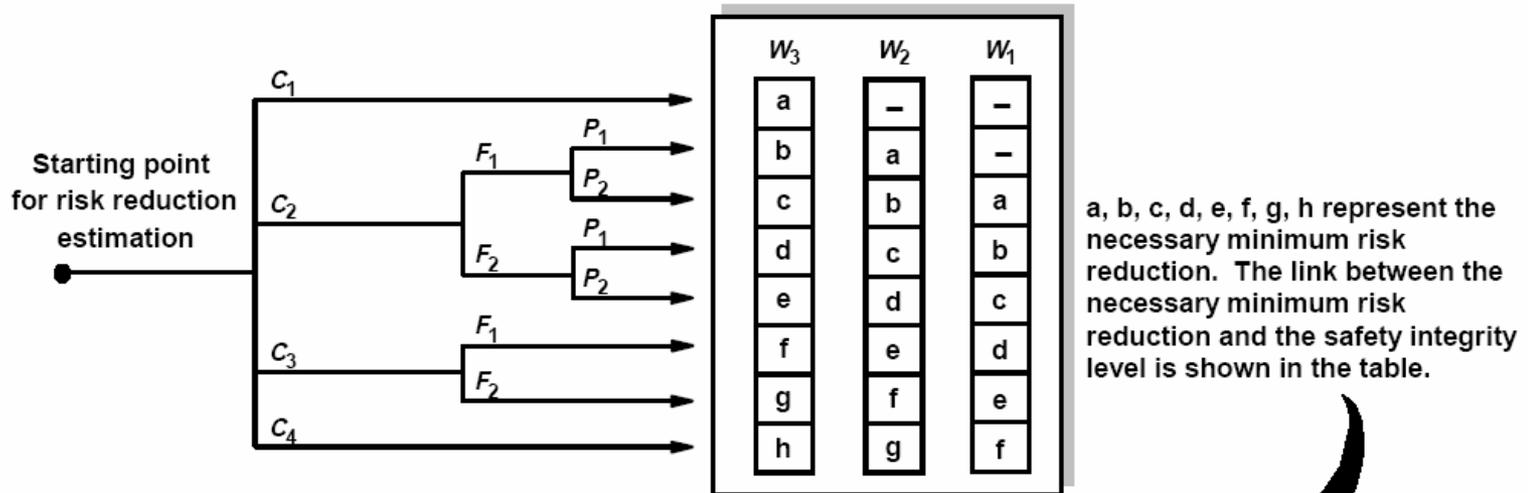
External Risk Reduction	2					
Other Technology Based Systems	1					
SIL	0					
Risk Matrix	Color code	Intolerable		0	4	User Defined Range
		Undesirable		4	5	
		Tolerable		5	7	
		Acceptable		7	>	
User Defined Likelihood						
Immanent	0 Frequent	6	5	4	3	
1day-1year	1 Probable	7	6	5	4	
1-10 years	2 Occasional	8	7	6	5	
Over life of facility	3 Remote	9	8	7	6	
100-1000 years	4 Unlikely	10	9	8	7	
>1000 years	5 Impossible	11	10	9	8	
		3	2	1	0	
	Consequences	Minimal	Marginal	Critical	Catastrophic	
		First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

# Risk Matrix

- ❖ Effect of SIL Levels Evaluated

External Risk Reduction	2					
Other Technology Based Systems	1					
SIL	3					
Risk Matrix	Color code	Intolerable		0	4	User Defined Range
		Undesirable		4	5	
		Tolerable		5	7	
		Acceptable		7	>	
User Defined Likelihood						
Immanent	0 Frequent	9	8	7	6	
1day-1year	1 Probable	10	9	8	7	
1-10 years	2 Occasional	11	10	9	8	
Over life of facility	3 Remote	12	11	10	9	
100-1000 years	4 Unlikely	13	12	11	10	
>1000 years	5 Impossible	14	13	12	11	
		3	2	1	0	
	Consequences	Minimal	Marginal	Critical	Catastrophic	
		First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

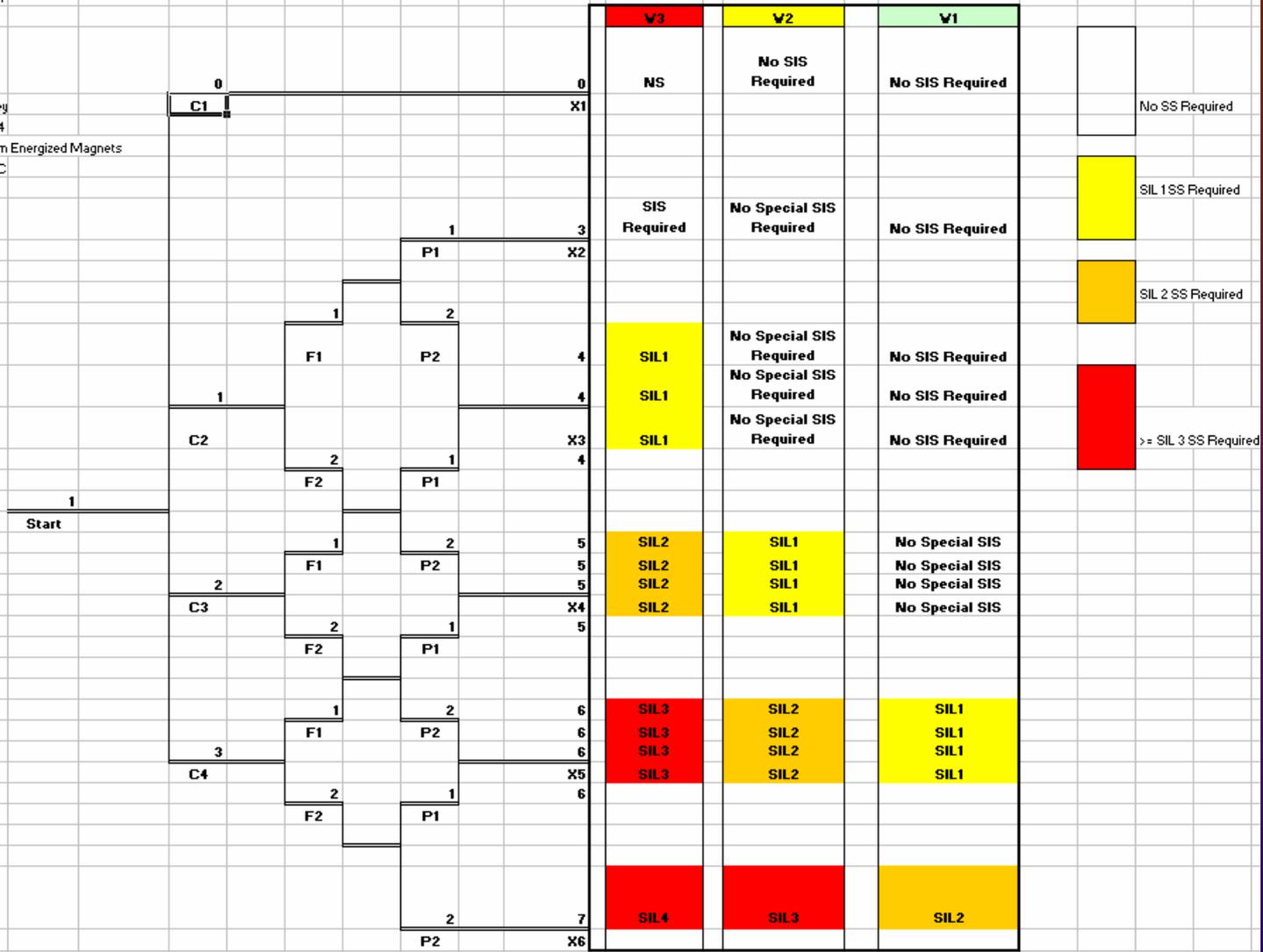
# Risk Graph



**C** = Consequence risk parameter  
**F** = Frequency and exposure time risk parameter  
**P** = Possibility of avoiding hazard risk parameter  
**W** = Probability of the unwanted occurrence  
**a, b, c ... h** = Estimates of the required risk reduction for the SRS

Necessary minimum risk reduction	Safety integrity level
-	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

Project USPAS  
 Evaluato K. Mahoney  
 Date 6/22/2004  
 Hazard Shock from Energized Magnets  
 Constrail 50-250VDC  
 Constrail <5mA



Consequence	
C1	Minor Injury 1
C2	Serious Injury 2
C3	Death 3
C4	Multiple Deaths 4

Frequency and Exposure Time	
F1	Rare to Frequent 1
F2	Frequent to Continuous 2

Possibility of Avoidance	
P1	Avoidance Possible 1
P2	Avoidance not likely, almost impossible 2

Probability of outcome	
V1	Very Slight probability 1
V2	Slight Probability, few occurrences 2
V3	High Probability 3

# Quantitative

- ❖ Calculate Initial Risk using risk analysis tools
- ❖ Calculate the residual risk using
  - ❖ Event Tree
  - ❖ LOPA
- ❖ Calculate the necessary risk reduction to reach acceptable level
  - ❖ Requires numerical expression of acceptable risk

# Quantitative Risk Reduction

$$RR = \frac{\textit{InherentRisk}}{\textit{AcceptableRisk}}$$

$$\textit{Safety Function PFD}_{avg} = \frac{1}{RR}$$



# Introduction to Safety Systems in Research Accelerators

Architectures

USPAS

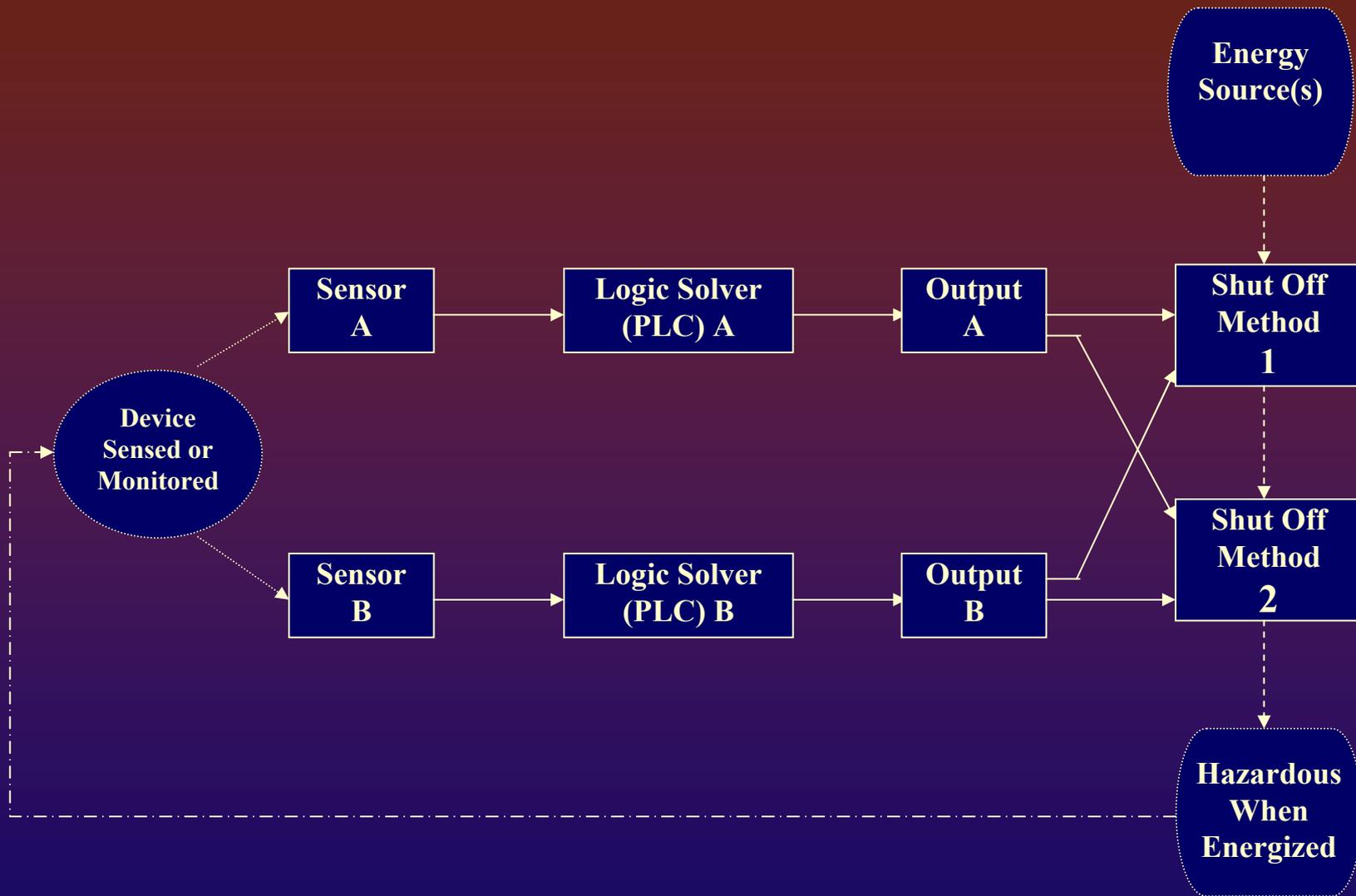
June, 2004

# Architectures

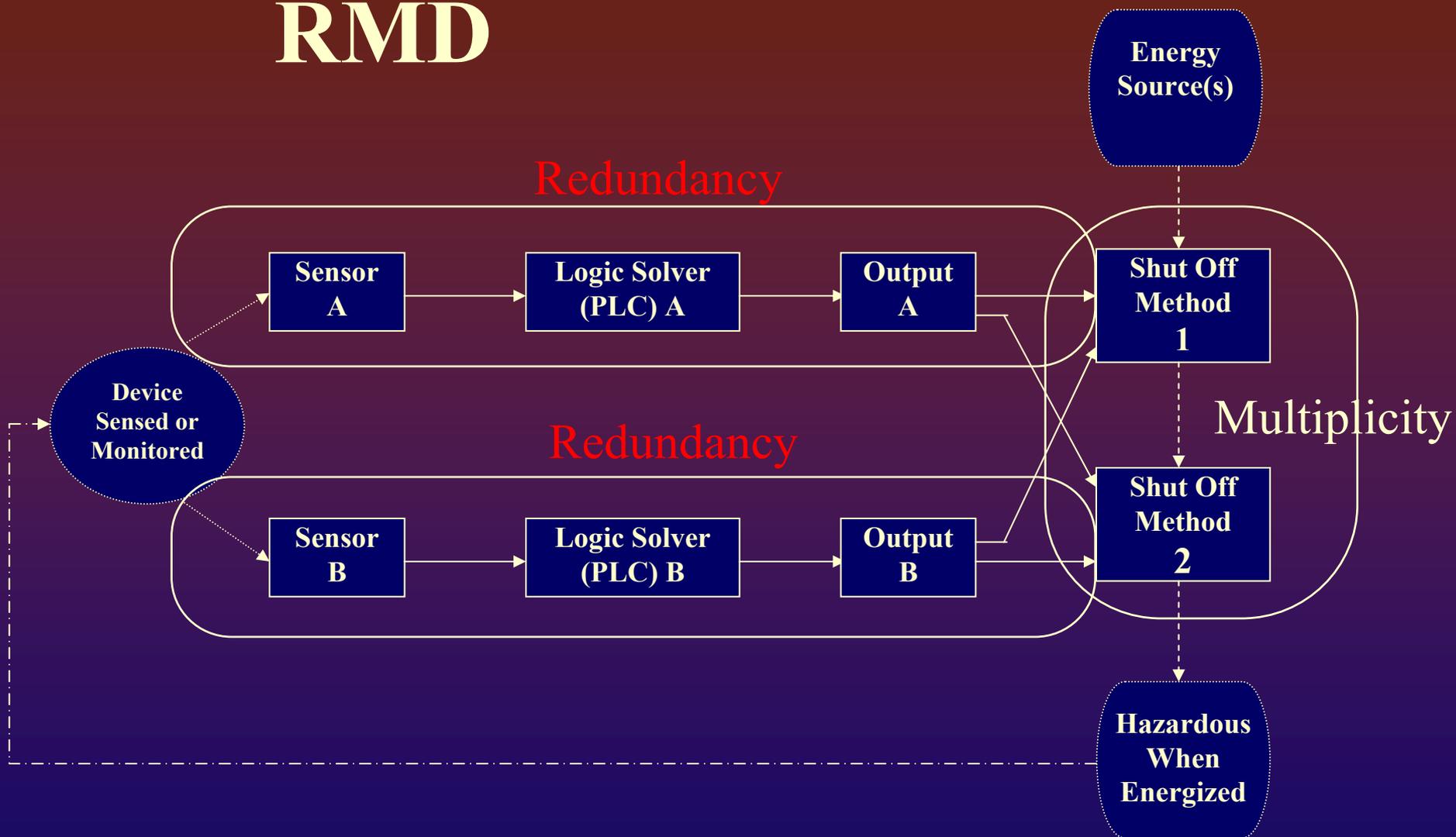
- ❖ **High level implementation of system**
- ❖ **Takes in to account:**
  - ❖ **Final control devices**
  - ❖ **Physical Environment**
  - ❖ **Constraints on physical design**
  - ❖ **R-M-D**

# RMD – Redundancy Multiplicity Diversity

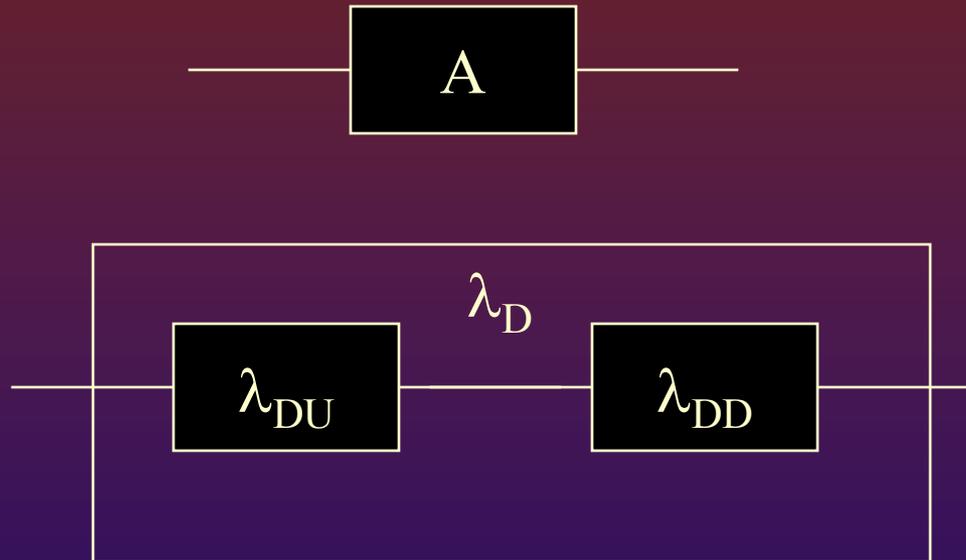
- ❖ **Three elements of the architecture are used to achieve the required safety integrity level**
- ❖ **Redundancy** – is the use of identical safety functions to achieve a high safety reliability
- ❖ **Multiplicity** - is the use of multiple shutdown paths or protection devices
- ❖ **Diversity** – is the use of different types of devices to reduce the probability that multiple or redundant devices can be affected by common failure modes.
- ❖



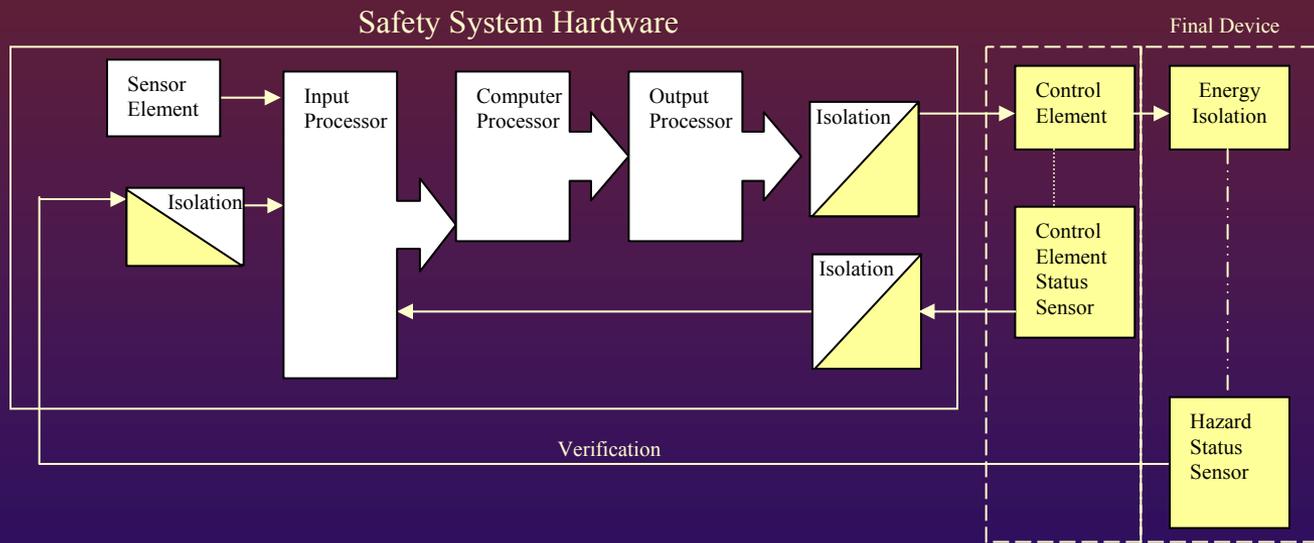
# RMD



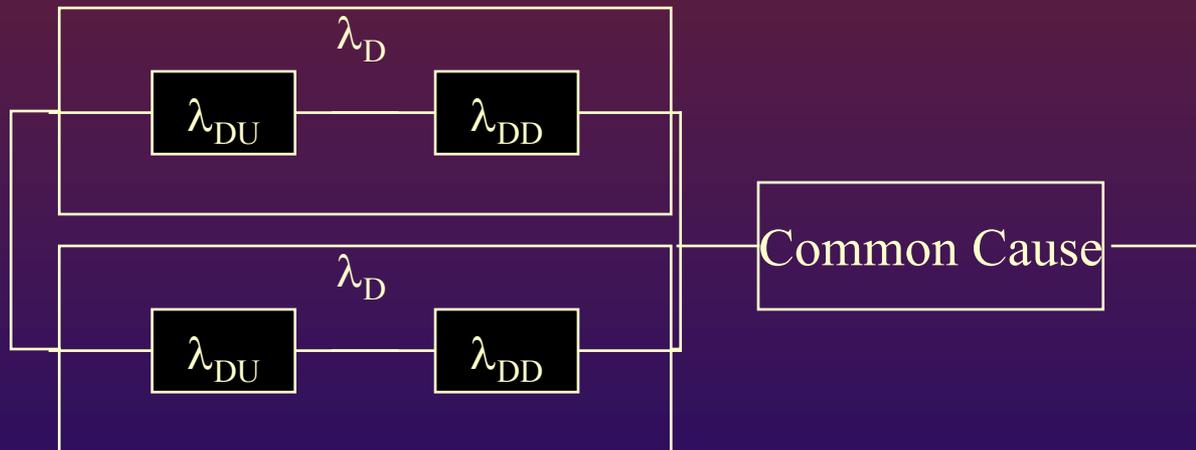
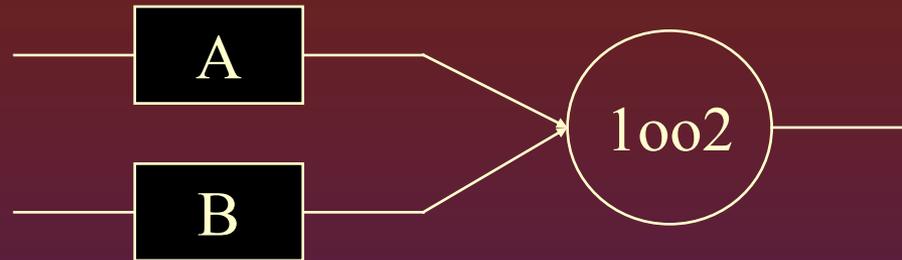
# 1001



$$\text{PFD} \approx \lambda_D \text{TI}$$

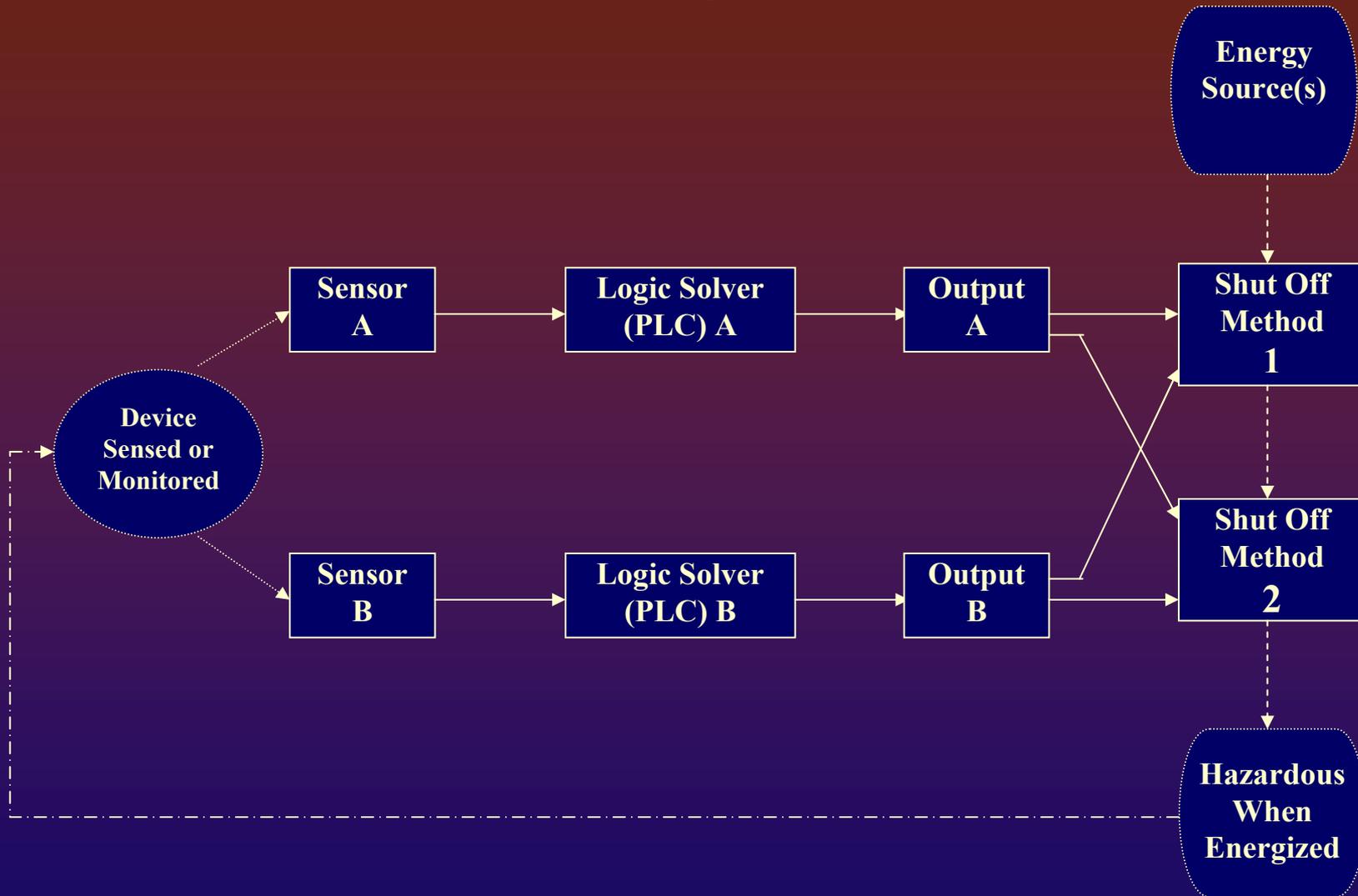


# 1002

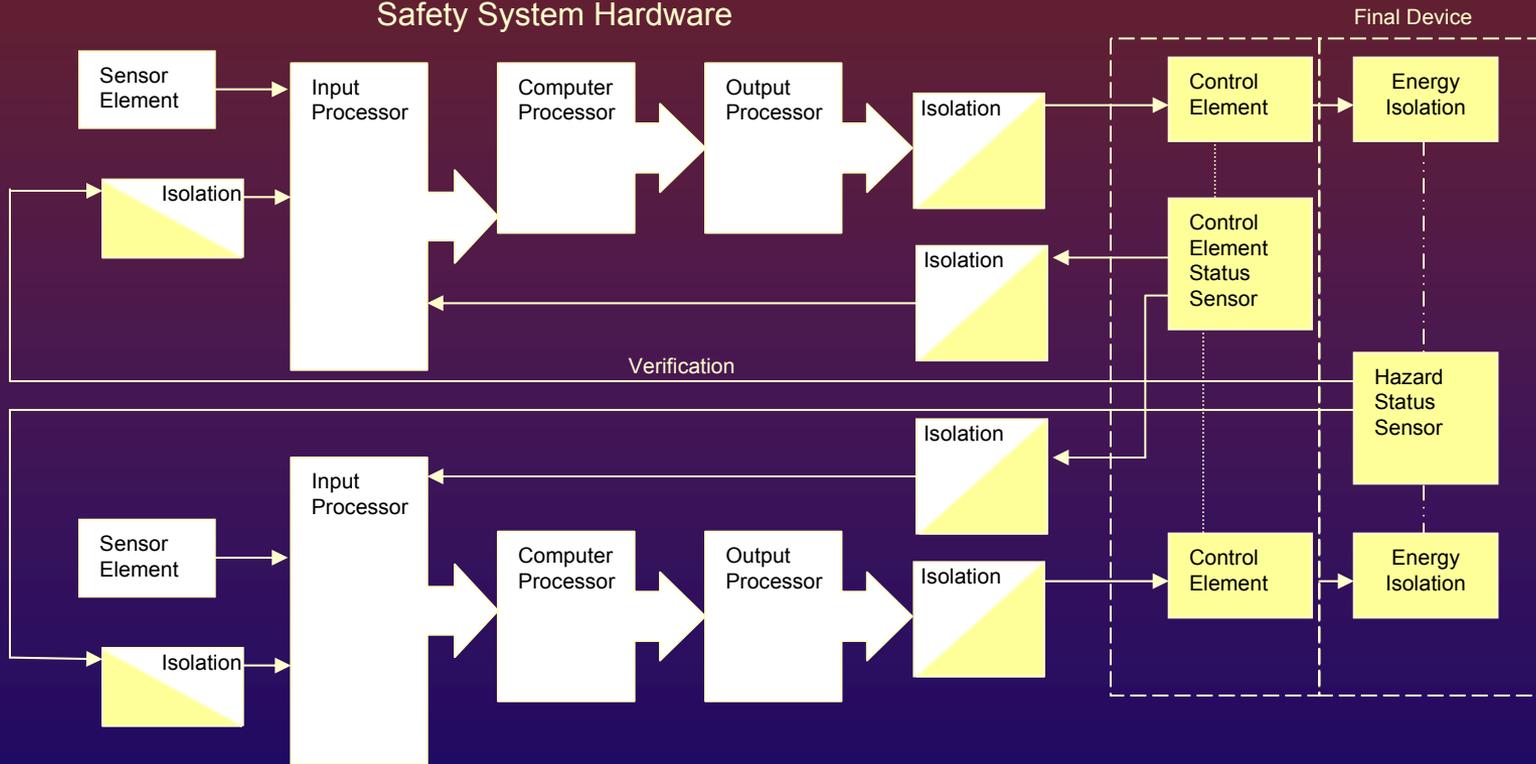


$$PFD_{avg} = 2((1 - \beta)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 TI + \beta\lambda_{DD} MTTR + \left(\frac{TI}{2} + MTTR\right)$$

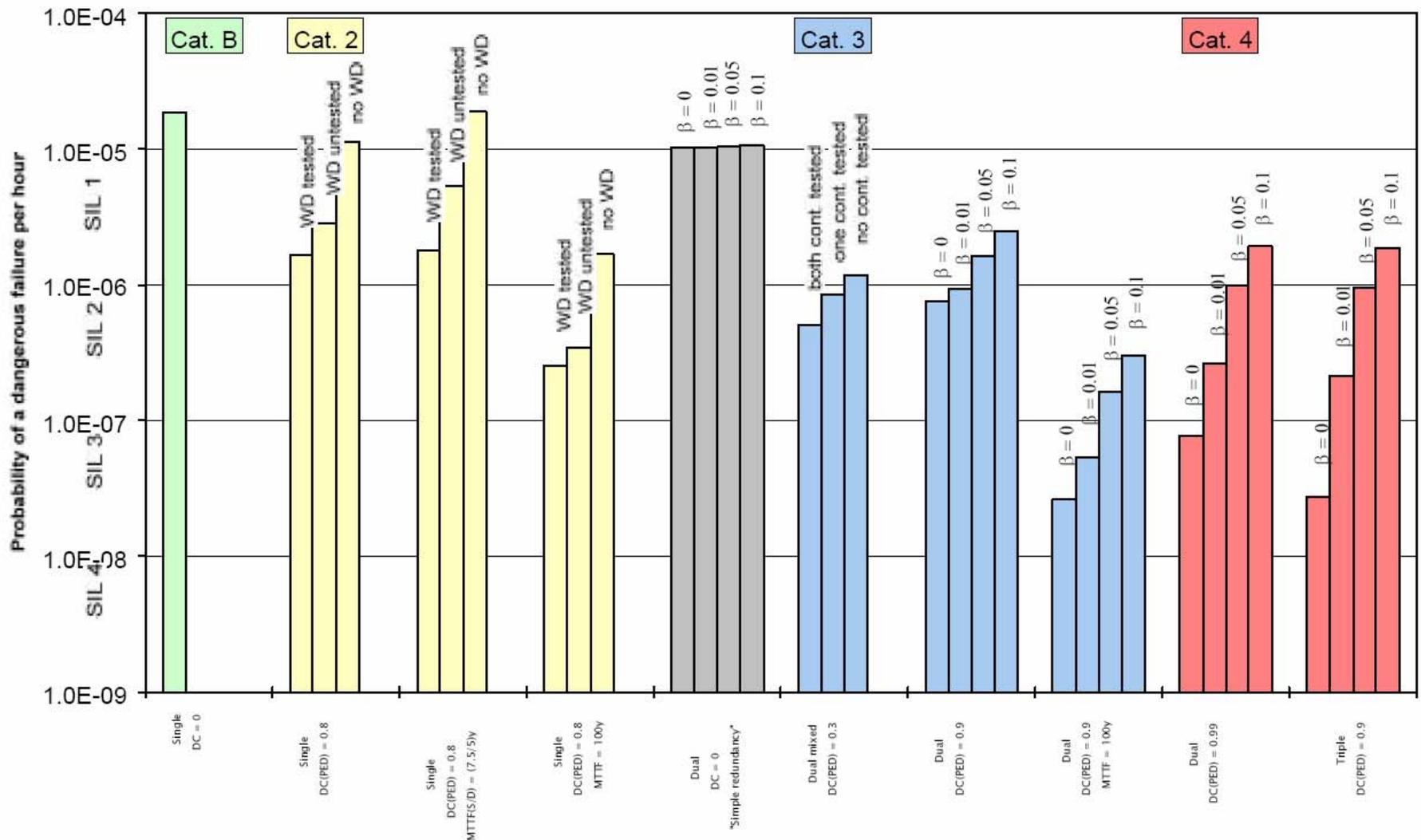
# 1oo2 Block Diagram



## Safety System Hardware



# Comparison of Architectures used in Machinery Industry



ST SARCES

Standards for Safety Related Complex Electronic Systems

# Comparison of architectures from STARCES

## Attempt to reconcile IEC61508 and machine standard EN954

SIL	System Architecture	Mean Time to dangerous Failure MTTF <sub>d</sub> (years)	CCF □ (%)	Diagnostic Coverage (each Channel) (%)	Cat.
		In/Processing/Out		In/Processing/Out	
-	Single PE, Single I/O	15/15/30	-	0/0/0	B
	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	0/60/0	B
	Dual PE, Dual I/O, 1oo2	15/15/30	5	0/0/0	B
1	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	100/60/100	2
	Single PE, Single I, Ext. WD(u/t)	7.5/15/10	-	100/60/100	2
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	5	100/60/100	3
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	10	100/90/100	3
	Dual PE, IPC, Dual I/O, 1oo2	45/15/60	10	100/90/100	3
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	5	100/60/100	3
2	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	10	100/90/100	4
	Single PE, Single I, Ext. WD(t)	15/15/30	-	100/90 <sup>†</sup> /100	2
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	1	100/90/100	3
	Dual PE, IPC, Dual I/O, 1oo2	30/30/60	5	100/90/100	3
	Dual PE, IPC, Dual I/O, 1oo2	7.5/15/10	1	100/99/100	4
	Mixed Dual Processing, Dual O, 1oo2	∩(15/100)/(15/100)	-	0/(30/100)/(100/100)	3
3	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	1	100/60/100	3
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	10	100/90/100	4
	Single PE, Single I, Ext. WD(t)	30/30/60	-	100/99 <sup>†</sup> /100	2
3	Dual PE, IPC, Dual I/O, 1oo2	45/45/90	1	100/99/100	4
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	1	100/90/100	4

### Conditions for single channel systems :

All test rates : 1/(15 min)

Demand rate : 1/(24 h)

Repair rate : 1/(8h)

Mission time (life time) : 10 years

MTTF<sub>d</sub> of watchdog: 100 years

MTTF<sub>d</sub> of switch-off path for watchdog:

WD(u/t): Watchdog and pertinent switch-off path untested or tested

WD(t): Watchdog and pertinent switch-off path tested

(\* not achievable by simple watchdog)

### Conditions for dual or triple channel systems :

All test rates: 1/(24h)

Demand rate: 10/h

Repair rate: 1/(8h)

Mission time (life time): 10 years

MTTF<sub>d</sub> of output sensor of mixed system: 15 years  
equal to normal switch-off path (output sensor not tested)

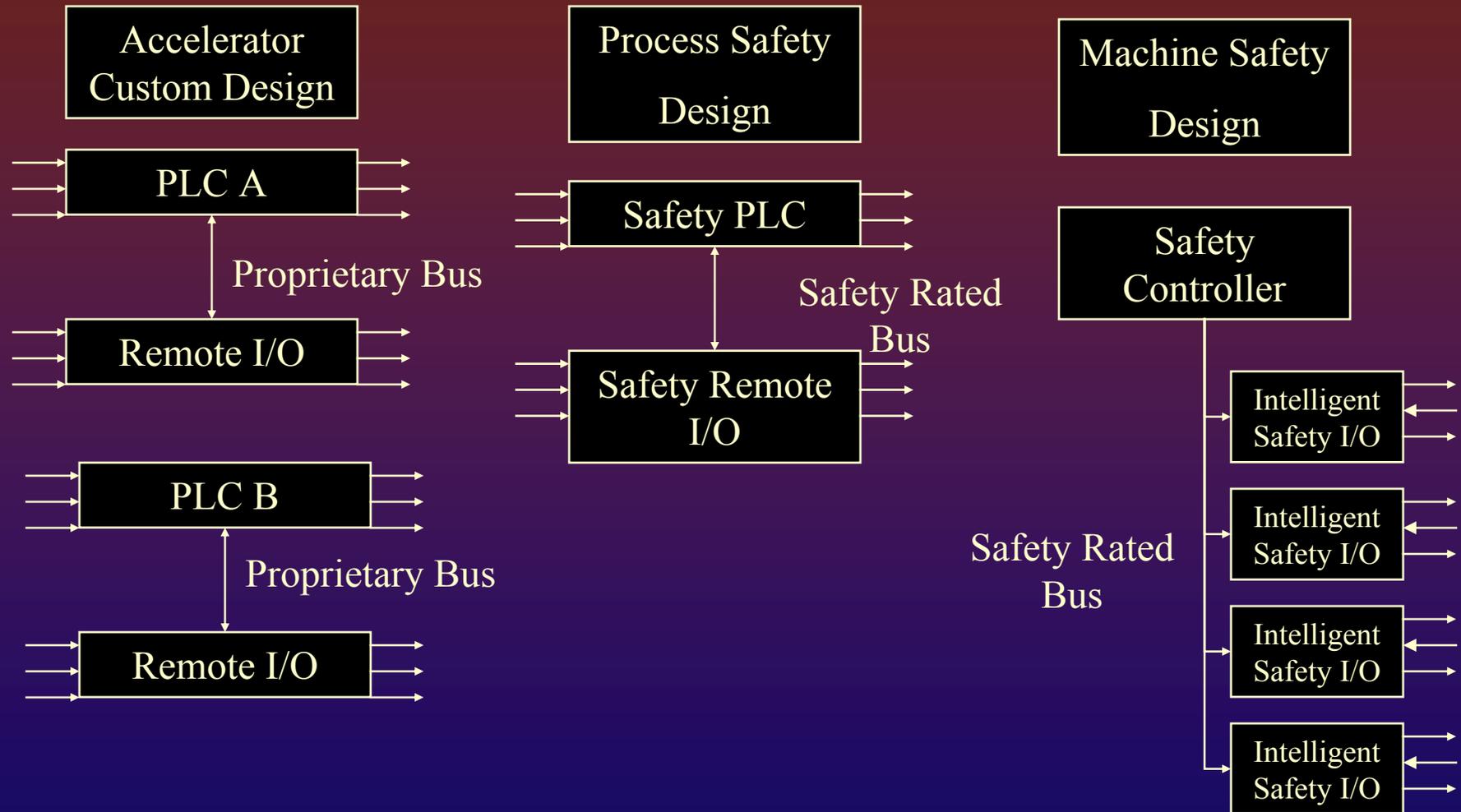
IPC : Inter-processor communication

ST SARCES

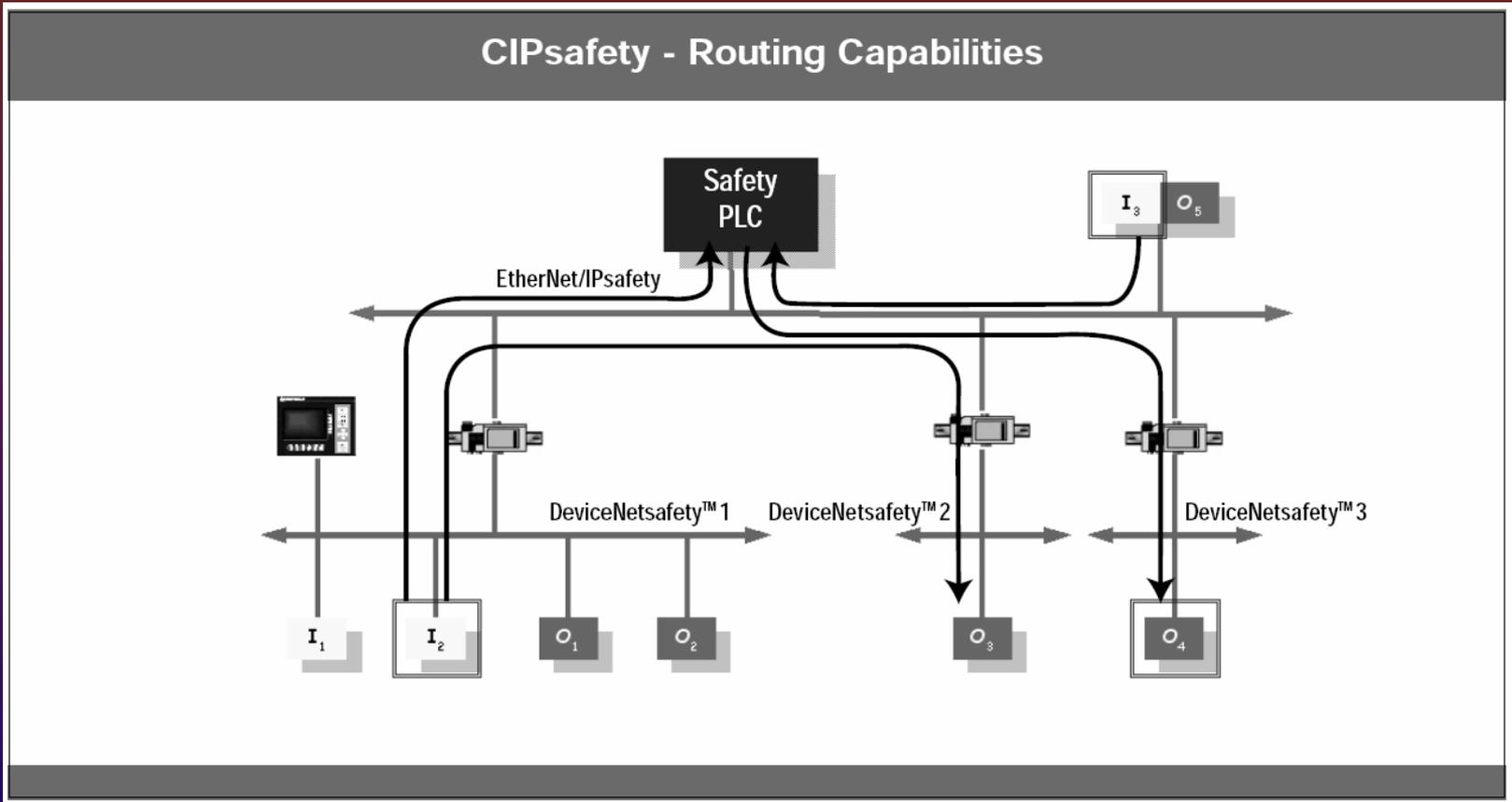
Standards for Safety Related Complex Electronic Systems

© K Mahoney/S. Prior  
2002-2004

# Sample Architectures for SIL 2/3

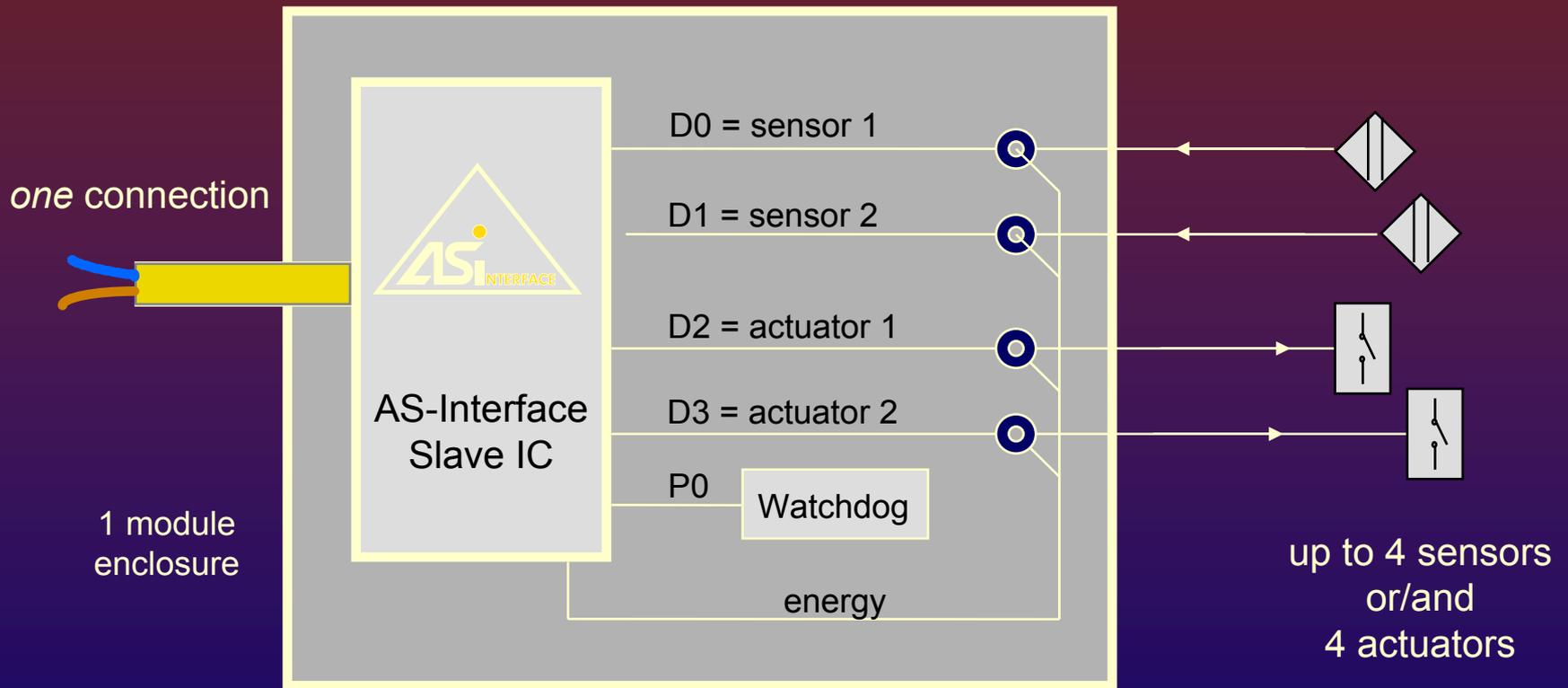


# CIP Safety Net

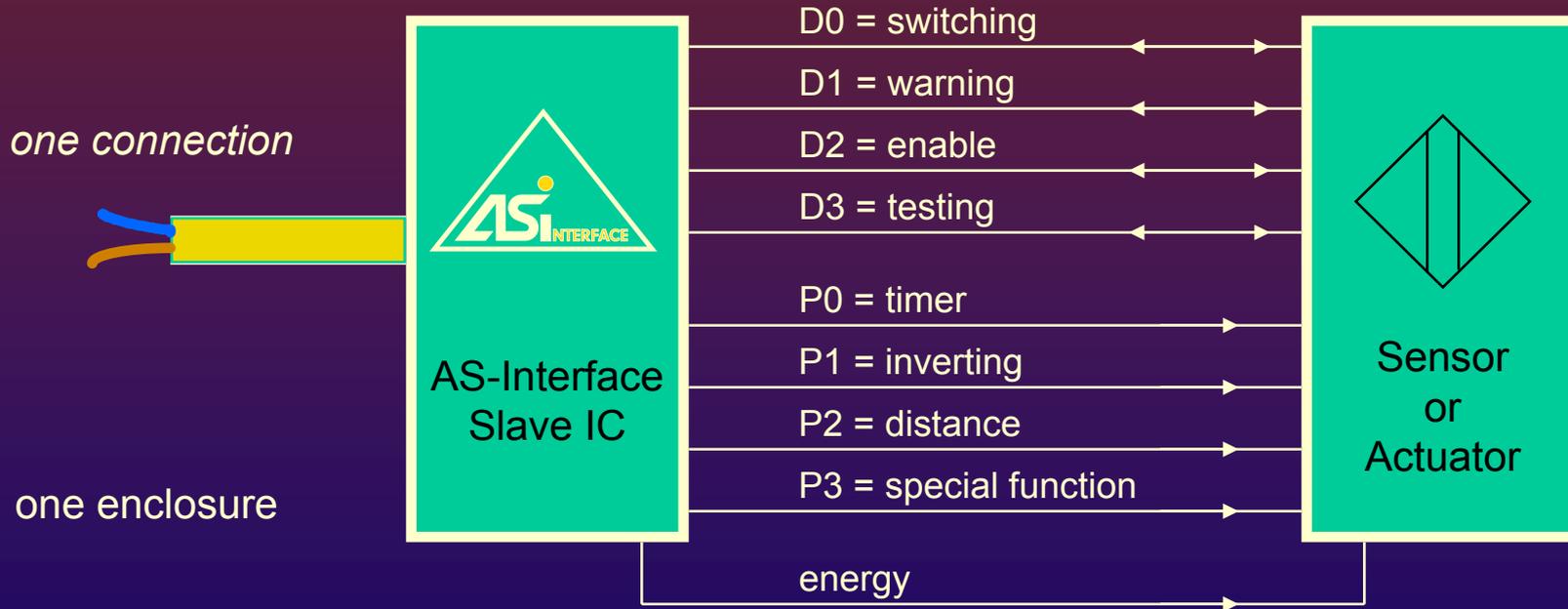


CIP=Common Industrial Protocol

# Actuator Sensor Interface

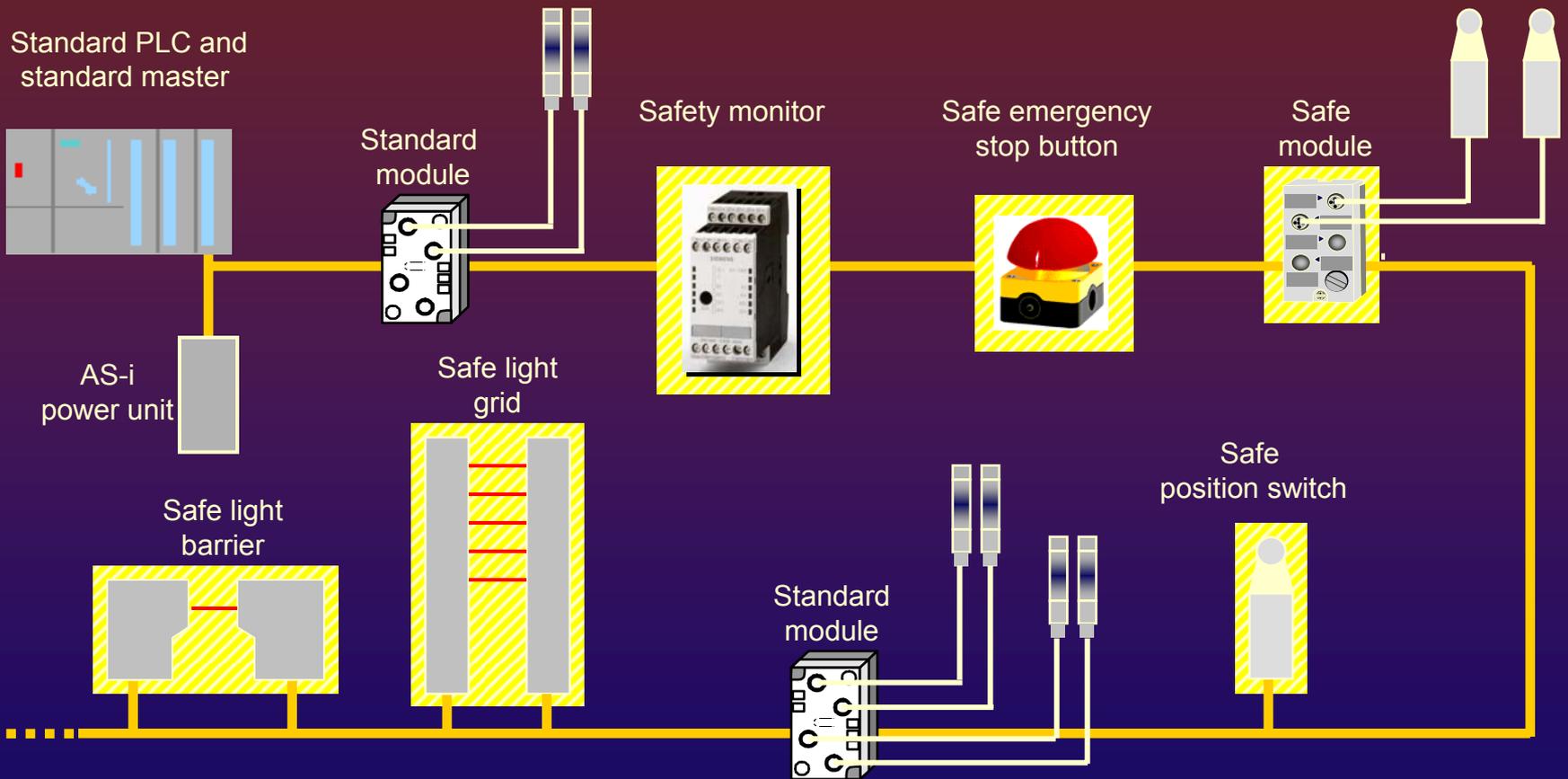


Courtesy of ASI International Foundation



Courtesy of ASI International Foundation

# ASI-Safety



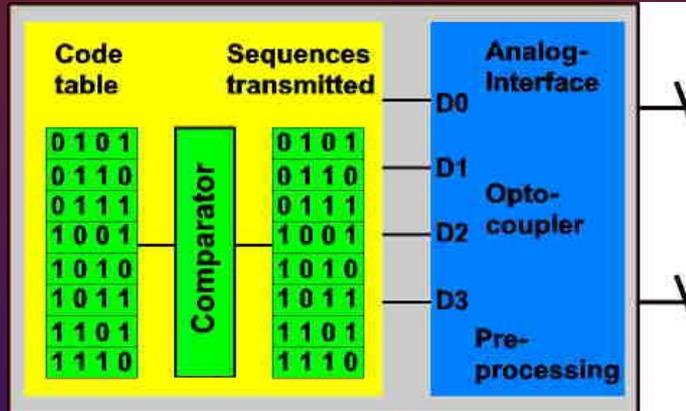
Standard PLC and standard master



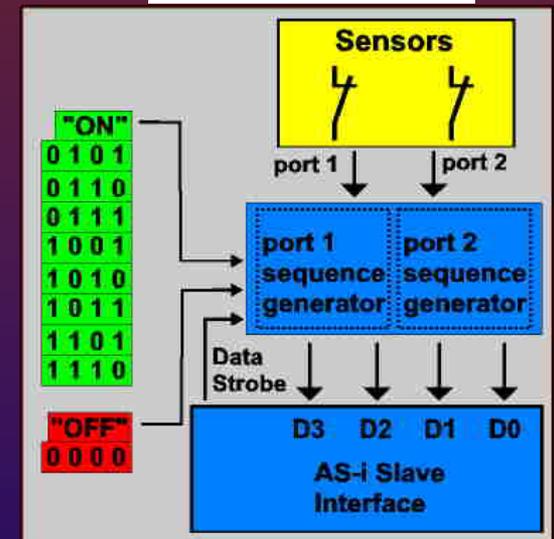
AS-i power unit



### Safety monitor



### Safety-related slave



Master call

Slave response

**Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design**

	<b>Technique/measure</b>	<b>See IEC 61508-7</b>	<b>SIL1</b>	<b>SIL2</b>	<b>SIL3</b>	<b>SIL4</b>
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Diverse hardware	B.1.4	– low	– low	R medium	R high

**Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences**

Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
Measures against voltage breakdown, voltage variations, overvoltage, low voltage	A.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Separation of electrical energy lines from information lines (see note 4)	A.11.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Increase of interference immunity	A.11.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
Failure detection by on-line monitoring (see note 5)	A.1.1	R low	R low	R medium	R high
Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
Code protection	A.6.2	R low	R low	R medium	R high
Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
Diverse hardware (see note 6)	B.1.4	– low	– low	– medium	R high
Software architecture	7.4.3 of IEC 61508-3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A and B of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 Separation of electrical energy lines from information lines is not necessary if the information is transported optically, nor is it necessary for low power energy lines which are designed for energising components of the E/E/PES and carrying information from or to these components.

NOTE 5 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

NOTE 6 Diverse hardware is not required if it has been demonstrated, by validation and extensive operational experience, that the hardware is sufficiently free of design faults and sufficiently protected against common cause failures to fulfil the target failure measures.

**Table A.18 – Techniques and measures to control systematic operational failures**

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Modification protection	B.4.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
	Input acknowledgement	B.4.9	R low	R low	R medium	R high
	Failure assertion programming	C.3.3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Two of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A, B, and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low-demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.



# Introduction to Safety Systems in Research Accelerators

Safety System Management

USPAS

June, 2004

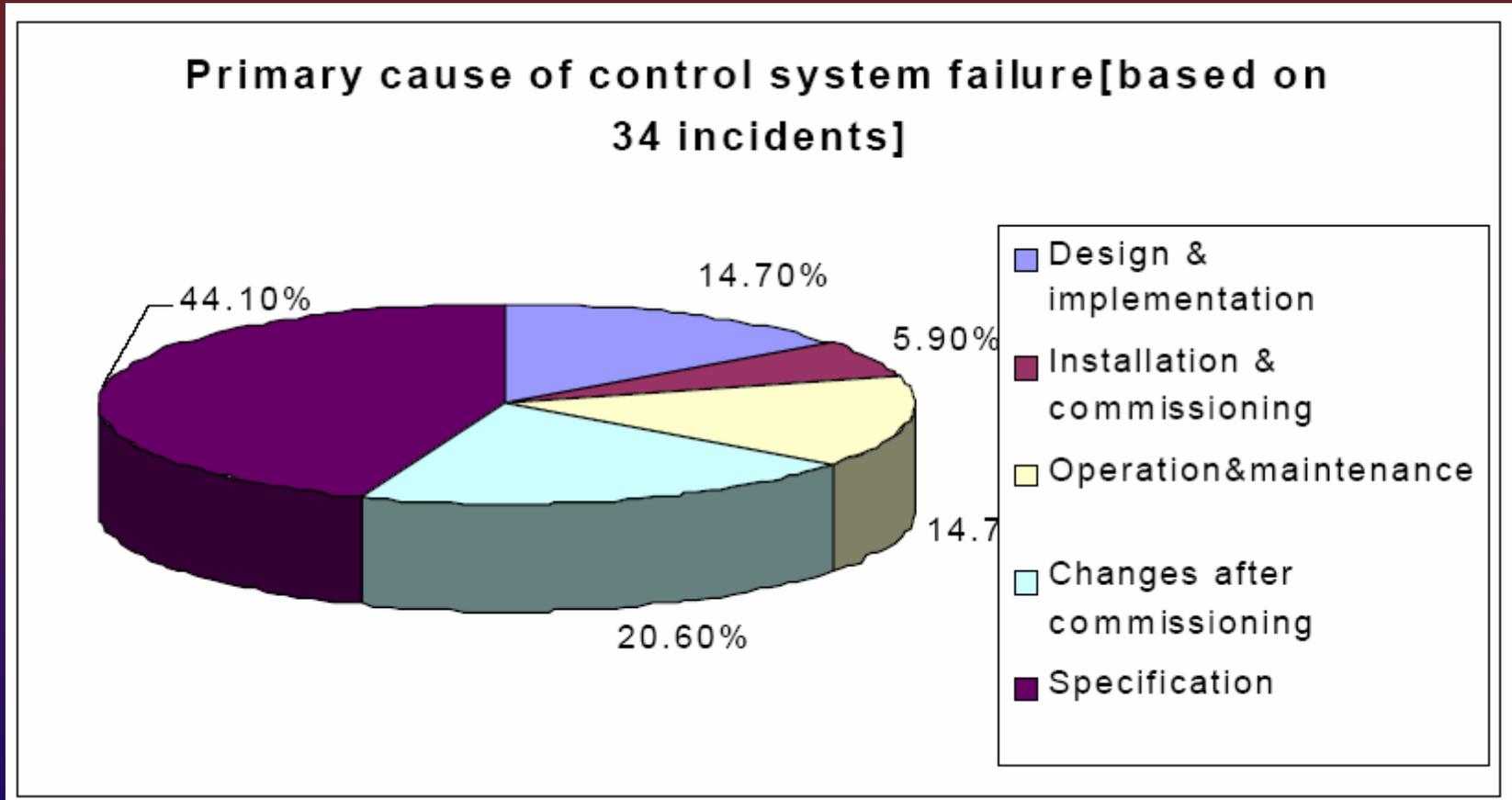
# Elements of SS Management

- ❖ The objective of safety system management is to ensure that the desired level of risk reduction is maintained over the lifetime of the system.
- ❖ In reality, and in accordance with the ALARP principle, there is a continual vigilance of and incremental improvement in the integrity of the system and how it is used.
- ❖ This involves all persons that are affected by the operation and use of the system.

# Management of Change

- ❖ Ensure that lifecycle is not broken
- ❖ Established procedures for change
- ❖ Plan for decommissioning

# HSE Report on Causes of Safety System Failure



# IEC61508 – SS Management Requirements

Those organizations or individuals that have overall responsibility for one or more phases of the overall [*safety system*] in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the safety-related systems achieve and maintain the required functional safety. In particular, the following should be considered:

- a) the policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;
- b) identification of the persons, departments and organizations which are responsible for carrying out and reviewing the applicable overall [*safety system*] lifecycle phases (including, where relevant, licensing authorities or safety regulatory bodies);
- c) the overall [*safety system*] lifecycle phases to be applied;
- d) the way in which information is to be structured and the extent of the information to be documented;

# IEC61508 – SS Management Requirements

- e) the selected measures and techniques used to meet the requirements of a specified [*requirement*]
- f) the functional safety assessment activities
- g) the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems arising from
  - hazard and risk analysis
  - functional safety assessment
  - verification activities
  - validation activities
  - configuration management
- h) the procedures for ensuring that applicable parties involved in any of the overall [*safety system*] lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:
  - the training of staff in diagnosing and repairing faults and in system testing;
  - the training of operations staff;
  - the retraining of staff at periodic intervals;
- i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;

# IEC61508 – SS Management Requirements

- j) the procedures for analysing operations and maintenance performance. In particular procedures for – recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which detect recurring faults;
  - assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system;
- k) requirements for periodic functional safety audits in accordance with this subclause including
  - the frequency of the functional safety audits;
  - consideration as to the level of independence required for those responsible for the audits;
  - the documentation and follow-up activities;
- l) the procedures for initiating modifications to the safety-related systems;
- m) the required approval procedure and authority for modifications;

# IEC61508 – SS Management Requirements

- n) the procedures for maintaining accurate information on potential hazards and safety-related systems;
- o) the procedures for configuration management of the [*safety system*] during the overall [*safety system*] lifecycle phases; in particular the following should be specified:
  - the stage at which formal configuration control is to be implemented;
  - the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
  - the procedures for preventing unauthorized items from entering service;
- p) where appropriate, the provision of training and information for the emergency services.

# Management of Management

Management must understand their responsibilities



- ❖ Assume responsibility for acceptable level of risk
- ❖ Provide staff adequate resources and training
- ❖ Establishment of policy and strategy for achieving safety goals

# Step 1: Policy

- ❖ Senior management provides
  - ❖ Establish expectations
  - ❖ Sources of info
    - ❖ Institutional plans
    - ❖ Strategic plans
    - ❖ Contract requirements
    - ❖ External/internal commitments

# Step 2: Planning

- ❖ Defining work scope
- ❖ Budget
- ❖ Timelines
- ❖ Hazard identification & characterization
- ❖ System Interfaces

# Step 2: Planning

- ❖ Civil construction or modifications
  - ❖ Access Control
  - ❖ Life Safety
  - ❖ Shielding
  - ❖ Potential impact on SS hardware
- ❖ Potentially hazardous equipment design, development, and modification.
  - ❖ Shutdown Methods
  - ❖ Status Feedback

## Step 2: Planning

- ❖ Spare parts
- ❖ Determine the level of review and approval needed to bring system into operation
  - ❖ Readiness Review
  - ❖ Peer Review (internal or external; formal or informal)
- ❖ Start configuration management (CM) program development early

# Purpose of CM Program

- ❖ The purpose of the Configuration Management (CM) Program is to establish the CM mechanisms for consistency between the appropriate design requirements, physical configuration, and documentation of critical items necessary to protect workers and the public during the lifecycle of a facility.

# Configuration Management (CM)

- ❖ Consists of 5 components
  - ❖ Program Management
  - ❖ Design Requirements
  - ❖ Document Control
  - ❖ Change Control
  - ❖ Assessments
- ❖ Graded Approach

# CM: Program Management

- ❖ Identify critical items based on facility safety basis documents
- ❖ Determine the configuration level for each critical item
- ❖ Establish a system for controlling changes
  - ❖ How, and by whom, shall changes be reviewed
  - ❖ Who has approval authority for changes

# CM: Design Requirements

- ❖ Documents are added, changed, or deleted using the change control process which ensures the current configurations are known and controlled at all times.
- ❖ Interfaces with other systems are clearly identified.
- ❖ Identifying interfaces is important both for clearly identifying the scope of the CI and for interfacing systems that may have different CM levels or CM owners.

# CM: Document Control

- ❖ Identify the types and specific documents to be included within the CM Program.
- ❖ Determine how they will be stored to protect them from loss or damage.
- ❖ How will the documents & drawing be numbered and tracked so that you are sure most current documents are in use?
- ❖ Ensure documents can be easily retrieved

# Step 3: Implementation & Operation

- ❖ Develop Users' Manual and other work procedures documents
  - ❖ Sweep procedures
  - ❖ Certification procedures/checklists
  - ❖ Integrate into facility operational procedures
  - ❖ Maintenance procedures
  - ❖ Safety system bypass CM requirements
  - ❖ Troubleshooting guides
  - ❖ Training/education documents
  - ❖ Change Control procedures

# CM: Change Control

- ❖ The objective of the change control element is to maintain consistency among the design requirements, physical configuration, and facility documentation as changes are made.
- ❖ This objective can be met if needed changes to a CI are properly identified, evaluated for impact to safety and to other components of the CI, executed in a controlled manner, and verified when complete.

# Change Control

- ❖ Changes may include changes to hardware, maintenance procedures, processes, operations, documents, computer software, and inventory limits, as well as temporary modifications.
- ❖ Review each specific proposed change to determine whether it is within the bounds of the design requirements
- ❖ Ensure affected parties are made aware of the change.

# System Maintenance

- ❖ Don't rely on "reactive maintenance"
- ❖ Instead, focus on
  - ❖ Preventive maintenance
  - ❖ Training
  - ❖ Spare part quality
  - ❖ Design improvements

# Step 4: Checking & Corrective Action

- ❖ Assessments also 5<sup>th</sup> element of CM program
- ❖ Should be conducted periodically during the life of the system
- ❖ Should also be conducted whenever a change or modification is performed that impacts the safety basis

# Step 4: Checking & Corrective Action

- ❖ Documented
- ❖ Corrective actions tracked
- ❖ Evaluated for trends and opportunities for continuous improvement

# Step 5: Management Review

- ❖ Top management should periodically review system management to ensure it is meeting performance expectations
  - ❖ Line Self-Assessments
  - ❖ Contract performance review

# Why Quality Initiatives Fail

- ❖ Quality programs often struggle to gain initial acceptance and to sustain continuous improvement. (U.S. General Accounting Office, 1991)
- ❖ The inability to manage an improvement program as a dynamic process is the main determinant of program failure.

# Certification

- ❖ Safety systems require periodic certification in order to uncover dangerous undetected failures.
- ❖ Exercises all components of a system
- ❖ Should have an independent reviewer

# Training

- ❖ SS Designers
- ❖ Maintenance Personnel
- ❖ Machine Operators
- ❖ Management

# Bypass

- ❖ Bypassing of safety system components during the lifetime of a facility is inevitable.
  - ❖ Final devices should have a manual energy isolation method that will provide equivalent protection as the automated safety system, e.g. lock out/tag out. This should be in the design requirements for the device.

# Tracking & Trending

Sandra L. Prior, REM, CHMM  
System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School  
June 28 – July 2, 2004

# Why Track Data?

- Good business practice
- Establishes history/audit trail for decisions and actions
- Can use data history for
  - Continuous improvement
  - Risk analysis
  - design justification
- Tracking commitments forces people to act

# Cost vs Benefit

- Setting up a tracking system requires
  - Knowing what outcomes you want first
  - Resources for development
- Initial data entry can be viewed as time consuming
  - Requires disciplined, systematic approach
  - Benefits over time far outweigh initial data entry investment

# Jlab EH&S Tracking System

EH&S Tracking Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address <https://mis.jlab.org/ehs/index.php> Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** **EH&S Tracking Home**

HOME | SEARCH | CONTACT JLAB

**Tracking, trending, & training**

Sandra Prior  
[View my open findings](#)

Problems? Questions? Contact an [Administrator](#).

- Home
- Admin
- Tracking Records
- EH&S Info
- Requirements
- Work Control Docs
- Work Requests
- JIT training
- Help

**SAFETY FIRST**

## Welcome, Sandra, to the EH&S Tracking System.

What would you like to do?

- [Show me all open items assigned to me.](#)
- Show me all inspection items for area:
- [Take me to the search page.](#)
- [I would like to add a record.](#)

Our EH&S tracking and reporting mechanisms, presented at the the international [IRIA conference](#), have been selected as categorical winner by the National Registry of Environmental Professionals.

### Lessons Learned

**Finding:** [AI-2004-05-02](#)  
Staff need to promptly report injuries to line management and cofer on next steps.

### Current Status

**EH&S Tracking Items**  
(Count of Open Findings)

Inspections	105
(Accident/Incident)s	11
Assessments	98
RDRs	3

[More...](#)

Maintained by: [inagops@jlab.org](mailto:inagops@jlab.org)

EH&S

1 Hierarchical Menu Trees Created

Internet

# Sources of Data

Data Source	Description	Comments
Inspections	Scheduled Internal/External	Proactive & reactive Compliance driven
Observations	Informal EHSLOG, verbal, email	Proactive ISMS Core Function 5
Accident/Injury/Occurrence	Crosses DOE/OSHA reporting threshold	Reactive
Notable Event	May be good or bad Lessons Learned	Proactive ISMS Core Function 5
Assessment	Line Self Independent	Proactive ISMS Core Function 5

# Data Source: Inspections

- 4 Categories of main data sources, or “events”
  - Inspections
    - Scheduled
    - Safety Warden
    - EH&S staff observations
    - Laser Audits
    - External Agency

# Data Source: Accident/Incident

- ❖ Reportable Injuries/Illnesses
- ❖ First Aid
- ❖ Reportable Incidents – as defined by DOE Occurrence Reporting requirements
- ❖ Notable Events – non reportable occurrences
  - Can be good or bad
  - Focus is on Lessons Learned

# Data Source: Assessments

- ❖ Line Self Assessments
- ❖ Independent Assessments
- ❖ EH&S Manual Revisions

# Data Source: RDRs

## Radiation Deviation Reports (RDR)

- Radiological events that do not cross Price Anderson Act Amendments threshold for reporting
- 3 similar events w/in 1 year rise to reportable level
  - Ex. Recent VTA ORPS report

# Data Sources: Common Features

- All categories share a common set of data fields: date, location, evaluator, division, department, & responsible manager
- Each category also has unique data set

## Accidents/Incidents

ISMS Core Values

Report Link

Lessons Learned

Classification

## Inspections

Risk Codes

EH&S Manual Reference

# Data Format: Events

- Two tiered approach
  - Events
    - Contains data common to a subset of related findings – the event “Header”
    - Mixture of common and unique data fields
    - Useful for periodic roll up reports that assess the numbers of inspections performed or accidents that occurred in a given timeframe
    - More efficient means of managing data

# Data Format: Findings

- Two tiered approach – cont
  - Findings
    - Individual observations or causes that require some action to correct
    - May have different responsible managers, risk codes, ISMS core value, or lesson learned
    - Multiple findings may be generated from one event
- Both have unique but related record numbers using category, year, and sequence #

# System Access

- Access is Intranet only
- Requires JLab user name and password
- Anyone can view data, post status updates, conduct queries and generate reports
- User privileges required to add new records, and edit, delete, or close existing records

# System Access - cont

- Anyone may post an EHSLOG entry and email it at the time the entry is posted
  - Expedites notice to EH&S staff or supervisor
  - Primary route for worker observations added to tracking system
  - Also a good means of sharing information

# Querying the System

- May query events or findings w/in a category or across all categories
- Cross category queries yield data from common fields only
- Event & Finding queries w/in a category yield data from all fields, common and unique
- Anyone may query the system; no password or privileges are needed
- Query results provided in HTML or MS Excel

# Quick View of Your Findings

- Menu bar “View my open findings” appears on every page
- Provides quick view of open items in the system that are your responsibility to close
- Knows who you are based upon log-in to the system

# Jlab EH&S Tracking System

EH&S Tracking Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address <https://mis.jlab.org/ehs/index.php> Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** **EH&S Tracking Home**

HOME | SEARCH | CONTACT JLAB

Tracking, trending, & training

Sandra Prior  
[View my open findings](#)

Problems? Questions? Contact an [Administrator](#).

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

**SAFETY FIRST**

**Welcome, Sandra,**  
**to the EH&S Tracking System.**

What would you like to do?

- [Show me all open items assigned to me.](#)
- Show me all inspection items for area:
- [Take me to the search page.](#)
- [I would like to add a record.](#)

Our EH&S tracking and reporting mechanisms, presented at the the international [IRIA conference](#), have been selected as categorical winner by the National Registry of Environmental Professionals.

**Lessons Learned**

**Finding: AI-2004-05-02**  
Staff need to promptly report injuries to line management and cofer on next steps.

**Current Status**

**EH&S Tracking Items**  
(Count of Open Findings)

Inspections	105
(Accident/Incident)s	11
Assessments	98
RDRs	3

[More...](#)

Maintained by: [inagops@jlab.org](mailto:inagops@jlab.org)

Jefferson Lab EH&S

1 Hierarchical Menu Trees Created

Internet

# Menu Selection: EH&S Info

EH&S Tracking Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://mis.jlab.org/ehs/index.php>

Privacy and Security Notice Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** **EH&S Tracking Home**

HOME | SEARCH | CONTACT JLAB

Tracking, trending, & training

Sandra Prior  
View my open findings

Problems? Questions? Contact an [Administrator](#).

Home  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Request  
JIT training  
Help

EH&S Info  
EH&S HomePage  
EH&S Manual  
EH&S Log  
Monthly Highlights  
Alerts / Notices

**Welcome, Sandra,**  
**to the EH&S Tracking System.**

What would you like to do?

[Show me all open items assigned to me.](#)

Show me all inspection items for area:

[Take me to the search page.](#)

- [I would like to add a record.](#)

Our EH&S tracking and reporting mechanisms, presented at the the international [IRIA conference](#), have been selected as a categorical winner by the National Registry of Environmental Professionals.

**Lessons Learned**

Finding: [AI-2004-05-02](#)  
Staff need to promptly report injuries to line management and cofer on next steps.

**Current Status**

**EH&S Tracking Items**  
(Count of Open Findings)

Category	Count
Inspections	105
(Accident/Incidents)	11
Assessments	98
RDRs	3

[More...](#)

Maintained by: [inapps@jlab.org](mailto:inapps@jlab.org)

Jefferson Lab EH&S

# Menu Selection: EH&S Manual

Jefferson Lab Environment, Health, & Safety Manual - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Refresh Print

Address <http://www.jlab.org/ehs/manual/EHSbook.html> Go Links

[Privacy and Security Notice](#)

  EH&S    

Jefferson Lab EH&S Manual - Rev. 5.6 - 29 January 2004 | [JLab EH&S Info](#)

---

## Jefferson Lab Environment, Health, & Safety Manual

---

### [In the Event of an Emergency](#)

The EH&S Manual is structured in six major sections. The 1000 - 5000 sections deal with policy, responsibilities, and administrative procedures. For topical information, see the [6000-series](#) section.

---

Standard forms are available in PDF and MSWd formats: [Index of Forms](#)

Full-text search is available through the EH&S Manual [search page](#).

---

PDF version: ( with active cross-references, best viewed with browser plug-in.)

[Table of Contents](#)

[Topical Index](#)

Done Internet

# Menu Selection: EH&S Manual

2000 Organization and Responsibilities

- 2100 Laboratory Organization
- 2210 EH&S Responsibilities of Individuals
  - Appendix 2200-R1 Current EH&S Staff Assignments
- 2220 Landlord and Tenant EH&S Responsibilities
- 2230 EH&S Responsibility for Products
- 2240 Jefferson Lab EH&S Committees
- 2310 EH&S Concern Resolution
  - EH&S Concern Report
  - 2320 External EH&S Reviews
- 2410 Applicable Regulations and Contractual Commitments**
  - Appendix 2410-T1 Jefferson Lab Hazard Issue List
  - Appendix 2410-T2 TJNAF Work Smart Standards Set
  - Appendix 2410-T3 Administrative EH&S Documents
- 2420 Permits and Authorizations from External Agencies

3000 Planning for Safe Operations

- 3110 EH&S Assessments of New Facility Plans
- 3120 The CEBAF Experiment Review Process
  - Appendix 3120-A Conduct of Operations (COO) for Jefferson Lab
  - Appendix 3120-B Typical Outline for a Radiation Safety Assessment Document
  - Appendix 3120-C Typical Outline for a Preliminary Experiment Safety Assessment or an Experiment Safety Assessment Document
  - Appendix 3120-D The Experiment Review Process for a New Experiment Using the Base Equipment (Type 2)
  - Appendix 3120-E The Experiment Review Process for an Experiment Requiring Temporary (Type 3) or Permanent (Type 4) Modification of the Base Equipment

**EH&S Manual**  
2410-T2 Work Smart Standards Set

Thomas Jefferson National Accelerator Facility

**Table 1: TJNAF Work Smart Standards Set**

Issue #	Hazard Issue	Necessary Standards	Sufficient External Standards	Sufficient Internal Standards (Chapters/Appendices from the JLab EH&S Manual)
003	Bio - bloodborne pathogens	29 CFR 1910.1030; 9 VAC 20-120-10 et. seq., Regulated Medical Waste Management Regulations	CDC Guidelines for Immunizations	Chapter 6840 <i>Bloodborne Pathogen Protection</i> ; Chapter 6850 <i>Regulated Medical Waste Management</i>
006	Chem - acids, solvents, toxic agents and haz. liquids	29 CFR 1910.1200; 29 CFR 1910.1000; 29 CFR 1910.1450, Occupational Exposure to Hazardous Chemicals in Laboratories	ACGIH TLV, current edition; ANSI Standard A 13.1- 1996, Scheme for the Identification of Piping Systems, with 1998 change, or current edition, applicable for: 1) new piping installation and 2) when poor labeling constitutes a safety hazard	Chapter 6610 <i>Chemical Hygiene</i> and appendices
007	Chem - carbon monoxide	29 CFR 1910.1200, Hazard Communication Standard; 29 CFR 1910.146, Permit-Required Confined Space Entry; 29 CFR 1910.1000, Table of OSHA Permissible Exposure Limits (PEL); 29 CFR 1910.178(i), Control of	ACGIH TLV, current edition	Chapter 6610 <i>Chemical Hygiene</i> and appendices; Chapter 3220 <i>Communication of Hazards to Employees and Users</i> ; Chapter 6145 <i>Forklifts</i> ; Chapter 6160 <i>Confined Space Entry &amp; Appendices</i>

# Menu Selection: EH&S Manual

http://www.jlab.org/ehs/manual/PDF/EHSbookTOC.pdf - Microsoft Internet Explorer

Address: http://www.jlab.org/ehs/manual/PDF/EHSbookTOC.pdf

Options x

Table of Contents

- 1000 Policy
- 2000 Organic
- 3000 Planner
- 4000 Training
- 5000 Inventory
- 6000 Topical
  - 6100 Industrial
  - 6200 Electric
  - 6300 Ionizing
    - 6400 Non-ionizing
    - 6500 Cryogenic
    - 6600 Industrial
    - 6700 Environmental
    - 6800 Occupational
    - 6900 Fire
- 7000 Laser
- 8000 Radio Frequency and Microwave
- 9000 Ultraviolet, Visible, and Infrared
- 10000 Static Magnetic Fields

**6300 Ionizing Radiation**

- 6310 Ionizing Radiation Protection
  - Appendix 6310-T2 Prompt Radiation Control Policy
  - Appendix 6310-T3 Policy on Disposal of Beam Dump Tritium and Other Dissolved Radionuclides
- 6311 Prompt Radiation Control**
  - Appendix 6311-T1 Safety and Operations Envelopes
- 6315 Environmental Monitoring of Ionizing Radiation
  - Appendix 6315-T1 Ionizing Radiation Monitoring Procedures

**6400 Non-ionizing Radiation**

- 6410 Laser Safety
  - Appendix 6410-T1 Laser Bioeffects & Non-Beam Hazards
  - Appendix 6410-T2 Laser Hazard Labels
  - Appendix 6410-T3 Laser Standard Operating Procedures
  - Appendix 6410-T4 Laser System Supervisor Control Inspection Checklist
- 6420 Radio Frequency and Microwave Radiation
  - Appendix 6420-T1 RF Surveys
- 6430 Ultraviolet, Visible, and Infrared Radiation
  - Appendix 6430-T1 Physical Effects of Non-Ionizing Radiation
  - Appendix 6430-T2 Assessment of and Protection from Welding Arc Radiant Hazards
- 6440 Static Magnetic Fields
  - Appendix 6440-T1 Medical Screening Questionnaire for Exposure to Static Magnetic Fields

5 of 8

http://www.jlab.org/ehs/manual/PDF/6311PromptRadCon.pdf - Microsoft Internet Explorer

Address: http://www.jlab.org/ehs/manual/PDF/6311PromptRadCon.pdf

Options x

EH&S Manual

6311 Prompt Radiation Control

6311

**Prompt Radiation Control**

Introduction

The design of prompt radiation-producing systems/components, the facilities that house them and the associated safety procedures should be integrated when developing control methods. The Jefferson Lab Radiation Protection Program Plan identifies the fundamental requirements for radiation safety at Jefferson Lab. The Lab's RadCon Manual implements those requirements by specifying the appropriate actions for a given situation.

Depending upon the circumstances, however, a control system need for life

1 of 15

# EH&S Electronic Logbook

Electronic Logbook & OPS-PR System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://opweb.acc.jlab.org/CSUEApps/elog.php?sort\_order=DESCENDING&sd\_Month=06&sd\_Day=01&sd\_Year=2004&sd\_Hour=00&ed\_Month=07&ed\_Day=01&ed\_Year=2004&ed\_... Go Links

Logbooks: [ELOG](#) | [CLOG](#) | [SLOG](#) | [SADLOG](#) | [POLOG](#) | [BDLOG](#) | [FLOG](#) | [FUNLOG](#) | [TLOG](#) | [EHSLOG](#)  
[PMXLOG](#) | [RFLOG](#) | [GOLOG](#) | [HALOG](#) | [HBLOG](#) | [HCLOG](#) | [MYELOG](#)

actions: [Make an Entry](#) | [Logbook prefs](#) | [Scrollable/printable logbook](#) | [Pending entries](#) | [Administer](#) | [Login](#)

Other Links:

<a href="#">ACE-PR</a>	<a href="#">OPS-PR Query</a>	<a href="#">SWIS</a>
<a href="#">ATLis</a>	<a href="#">Ops Documentation</a>	<a href="#">Software Documentation</a>
<a href="#">AccelTest Plan</a>	<a href="#">Ops Reconfiguration Plans</a>	<a href="#">Whiteboard Schedule</a>
<a href="#">Approved Sweepers List</a>	<a href="#">PD Shift Plans</a>	
<a href="#">Beam Charts</a>	<a href="#">Pager</a>	
<a href="#">Experiment Schedule</a>	<a href="#">Run Coord Weekly Summary</a>	

(If you are unable to select alternate date range...)

Start Date: June 1 2004 0:00 End Date: July 1 2004 0:00

Entry Type(s):  DOWNTIME  LOGENTRY  MDTASK  OPS-PR  TUNE

Logbook: [EHSLOG](#) Sort Order: [DESCENDING](#) Source: [ALL LOGS](#)

Search(?):  in [Titles and Text](#)

number	date	name	type	title
<b>Tuesday</b>				
• <a href="#">1221581</a>	29-Jun-04 15:24	<a href="#">E_Abkemeier</a>	LOGENTRY	<a href="#">Test Plan for Changing Hall C Beam Dump</a>
<b>Monday</b>				
• <a href="#">1221198</a>	28-Jun-04 10:02	<a href="#">P_Hunt</a>	LOGENTRY	<a href="#">EMS audits</a>
<b>Wednesday</b>				
• <a href="#">1220292</a>	23-Jun-04 10:10	<a href="#">J_Jefferson</a>	LOGENTRY	<a href="#">CARM Removal Upgrade</a>
<b>Tuesday</b>				
• <a href="#">1220147</a>	22-Jun-04 15:26	<a href="#">B_May</a>	LOGENTRY	<a href="#">EH&amp;S Occurrence (Accident/Incident) Find:</a>
• <a href="#">1220064</a>	22-Jun-04 09:54	<a href="#">H_Robertson</a>	LOGENTRY	<a href="#">COMPLETED TASK: Penetration stone drops</a>
<b>Monday</b>				
• <a href="#">1219830</a>	21-Jun-04 09:58	<a href="#">J_Faulkner</a>	LOGENTRY	<a href="#">South Linac dropped to Restricted Access</a>
• <a href="#">1219815</a>	21-Jun-04 08:54	<a href="#">B_May</a>	LOGENTRY	<a href="#">VTA crane snags power cable</a>
<b>Friday</b>				
• <a href="#">1219245</a>	18-Jun-04 16:02	<a href="#">P_Hunt</a>	LOGENTRY	<a href="#">EMS Walkthrough</a>
• <a href="#">1219244</a>	18-Jun-04 15:59	<a href="#">S_Singleton</a>	LOGENTRY	<a href="#">Oil Spill Canon Boneyard</a>
<b>Tuesday</b>				

Internet

# Work Control Documents

Template Documents - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address [https://mis.jlab.org/ehs/work\\_control/templates.html](https://mis.jlab.org/ehs/work_control/templates.html) Go Links

## WORK CONTROL DOCUMENTS TEMPLATE INSTRUCTIONS

*Table of contents*

- [Section 1.0 Steps for completing a SOP, OSP, or TOSP](#)
- [Section 2.0 Using a Procedure Template](#)
- [Section 3.0 Using MS Word Formatting](#)

**Current work control documents:**

- Current [SOP's, OSP's, and TOSP's](#) on Docushare
- [Other Work control documents](#)

### 1.0 STEPS FOR COMPLETING AN SOP, OSP, OR TOSP:

---

- Determine whether the procedure needs an [SOP, OSP, or TOSP](#).
- Open a blank document template in MS Word.  
**Click here to open a blank SOP, OSP or TOSP template->** 
- Save the template using the following convention:  
(SOP / OSP / TOSP)\_document\_title-last\_name
- Fill out the document template according to the [2.0 Using a Procedure Template](#) section of this document.
- Print out a copy of your completed document.

Done Internet

# Work Control Document Template

Standard Operating Procedure

1. → **Scope:**  
This Standard Operating Procedure (SOP) outlines specific activities associated with...
2. → **Background:**
3. → **Authority and Responsibility:**
4. → **Hazard Analysis:**

Hazard	Cause	Risk-Code (pre)	Mitigation-Administrative	Mitigation-Engineering	Risk-Code (post)
5. → **Procedures:**
6. → **Personnel Training/Qualification:**
7. → **Other:**
8. → **Attachments:**

# WCD: Hazard ID & Mitigation

Template Documents - Microsoft Internet Explorer

Address: [https://mis.jlab.org/ehs/work\\_control/templates.html](https://mis.jlab.org/ehs/work_control/templates.html)

**11. Hazard Analysis:**  
 Briefly outline potential hazards for personnel or equipment associated with the procedure. Characterize the specific potential hazards, assess the level of risk involved, and note any specific controls that will be used to mitigate the hazard. Controls fall into two types - administrative (ex. ODH monitoring system; personal protective equipment; and written procedures) and engineering (isolating worker from the hazard by using a glovebox; access control system; substituting a less hazardous material for a more hazardous one, shielding, and interlocks). Summarize your hazard assessment in the following table format:

Hazard	Cause	Risk Code (pre)	Mitigation Administrative	Mitigation Engineering	Risk Code (post)
Potential Hazard1	The cause of this specific hazard.	4	How one plans to overcome this hazard.	Specific initiatives to be taken to see this hazard does not become reality.	1

Consult the EH&S Manual, [Section 3210. Hazard Identification and Characterization](#), for the specifics of evaluating hazards, assigning an appropriate risk code to the task, and providing sufficient controls. For questions or clarification, contact a Jefferson Lab safety professional.

If you are assessing **electrical or electronic equipment hazards**, remember to also identify the electrical Mode and Class for the activities performed. See Table 2 below for a list of all JLab potential hazard causes and the EH&S Manual reference for assessment guidance.

Hazard Origin/Type	EH&S Manual Reference (PDF)	Additional Comments
Tools: Hand and Power Machine	<a href="#">Chapter 6120</a> <a href="#">Chapter 6121</a>	
Welding/cutting/brazing/grinding	<a href="#">Chapter 6122</a>	
Ladders & scaffolds	<a href="#">Chapter 6132</a>	
Cranes use	<a href="#">Chapter 6140</a>	
Hoist use	<a href="#">Chapter 6140</a>	
Forklifts used in tunnel	<a href="#">Chapter 6145</a> <a href="#">Chapter 6146</a>	
Aerial work platforms (ManLifts)	<a href="#">Chapter 6147</a>	
Compressed gases Flammable gases	<a href="#">Chapter 6150</a> <a href="#">Chapter 6152</a>	

# WCD: Electronic Copies

Work Control Documents - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://docushare.jlab.org/View/Collection-852 Go Links

DocuShare Guest Login Accounts Contents Search New Help

## Work Control Documents

All work control documents

Edit... Go Add... Go [Search] Within here Search

Appears In: [EH&S](#)

- [EES](#) [whithaus](#) 07/18/2003 6
- [OSP](#) [whithaus](#) 06/24/2003 4  
Operational Safety Procedure
- [RadCon](#) [whithaus](#) 06/24/2003 2  
Radiation Control
- [SOP](#) [whithaus](#) 06/24/2003 4  
Standard Operating Procedures
- [TOSP](#) [whithaus](#) 06/24/2003 4  
Temporary Operational Safety Procedure

Copyright © 1996-2001 Xerox Corporation. All Rights Reserved.

Done Internet

# Documents Management System

The screenshot shows a Microsoft Internet Explorer browser window displaying the DocuShare website. The browser's address bar shows the URL <http://docushare.jlab.org/>. The website header includes a navigation menu with links for [Login](#), [Accounts](#), [Contents](#), [Search](#), [New](#), and [Help](#). The main content area features the Jefferson Lab logo and the text "INSTITUTE FOR SRF SCIENCE AND TECHNOLOGY DOCUSHARE SYSTEM". A sidebar on the left titled "What's New" includes a dropdown menu set to "in the last hour" and a "GO" button. Below this, there are sections for "Login", "Accounts", "Help", and "Site Map". The main content area lists several categories with brief descriptions:

- [Development Projects](#): Progress of major development projects
- [EH&S](#): Information and resources on environment, safety and health
- [Facilities](#): Documentation on our technical facilities
- [Operations Support](#): Support to Accelerator Operations
- [Organizational Information](#): Institute structure, meeting minutes, staff information, etc..
- [Pansophy](#): Pansophy - A system of universal knowledge
- [Presentations](#): Sets of viewgraphs used in oral presentations at Jlab and elsewhere
- [Procedures](#)

The browser's status bar at the bottom indicates "Done" and "Internet".

# Documents Management System

EH&S  
*Information and resources on environment, safety and health*

Edit... Go Add... Go  Within here Search

**Appears In:**

<a href="#">Assessments</a> Assessments by department	<a href="#">whithaus</a>	06/24/2003	8	
<a href="#">EH&amp;S Departments</a> An area for shared documents from each department for archival and informational purposes.	<a href="#">whithaus</a>	06/24/2003	5	
<a href="#">EH&amp;S PMG Highlights</a> EH&S Policies & Manual Group Highlights	<a href="#">prior</a>	11/11/2003	3	
<a href="#">Investigation Reports</a> Includes all types of investigation reports	<a href="#">whithaus</a>	06/24/2003	4	
<a href="#">Monthly Highlights</a> Monthly highlights, listed by calendar year	<a href="#">whithaus</a>	09/12/2003	4	
<a href="#">OSHA External Audit Reports</a> summary of findings from OSHA visits to National Labs	<a href="#">hunt</a>	07/18/2003	3	
<a href="#">Safety Alerts and Notices</a> All safety alerts and notices will be posted here	<a href="#">whithaus</a>	06/24/2003	10	
<a href="#">Work Control Documents</a> All work control documents	<a href="#">whithaus</a>	06/24/2003	5	
<a href="#">What ISMS means</a> Integrated Safety Management at the Institutional and Working levels	<a href="#">reece</a>	03/29/2002	43K	
<a href="#">EH&amp;S Tracking System</a> This is the JLab online system for tracking safety findings.	<a href="#">robertl</a>	04/29/2004	-	

Copyright © 1996-2001 Xerox Corporation. All Rights Reserved.

Done Internet

# Safety Alerts & Notices

Safety Alerts and Notices - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://docushare.jlab.org/View/Collection-860 Go Links

 **DocuShare** [Guest](#) [Login](#) [Accounts](#) [Contents](#) [Search](#) [New](#) [Help](#)

## Safety Alerts and Notices

*All safety alerts and notices will be posted here*

Edit... Go Add... Go Within here Search

**Appears In:** [EH&S](#)

 <a href="#">DOE Electrical Safety</a> DOE report of electrical safety operating experience and lessons learned.	<a href="#">prior</a> 06/01/2004 386K   
 <a href="#">DOE Hoisting and Rigging Events</a> Report of DOE Hoisting and Rigging Operating Experience and Lessons Learned	<a href="#">prior</a> 06/01/2004 1537K   
 <a href="#">Extension Cord Safety at JLab</a> Notice to all staff about safe and unsafe extension cord usage	<a href="#">prior</a> 01/19/2004 434K   
 <a href="#">Fluke Test Leads Recall</a> Recall of test leads sold for use with or as an accessory to Fluke test meters.	<a href="#">prior</a> 05/06/2004 6K  
 <a href="#">Hazards of Acetylene Gas</a> Facts about acetylene gas	<a href="#">prior</a> 04/27/2004 24K   
 <a href="#">Ice Grippers Available Thru Webstock</a> Information on ice grippers selection and ordering thru JLab Stockroom	<a href="#">prior</a> 02/13/2004 102K   
 <a href="#">On Target Briefs - January 27, 2004</a> Summary of JLab weekly activities and EH&S notices	<a href="#">prior</a> 02/26/2004 39K   
 <a href="#">Pump Cart Notice</a> Electrical & maintenance requirements for vacuum pump carts	<a href="#">prior</a> 06/03/2004 61K   
 <a href="#">Safety Notice: Roll-up Door Fire</a> Smithfield Foods roll-up door fire from welding activity	<a href="#">prior</a> 04/27/2004 64K   
 <a href="#">Walking on Snow and Ice Safely</a> Safety Tips for Walking on Snow and Ice	<a href="#">prior</a> 02/09/2004 55K   

Copyright © 1996-2001 Xerox Corporation. All Rights Reserved.

Done Internet

# Search Function

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print TV

Address <https://mis.jlab.org/ehs/tracking/search.php> Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** *tracking, trending, & training*

HOME | SEARCH | CONTACT JLAB Search the EH&S Tracking System

Problems? Questions? Contact an [Administrator](#) Sandra Prior  
View my open findings

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

[Hazards of Acetylene Gas](#)

**Please select a category to search within:**

- Assessments
- Inspections
- Occurrence (Accident/Incident)s
- RDRs

Or:

- [Browse all records between categories](#)

Maintained by: [ingapps@jlab.org](mailto:ingapps@jlab.org)

Jefferson Lab EH&S

[https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC) Internet

# Search By: Findings or Events

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC) Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** Search the EH&S Tracking System

HOME | SEARCH | CONTACT JLAB

3 tracking, trending, & training

Problems? Questions? Contact an [Administrator](#).

Sandra Prior  
[View my open findings](#)

Home  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

[Fluke Test Leads Recall](#)

Please select which results you would like to see:

- Search for all findings from Occurrence (Accident/incident)s
- Search for all Occurrence (Accident/incident) events

Maintained by: [lngaops@jlab.org](mailto:lngaops@jlab.org)

Jefferson Lab EH&S

[https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items) Internet

# Accident/Occurrence Event Search

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items) Go Links

Problems? Questions? Contact an [Administrator](#).

Sandra Prior  
[View my open findings](#)

- Home
- Admin
- Tracking Records
- EH&S Info
- Requirements
- Work Control Docs
- Work Requests
- JIT training
- Help

**SAFETY FIRST**

[Add an Occurrence](#) (Accident/Incident)

**Select any combination of criteria to search by in order to refine your search.**

All items will be sorted by source and logdate.

<b>Search by source:</b>	<input type="text"/>	<input type="button" value="Search &gt;"/>
<b>Search by category:</b>	<input type="text"/>	
<b>Search for keyword(s):</b>	<input type="text"/>	
<b>Search by ISM principal:</b>	<input type="text"/>	
<b>Search by ISM core causes:</b>	<input type="text"/>	
<b>Search by author:</b>	<input type="text"/>	
<b>Search by lead investigator:</b>	<input type="text"/>	
<b>Search by record:</b>	<input type="text"/>	
<b>Search by date:</b>	<input type="radio"/> Logdate <input type="radio"/> Report date <input type="radio"/> Estimated Completion date <input type="radio"/> Closure date	
	Between <input type="text"/>	and <input type="text"/>
<b>Search by division:</b>	<input type="text"/>	
<b>Search by department:</b>	<input type="text"/>	
<b>Search by area:</b>	ARC - Building Management ARC - L104 ARC - L306 ARC - L307 ARC - L309	<input type="button" value="Browse"/>
<b>Search by safety warden:</b>	<input type="text"/>	
<b>Search by responsible manager:</b>	<input type="text"/>	
<b>Search by EH&amp;S reference:</b>	<input type="text"/>	<input type="button" value="Browse"/>
<b>Display list of items:</b>	<input type="radio"/> Open <input type="radio"/> Closed	
<b>Display overdue items?</b>	<input type="radio"/> Yes <input type="radio"/> No	

[Check here to generate a report from the selected criteria in MS Excel](#)

1 Hierarchical Menu Trees Created

Internet

# Accident/Occurrence Event Search

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address: [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items) Go Links

Problems? Questions? Contact an [Administrator](#) Sandra Prior  
View my open findings

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help  
DOE Electrical  
Safety Operating Experience & Lessons Learned

[Add an Occurrence](#) (Accident/Incident)

**Select any combination of criteria to search by in order to refine your search.**

All items will be sorted by source and logdate.

**Search by source:** [Dropdown] Search >

**Search by category:** [Dropdown]

**Search for keyword(s):** [Text] [Dropdown]

**Search by ISM principal:** [Dropdown]

**Search by ISM core causes:** [Dropdown]

**Search by author:** [Dropdown]

**Search by lead investigator:** [Dropdown]

**Search by record:** [Dropdown]

**Search by date:**  
 Logdate [Dropdown] [Dropdown] [Dropdown]  
 Report date  
 Estimated Completion date Between [Text] [Calendar] and [Text] [Calendar]  
 Closure date

**Search by division:** [Dropdown]

**Search by department:** [Dropdown]

**Search by area:**  
Ctrl click to select multiple areas  
ARC - Building Management  
ARC - L104  
ARC - L306  
ARC - L307  
ARC - L309 [Dropdown] Browse

**Search by safety warden:** [Dropdown]

**Search by responsible manager:** [Dropdown]

**Search by EH&S reference:** [Dropdown] [Dropdown] [Dropdown] Browse

**Display list of items:**  Open  Closed

**Display overdue items?**  Yes  No

Check here to generate a report from the selected criteria in MS Excel

Reset Search >

1 Hierarchical Menu Trees Created Internet

# Accident/Occurrence Event Search

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items) Go Links

Problems? Questions? Contact an [Administrator](#) Sandra Prior  
View my open findings

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

[Safety Notice: Roll-up Door Fire](#)

[Add an Occurrence](#) (Accident/Incident)

**Select any combination of criteria to search by in order to refine your search.**

All items will be sorted by source and logdate.

**Search by source:** [Dropdown] [Search >]

**Search by category:** [Dropdown]

**Search for keyword(s):** [Text]

**Search by ISM principal:** [Dropdown]

**Search by ISM core causes:** [Dropdown]

**Search by author:** [Text]

**Search by lead investigator:** [Text]

**Search by record:** [Text]

**Search by date:**  
 Logdate  
 Report date  
 Estimated Completion date  
 Closure date

**Search by division:** [Text]

**Search by department:** [Text]

**Search by area:**  
\*Ctrl click to select multiple areas  
[List: Fire / Explosion, Radioactive Material - loss of control, Violation / Inadequate procedures, Operations, Environmental, Facility Safety, Agreement / Compliance, Personnel Safety, Radiation Exposure, Security, Substance Abuse, Facility or system / component damage, Facility Status, Cross-Category - Near Miss, Head, Back, Extremity, Hand, Foot, Face, Eye, Other] [Browse]

**Search by safety warden:** [Dropdown]

**Search by responsible manager:** [Dropdown]

**Search by EH&S reference:** [Text] [Browse]

**Display list of items:**  
 Open  Closed

**Display overdue items?**  
 Yes  No

Check here to generate a report from the selected criteria in MS Excel

[Reset] [Search >]

1 Hierarchical Menu Trees Created

Internet

# Accident/Occurrence Event Search

The screenshot shows a web browser window titled "Search the EH&S Tracking System - Microsoft Internet Explorer". The address bar contains the URL: [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items). The page content includes a navigation menu on the left with items like Home, Admin, Tracking Records, EH&S Info, Requirements, Work Control Docs, Work Requests, JIT training, and Help. The main content area features a search interface with the following sections:

- Search by source:** A dropdown menu and a "Search >" button.
- Search by category:** A dropdown menu.
- Search for keyword(s):** A text input field.
- Search by ISM principal:** A dropdown menu.
- Search by ISM core causes:** A dropdown menu with a list of causes: Failure to Define Scope of Work, Failure to Analyze Hazards, Failure to Develop and Implement Hazard Controls, Failure to Perform Work Within Controls, and Failure to Provide Feedback and Continuous Improvement.
- Search by author:** A dropdown menu.
- Search by lead investigator:** A dropdown menu.
- Search by record:** A dropdown menu.
- Search by date:** Radio buttons for Logdate, Report date, Estimated Completion date, and Closure date. A date range selector with "Between" and "and" labels and calendar icons.
- Search by division:** A dropdown menu.
- Search by department:** A dropdown menu.
- Search by area:** A list of areas: ARC - Building Management, ARC - L104, ARC - L306, ARC - L307, and ARC - L309. A "Browse" button.
- Search by safety warden:** A dropdown menu.
- Search by responsible manager:** A dropdown menu.
- Search by EH&S reference:** A date range selector with dropdown menus for the start and end dates.
- Display list of items:** Radio buttons for Open and Closed.
- Display overdue items?:** Radio buttons for Yes and No.

Below the search form, there is a checkbox labeled "Check here to generate a report from the selected criteria in MS Excel". At the bottom of the search area are "Reset" and "Search >" buttons.

The browser's status bar at the bottom shows "1 Hierarchical Menu Trees Created" and "Internet".

# Accident/Occurrence Event Search

Search the EH&S Tracking System - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=OCC&return=items](https://mis.jlab.org/ehs/tracking/search.php?search_type=OCC&return=items) Go Links

Problems? Questions? Contact an [Administrator](#)

Sandra Prior  
View my open findings

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

[Report April 2004](#)

[Add an Occurrence](#) (Accident/Incident)

**Select any combination of criteria to search by in order to refine your search.**

All items will be sorted by source and logdate.

<b>Search by source:</b>	<input type="text"/>	<input type="button" value="Search &gt;"/>
<b>Search by category:</b>	<input type="text"/>	
<b>Search for keyword(s):</b>	<input type="text"/>	
<b>Search by ISM principal:</b>	<input type="text"/>	
<b>Search by ISM core causes:</b>	<input type="text"/>	
<b>Search by author:</b>	<input type="text"/>	
<b>Search by lead investigator:</b>	<input type="text"/>	
<b>Search by record:</b>	<input type="text"/>	
<b>Search by date:</b>	<input type="text"/> <input type="text"/>	
<input type="radio"/> Logdate		
<input type="radio"/> Report date		
<input type="radio"/> Estimated Completion date	Between <input type="text"/> and <input type="text"/>	
<input type="radio"/> Closure date		
<b>Search by division:</b>	<input type="text"/>	
<b>Search by department:</b>	<input type="text"/>	
<b>Search by area:</b>	Test Lab - Survey Lab, Rm 14 Test Lab - Tensile Test and Storage Areas (Rms 321, 322) <b>Test Lab - VTA (Rm 150, 151, 152)</b> Test Lab - Vacuum Assembly (Rm, 300) Test Lab - Vacuum Furnace and Brazing (Rm 264 - 266)	<input type="button" value="Browse"/>
<small>*Ctrl click to select multiple areas</small>		
<b>Search by safety warden:</b>	<input type="text"/>	
<b>Search by responsible manager:</b>	<input type="text"/>	
<b>Search by EH&amp;S reference:</b>	<input type="text"/>	<input type="button" value="Browse"/>
<b>Display list of items:</b>	<input type="radio"/> Open <input type="radio"/> Closed	
<b>Display overdue items?</b>	<input type="radio"/> Yes <input type="radio"/> No	

Check here to generate a report from the selected criteria in MS Excel

1 Hierarchical Menu Trees Created

Internet

# Search Results: Vertical Test Area

Search results for events - Microsoft Internet Explorer

Address: [https://mis.jlab.org/ehs/tracking/item\\_search\\_list.php?search\\_type=OCC&item\\_type=2&occ\\_source=&occ\\_category=&keywords=&ism\\_principal=&ism\\_cause=&author=&originator=&item\\_id](https://mis.jlab.org/ehs/tracking/item_search_list.php?search_type=OCC&item_type=2&occ_source=&occ_category=&keywords=&ism_principal=&ism_cause=&author=&originator=&item_id)

Privacy and Security Notice    Optimized for IE 5+ and Netscape 6+

**Jefferson Lab**    Search results for events    tracking, trending, & training

HOME | SEARCH | CONTACT JLAB    Sandra Prior  
View my open findings

Problems? Questions? Contact an [Administrator](#).

[Home](#)  
[Admin](#)  
[Tracking Records](#)  
[EH&S Info](#)  
[Requirements](#)  
[Work Control Docs](#)  
[Work Requests](#)  
[JIT training](#)  
[Help](#)

- [Add an event](#)
- [Search for other Occurrence \(Accident/Incident\) events](#)
- [New Search](#)

Found: 5 event(s)

[Click on the event number to see the full details.](#)

DELETE	EVENT #	TITLE	AREA	SOURCE	EVENT DATE	FINDINGS
<input type="checkbox"/>	<a href="#">OR-2004-11</a>	Unauthorized Modification of Safety Interlock System for Accelerator Component RF Testing	Test Lab - VTA (Rm 150, 151, 152)	Occurrence	MAY 05, 04	1 of 9 open
<input type="checkbox"/>	<a href="#">OR-2002-07</a>	Failure to Verify LOTO at VTA	Test Lab - VTA (Rm 150, 151, 152)	Occurrence	OCT 03, 02	0 of 5 open
<input type="checkbox"/>	<a href="#">NE-2003-09</a> <small>No Report</small>	VTA HEPA Filter Overheated	Test Lab - VTA (Rm 150, 151, 152)	Notable Event	MAY 08, 03	1 of 1 open
<input type="checkbox"/>	<a href="#">NE-2002-02</a>	VTA Radiation Alarm	Test Lab - VTA (Rm 150, 151, 152)	Notable Event	MAY 01, 02	0 of 10 open
<input type="checkbox"/>	<a href="#">AI-2003-17</a>	Test Lab VTA back injury	Test Lab - VTA (Rm 150, 151, 152)	Accident/Incident	AUG 26, 03	0 of 1 open

[Back to top](#)

Maintained by: [ingapps@jlab.org](mailto:ingapps@jlab.org)




Address: [https://mis.jlab.org/ehs/tracking/view\\_item.php?item\\_id=2966](https://mis.jlab.org/ehs/tracking/view_item.php?item_id=2966)    Internet

# Occurrence Record: PSS Interlocks

EH&S Event: OR-2004-11 - Microsoft Internet Explorer

Address: [https://mis.jlab.org/ehs/tracking/view\\_item.php?item\\_id=2966&view\\_findings=list](https://mis.jlab.org/ehs/tracking/view_item.php?item_id=2966&view_findings=list)

Problems? Questions? Contact an [Administrator](#)

Sandra Prior  
View my open findings

Home

Admin

Tracking Records

EH&S Info

Requirements

Work Control Docs

Work Requests

JIT training

Help

[Radio on work Permit for Accelerator Site 2004](#)

Only the author, lead investigator, or an Administrator can edit this event record.

**Actions**

- [Return to search results](#)
- [Add a new event to the database](#)
- [Search for other Occurrence \(Accident/Incident\) events](#)
- [New Search](#)

**Event Number:** OR-2004-11  
**Event Type:** Occurrence (Accident/Incident)  
 Created: JUN 14, 04

**Title:** Unauthorized Modification of Safety Interlock System for Accelerator Component RF Testing  
**Author:** [Prior, Sandra](#)

**Event date:** MAY 05, 04 [Edit Event](#)

**Lead investigator:** [Mutton, Philip](#)

**Division:** ACCELERATOR

**Department:** SRF Institute

**Area:** Test Lab - VTA (Rm 150, 151, 152)

**Safety Warden:** [Kushnick, Peter](#)

**Source:** Occurrence

**Category:** Facility Safety

**Event Description:** An ISRF worker noted that a metal plate had been attached to an actuator bracket in the Dewar #3 shield lid. The actuator contains a pair of switches that in turn send a signal to the PSS that the equipment can be safely operated. The worker quickly recognized the addition of the metal plate to the actuator as an unauthorized modification to the PSS. The worker noted a similar modification had been made to the Dewar #6 shield lid actuator.

**Report Link:** [http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA\\_Dewar\\_Switch\\_040505-1\\_rtm.doc](http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA_Dewar_Switch_040505-1_rtm.doc)

[Delete Event](#)

**9 Finding(s) for this item:**

View as:  List  Individual Findings [Add a Finding](#)

Click on the finding number to see the full details of the record

Delete	Finding Number	Finding Description	Responsible Manager	Completion Date	Closure Date
<input type="checkbox"/>	<a href="#">OR-2004-11-01</a>	Unauthorized modification to PSS.	<a href="#">Funk, L.</a>	MAY 06, 04	MAY 06, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-02</a>	VTA personnel did not follow SOP for VTA operations and failed to alert SSG staff of problems with the shield interlock switch.	<a href="#">Funk, L.</a>	MAY 10, 04	MAY 10, 04

1 Hierarchical Menu Trees Created

# Occurrence Record: PSS Interlocks

http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA\_Dewar\_Switch\_040505-1\_rtm.doc - Microsoft Internet Explorer

File Edit View Insert Format Tools Table Go To Favorites Help

Address http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA\_Dewar\_Switch\_040505-1\_rtm.doc

## Notable Event Worksheet

This form is to be completed by the Division EH&S Officer or a designated line manager within three days of an event and provided to the EH&S Reporting Manager. References to applicable EH&S Manual guidance should be included.

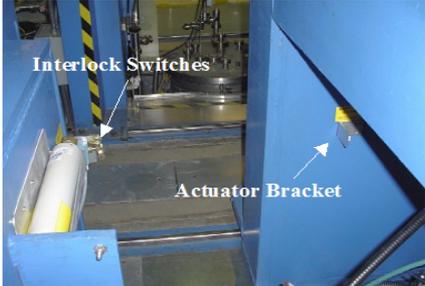
Division: Accelerator → Dept./Hall/Group: SRF

### SUMMARY OF EVENT:

The following describes a two-part event:

- #1: unauthorized modification of PSS hardware
- #2: high likelihood of consequential inadvertent operation a radiation generating device (RGD), namely dewar No. 6, without functional primary engineered safeguard.

A VTA operator, Ann Marie Valente, was preparing to run a test in Dewar 3 in the Vertical Test Area (VTA) in the Test Lab on Wednesday May 5<sup>th</sup> 2004 at approximately 4:45 p.m. She noticed that if the lid were closed, a safety interlock switch actuator in the shield lid would interfere with a Residual Gas Analyzer (RGA) that was part of the test setup. The operator requested assistance to resolve the problem and I was called to the VTA to assess the situation. The actuator is a bracket that is part of the VTA Personnel Safety System (PSS). It is attached to the inside of the shield lid such that when the lid is closed it contacts a pair of switches, which in turn send a signal to the PSS.



The photograph shows a close-up of the interlock system. Two white cylindrical interlock switches are mounted on a blue metal structure. A white arrow points to the switches, and another white arrow points to a blue actuator bracket. The background shows a complex industrial environment with various pipes and machinery.

This closure signal is one of the conditions that the safety interlock system must detect prior to providing an rf permit signal to the controller for the high power rf amplifier. Therefore when the dewar is open, i.e. the radiation shield is not in place, it is not possible to generate high power rf or radiation.

A plate had been attached to the actuator bracket effectively reducing the spacing between the actuator and

Unknown Zone

# Findings View – As A List

EH&S Event: OR-2004-11 - Microsoft Internet Explorer

Address: [https://mis.jlab.org/ehs/tracking/view\\_item.php?item\\_id=2966&view\\_findings=list](https://mis.jlab.org/ehs/tracking/view_item.php?item_id=2966&view_findings=list)

switches that in turn send a signal to the PSS that the equipment can be safely operated. The worker quickly recognized the addition of the metal plate to the actuator as an unauthorized modification to the PSS. The worker noted a similar modification had been made to the Dewar #6 shield lid actuator.

**Report Link:** [http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA\\_Dewar\\_Switch\\_040505-1\\_rtm.doc](http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA_Dewar_Switch_040505-1_rtm.doc)

Delete Event

**9 Finding(s) for this item:** Add a Finding

View as:  List  Individual Findings

Click on the finding number to see the full details of the record

Delete	Finding Number	Finding Description	Responsible Manager	Completion Date	Closure Date
<input type="checkbox"/>	<a href="#">OR-2004-11-01</a>	Unauthorized modification to PSS.	<a href="#">Funk, L.</a>	MAY 06, 04	MAY 06, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-02</a>	VTA personnel did not follow SOP for VTA operations and failed to alert SSG staff of problems with the shield interlock switch	<a href="#">Funk, L.</a>	MAY 10, 04	MAY 10, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-03</a>	Shield lid interlock switches do not function correctly which led to unauthorized modification.	<a href="#">Mahoney, Kelly</a>	MAY 06, 04	MAY 06, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-04</a>	Verify that radiation levels remained consistent with normal operations in lieu of the unauthorized modification.	<a href="#">Abkemeier, Erik</a>	MAY 28, 04	MAY 20, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-05</a>	Verify that personnel exposures were consistent with normal operations.	<a href="#">Abkemeier, Erik</a>	MAY 28, 04	MAY 25, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-06</a>	Maintenance plans and procedures failed to ensure reliable operations of the shield lids.	<a href="#">Mutton, Philip</a>	MAY 19, 04	MAY 19, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-07</a>	RCG did not notify SSG when configuration controlled safety equipment had been modified.	<a href="#">Abkemeier, Erik</a>	MAY 25, 04	MAY 25, 04
<input type="checkbox"/>	<a href="#">OR-2004-11-08</a>	Alignment of shield interlock switches is too critical to the reliable performance of the switches.	<a href="#">Mahoney, Kelly</a>	OCT 31, 04	open
<input type="checkbox"/>	<a href="#">OR-2004-11-09</a>	An additional safety measure is needed to ensure reliable function of the shield interlock switches until the switches are replaced.	<a href="#">Mutton, Philip</a>	MAY 28, 04	MAY 25, 04

Delete Findings

Back to top

Maintained by: [inapps@lab.org](mailto:inapps@lab.org)

1 Hierarchical Menu Trees Created

Internet

# Findings View – Individually

EH&S Event: OR-2004-11 - Microsoft Internet Explorer

Address [https://mis.jlab.org/ehs/tracking/view\\_item.php?item\\_id=2966&view\\_findings=indv](https://mis.jlab.org/ehs/tracking/view_item.php?item_id=2966&view_findings=indv)

Report Link: [http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA\\_Dewar\\_Switch\\_040505-1\\_rtm.doc](http://docushare.jlab.org/Get/File-8579/NotableEventWS-VTA_Dewar_Switch_040505-1_rtm.doc)

Delete Event

**9 Finding(s) for this item:**

View as:  List  Individual Findings

Add a Finding

Only the author, lead investigator, or an Administrator can edit this finding. All other users may add status updates to this record if it is NOT closed. 1 of 9

Finding Number: OR-2004-11-01  
Created: JUN 14, 04

Responsible Manager: [Funk, L.](#) Edit Finding

Finding Description: Unauthorized modification to PSS.

Recommended Corrective Action: Suspend all test and development RF operations in the VTA pending resolution of the event issues.

ISM Principal: Operations Authorization  
ISM Cause: Failure to Perform Work Within Controls  
Estimated Completion Date: MAY 06, 04  
Closure Date: MAY 06, 04

Delete Finding

**0 Status Update(s) for this finding:** Add a status update

Delete	Date	Description	Author
--------	------	-------------	--------

Delete Updates

Back to top

Maintained by: [inagpps@lab.org](mailto:inagpps@lab.org)

Jefferson Lab EH&S

1 Hierarchical Menu Trees Created Internet

# Excel Download of Search Results

Search the EH&S Tracking System - Microsoft Internet Explorer

Address: [https://mis.jlab.org/ehs/tracking/search.php?search\\_type=ASMT&return=findings](https://mis.jlab.org/ehs/tracking/search.php?search_type=ASMT&return=findings)

Privacy and Security Notice | Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** Search the EH&S Tracking System

Tracking, trending, & training

Sandra Prior  
View my open findings

Problems? Questions? Contact an [Administrator](#).

**Home**  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

[Excel](#)

**Select any combination of the following criteria to search by in order to refine your search.**

All findings will be sorted by date of Assessment

**Search by author:**  
**Search by evaluator:**  
**Search for keyword(s):**  
**Search by record:**  
**Search by date:**  
 Logdate  
 Report date  
 Estimated Completion date  
 Closure date  
**Search by type:**  
**Search by division:**  
**Search by department:**  
**Search by responsible manager:**  
**Display list of items:**  Open  Closed  
**Display overdue items?**  Yes  No

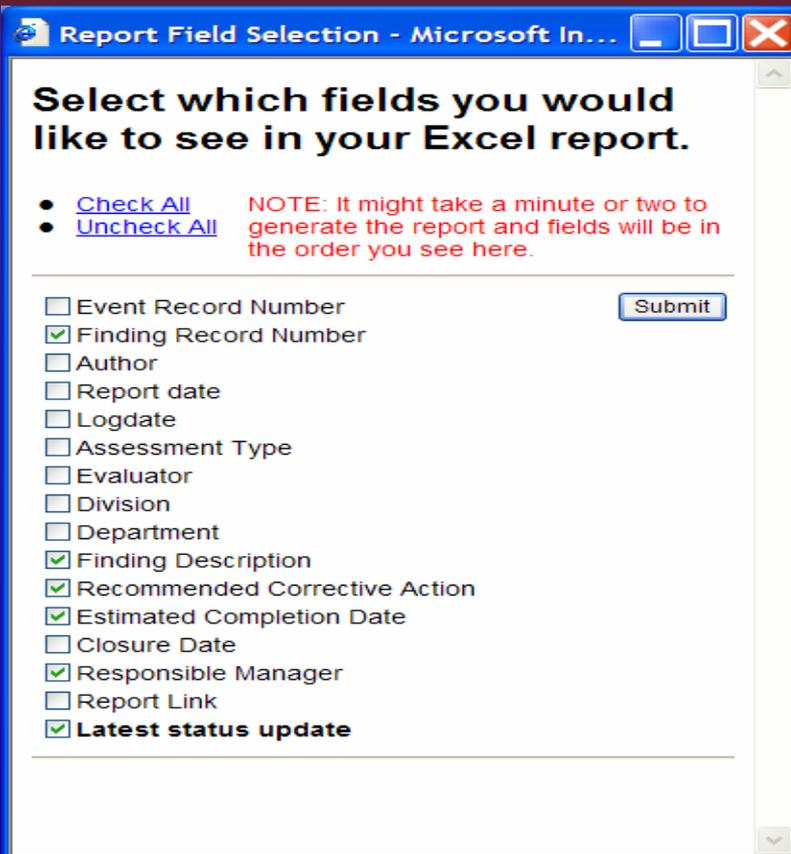
Check here to generate a report from the selected criteria in MS Excel

Reset Search >

Maintained by: [inapps@jlab.org](mailto:inapps@jlab.org)

1 Hierarchical Menu Trees Created | Internet

# Excel Download of Search Results



Report Field Selection - Microsoft In...

Select which fields you would like to see in your Excel report.

- [Check All](#)
- [Uncheck All](#)

NOTE: It might take a minute or two to generate the report and fields will be in the order you see here.

Event Record Number

Finding Record Number

Author

Report date

Logdate

Assessment Type

Evaluator

Division

Department

Finding Description

Recommended Corrective Action

Estimated Completion Date

Closure Date

Responsible Manager

Report Link

**Latest status update**

Submit

- Pop up box appears with field list
- User checks the fields desired in the spreadsheet
- Click on the submit button and search results open up in Excel

# More...Graphs & Charts

EH&S Tracking Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <https://mis.jlab.org/ehs/index.php> Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** **EH&S Tracking Home**

HOME | SEARCH | CONTACT JLAB

3  
Tracking, trending, & training

Sandra Prior  
[View my open findings](#)

Problems? Questions? Contact an [Administrator](#).

Home  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help  
[Back on work Permit for Accelerator Site 2004](#)

**Welcome, Sandra, to the EH&S Tracking System.**

What would you like to do?

- [Show me all open items assigned to me.](#)
- Show me all inspection items for area:
- [Take me to the search page.](#)
- [I would like to add a record.](#)

Our EH&S tracking and reporting mechanisms, presented at the the international [IRIA conference](#), have been selected as a categorical winner by the National Registry of Environmental Professionals.

**Lessons Learned**

**Finding: [NE-2003-23-03](#)**  
The potential exists for unauthorized individuals for operating equipment affecting discharges to groundwater.

**Current Status**

**EH&S Tracking Items**  
(Count of Open Findings)

Inspections	105
(Accident/Incidents)	11
Assessments	98
RDRs	3

[More...](#)

Maintained by: [ingapcs@jlab.org](mailto:ingapcs@jlab.org)

<https://mis.jlab.org/ehs/images/graphs/index.php> Internet

# More...Graphs & Charts

EH&S Tracking Graphs - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print TV

Address <https://mis.jlab.org/ehs/images/graphs/index.php> Go Links

[Privacy and Security Notice](#) Optimized for IE 5+ and Netscape 6+

**Jefferson Lab** **EH&S Tracking Graphs**

HOME | SEARCH | CONTACT JLAB

tracking, trending, & training

Problems? Questions? Contact an [Administrator](#).

Sandra Prior  
[View my open findings](#)

Home  
Admin  
Tracking Records  
EH&S Info  
Requirements  
Work Control Docs  
Work Requests  
JIT training  
Help

**SAFETY FIRST**

## What kinds of graphs or reports would you like to see?

Tell me... [ingapps@jlab.org](mailto:ingapps@jlab.org)

### Graphs

- [Average Days to Close Inspection Findings](#)
- [Average Months Overdue for closed Inspection Findings](#)
- [Percentage of findings by Department](#)
- [Percentage of findings by EH&S Manual Chapter](#)

### Quick Reports

Select a Report to view:

- Open Findings per Division/Department
- Avg Months Overdue per Division/Department
- Avg Number of days left to close open findings per Division/Department

Maintained by: [ingapps@jlab.org](mailto:ingapps@jlab.org)

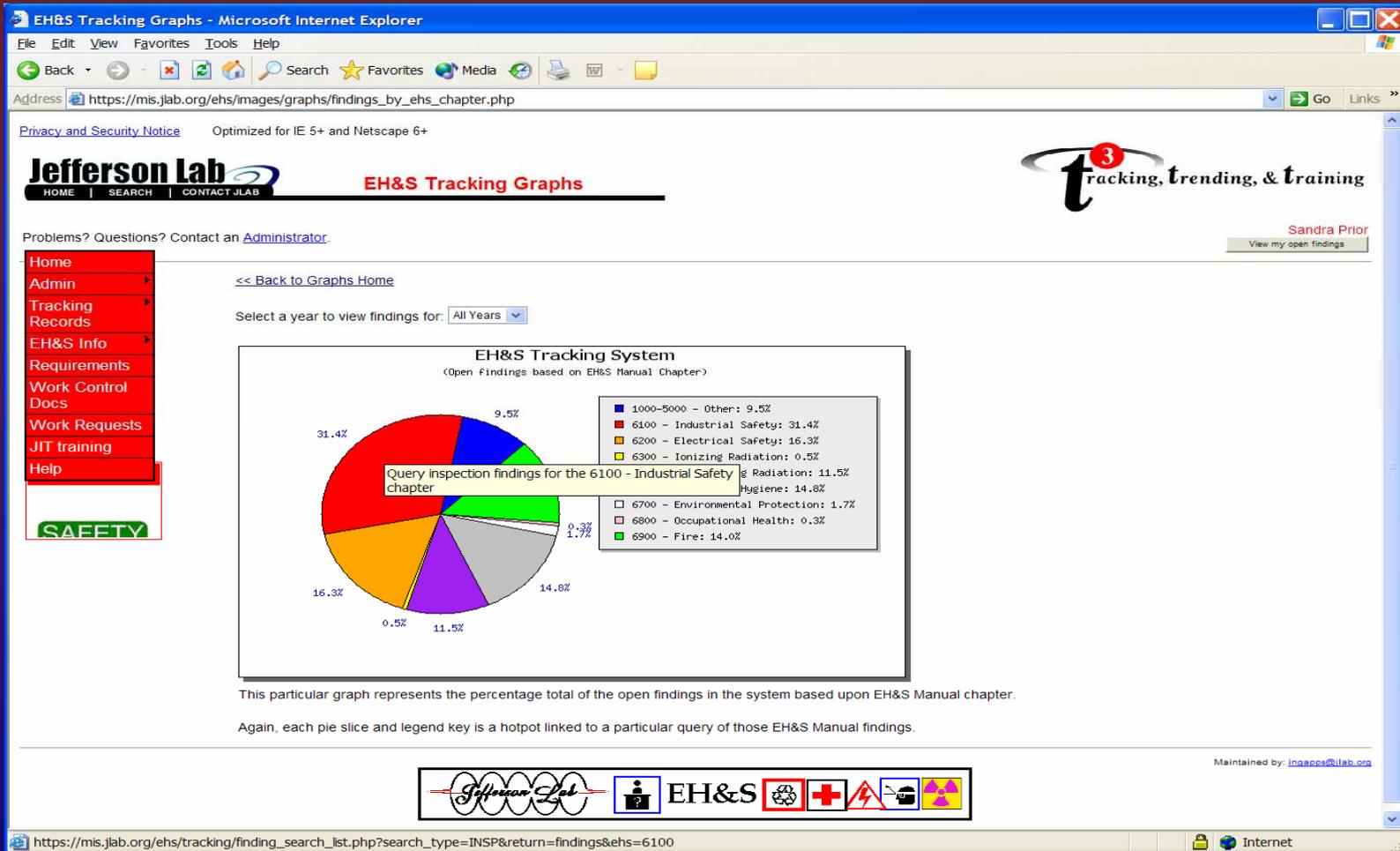
1 Hierarchical Menu Trees Created

Internet

# Closure Stats for Inspection Items



# Findings Distribution by Functional Area



# Findings Distribution Across Lab By Department

https://mis.jlab.org/ehs/images/graphs/view\_report.php?report\_name=Open+Findings+per+Division/D - Microsoft Internet Explorer

Address: https://mis.jlab.org/ehs/images/graphs/view\_report.php?report\_name=Open+Findings+per+Division%2FDepartment

Open Findings per Division/Department

	Department	Inspections	Accident/Incidents	Assessments	RDRs
ACCELERATOR	Acc. Engineering	7	3	5	0
	Acc. Operations	36	0	5	0
	Acc. EH&S	2	3	36	3
	SRF Institute	24	5	3	0
	FEL	25	0	3	0
	CASA	0	0	0	0
	Projects	0	0	0	0
	Acc. Division Office	8	0	0	0
PHYSICS	Physics Division Office	1	0	11	0
	Hall A	0	0	0	0
	Hall B	0	0	4	0
	Hall C	0	0	0	0
	Physics EH&S	0	0	0	0
	QA	0	0	0	0
	Theory Group	0	0	0	0
	Data Acquisition	0	0	0	0
	Electronics Group	0	0	0	0
	Computer Center	0	0	0	0
	Polarized Target	0	0	1	0
	Detector Group	0	0	0	0
	User Liaison	0	0	0	0
	Electronic Media	0	0	0	0
ADMINISTRATION	Admin Division Office	0	0	2	0
	Procurement	0	0	0	0
	Medical Services	0	0	1	0
	Facilities Management	1	0	11	0
	Finance	1	0	0	0

Done Internet

# Operations Problem Reporting (OPS-PR)

http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr\_query.php?PHPSESSID=3781370d04385bffe0a9ccc110 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr\_query.php?PHPSESSID=3781370d04385bffe0a9ccc1106df78b

**Fields to Return:**

<input type="checkbox"/> Creation time	<input type="checkbox"/> Entry type	<input type="checkbox"/> Logbook(s)	<input type="checkbox"/> Title
<input type="checkbox"/> Username(s)	<input type="checkbox"/> Originating host	<input type="checkbox"/> OS account	
<hr/>			
<input type="checkbox"/> Area	<input type="checkbox"/> Component	<input type="checkbox"/> System	<input type="checkbox"/> Problem
<input type="checkbox"/> Timestamp	<input type="checkbox"/> Assignee	<input type="checkbox"/> Action by	<input type="checkbox"/> Annotation/Solution
<input type="checkbox"/> Action			
<hr/>			
<input type="checkbox"/> Time Down	<input type="checkbox"/> Time Up	<input type="checkbox"/> Time Restored	<input type="checkbox"/> Time until Up
<input type="checkbox"/> Time until Restore	<input type="checkbox"/> Time between Up and Restore		
<hr/>			
<input type="checkbox"/> Official Time Down	<input type="checkbox"/> Official Time Up	<input type="checkbox"/> Official Time Restored	<input type="checkbox"/> Downtime
<input type="checkbox"/> Recovery Time	<input type="checkbox"/> Total Time	<input type="checkbox"/> System	<input type="checkbox"/> Item
<input type="checkbox"/> Problem	<input type="checkbox"/> Description	<input type="checkbox"/> Note	

CONTROLS     ELOG fields     DOWNTIME fields     Official DOWNTIME fields

CRYO

DIAGNOSTICS

EHS

ENDSTATIONS

GUN

HALL A

HALL B

HALL C

INJECTOR

MAGNETS

MISC

OPS

OPTICS

PLANTENG

RADCON

RF

SAFETY

SAFETY BELS

SAFETY MFS

SAFETY ODH

SAFETY PSS

SOFTWARE

SRF

TEST

VACUUM

Select One...

Select One...

Start: 23 2004 0:00 End Date: July 1 2004 0:00

MERGE  OPEN  REASSIGN  UPDATE

ers only.

PS-PRs.

igned to:

ea:

Component:

blem:

blem category:

Retrieve Official Downtime. Include Entries w/o OPS-PR.

Include subcategories when applicable?

Done Internet

# Operations Problem Reporting (OPS-PR)

Address: [http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr\\_query.php?PHPSESSID=3781370d04385bffe0a9ccc1106df78b](http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr_query.php?PHPSESSID=3781370d04385bffe0a9ccc1106df78b)

Action

Time Down     Time Up     Time Restored     Time until Up

Time until Restore     Time between Up and Restore

RM RM41  
RM RM42  
 CRM RM43  
 RM RM44  
 RM RM45  
 RM RM46  
RM RM47  
RM RM48

SAFETY  
SCAN IT  
SEE

**Basic**  
SOFTWARE  
SOFTWARE BPM  
SOFTWARE HALL

**Logb**  
SOFTWARE INFO TOOLS  
SOFTWARE INJ  
SOFTWARE MAGNETS  
SOFTWARE MEDM  
SOFTWARE OPTICS TOOLS

**Pre**  
SOFTWARE RF  
SRFvacuum  
SWIS Announcement Editor  
Safety System Status (tcl)  
Scanner  
Scanner BOX SUPPLY SCANNER  
Scanner FEL BOX SUPPLY SCANNER  
Scanner FEL SHUNT SCANNER  
Scanner FEL TRIM SCANNER  
Scanner Other  
Scanner SHUNT SCANNER

Restored     Downtime  
 Item

Fields     Official DOWNTIME fields

Start: July 1 2004 0:00

ATE

Find all OPS-PRs in problem:

Find all OPS-PRs in problem category:

Retrieve Official Downtime. Include Entries w/o OPS-PR.

Include subcategories when applicable?

**Output Preference:**  
 HTML Table     Excel Spreadsheet     Scrollable Output

# Operations Problem Reporting (OPS-PR)

http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr\_query.php?PHPSESSID=3781370d04385bffe0a9ccc1106df78b - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://opweb.acc.jlab.org/CSUEApps/elog02/ops-pr\_query.php?PHPSESSID=3781370d04385bffe0a9ccc1106df78b Go Links

J Ludwig  
 J Musson  
 J Preble  
 J Sage  
 J Wilson  
 K Capek  
 K Cole  
 K Mahoney  
 K Welch  
 K White  
 L Broecker  
 L Clancy  
 L Harris  
 L Reynolds  
 M Backley  
 M Joyce  
 M Keesee  
 M Poelker  
 M Spata  
 M Stutzman  
 M Tiefenback  
 M Washington  
 N Okay  
 N Wilson  
 O Garza  
 P Chevtsov  
 P Francis  
 P Gueye  
 P Hunt  
 P Kjeldsen  
 K Mahoney

Time Up  Time Restored  Time until Up

Time between Up and Restore

Official Time Up  Official Time Restored  Downtime

Total Time  System  Item

Description  Note

ELOG fields  DOWNTIME fields  Official DOWNTIME fields

Start: 23 2004 0:00 End Date: July 1 2004 0:00

MERGE  OPEN  REASSIGN  UPDATE

Find all OPS-PRs in area:

Find all OPS-PRs in component:

Find all OPS-PRs in problem:

Find all OPS-PRs in problem category:

Retrieve Official Downtime. Include Entries w/o OPS-PR.

Include subcategories when applicable?

Output Preference:  
 HTML Table  Excel Spreadsheet  Scrollable Output

# Safety System Group & EH&ST3 Web Pages

Safety Systems Group - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://www.jlab.org/accel/ssg/

Privacy and Security Notice

**Jefferson Lab**  
Jefferson Lab

**S Safety Systems Group**

HOME SEARCH CONTACT JLAB

- ▶ SSG Home
- ▶ Personnel Safety System
- ▶ Machine Protection System
- ▶ Beam Envelope Limit System
- ▶ Fast Protect Systems
- ▶ New Initiatives
- ▶ USPAS Course
- ▶ Internal Only
  - ▶ SSG
  - ▶ User Info & Training
- ▶ The SSG Team
- ▶ Publications
- ▶ Online Forms
- ▶ Links
- ▶ Site Index

The Safety Systems Group provides the Personnel Safety Systems (PSS) and the Machine Protection Systems (MPS) for the CEBAF and FEL accelerators, as well as the experimental endstations.

The group is involved in research in the use of programmable electronics for safety applications and was the first to use Programmable Logic Controllers (PLC) in a large scale accelerator radiation protection system. The group's expertise extends to risk and reliability analysis, fail safe design, programming techniques, and development of standards and practices.



Email us at [ssg\\_list@jlab.org](mailto:ssg_list@jlab.org)

maintained by [accs@jlab.org](mailto:accs@jlab.org)

http://www.jlab.org/index.html

T3 - Tracking, Trending, and Training - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://www.jlab.org/accel/T3/

Privacy and Security Notice

**Jefferson Lab**  
Jefferson Lab

HOME SEARCH CONTACT JLAB T3 - Tracking, Trending & Training

**T<sup>3</sup> tracking, trending, & training**





EH&S T3 (Tracking, Trending and Training) monitors the safety performance of the Lab and its work areas within.

We track different EH&S related items and the corrective actions that come from these items. By observing the lessons learned from this information, we hope to accurately recognize trends in the way that work gets done at the Lab and hope to make this work as safe as possible.

Many of these items are also closely monitored by the DOE in order to help other research facilities avoid potential safety problems and require certain documentation and/or recordkeeping requirements.

- o [EH&S Online Tracking Database](#)
- o [EH&S Electronic Logbook](#)
- o [Training & Performance Office](#)
- o [Accelerator Division](#)
- o [EH&S Department](#)

**Personnel:**  
Sandy Prior - [prior@jlab.org](mailto:prior@jlab.org)

Done

# What is Your Legal Basis?

Sandra L. Prior, REM, CHMM  
System Safety and Safety Systems for  
Accelerators

US Particle Accelerator School  
June 28 – July 2, 2004

# What is Your Legal Basis?

California

Illinois

New Mexico

Tennessee

New York

Utah

Brazil

DOE



State Occupational Safety and Health Plans - Microsoft Internet Explorer

Address http://www.osha.gov/fso/osp/

U.S. Department of Labor  
Occupational Safety & Health Administration  
www.osha.gov

June 30, 2004

Site Index: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

## State Occupational Safety and Health Plans

Section 18 of the Occupational Safety and Health Act of 1970 (the Act) encourages States to develop and operate their own job safety and health programs. OSHA approves and monitors State plans. The following states have approved State Plans:

<a href="#">Alaska</a>	<a href="#">Arizona</a>	<a href="#">California</a>	<a href="#">Connecticut</a>
<a href="#">Hawaii</a>	<a href="#">Indiana</a>	<a href="#">Iowa</a>	<a href="#">Kentucky</a>
<a href="#">Maryland</a>	<a href="#">Michigan</a>	<a href="#">Minnesota</a>	<a href="#">Nevada</a>
<a href="#">New Jersey</a>	<a href="#">New Mexico</a>	<a href="#">New York</a>	<a href="#">North Carolina</a>
<a href="#">Oregon</a>	<a href="#">Puerto Rico</a>	<a href="#">South Carolina</a>	<a href="#">Tennessee</a>
<a href="#">Utah</a>	<a href="#">Vermont</a>	<a href="#">Virgin Islands</a>	<a href="#">Virginia</a>
<a href="#">Washington</a>	<a href="#">Wyoming</a>		

**NOTE:** The *Connecticut*, *New Jersey*, *New York* and *Virgin Islands* plans cover public sector (State & local government) employment only.

Frequently asked questions related to State OSH Plans include:

- [What is a State OSH Program?](#)
- [How does a State establish its own program?](#)

What would you like to do?  
 Find state government agency  
 Find Domestic & Foreign government agencies  
 Automatically send your search to other search engines  
 Highlight words on the results page

Change current search:

Find It! in DOL  
 Department of Labor  
**Compliance Assistance**  
 Consultation  
 eTools  
 Grants  
 Posters  
 Recordkeeping  
 Training  
**Laws & Regulations**  
 Standards  
 Interpretations  
 Federal Registers  
 Directives  
 Dockets & E-Comments  
**Cooperative Programs**  
 Alliances  
 SHARP  
 Strategic Partnerships  
 VPP  
**State Programs**  
**Newsroom**  
 News Releases  
 Publications  
 Speeches  
 Testimonies

http://www.osha.gov/fso/osp/

# California

- ❖ Agreement State since 1962
- ❖ Accelerators fall under “radiation generating machinery” of California Code of Regulations, Title 17 (Public Health), Division 1 (the Department), Chapter 5 (Sanitation), Subchapter 4, Radiation
- ❖ Radiation program oversight performed by Radiologic Health Branch w/in Food, Drug, & Radiation Safety Division of CA Department of Health Services NRC Has OSHA-approved state plan
- ❖ California Department of Industrial Relations oversees state OSHA program
- ❖ CA last NRC performance review – Satisfactory rating

# Illinois

- ❖ Illinois Administrative Code, Title 32: Energy, Chapter II: Department of Nuclear Safety, Subchapter b: Radiation Protection, Part 390, Particle Accelerators
- ❖ NRC Agreement State
- ❖ Radiation program oversight run by the Illinois Department of Nuclear Safety
- ❖ State may regulate Federal entities if they agree
- ❖ Does not have an approved OSHA state plan therefore Federal OSHA oversees health & safety programs
- ❖ IL last NRC performance review – Satisfactory w/ recommendations for improvement

# New Mexico

- ❖ Particle Accelerator requirements defined under Title 20 Chapter 3, Part 9 of New Mexico Code
- ❖ The New Mexico Agreement State Program is administered by the Community Services Bureau in the Field Operations Division of the New Mexico Environment Department.
- ❖ The day-to-day operations are carried out by the Radiation Protection Program which reports to the Bureau Chief.
- ❖ NRC Approved State

# New Mexico

- ❖ Has OSHA approved state plan
- ❖ Occupational Safety & Health program oversight performed by New Mexico Occupational Health and Safety Bureau (NMOHSB) of New Mexico Environment Department
- ❖ Incorporated Federal OSHA regs directly into state regulations
- ❖ NM last NRC performance review – Satisfactory rating

# Tennessee

- ❖ Department of Environment & Conservation, Division of Radiological Health, Chapter 1200-2-9, Requirements for Accelerators
- ❖ Radiation Protection program oversight by Department of Environment & Conservation, Division of Radiological Health
- ❖ NRC Agreement State, adopted in Title 68, Chapter 202-101 thru 202-704 of Tennessee Code Annotated.
- ❖ Has OSHA approved state plan
- ❖ Tennessee Department of Labor and Workforce Development oversees state OSHA program
- ❖ TN last NRC performance review – Satisfactory rating

# New York

- ❖ New York is an NRC Agreement State. It's program implementation is divided across several agencies. Authority is delegated to local governments with a population > 2 million
- ❖ NYC's radiation protection program is delegated to the City Department of Health from the State DOH in Part 16 of NY & State Health Code
- ❖ Legislative authority for NYC's portion of Agreement State program is in Chapter 22 of NYC Charter, section 556.

# New York

- ❖ Department of Health authority to administer its portion of Agreement State program is in NY Public Health Law, Article 2, Title II, Sections 201 & 225
- ❖ NY last NRC performance review – Satisfactory w/ recommendations for improvement

# New York

- ❖ The New York PESH program covers the workplace safety and health of public sector employees only. Private sector employees in New York are covered by Federal OSHA.
- ❖ Department of Labor authority to administer its portion of the Agreement is in Section 27 of the Labor Law & Article 28-D of the General Business Law.
- ❖ The Department of Environmental Conservation administers its portion of the Agreement via Law Articles 1, 3, 17, 19, 27, and 29.

# Utah

- ❖ Utah is an NRC Agreement State
- ❖ Division of Radiation Control, Department of Environmental Quality has authority to implement program under Utah Code Annotated, Title 19, Chapter 3, Radiation Control Act.
- ❖ State radiation control regulations are in Utah Administrative Code, Title 313
- ❖ State of Utah Labor Commission oversees OSHA state approved program
- ❖ UT last NRC performance review - Satisfactory

# Brazil

- ❖ Comissão Nacional de Energia Nuclear = National Nuclear Energy Commission (CNEN)
  - ❖ Oversees policy planning, monitoring, and control of nuclear energy IAW National Nuclear Energy Policy Act
  - ❖ Comprised of 3 directorates
  - ❖ Promotes, orients, & coordinates R&D in all areas of peaceful uses of nuclear energy.
  - ❖ Five nuclear research centers carrying out R&D in nuclear science & engineering

# CNEN Responsibilities

- ❖ Prepare and issue regulations on nuclear safety, radiation protection, radioactive waste management, and physical protection
- ❖ Nuclear facilities oversight from licensing to decommissioning
- ❖ Acting as a national authority for implementing international agreements/treaties related to nuclear safety

# CNEN Responsibilities

- ❖ Account for and control nuclear materials
- ❖ Conduct regulatory inspections of nuclear reactors
- ❖ Participate in national preparedness for and in response to nuclear emergencies
- ❖ Nuclear plants come from different supplying countries
  - ❖ Made it necessary to develop tailored Brazilian approach to plant operation & management
  - ❖ based on best practices from USA & Germany – primarily NRC
  - ❖ Use of international practices including IAEA safety standards

# Department of Energy (DOE)

- ❖ Presidential Executive Order 12196, Occupational Safety & Health Programs for Federal Employees
- ❖ DOE oversees accelerator and worker health & safety programs
- ❖ 10 CFR 835, Radiation Protection Program
- ❖ DOE Order 440.1, *Worker Protection Management for DOE Federal and Contractor Employees*
- ❖ Work Smart Standards establish specific legal basis tailored to each DOE site

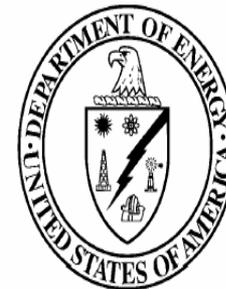
# DOE-STD-3024-98

- ❖ Primarily for DOE Hazard Category 2 non-reactor nuclear facilities
- ❖ Applies either to new facilities and systems or to existing systems
- ❖ Recommended for non-nuclear facilities

DOE-STD-3024-98  
October 1998

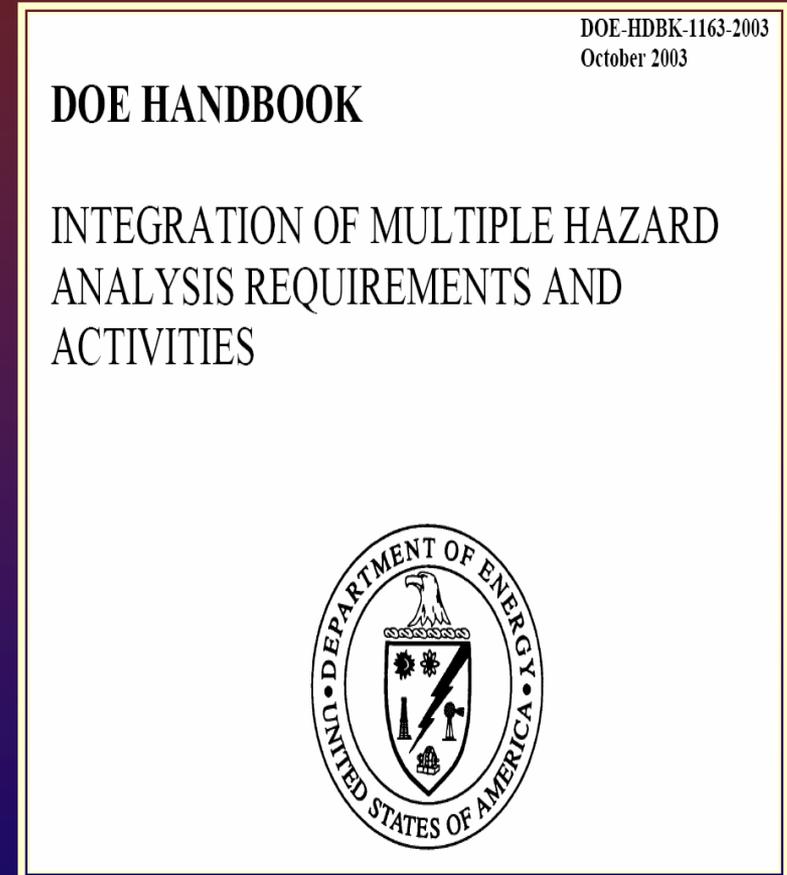
DOE STANDARD

CONTENT OF SYSTEM DESIGN  
DESCRIPTIONS



# DOE-HDBK-1163-2003

- ❖ DOE Technical Standard
- ❖ Provides regulatory overview
- ❖ Highlights opportunities for integrated hazard analysis
- ❖ Provides improved HA methods
- ❖ Applicable to all DOE organizations



# World Trade Organization

- ❖ Member countries are encouraged to use international standards, guidelines and recommendations where they exist.
- ❖ May use measures which result in higher standards if there is scientific justification.
- ❖ ISO/IEC intermediary for notices of codes of good practice

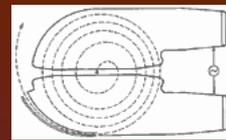


# Introduction to Safety Systems in Research Accelerators

Software

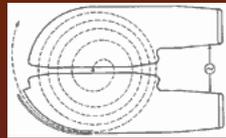
USPAS

June, 2004

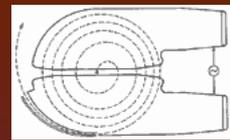


# Outline

- ❖ Overview of software considerations for use in safety applications
- ❖ Objective
  - ❖ Introduce some of the concerns in using programmable devices and some of the methods used to address them.

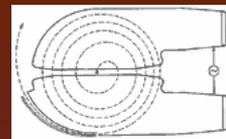


- ❖ Nancy Leveson will argue that “software” cannot fail, only hardware. Software is an abstract concept executed by physical hardware.



- ❖ A stress-strength model can be used.
- ❖ Instead of physical stress on a component, software is stressed by demands placed on the constraints within the context of the system.
- ❖ These constraints can be:
  - ❖ physical, e.g. hardware failure,...
  - ❖ logical, e.g. out of bounds data,...
  - ❖ temporal, e.g. old data, mis-synchronized functions,...
- ❖ It is a matter of how well the constraints are defined and how well the system can handle excursions beyond the constraints.

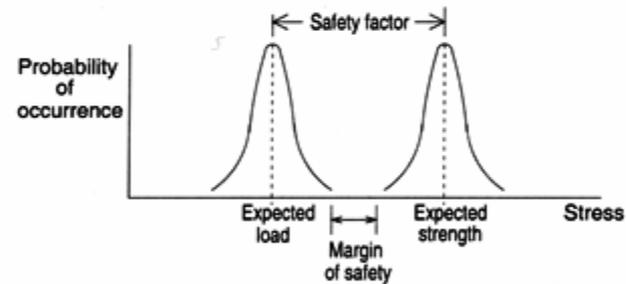
# Stress Strain



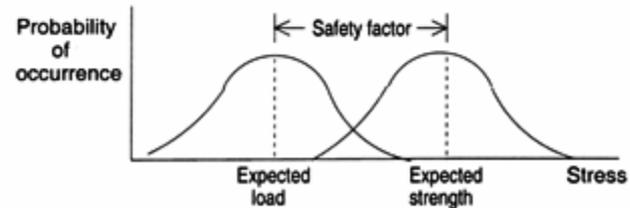
## Safety Margins and Safety Factors



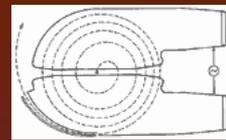
(a) Probability density function of failure for two parts with same expected failure strength.



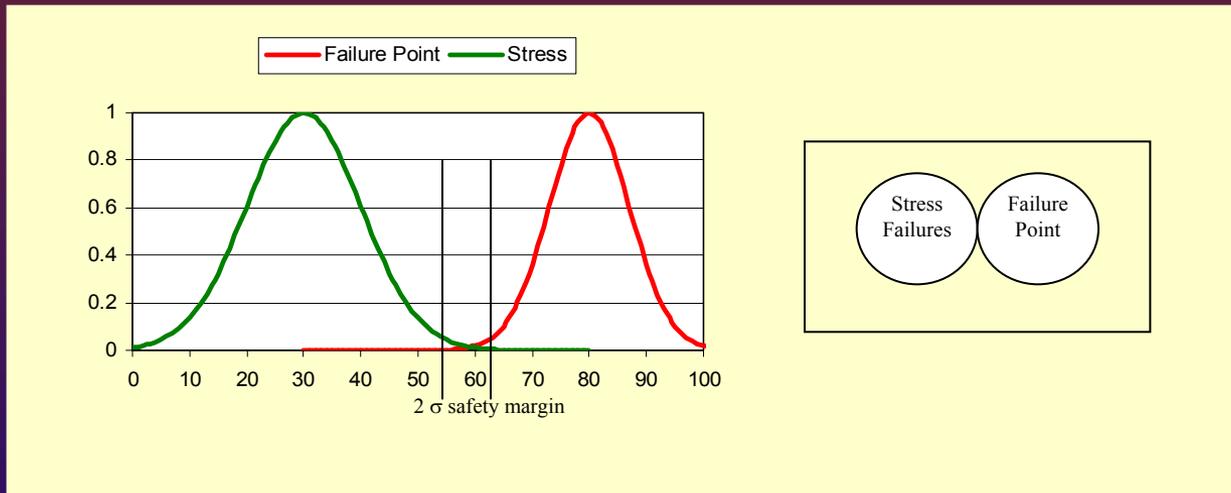
(b) A relatively safe case.

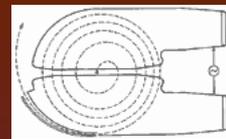


(c) A dangerous overlap but the safety factor is the same as in (b)

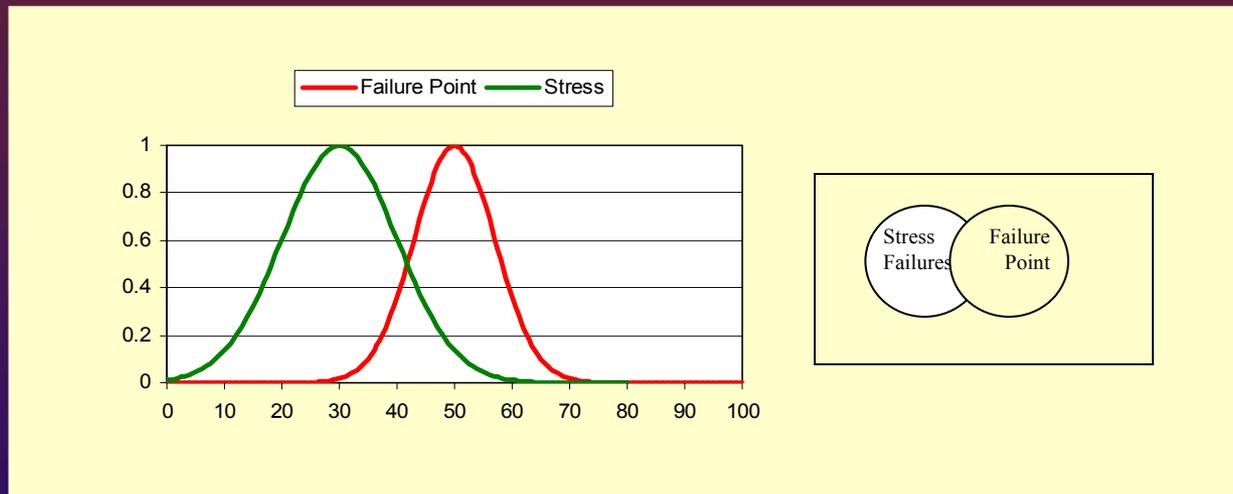


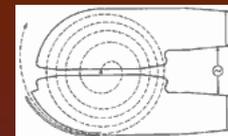
# Safety Margin



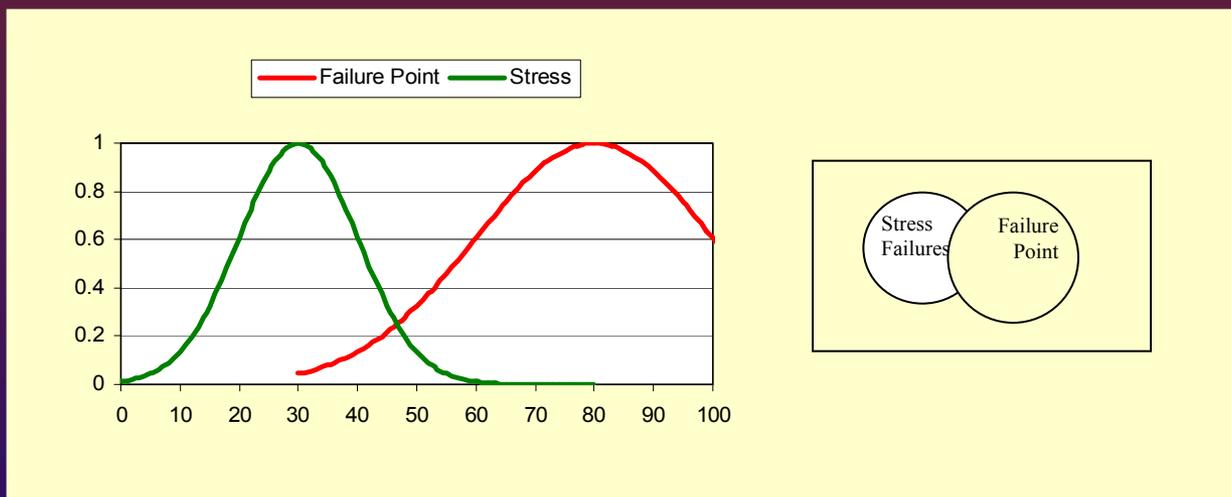


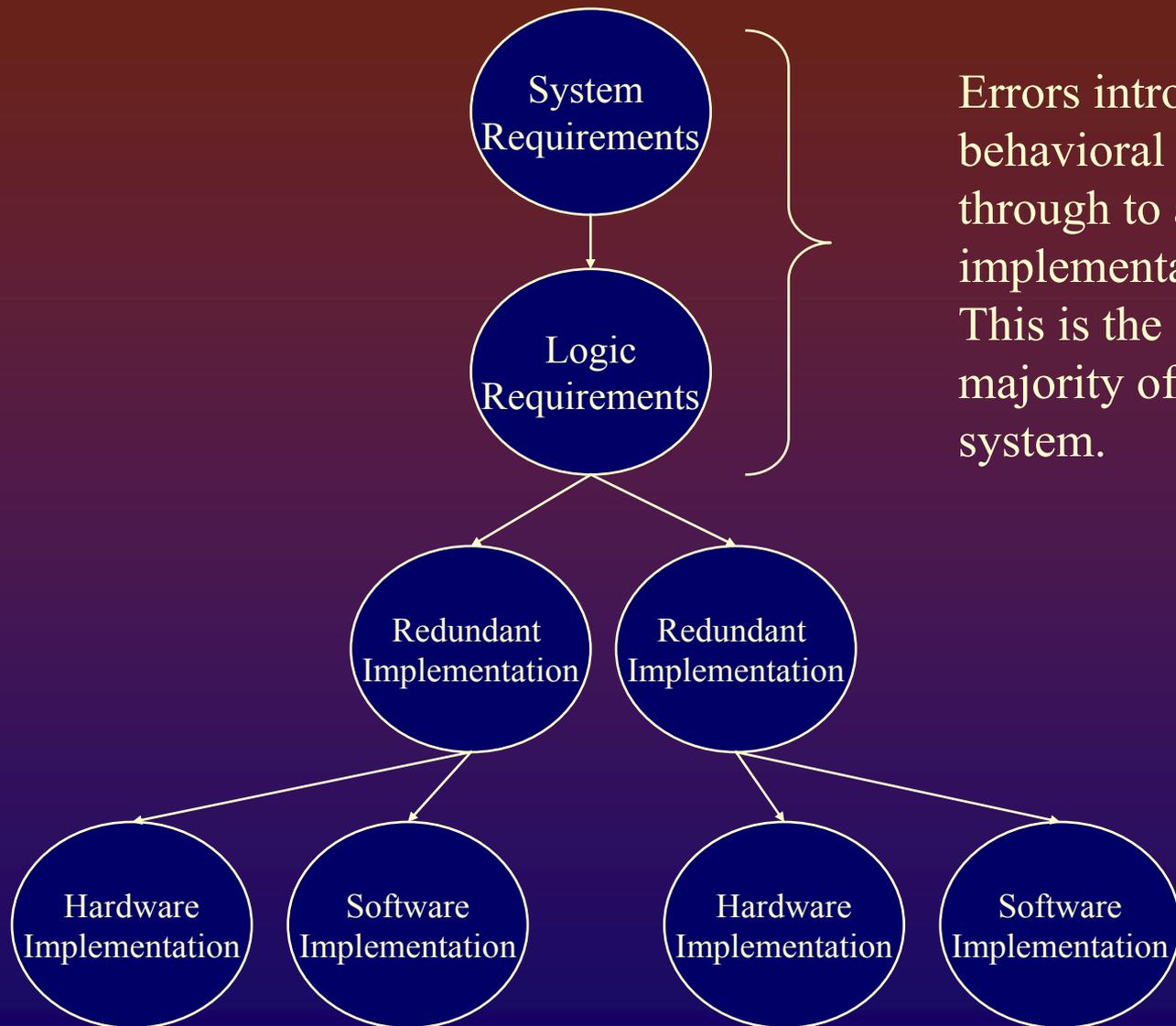
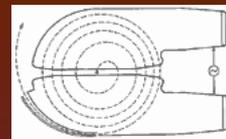
# Increase in Failures Due to Insufficient Safety Margin



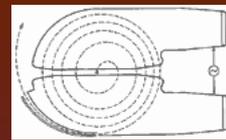


# Increase in Failures Due to Poor QA





Errors introduced in the behavioral phase will propagate through to any type of system implementation. This is the source of the majority of functional errors in a system.

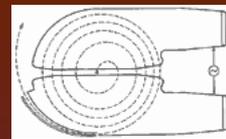


# Requirements

The most important document in safety systems is the requirements document.

Requirements should include

- ❖ Context
- ❖ Scope and intended use
- ❖ Constraints
- ❖ Assumptions
- ❖ Desired behavior
- ❖ Timing requirements
- ❖ Exception handling
- ❖ Verification/Validation requirements
- ❖ Definition of inputs and expected outputs

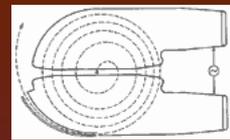


## ❖ Languages

- ❖ IEC61131-3 Defines PLC programming Languages

## ❖ Applications

- ❖ Software application development is left to “Good Practice”
- ❖ A good start is in IEC 61508 and 61511
- ❖ IEC880 (Software for Computers in the Safety Systems of Nuclear Power Stations) is a good reference



# Programming Languages

## ❖ Three Categories

### ❖ Fixed Program Language

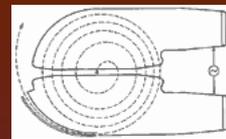
- ❖ Application is unalterable
- ❖ Ex. Smart Transmitter

### ❖ Limited Variability Language

- ❖ Well defined functions may be programmed within a structured framework
- ❖ Ex. Ladder Logic, Instruction List, Structured Text

### ❖ Full Variability Language

- ❖ General purpose programming language
- ❖ Ex. ADA, C, C++

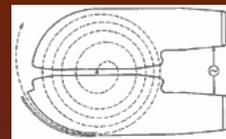


# Safety Software Design

Really, it is high QA design.

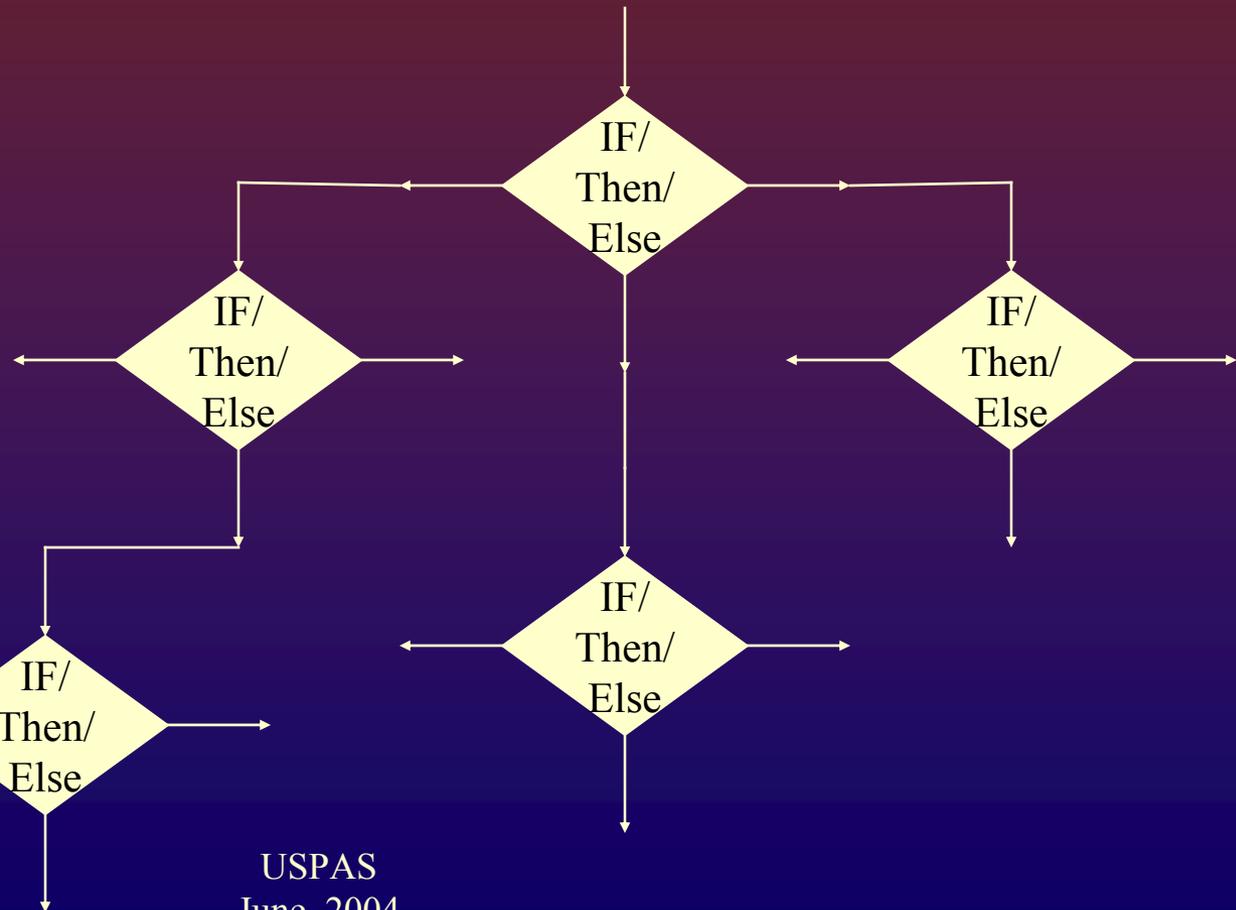
Apply standards and good practice that reflect lessons learned from past accidents. Includes things like checklists.

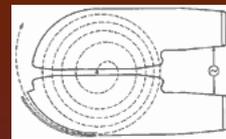
Make use of hazard analysis techniques to help avoid introduction of systematic errors.



# Branches

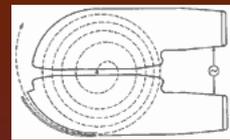
- ❖ Every decision branch in a logical system increases the complexity of the system exponentially





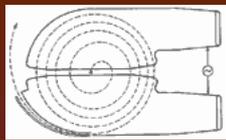
# Software Analysis Techniques

- ◆ Software FMEA
- ◆ HAZOP
  - Hazard and Operability analysis
  - Qualitative
  - Carried out on design, not a FMEA
- ◆ Fault/Event Trees
  - Quantitative
  - Only follows defined faults/events
- ◆ Formal Methods
  - Rigorous but unwieldy



# IEC 61508 Part 3 Software

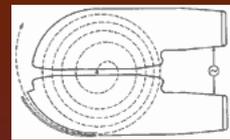
- ❖ Defines requirements for software practices based on target SIL level.
- ❖ Includes appendices with recommended practice.
  - ❖ Practice may be:
    - ❖ HR                      Highly Recommended
    - ❖ R                        Recommended
    - ❖ ---                      mute/no recommendation
    - ❖ NR                      Not Recommended



# Recommendations from IEC 61508 Part 3-Software

❖ <b>Technique/Measure</b>	<b>Ref</b>	<b>SIL1</b>	<b>SIL2</b>	<b>SIL3</b>	<b>SIL4</b>
1 Use of coding standard		HR	HR	HR	HR
2 No dynamic objects		R	HR	HR	HR
3a No dynamic variables		---	R	HR	HR
3b Online checking of the installation of dynamic variables		---	R	HR	HR
4 Limited use of interrupts		R	R	HR	HR
5 Limited use of pointers		---	R	HR	HR
6 Limited use of recursion		---	R	HR	HR
7 No unconditional jumps in programs in higher level languages		R	HR	HR	HR

**Table B.1 – Design and coding standards**

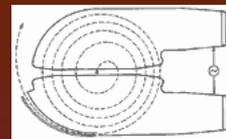


## Recommendations from IEC 61508 Part 3-Software

<b>Technique/Measure</b>	<b>Ref</b>	<b>SIL1</b>	<b>SIL2</b>	<b>SIL3</b>	<b>SIL4</b>
1 Software module size limit		HR	HR	HR	HR
2 Information hiding/encapsulation		R	HR	HR	HR
3 Parameter number limit		R	R	R	R
4 One entry/one exit point in subroutines and functions		HR	HR	HR	HR
5 Fully defined interface		HR	HR	HR	HR

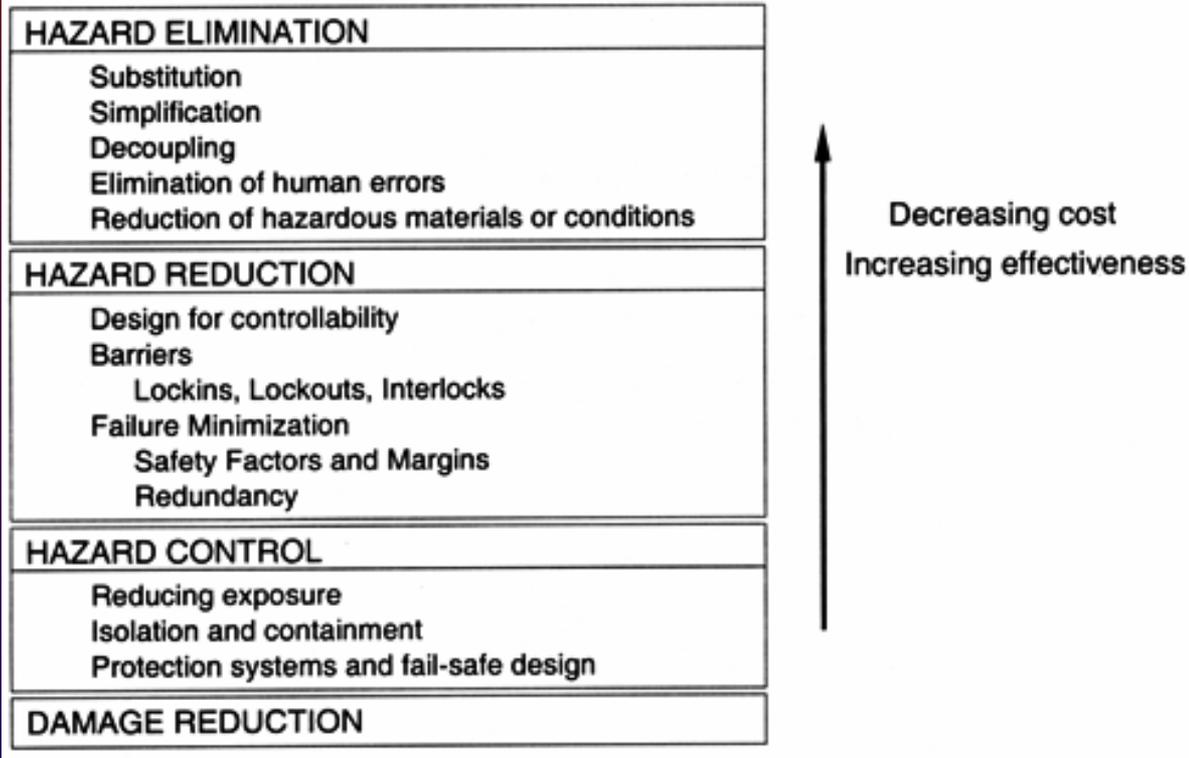
**From Table B.9 – Modular approach**

# Hazard Mitigation from Software Perspective



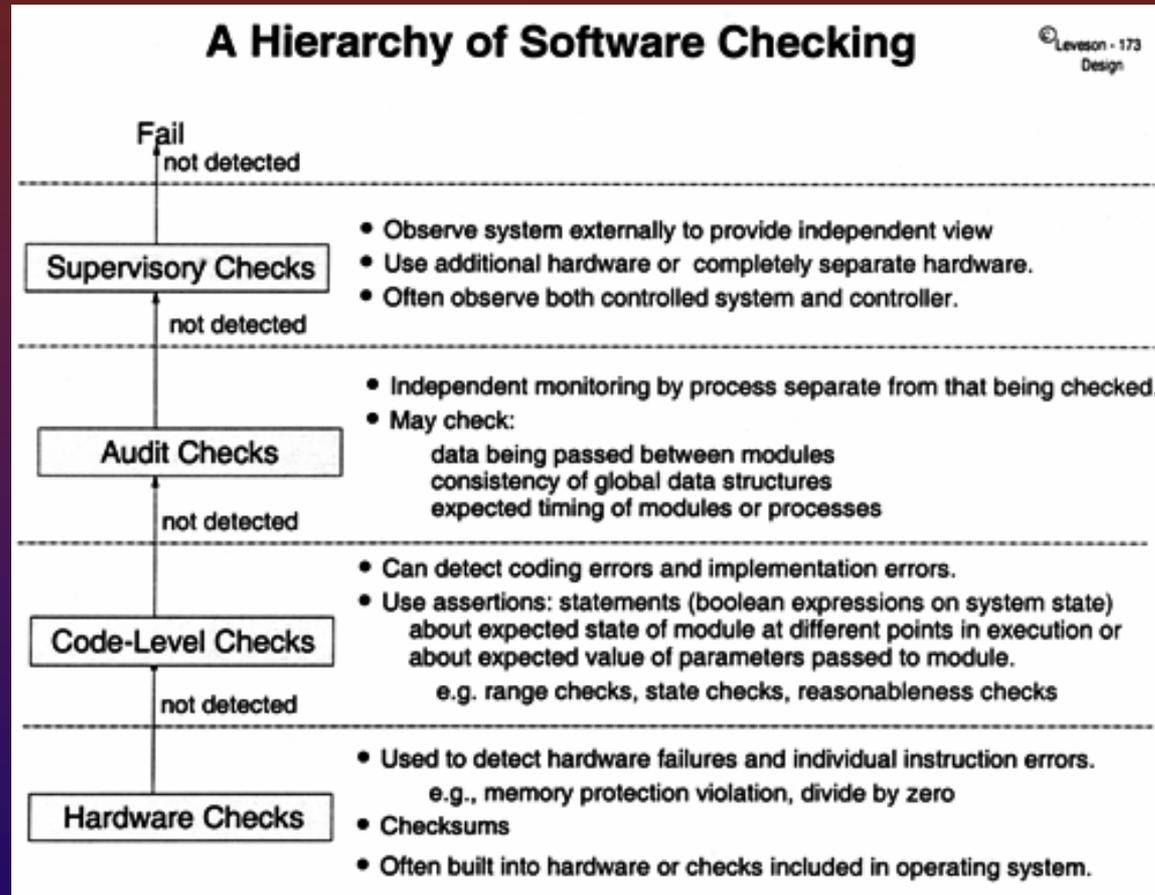
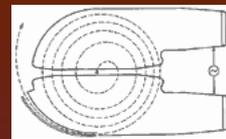
Leveson - 100  
Design

## Safe Design Precedence



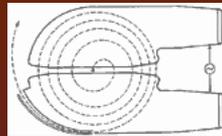
N. Leveson

# Software Checking



N. Leveson

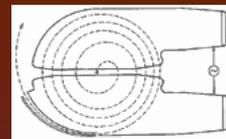
# Self-Checking Software (2)



	Already Known Errors			Other Errors			Added Errors	
	#	Detected		Detected				
		SP	CR	CD	SP	CR	CD	
3a	4		1					
3b								
3c								
6a	3		2			1	1	
6b							1	
6c								
8a	2			2			1	
8b							3	
8c						1		
12a	2	1				1	2	
12b							2	
12c			1			1	2	
14a	2						4	
14b								
14c								
20a	2		1		1		1	
20b			1				2	
20c				1				
23a	2	2					4	
23b								
23c								
25a	3		2			1	1	
25b					1			
25c								
<b>Total</b>	<b>60</b>	<b>3</b>	<b>8</b>	<b>3</b>	<b>1</b>	<b>0</b>	<b>5</b>	<b>22</b>

Spec Read Chks    Spec Read Chks    ADDED  
 KNOWN                      NEWLY FOUND

# State Machine Design



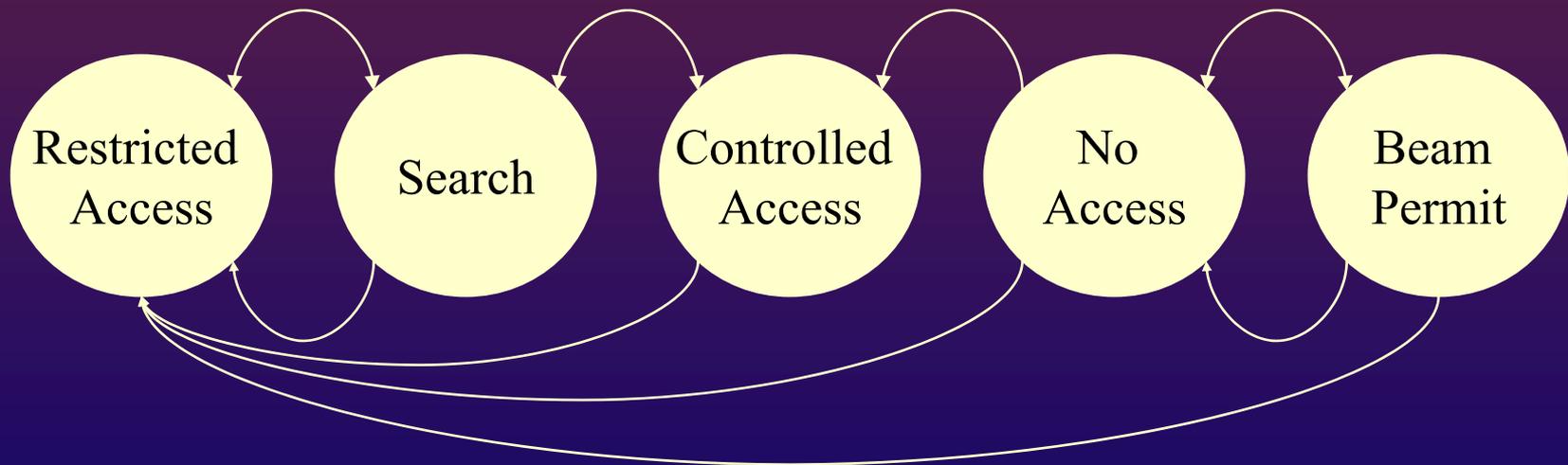
State or state machine based design

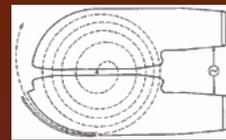
Each state must be complete

Each state and transition in-to and out-of must be deterministic, e.g. fail safe states.

Define “safe” states and “dangerous” states

Error handling for each condition/state/transition

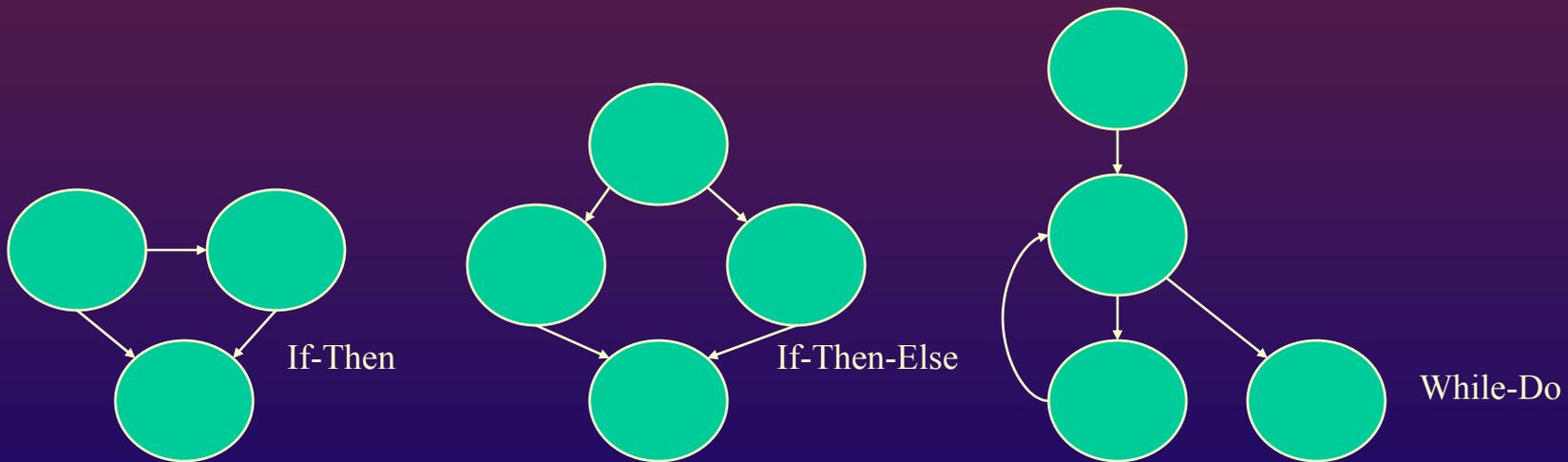




# McCabe Complexity

- ❖  $e$  is number of edges
- ❖  $n$  is number of states

$$Paths = e - n + 2$$



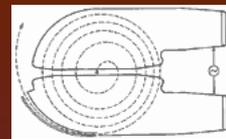


# Introduction to Safety Systems in Research Accelerators

Lifecycle Costs

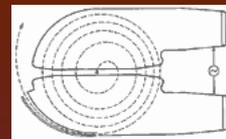
USPAS

June, 2004



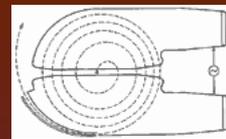
# Cost Benefit

- ❖ Method for making risk based decisions
- ❖ Senior management assumes risk of consequences whether they know it or not



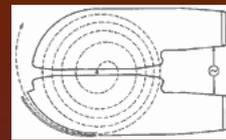
# Costs/Benefits

- ❖ Measure of “value”
- ❖ For accelerators this may not be monetary
  - ❖ Cost in Contract Metrics
    - ❖ DART
    - ❖ TRC
    - ❖ Type (n) investigation
  - ❖ Cost can be expressed in operating hours (Availability)
    - ❖ Machine hours
    - ❖ Experiment hours



# Human Cost

- ❖ Driven by most senior management
- ❖ Driven by ALARP
- ❖ Regulatory requirements
- ❖ Tolerable Risk
- ❖ Perceived Risk includes ethical judgments



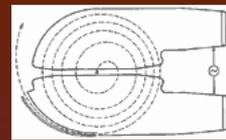
# Loss Continuous Functions

$$\textit{Cost of failures} = \left[ (C_r + C_{lp}) \times (1 - A) \right]$$

$C_r$  – Repair Costs

$C_{lp}$  – cost of lost Production

$A$  – Availability



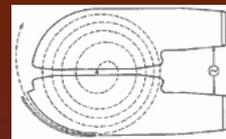
# Loss for Event-based Functions

$$\textit{Cost of failures} = [C_E \times P(E)]$$

$C_r$  – Repair Costs

$C_{lp}$  – cost of lost Production

$A$  – Availability



# Operating Costs

$$\textit{Operating Costs} = \left[ \left( C_{\textit{Change}} + C_{\textit{MAINT}} + C_{\textit{Consumables}} + C_{\textit{Failure}} \right) \times \textit{Lifetime} \right]$$