Controlling Risks
Safety Systems

Ken Barat

Patrick Bong

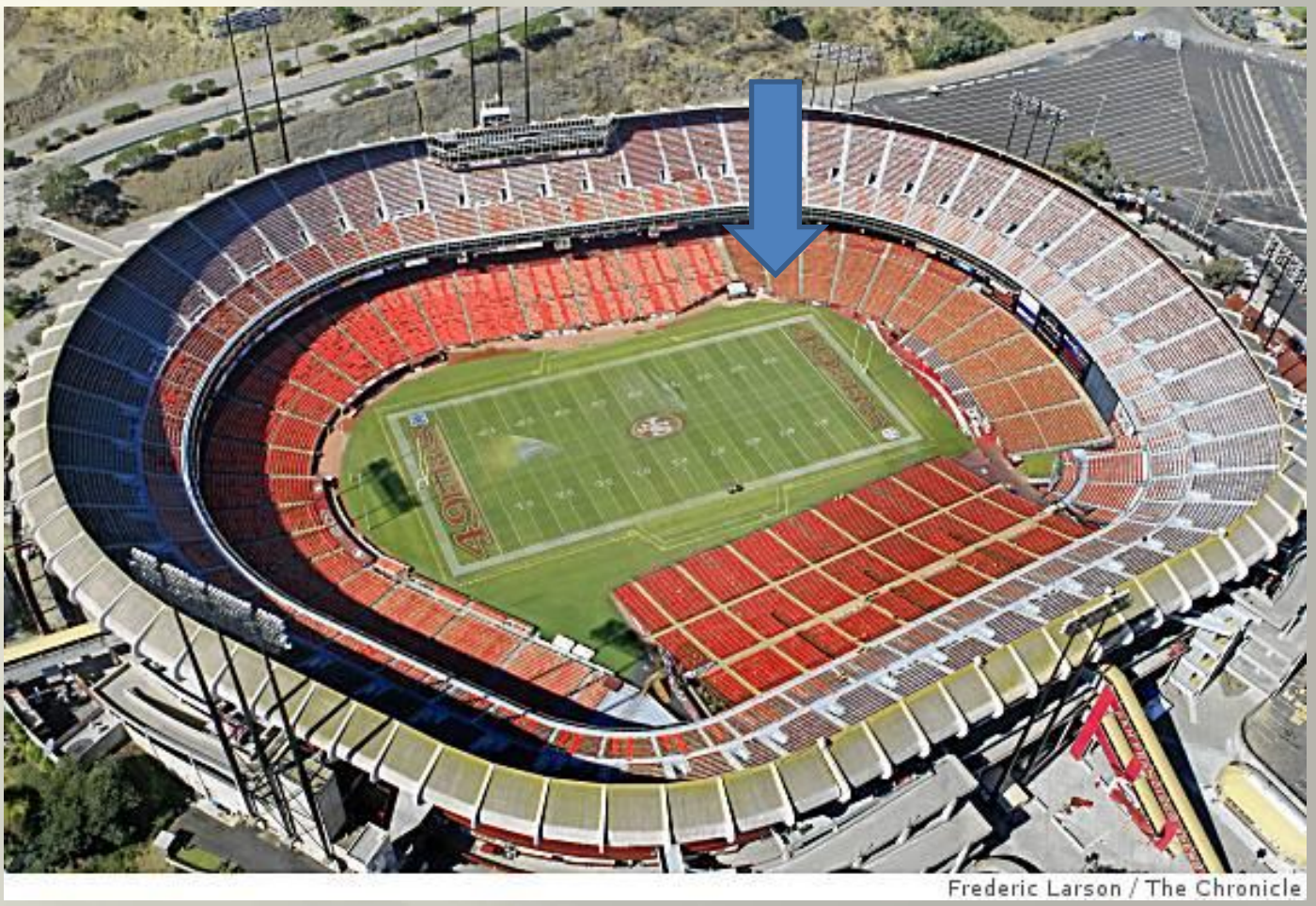
Lawrence Berkeley National Laboratory

Advanced Light Source at LBNL

San Francisco 49ers

TE Vernon Davis catches his historic touchdown

My seats for the last 8 seasons



What happened yesterday?

- I had to give up tickets to the game to be here
- My flight was in the air the entire game

Introductions

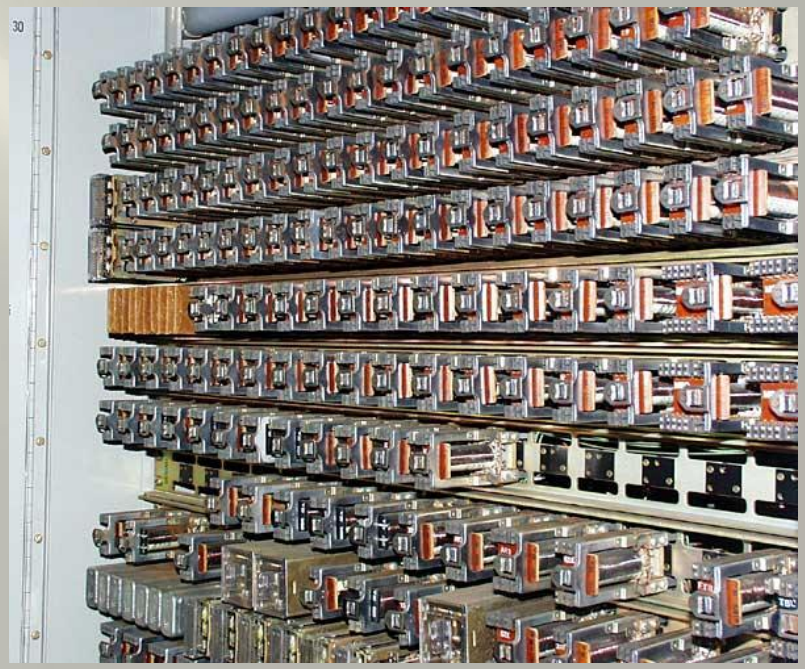
- Instructors
- You
  - Your name
  - Facility
  - What do you do for a living

Introduction to Safety Systems

- Safety System Evolution
- Definitions
- Safety Systems/Safety Functions
- Failure Rates and Reliability

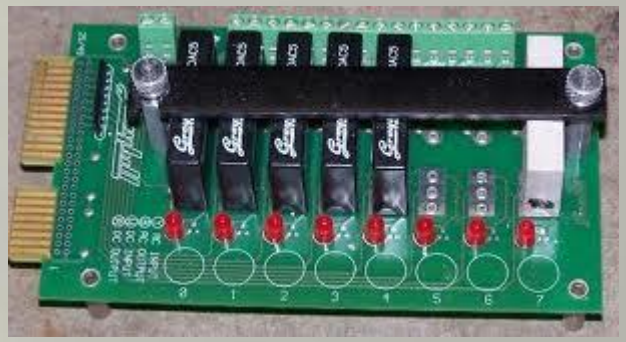
Safety Evolution

- 1960's
- Hardwired relays interlock systems as needed



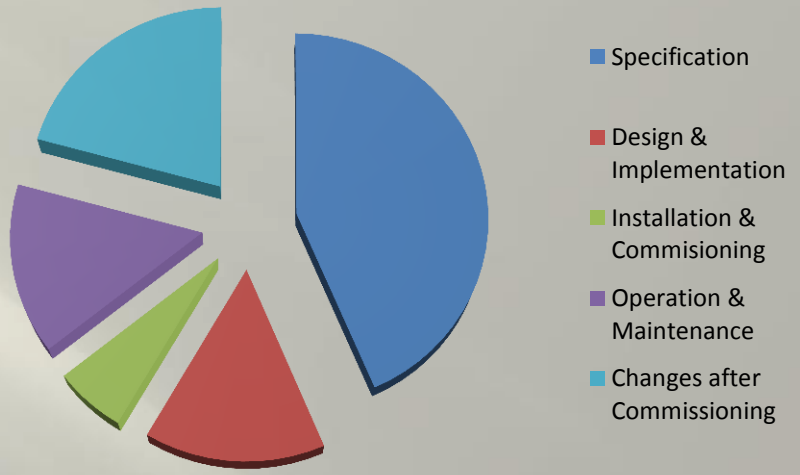
Safety Evolution

- 1970’s
- Hardwired Relays
- Solid State logic
- Install where need is recognized.



Safety Evolution

- 1980's
- Started using PLCs



- HAZOP, Risk Analysis procedures developed

Safety Evolution

- 1990's
- Safety PLCs

- Standards for PLCs
- Development of Quantitative Risk Analysis
- Systematic approach for Risk Identification

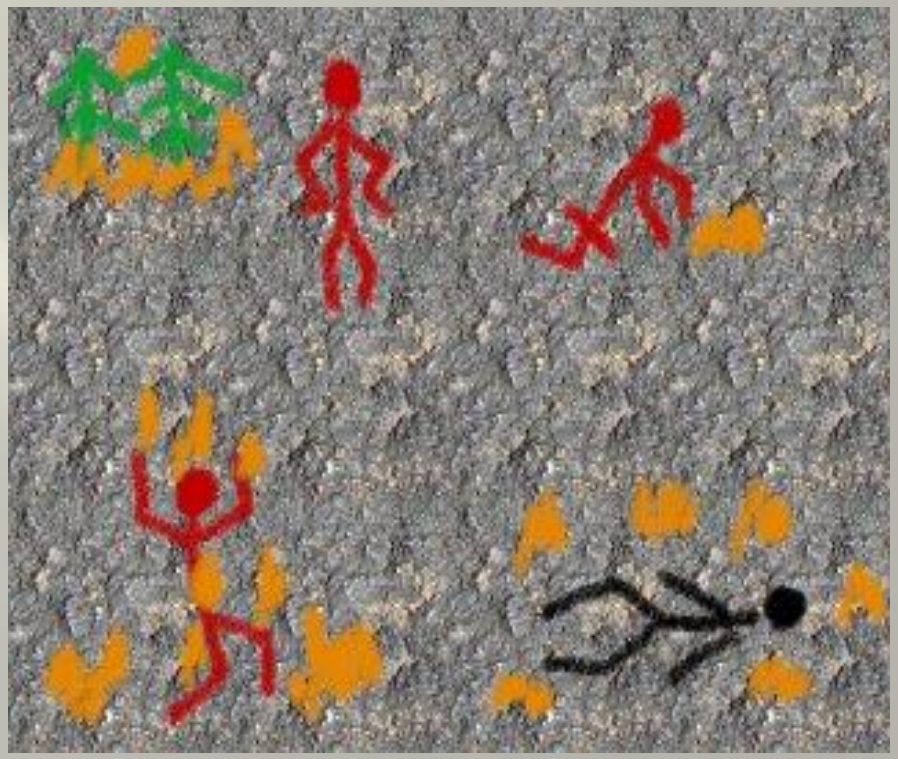
Evolution of a Safety System

(that I have some experience with)

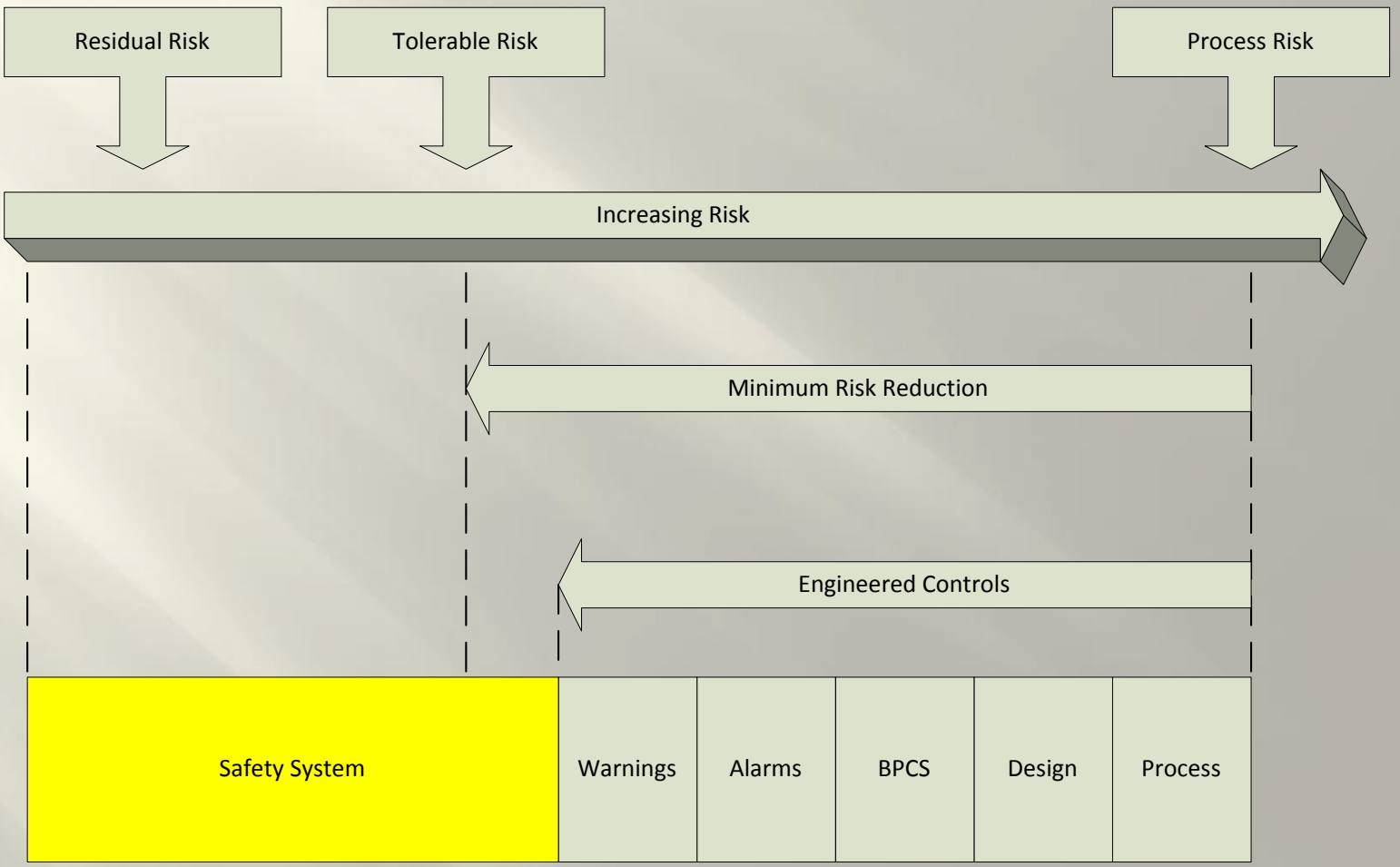
- 1966 – SLAC begins operation with a non-redundant relay based Personnel Protection System (PPS)
- 1980 – PEP, relay based, semi-redundant
- 1989 – SLC, relay based, redundant
- 1993 – FFTB, relay based, redundant
- 1996 – NLCTA, relay based, redundant
- 1997 – PEP-II, relay based, redundant
- 1999 – PLC R&D project for use in the PPS
- 2005 – LCLS Injector, First PLC base PPS

Safety Systems

- Safety Systems exist to manage risk.
- A Tolerable Risk level is achieved by applying risk reduction
  - Process
  - Design
  - BPCS (Basic Process Control System)
  - Alarms
  - Warnings
  - Interlocks



Safety Systems



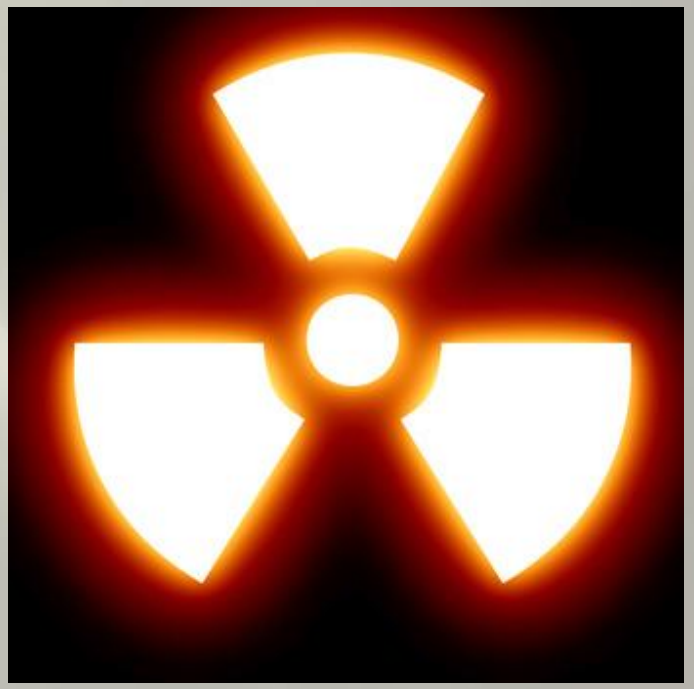
Hazards and Risks

- **Hazard** is the potential to cause harm
- **Risk** is the likelihood of harm

- This photograph was taken in a bakery, where flour dust was liberally scattered. The baker suffered from occupational asthma, and it was difficult for the employer to appreciate that something as apparently innocuous as flour could cause asthma, especially in conditions of high exposure.

Accident

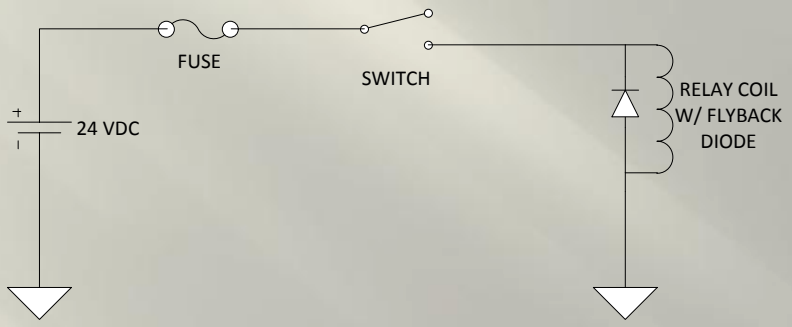
- Accident. The term "accident" can be defined as an unplanned event that has a resulted in or suggests the failure of a DOE safety management system, barriers, or loss of controls that rises to the threshold criteria specified in this Appendix A of DOE Order 225.1B
- Death, hospitalization, multiple employee injuries, dose limits exceeded, public exposure…



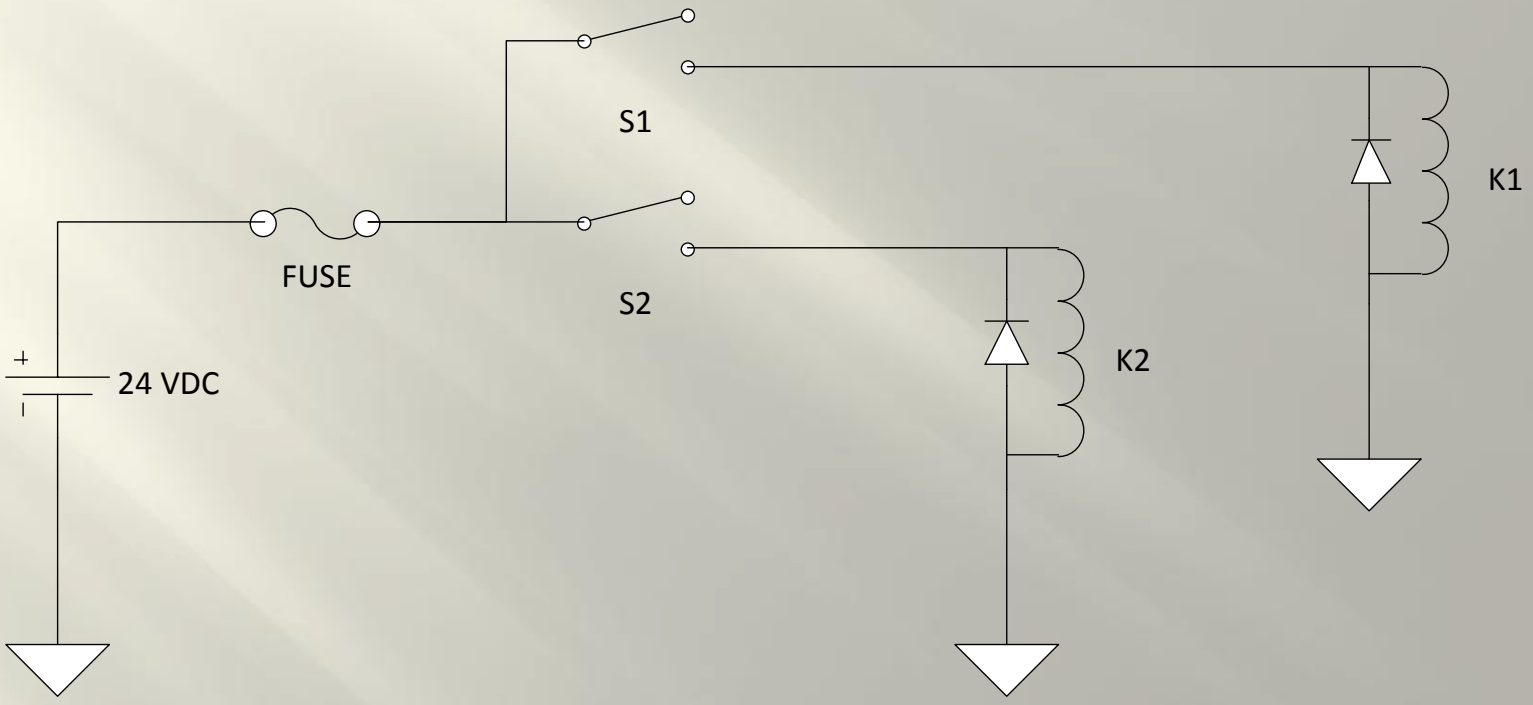
Fail-Safe and Redundant

- Fail-Safe
  - Fail-Safe circuits are designed for closed-circuit operation which requires that the energized or closed contact state of sensors and actuators is the normal running condition. The de-energized or open contact state is the safe state. The protective functions of the interlock system should render the energy source/system safe during the most likely interlock system failure events (e.g., loss of power/pressure, open circuit, short to ground).
- Redundant
  - Redundant systems use multiple, independent equipment arrangements such that each interlock system is isolated from the others to perform similar safety functions such that any single failure will not result in loss of protection

Basic Fail-Safe Circuit



Basic Redundant Circuit



SIS and SIF

Safety Instrumented System

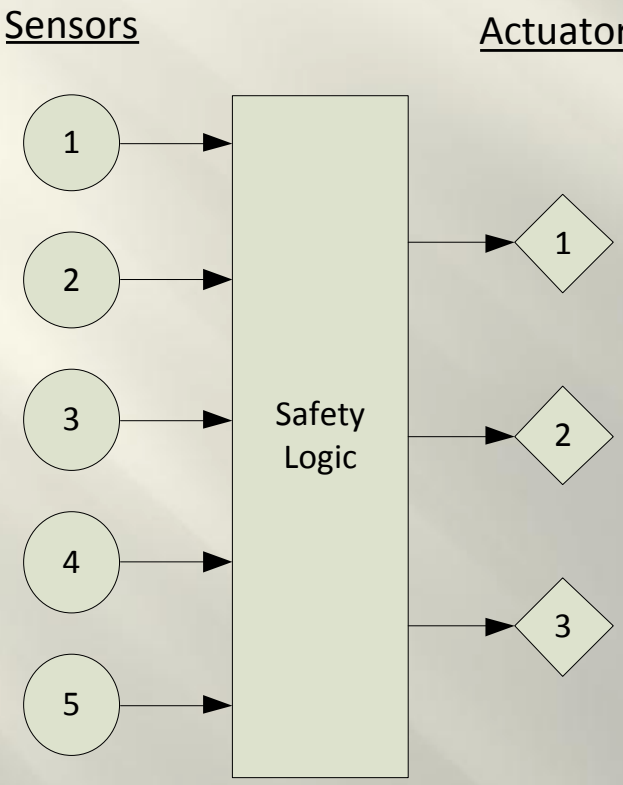
- Can encompass multiple functions and act in multiple ways to prevent multiple harmful outcomes.
- Any system, implemented in any technology, which carries out safety functions is a *safety instrumented system*.
- A safety-related system may be separate from any equipment control system or the equipment control system may itself carry out safety functions. In the latter case, the equipment control system will be a safety-related system.
- Higher levels of safety integrity necessitate greater rigour in the engineering of the safety-related system.

Safety Instrumented Function

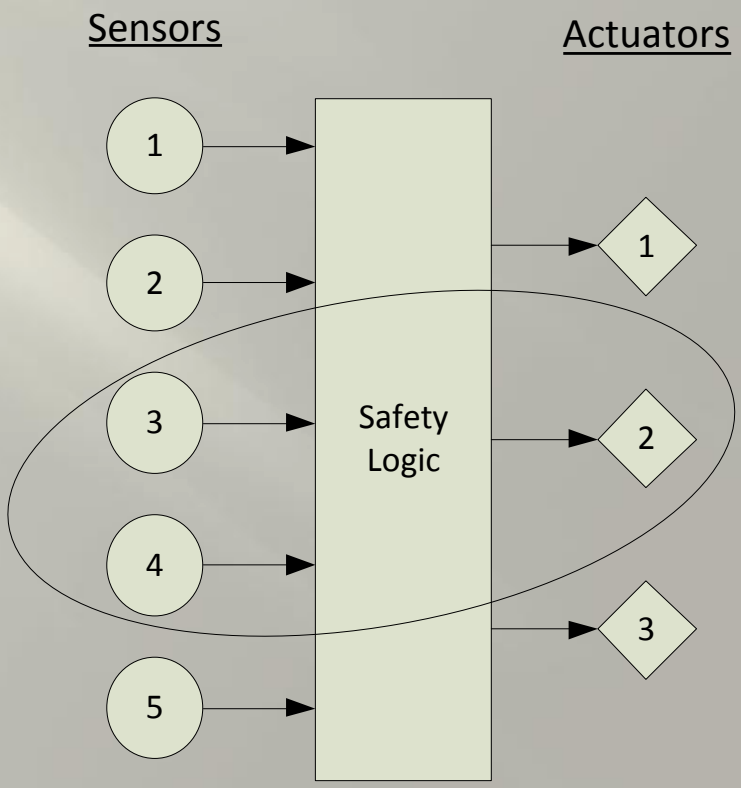
- Function to be implemented by a SIS which is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event.
- safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function

SIS and SIF

Safety System



Safety Function



SIF Examples

- Prevent radiation exposure by inserting stoppers between beam and occupied enclosure.
- Prevent electrical exposure by shutting off supply power to hazardous equipment.
- Prevent laser exposure by closing shutters at laser output.

Failure Rate

- A study to determine the average lifetime of a module
  - Provides statistical information about the future performance of similar modules

$$\lambda(t) = \frac{f(t)}{n}$$

Where f(t) = Failures per unit time (plug in → blow out)

n = number of modules

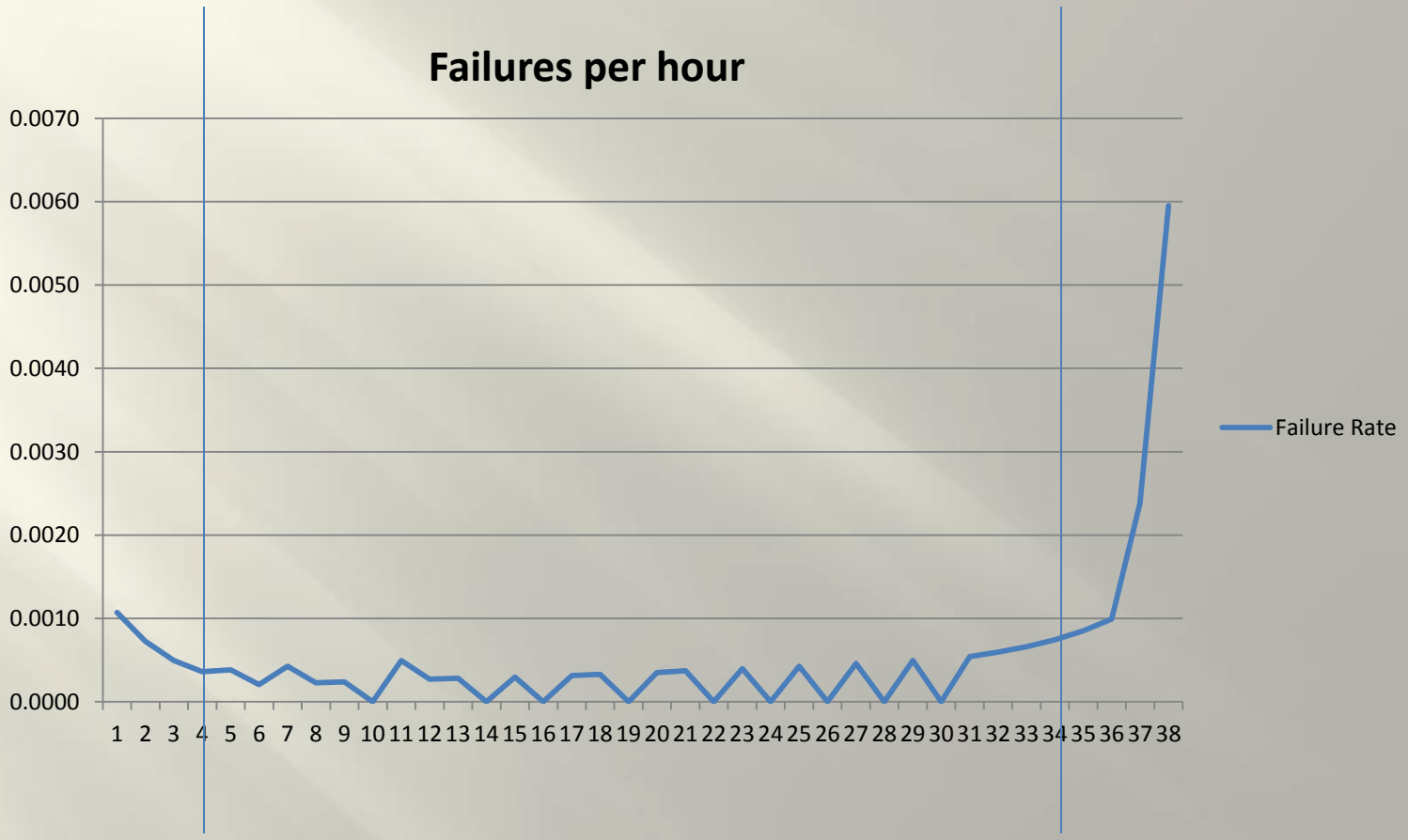
Failure Rate Example

- 1 week test
- 50 units
- 9 failures

$$\lambda(t) = \frac{f(t)}{n}$$

$$\lambda(t) = \frac{9}{7*24} * \frac{1}{50} = .0011$$

CSSE&R, Page 69



Infant Mortality

Wearout

Reliability and Availability

- In electronic reliability analysis it is assumed that the failures are **independent** and **random**. This means that a failure in one component, even though it may cause the system to malfunction, will not cause other components to fail and that the failures are distributed in time according to an exponential statistical distribution with a constant failure rate vs. time.
- The **failure rate**, λ, is the fundamental variable that defines reliability.
- The probability of survival over a period of time is given by the equation

Reliability, $R(t) = e^{-\lambda t}$

where λ = Intrinsic Failure Rate

t = time

- Note that reliability is dependent on the time interval under study and is otherwise meaningless.

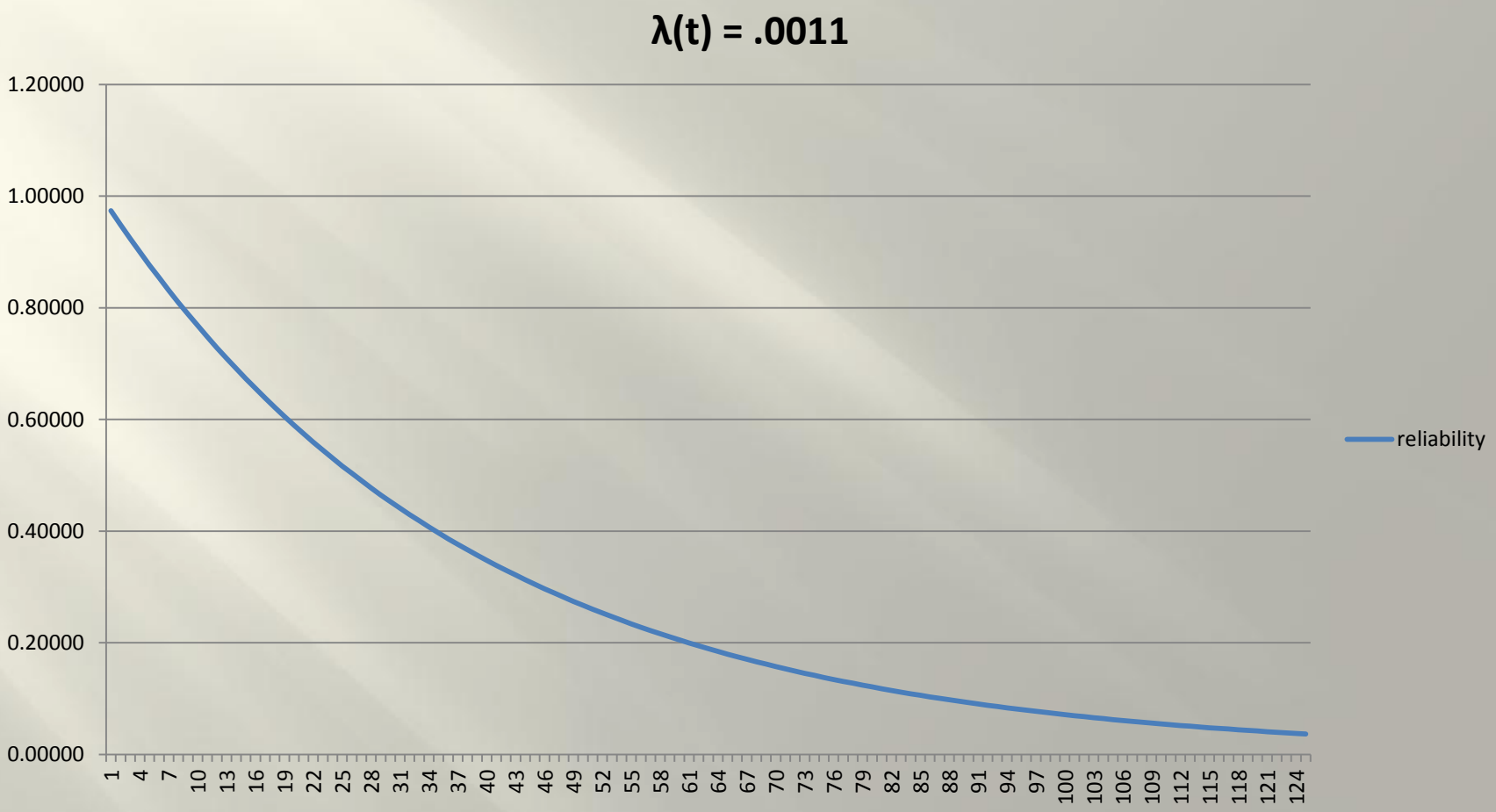
- **Availability** is the ratio of actual service to required service.
- For example, if a system is required to operate continuously and it is out of commission due to repair of failures for 12 hours per year, its actual availability is:

Availability

= (8760 - 12) hours / 8760 hours = 0.9986

= 99.86 %

Reliability



Mean Time to Failure

- MTTF is the expected lifetime of a component based on the failure rate.

$$MTTF = \frac{1}{\lambda}$$

$$MTTF = \frac{1}{.0011} = 909\ hours$$

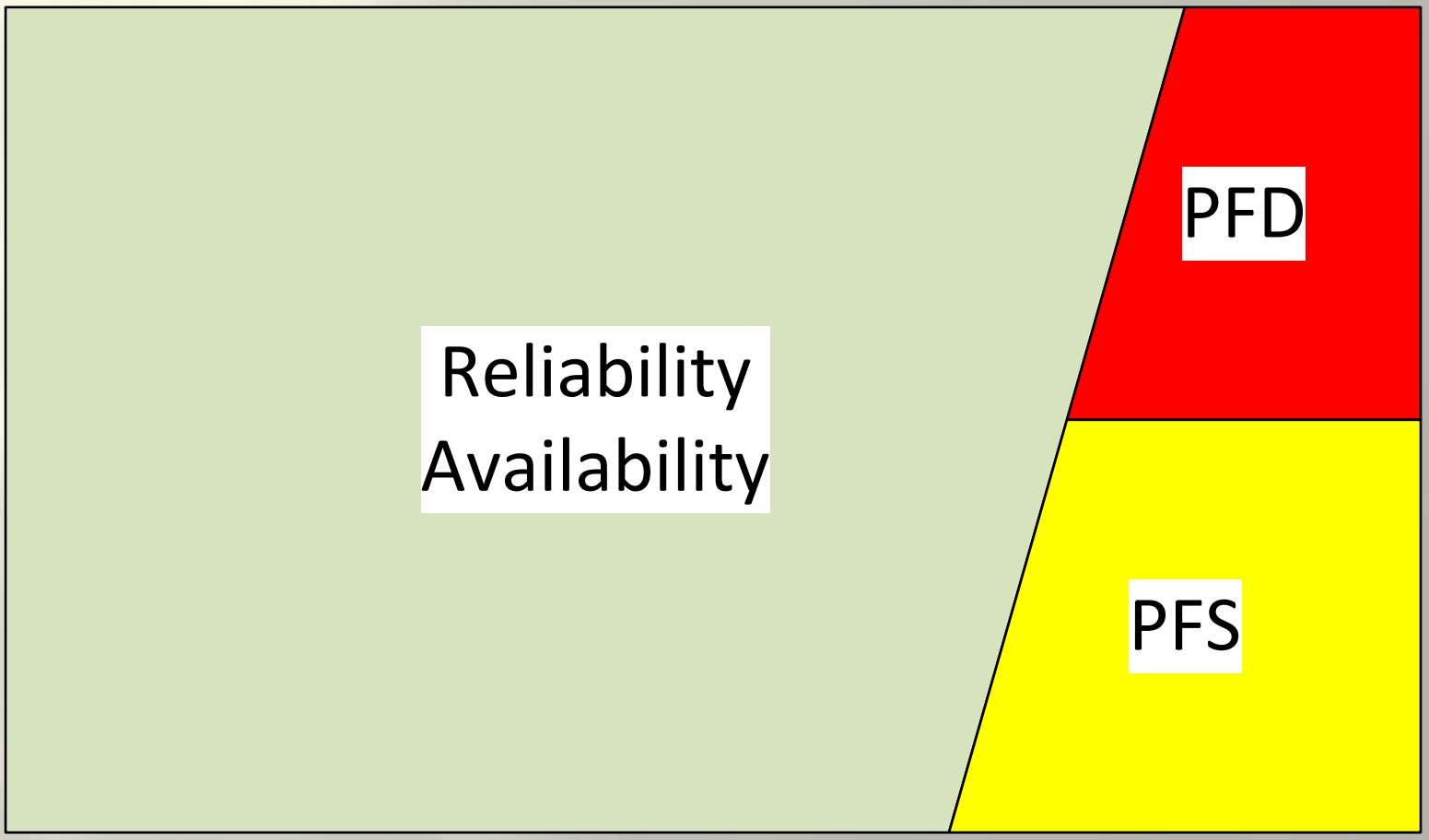
Failure Modes

- Safe State – is the state of the process when safety is achieved.
- Safe Failure Mode – any failure causes the device to go to the safe state.
- False Trip – process is halted in the safe state even though no fault is detected.
- Dangerous Failure Mode – failures which prevent a device from responding to a potentially dangerous condition known as a “demand”.

Failure Mode Story Time

- Overt failures – you know them when you see them.
- Covert failures – undetected except through testing.
- Other failures?

Probability = 1



Discussion

- Open General Discussion

Laws & Regulations

- Accelerator Laboratories
  - 10 CFR 835, Occupational Radiation Protection
  - DOE o 420.2B, Safety of Accelerator Facilities
  - DOE o 414.1c, Quality Assurance
  - ANSI N43.2-2001, Radiation Safety For X-ray Diffraction & Fluorescence Analysis Equipment
  - ANSI N43.3-2008, For General Radiation Safety – Installations Using Non-Medical X-Ray and Sealed Gamma-Ray Sources, Energies up to 10 MeV
  - NFPA 101, Life Safety Code

  There may be other requirements for your facility.

  Check your Work Smart Standards.

Standards - IEC61508

- uses a risk based approach to determine the safety integrity requirements of E/E/PE safety-related systems, and includes a number of examples of how this can be done;
- uses an overall safety lifecycle model as the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems;
- covers all safety lifecycle activities from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal;
- encompasses system aspects (comprising all the subsystems carrying out the safety functions, including hardware and software) and failure mechanisms (random hardware and systematic);
- contains both requirements for preventing failures (avoiding the introduction of faults) and requirements for controlling failures (ensuring safety even when faults are present);
- specifies the techniques and measures that are necessary to achieve the required safety integrity.

Standards - IEC61508

- (part 5) specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.
- specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.

Standards - IEC61508

- (part 6) specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
- specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.

Standards - IEC61508

- (part 7) The objectives and requirements for the E/E/PES and software safety lifecycle phases are contained in IEC 61508-2 and IEC 61508-3 respectively.
- (part 7.1) structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.
- (part 7.2) develop a level of understanding of the Equipment Under Control (EUC) and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.
- (part 7.3) determine the boundary of the EUC and the EUC control system.

Standards - IEC61508

- (part 7.4) determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and misuse.
- determine the event sequences leading to the hazardous events determined by the analysis.
- determine the EUC risks associated with the hazardous events determined by the analysis.

Standards - IEC61508

- (part 7.4) determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and misuse.
- determine the event sequences leading to the hazardous events determined by the analysis.
- determine the EUC risks associated with the hazardous events determined by the analysis.

Standards - IEC61508

- (part 7.5) develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.

Standards - IEC61508

- (part 7.6) allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety related systems, other technology safety-related systems and external risk reduction facilities.
- allocate a safety integrity level to each safety function.

Standards - IEC61508

- (part 7.7) develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.
- (part 7.8) develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.

Standards - IEC61508

- (part 7.9) develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.
- develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.

Standards - IEC61508

- (part 7.10) create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements). See IEC 61508-2 and IEC 61508-3.
- (part 7.11) create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.

Standards - IEC61508

- (part 7.12) create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities.
- (part 7.13) install the E/E/PE safety-related systems.
- commission the E/E/PE safety-related systems.

Standards - IEC61508

- (part 7.14) validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.
- (part 7.15) operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.

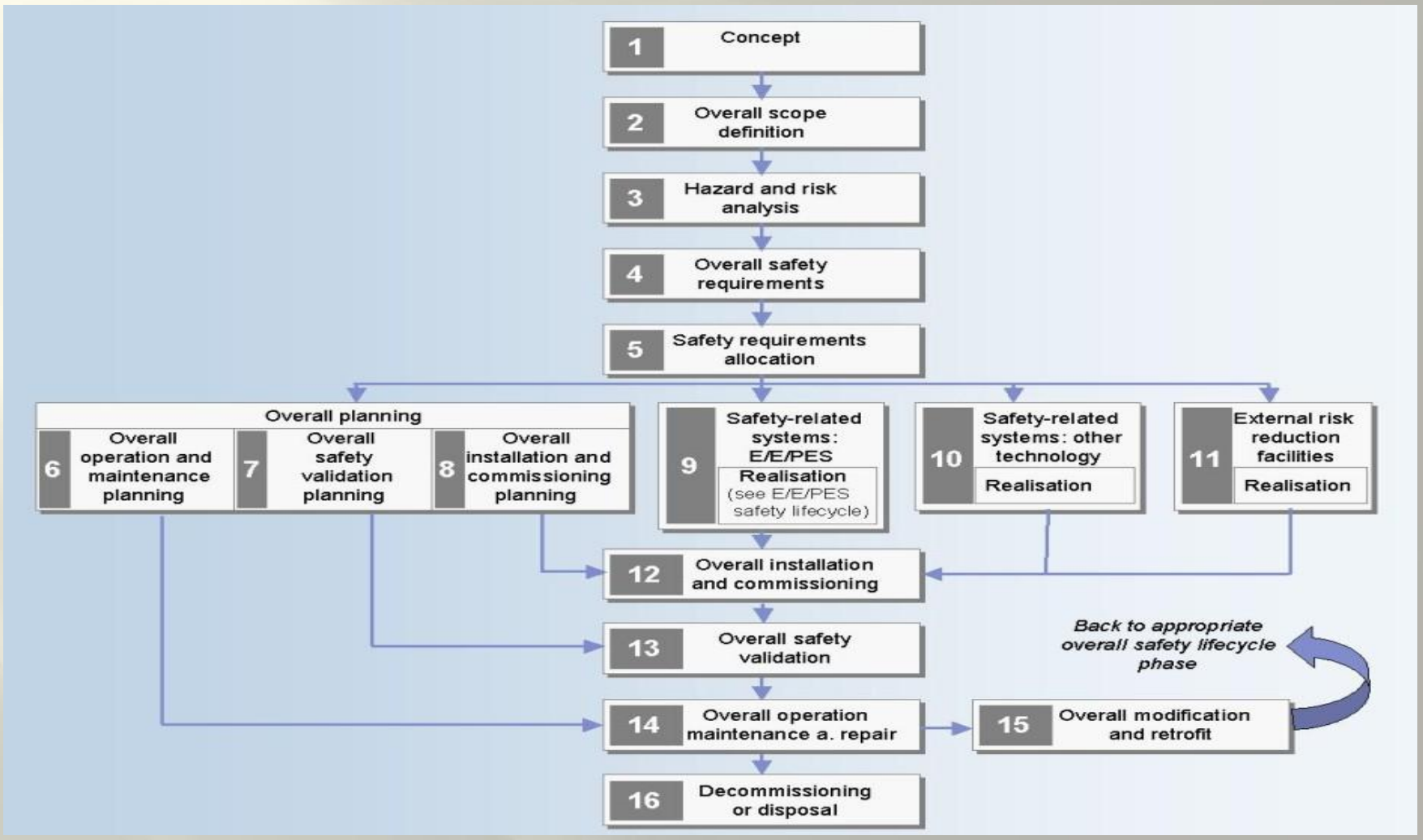
Standards - IEC61508

- (part 7.16) ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.
- (part 7.17) ensure that the functional safety for the E/E/PE safety-related systems is appropriate for the circumstances during and after the activities of decommissioning or disposing of the EUC.

Standards - IEC61508

- (part 7.18) demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- (part 8) investigate and arrive at a judgment on the functional safety achieved by the E/E/PE safety-related systems.

IEC61508 Safety Lifecycle



Standards - IEC61511

- (part 5) identify the management activities that are necessary to ensure the functional safety objectives are met.
- (part 6) define the phases and establish the requirements of the safety life-cycle activities;
- organize the technical activities into a safety life cycle;
- ensure that adequate planning exists (or is developed) that makes certain that the safety instrumented system shall meet the safety requirements.
- (part 7) demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases of the safety life cycle identified by the verification planning.

Standards - IEC61511

- (part 8) determine the hazards and hazardous events of the process and associated equipment;
- determine the sequence of events leading to the hazardous event;
- determine the process risks associated with the hazardous event;
- determine any requirements for risk reduction;
- determine the safety functions required to achieve the necessary risk reduction;
- determine if any of the safety functions are safety instrumented functions

Standards - IEC61511

- (part 9) allocate safety functions to protection layers;
- determine the required safety instrumented functions;
- determine, for each safety instrumented function, the associated safety integrity level.
- (part 10) specify the requirements for the safety instrumented function(s).
- (part 11) design one or multiple SIS to provide the safety instrumented function(s) and meet the specified safety integrity level(s).
- (part 12) define the activities required to develop the application software for each programmed SIS subsystem;
- define how to select, control, and apply the utility software used to develop the application software;
- ensure that adequate planning exists so that the functional safety objectives allocated to the application software are met.

Standards - IEC61511

- (part 13) perform a factory acceptance test (FAT) to test the logic solver and associated software together to ensure it satisfies the requirements defined in the safety requirement specification.
- By testing the logic solver and associated software prior to installing in a plant, errors can be readily identified and corrected.

Standards - IEC61511

- (part 14) install the safety instrumented system according to the specifications and drawings;
- commission the safety instrumented system so that it is ready for final system validation.
- (part 15) validate, through inspection and testing, that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirement specification.

Standards - IEC61511

- (part 16) ensure that the required SIL of each safety instrumented function is maintained during operation and maintenance;
- operate and maintain the SIS so that the designed functional safety is maintained.
- (part 17) modifications to any safety instrumented system are properly planned, reviewed and approved prior to making the change;
- ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

Standards - IEC61511

- (part 18) ensure that prior to decommissioning any safety instrumented system from active service, a proper review is conducted and required authorization is obtained;
- ensure that the required safety instrumented functions remain operational during decommissioning activities.

Standards - IEC61511

- (part 19) ensure that the necessary information is available and documented in order that all phases of the safety life cycle can be effectively performed; and
- ensure that the necessary information is available and documented in order that verification, validation and functional safety assessment activities can be effectively performed.

IEC61511 Safety Lifecycle