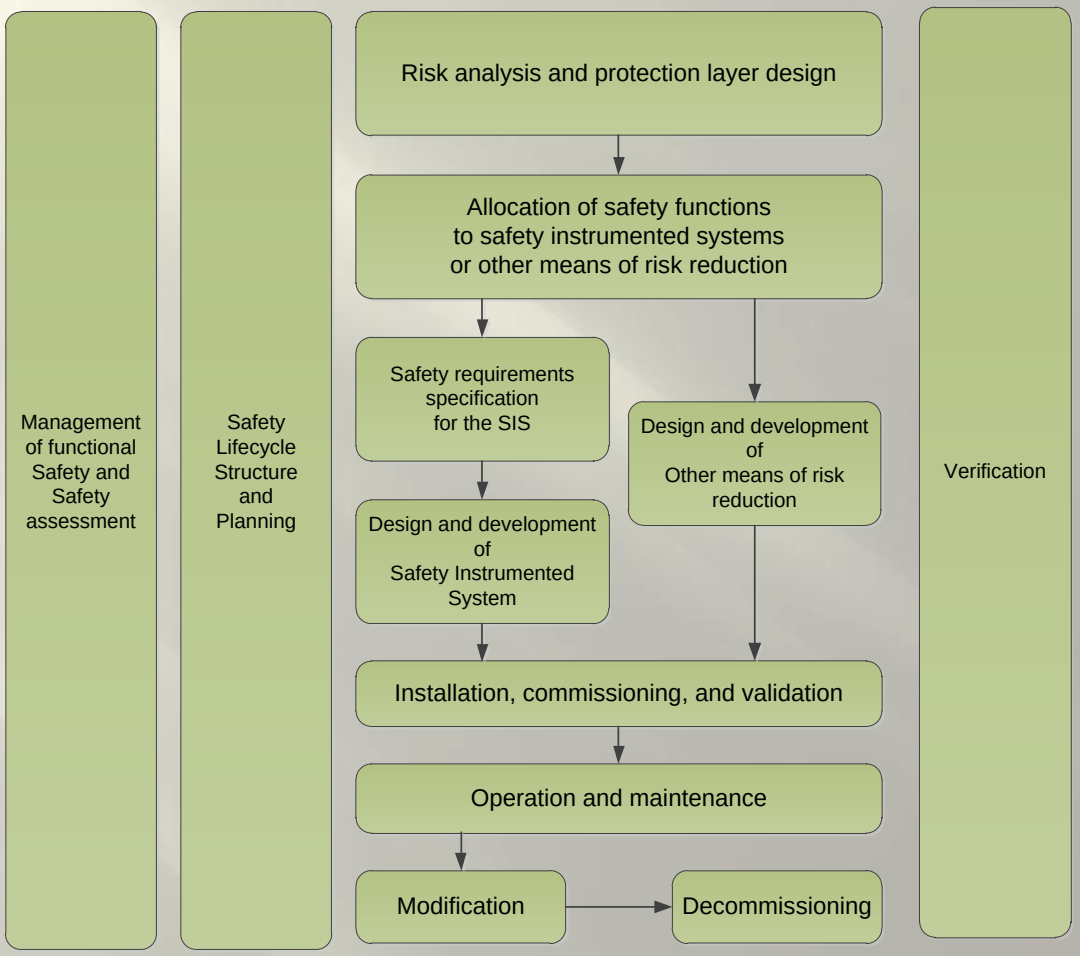
Controlling Risks
Hazard Assessment and Risk Analysis

Analysis Phase



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.

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.

*EUC= Equipment Under Control

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

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

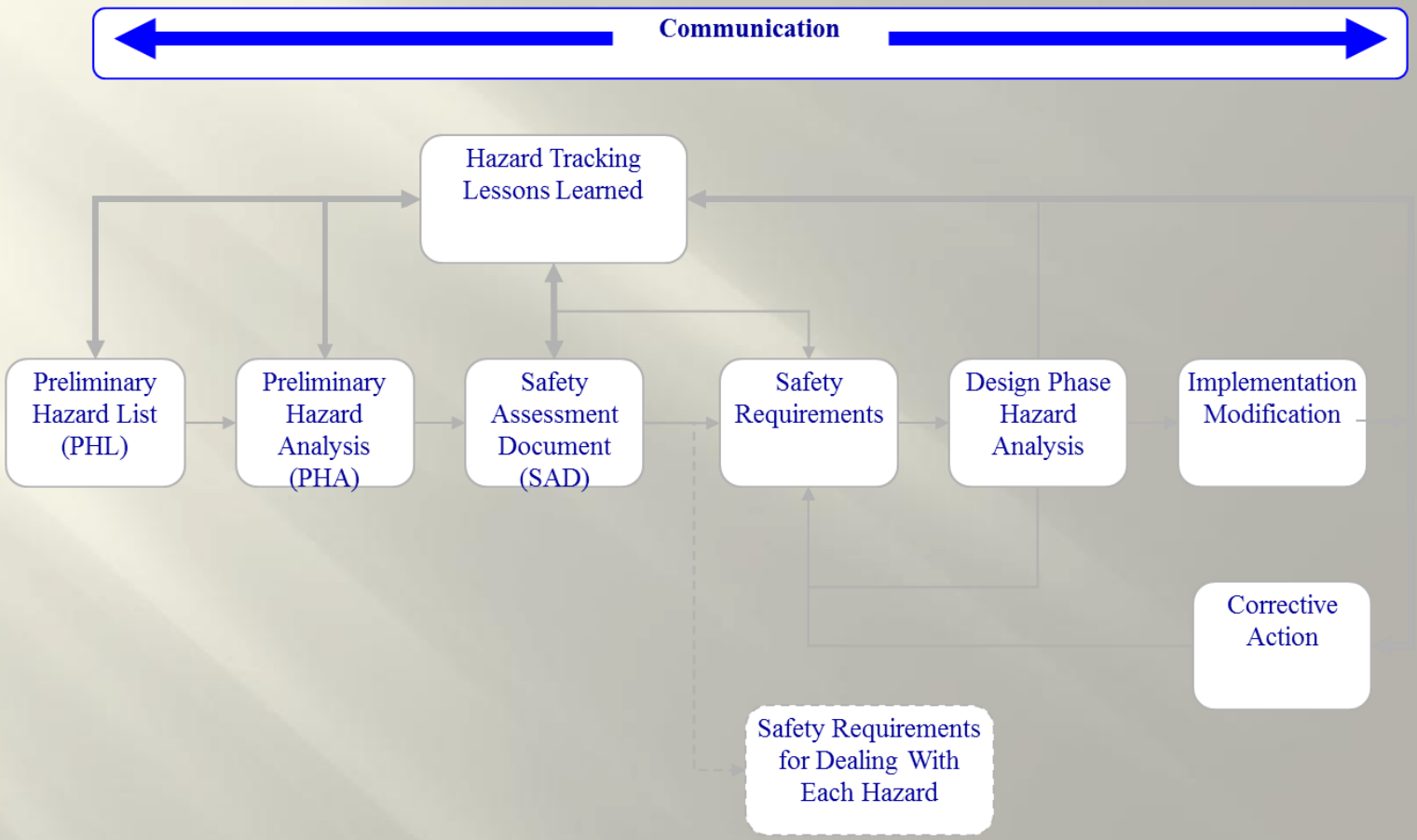
Hazard Assessment: Identification

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

Hazard Identification Processes

- Preliminary Hazard Assessment (PHA)
- Preliminary Safety Assessment Review (PSAR)
- Safety Assessment Document (SAD)

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

Title:	ASIS PHL Example
Date:	PHL4/20/04 PHA FHA
Evaluator:	K. Mahoney

Hazard Analysis Worksheet

To be completed during PHL
To be completed during PHA
To be completed during Final HA

Facility:	USPAS-A-TRON
Purpose:	Preliminary Hazard Li

Location: Univ. Wisc. Madison

				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
☐	1-1	Prompt ionizing radiation in beam enclosure due to source other than beam.	Radiological	Employee							
☐	2-1	Exposed energized electrical bus on dipole magnets in beam enclosure.	Electrical	Employee							
☐	3-1	Oxygen deficient environment due to helium leak	ODH	Employee							
☐	4-1	Microwave radiation in excess of 5mW/cm2 due to open waveguide.	Electromagnet	Employee							
☐	5-1	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Employee							
☐	5-2	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Equipment							

PHL Approved:_____ Date:_____

Classroom Exercise

- 32 MeV accelerator
  - Gun deck
  - Steering magnets
  - RF section
- Experimental Cave
  - Steering magnets
  - RF section
  - Experimental target

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