SAND2013-8335C

Exceptional service in the national interest

Sandia National Laboratories

STAR

Shock Thermodynamics Applied Research

Perspective on Engineered Safety: *Are All Accidents Preventable?*

Bill Reinhart

Condensed Matter Physics

Sandia National Laboratories

64th Aeroballistics Range Association

Destin, Florida

October 6-11th, 2013

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overture: Perspective

Sandia National Laboratories

Accident, mishap, misfortune, calamity, misadventure, happenstance, mistake, series of unfortunate events

Engineered Safety is a principle/assurance based approach for designing systems that are inherently safe

Corporate

Line Management

Worker

Understanding the Premise

Sandia National Laboratories

- ***Principle Base vs. Rules Based***
  - ***–thinking approach rather than rule approach***
    - *conceptual basis as rules are inevitable*
- ***Engineered Safety concepts are NOT new***
  - ***– thrust is on defining accountability***
  - ***– documentation***
  - ***– work planning and control practices are the driving force for conduct of operations***
- ***Recent events have brought on 'rethinking'***

Engineered Safety: Consequences

Sandia National Laboratories

- *Consequences of mistakes—no longer in the business to provide programmatic services to those customers*
  - *hence, forethought is required to maintain and provide services*
- *Corporate shut down of operations pending formal review prior to restart*
  - *Evaluate all technical processes, comprehensive safety engineering analysis, work planning and controls*
    - *Hope to take into account items taken for granted, complacency, and keeping defects out of planning*
  - *Undermines customer confidence*

Engineered Safety: Need for Improvements

Sandia National Laboratories

- *WPC are the driving focus for conduct of operation*
- *WPC practices will <u>not</u> in itself detect design flaws*
- *WPC does not prevent Engineered Safety (ES) from being incorporated*
  - *But also does not promote ES*

SAFETY NEEDS TO BE CONSIDERED IN A SYSTEM ENGINEERING CONTEXT

Engineered Safety: Review

Sandia National Laboratories

Utilize Engineered safety following the 5 point STAR on the integrated safety management system (ISMS)

- Emphasize engineering approach to design and safety controls
  - Poor engineering=>notable accidents
- Clarify operational (technical) requirements with emphasis on whom is responsible
  - Define programmatic requirements
  - Determine how to be safe while satisfying those requirements
    - Operational safety requirements need to be built into the requirements from the beginning
- Maintain consistency with ISMS and conduct of operations

Engineered Safety: Review

Sandia National Laboratories

Consideration of Risk: Rigor vs. Potential Consequence

- Rigor: builds probability
  - assume low probability without technical knowledge
- Consequence: worse thing that can happen
  - All the things that can happen, <u>regardless on the likelihood</u>

Implementation

Implementation comes from the Line Management

- They own the responsibilities, the accountability for the implementation within the design, operation, of all activity level work
- Line will bring together SME's, get to the point where you can make informed decisions
  - Line is NOT necessarily the SME
  - Ultimately be 'well-informed'
- Lessons Learned
  - research
- Implementation will be the governed by this one approach - ES
- Prioritize implementation based on consequences, new activities, and severity

ES Implementation: Line

Sandia National Laboratories

- Managers tasked to implement
  - Since this safety approach is new, must 'step back' to define the method and relax the staff (worker)
  - Follow the plan-define the task
- Director is responsible to ensure implementation
- Senior Manager will ensure implementation
- Department Manager is responsible for execution

ES Implementation: The approval Process

Sandia National Laboratories

ES Implementation: The approval Process

Sandia National Laboratories

Define Scope

- Identify Work Planner
- Establish Work Planning Team
- Identify Hazards and Authorization Bases
- Evaluate Key Factors Document Analysis

feeds into

Line Management Decision on Work Acceptance

- *Determine the highest potential unmitigated-accident-consequence category.*
- Line management approval authority's definition of unacceptable consequences.

ES Implementation: The approval Process

Analyze Hazards

- Detailed Identification Of Hazards
- Identify Safety Themes, Standards and Codes
- Perform Failure Mode Analyses

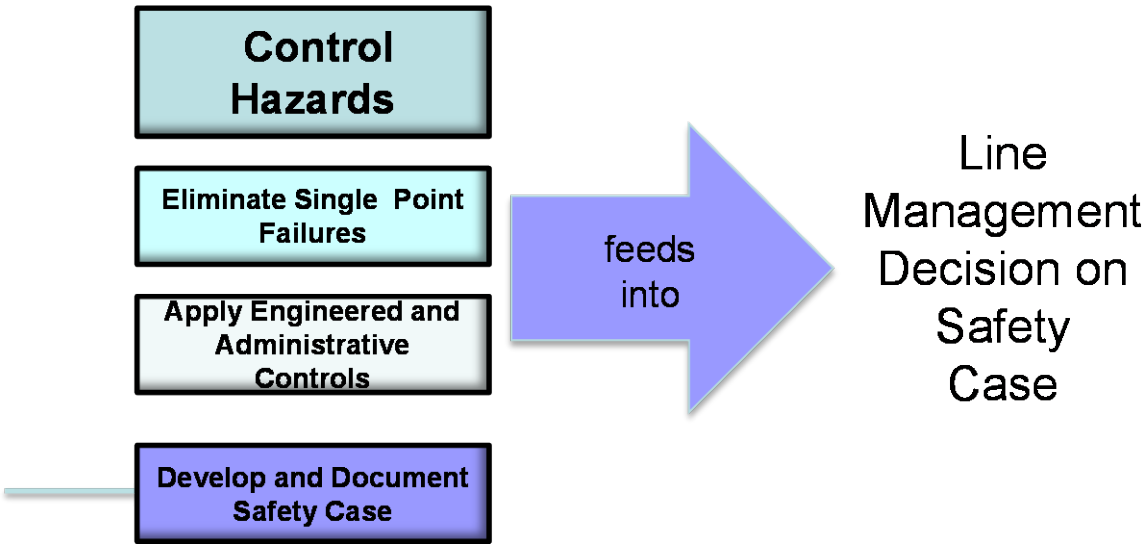
feeds into

Line Management Decision on Work Acceptance & Line Management Decision on Safety Case

- Concept: Safety theme is an overarching technical strategy aimed at stimulating upfront critical thinking on the prevention or mitigation of accident consequences.
- Failure modes of THE SYSTEM: method that identifies single-point failure modes that can result in accidents having unacceptable consequences
- No rigor-level determination

ES Implementation: The approval Process

Sandia National Laboratories



- Eliminate hazards and eliminate single-point failures.
- The safety case is line management's narrative explanation of how the criteria in Focus on understanding & control of energy source.
- The concept of independent engineered controls.

ES Implementation: The approval Process

Sandia National Laboratories

Prepare and Perform Work

Complete Preparations
Document Authorization
- **Complete TWDs**
- **Perform Final JSA**
- **Team Trained & Qualified**
- **Perform Readiness Review**

Perform Work

feeds into

Line Management Decision to Authorize Work

Feedback & Improve

Self Assessment

Lessons Learned

Corrective Actions

Management Surveillances

ES Implementation

Sandia National Laboratories

Implementation strategies corresponding to the following hazard categories:

- ***Industrial standard hazards and low***
- ***Industrial moderate***
- ***Accelerator hazard***
- ***Nuclear hazard***

From the process Define, Analyze, Control as well as other documents (PHS, HA); hazard categories are defined within its envelope

ES Implementation

Sandia National Laboratories

Hazard Category	Accident Consequences (Unmitigated)	Target Level Engineered Controls	SNL Approval
Nuclear	The consequences of unmitigated releases of radioactive and hazardous materials - See DOE Orders and Standards for details on Hazard Category 1, 2 and 3	2 to 3	VP
Accelerator	Potential to create a radiological area, ionizing radiation and consequences from numerous industrial hazards - See DOE Orders & Standards for Accelerators for details	2 to 3	VP
Industrial (high)	Potential for significant off-site impacts to the public or the environment	2 to 3	VP
Industrial (moderate)	Potential for significant on-site impacts to co-located workers or the environment	2	Director
Industrial (low)	Potential for significant localized impacts to the workers or the environment	1 to 2	Level II Manager
Industrial (standard)	Potential for significant localized impacts to workers from common industrial hazards - engineered controls may be sufficient in purchased equipment	1 to 2	Level I Manager

Worker/Planer Team

Sandia National Laboratories

- *responsible for completed safety documentation*
- *design and execute safe operations*
- *develop the safety case and the bounds of safe work*
- *know the training requirements*
- *know the operational requirements*
- *know how to perform assignments*
- *know how to implement safety requirements*

This team will support line management decision making by providing the 'data' to make informed decisions.

Worker/Planer Team: Documentation

Sandia National Laboratories

- *National Environmental Policy Act (NEPA), Primary Hazard Screening(PHS), Site wide Environmental Impact study (SWEIS), Hazard Assessment (HA)*
  - *These form the backbone for all work—corporate mandates*
  - *addressing hazards and environmental considerations across the laboratories*
  - *Define basic training requirements*

These are the basic documents that the worker compiles so that ANY work can be

Summary

Sandia National Laboratories

- *Corporate Mandates were provided*
- *Line management implementation*
- *Worker/Planner provides documentation, SME's:*

Line Management provides approval based on information provided (worker) there will be preventable accidents and safe working environment

But are we sure

How do we avoid the same old mistakes?

Sandia National Laboratories

- ***Turn hindsight (lessons learned) into foresight(best practices)***
  - ***you will achieve far greater long-term success than if you simply ignore or forget what occurred once a project ends. This approach can greatly reduce the negative effects of attrition on a company's intellectual assets when people leave because they quit, retire, are laid off, or were temporary workers to begin with.***
- ***It's said there are no new project management sins, just old ones repeated. It's also said that we don't learn the lessons from past projects and this must be true, otherwise why would we keep making the same old mistakes?***
- ***In looking at lessons learned, many times we find things like - should have had a better schedule, or better budgeting, or more communications, spent more time on requirements, etc. All of these things relate to how we do the work, not what we work on. Talking about how things get done or working on how things get done does not, in and of itself, get anything done. This is one of the reasons so many people hate planning - planning is not doing and we all like doing***
  - *"We should have - " as lessons for all managers to learn before their project fails to meet expectations. Prevention is much cheaper than cure.*

"Relying on luck is not a viable project strategy; however, this is what we do when we ignore lessons learned."

Accident Complexity

Sandia National Laboratories

An accident may have 10 or more events that can be causes.

When accidents are investigated, the emphasis should be concentrated on finding the root cause of the accident rather than the investigation procedure itself so you can prevent it from happening again

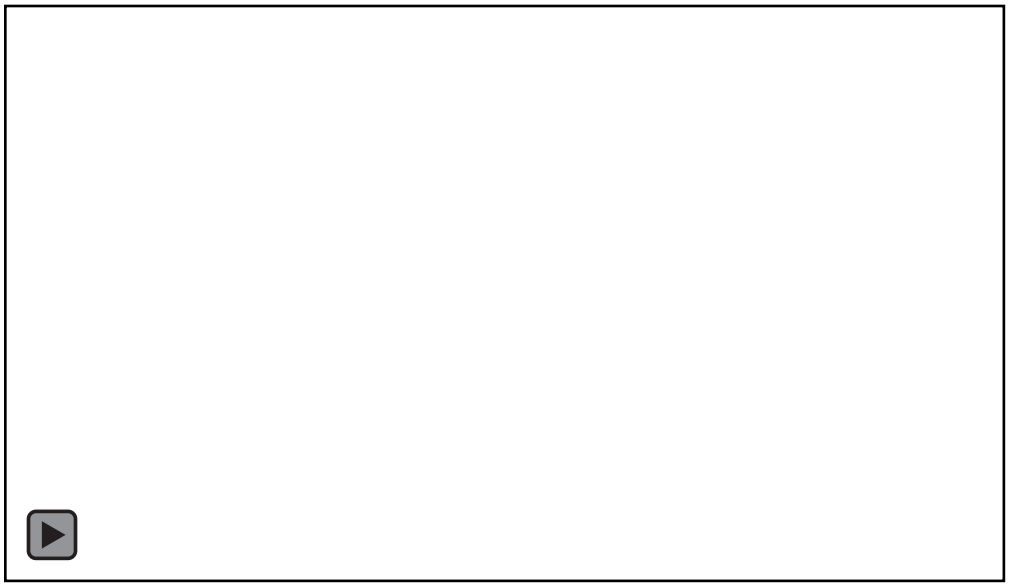
- ***Direct Cause: the immediate event (usually the result of the Indirect cause)***
- ***Indirect Cause (Root) : the factor that if corrected would have prevented the direct cause (can usually be traceable to the Basic Cause) and will prevent recurrence.***
- ***Basic Cause : policies, decisions, personal, environmental factors***

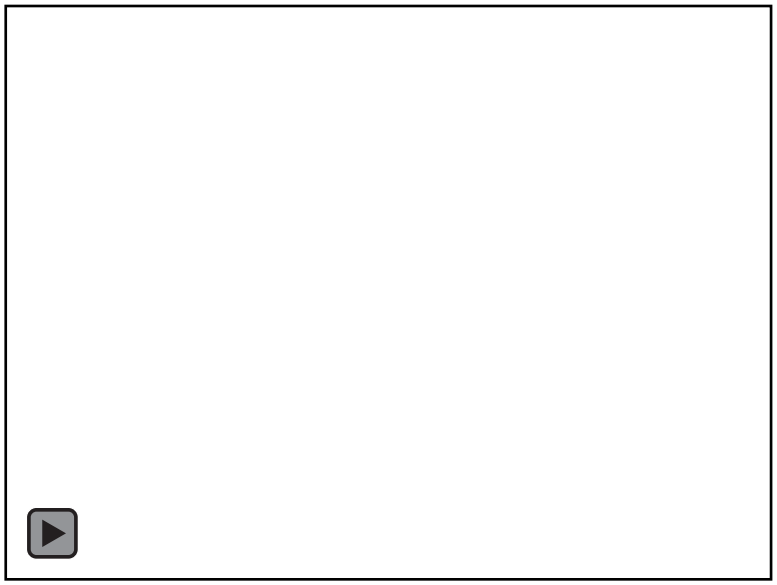
Are All Accidents Avoidable?

Sandia National Laboratories

This is a controversial subject

- ***Management tend to believe they are indeed preventable***
- ***Workers tend to believe that all accidents are NOT preventable***
- ***Safety professionals are split***





Sandia National Laboratories

Discussion:

Q & A

Interactive

All Accidents ARE Avoidable

Sandia National Laboratories

- ***An accident is avoidable, up to a certain point***
- ***Safety people think steps ahead, see patterns***
- ***An accident is not a sudden event, it is a series or chain of events***

If you believe that accidents are NOT avoidable, you may be thinking down the causal chain AT the point of the accident

- ***The further upstream thinking you do, the more prevention opportunities present themselves***

PREVENTABLE DOES NOT MEAN PREVENTED
STRATEGY, EARLY DETECTION – EARLY PREVENTION

Accidents: Good vs. Bad

Sandia National Laboratories

- *Each accident has a sequence of events that precludes the accident, such as the failure of a safety system-*
  - *which can be undetected faults, failure of components or unavailability, or the operator fails to act on a fault*
- *Accidents: Are they good? What do accidents bring to the table?*
  - *Lessons learned, improved safety features*
  - *"The cause of a problem which, if adequately addressed, will prevent a recurrence of that problem."*

No one really wants an accident to occur

  - *Injury, property damage, environmental consequences*