SAND2018-12329C

40th Tritium Focus Group Meeting
Albuquerque, New Mexico, USA
October 23-25, 2018

Philosophical Approaches to Safety for High Hazard Facilities

Alexander L. Brown; albrown@sandia.gov; (505)844-1008
Fire Science and Technology Department
Lynelle Takahashi; Analytical Technologies Department

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Outline

- Safety Culture
  - Introduce safety approaches for a variety of similar communities
- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Approaches
- Summary

Various Safety Communities

- This presentation will consider examples from other similar safety communities
- Intent is to initiate conversations around culture of being 'safe'
  - No magic solution
  - Some ideas and alternatives shown
  - Variety of approaches

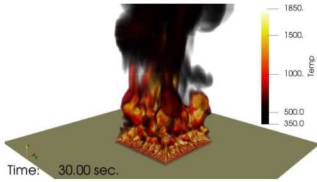
Nuclear Power Plants (NPP)

- Probabilistic Risk Assessment (PRA) based
- Safety to aircraft impact?
  - 10 CFR 50.150
  - NEI 07-13

Nuclear Weapons (NW)

- Always/Never
- ASC Program
- RCAS/PLOS
- Perennial Programs
  - Different safety at various handling points

Munitions Shipping (DoD)



- Test oriented
- Fast/Slow heat
- Governed by Regulations
  - STANAG 4240, 4382, 4439
  - MIL-STD-2105C
  - AOP-39E(3), TB 700-2

Various Safety Communities

Launch Safety (LS)

- Launch with radioactive material requires presidential signature
- Reviewed by INSRP committee
- 'Databook' provides consistent source of information
- Safety assessment prior to each launch
- Executive Order 12114, *Environmental Effects Abroad of Major Federal Actions*

Nuclear Material Shipping (Nuc)

- All about containers, governed by
  - 49CFR171-178
  - For radioactive materials 10CFR71
- Prescriptive testing
- Conservative test conditions
- Battery of tests
  - Fire/impact

Commercial Fire Safety (FS)

- Managed by fire safety engineers
- Lots of regulations, tools
- Commercial testing for safety (UL listing)
- Facility sprinklers, alarms
- Response teams constant training

Tritium Operations (T_2)

- HazCat regulated
- New regulatory proposals from 2017 working group
- Simplified risk categorization
- HDBK 3010

Outline

- Safety Culture
  - Introduce safety approaches for a variety of similar communities
- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Summary

Why Safety?

Sandia National Laboratories

- The obvious (direct):
  - We don't want to harm or kill, damage or destroy property
  - But we still have important hazardous work to perform
- The indirect (less obvious) factors:
  - Blame/fall-out when something occurs
  - We don't want lawsuits that come therefrom
  - Lapses result in operational investigations, lack of public trust
  - Diminished credibility, loss of employment
- Note there are multiple stakeholders
  - Operational PIC, workers, public, institution, customer of product, lawyers, etc.

Safety is a problem of infinite scope

- Infinite scenarios
  - People do random things
  - Institutional and project differences in handling and design

- Infinite sequences
  - Sometimes a cascade or comedy of errors can occur
- Infinite magnitudes
  - Largest magnitude may not be the most severe
- Large number of hazards
  - Fire, explosions, accidents, lapses in process/procedure, vandalism, etc.

To accommodate operations, scope needs limiting

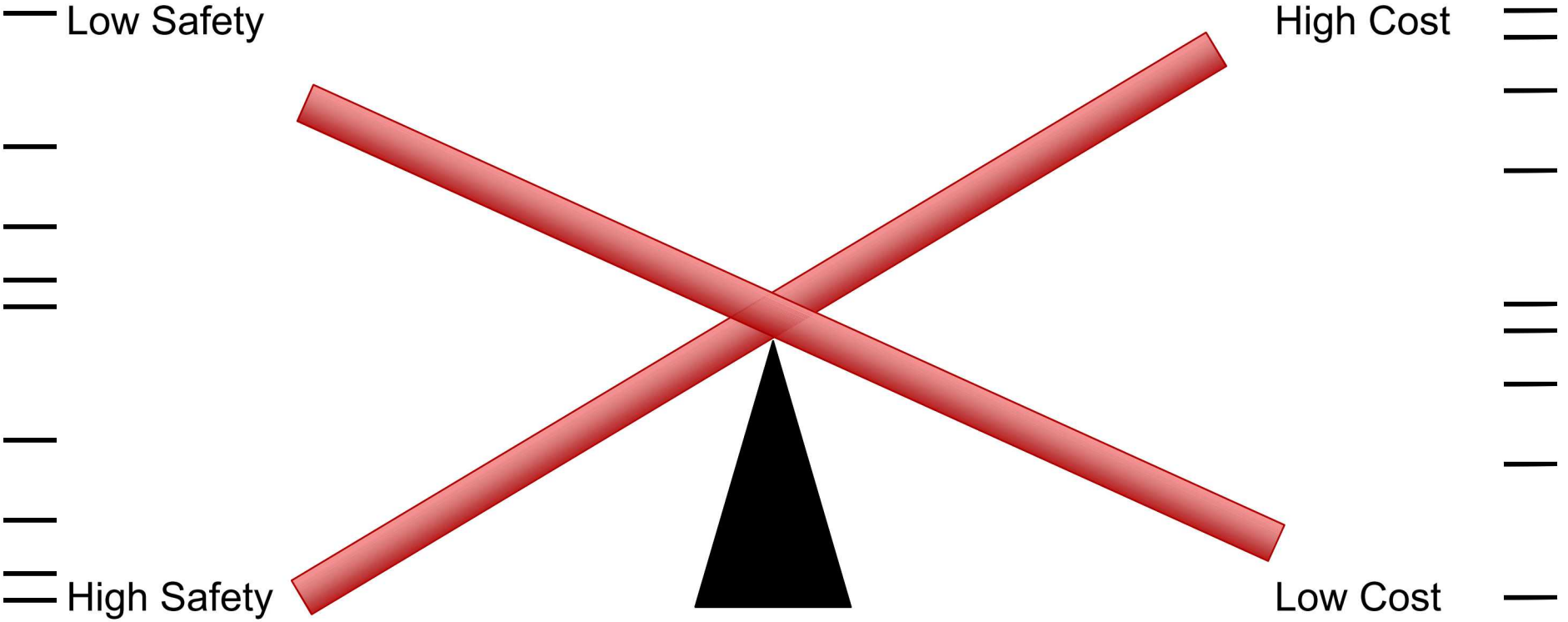
Safety Versus Cost

Sandia National Laboratories

A trade-off exists between safety and cost

Scales are not necessarily linear, and high cost isn't necessarily high safety and vice versa

This is really an optimization problem targeting acceptable safety risk (good enough?)



A strategic approach looks to maximize safety while minimizing cost

Complex Composition of Cost Function

Cost can be incurred at various stages, philosophy often dictates the cost structure:

1. Design and design variants
2. Understanding the physical processes
3. Protocol implementation and operational
4. Handling and protection systems
5. Post-event (usually undesirable)
6. Approvals
7. Scenario/event analysis
8. Stand-down, or operational limitations
9. Tie-in with security
10. Compliance

Just because one cost is down doesn't mean all are

Perception as part of Safety

Sandia National Laboratories

- Did something ever happen (the risk incident)?
  - Even if no, there may be a near miss that has repercussions
- Did the incident lead to a consequence?
  - We often get too focused on the last incident
- Are random and unforeseen events mitigated?
  - Fukushima-Daiichi (beyond design basis)
  - 9-11 (safe for ground vehicle explosions)
- Are processes sensible and clear such that they are followed?
- Exchange of information between institutions with similar hazards is helpful.
- Are future events properly foreseen?
  - Safety is often overly focused on past events, not future
- Redundancy?

Safety 'Solutions'

Sandia National Laboratories

- No single right answer
  - Just because community 'x' does it this way doesn't mean it is right or best for community 'y'
- Challenging problem
  - When is it enough?
- Multiple possible solutions
  - Safety is usually a compendium of approaches
- Use of subject matter experts
  - Experience is a good instructor

Observations

- Sometimes safety process is too prescriptive, not sufficiently flexible
  - Observed this in multiple communities
  - Over-design of 'safety' equipment and paperwork unlikely to do anything helpful
  - Focused on the wrong thing
- Case 1: Preparing for a fire test, management oversight was focused on firebrands, resulted in scrapping an informative pre-test experiment
  - We ended up in the wrong facility with sub-standard conditions and high programmatic risk
  - Weather inversion caused smoke from test to irritate another nearby facility (the real risk/hazard was truly unforeseen)
- Case 2: NPP design for aircraft impact
  - Saving the plant with doors rules, thin walls, overdesigning where potentially unnecessary; designing to the rule of thumb
- Case 3: SNL Rocket sled track accident
  - Hundreds of pages of 'safety' documents
  - Incident due to a cascade of multiple issues (combination of mishaps)

Outline

- Safety Culture
  - Introduce safety approaches for a variety of similar communities
- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Summary

On Managing Complexity

Sandia National Laboratories

- Infinite possibilities, problem of infinite proportion
  - Measures often taken to limit scenarios or simplify the problem
  - Comes with risk
- We often don't fully understand the physics (may require tests)
  - Tests or correlations might not be fully applicable to all scenarios of interest
  - Simplified abstractions are often deployed whether they are good or no
- Cost structure isn't always obvious from the start
  - Sometimes a cost savings in one area balloons costs in another
- Legacy 'safety' is often hard to amend, even if it badly needs improvement
  - It worked before, let's keep doing it; change is hard/perilous
  - If there is an issue, blame the guy who first implemented it 50-100 year ago
- A continuous incremental approach has some value
  - Acknowledges limitations, but consistently works to improve
  - Is receptive to alternative approaches
  - Helps train capable new people

Observed Approaches

Sandia National Laboratories

Regulate to a conservative assumption

Probabilistic/statistical approaches, high fidelity mod/sim

Physical experimentation to better understand hazards

Review committees for approving assessments and assertions

Approved methods for defining acceptable risk scenarios

Analysis of scenarios

Guides (handbooks), tools (correlations, simple software) approved for use

'Admiral' tests (show it passes once)

Engineered safety (preclude risks with engineering design)

Sub-system assessments (scale-up approach)

Critical thresholds

No single one of these makes operations safe, but each are sensible components of a safety approach

Approaches

Approach	NW	DoD	Nuc	NPP	FS	LS	T_2
Regulate to a conservative assumption				Y	Y		Y
Probabilistic/statistical approaches, high fidelity mod/sim	Y			Y	Y	Y	
Physical experimentation to better understand hazards	Y	Y	Y		Y	Y	
Review committees for approving assessments and assertions	Y			Y		Y	
Approved methods for defining acceptable risk scenarios	Y	Y	Y	Y		Y	
Analysis of scenarios	Y			Y	Y	Y	
Guides (handbooks), tools (correlations, simple software) approved for use				Y	Y	Y	Y
Admiral tests (show it passes once)	Y	Y	Y				
Engineered safety (preclude risks with engineering design)	Y		Y		Y		
Sub-system assessments (scale-up approach)	Y					Y	
Critical thresholds	Y	Y					Y

Summary

- Safety is of paramount importance to high consequence operations
- Safety can be very complex
  - Trade-off between components of cost and margins of safety
  - Challenging physics problems
  - Infinite scenario space
  - Optimization problem
- Different communities handle safety mandates differently
  - Variety of approaches, each with associated cost and risk
  - Approaches can be tailored to the problem to best deal with each scenario

Acknowledgements

- Sandia National Laboratories is a multimission laboratory operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc. for the United States Department of Energy's National Nuclear Security Administration under Contract No. DE-NE0003525.
- Russell Jarek, James Jessen, and Rajan Tandon provided review comments.

Questions?

Sandia National Laboratories

RCAS-Jim Nakos

- Methodology was documented in SAND92-2538, "Heavy Water New Production Reactor Design Review Guidelines," Appendix E.
- From a test engineer's point of view it was a major step forward. It provided structure to how one selects the test environment to test to, and the geometry to be modeled.
- There are cons:
  - How does one know if you have the "worst case" environment? – answer is you don't; all you can do is use your best judgment. Also, RCAS doesn't try to find worst case, just on that is conservative (try to find most severe)
  - The process requires some qualitative analysis and judgment that could be criticized – no way around this because enough data does not exist.

Bibliography

- Gelbard, F.; Brown, A.L.; Louie, D.L.Y.; Feng, C.; and Bixler, N.E.; "A Basic Principles Approach for Determining Radionuclide Aerosol Releases from Accidental Explosions in Reprocessing Facilities," November 10-14, 2013 American Nuclear Society's Winter Topical Meeting.
- Brown, A.L., C. Feng, F. Gelbard, D. Louie, and N.E. Bixler, "Predicted Liquid Atomization from a Spent Nuclear Fuel Reprocessing Pressurization Event," The 2014 ASME/AIAA Summer Conference, Atlanta, Georgia, June 16-20, 2014.
- Brown, A.L., "New Methods for Predicting Shock and Impact Induced Dispersal of Contained Liquids," The 2014 JANNAF conference, Albuquerque, New Mexico, December, 2014. SAND2014-19543C.
- Brown, A.L., and Louie, D. L. Y., "Contaminant Entrainment in a Liquid Fuel Fire," Proceedings of the 1st Thermal and Fluid Engineering Summer Conference, TFESC, New York City, USA, August 9-12, 2015. SAND2015-1360C.
- Brown, A.L., and Pierce, F., "A Modeling Method for Impact and Impulse Dispersed Liquids: Alternative Transfer Criteria and Sensitivity Analysis," ILASS Americas, the 27th Annual Conference on Liquid Atomization and Spray Systems, Raleigh, NC, May 2015. SAND2015-2042C
- Brown, A.L., Zepper, E., Louie, D. L. Y., and Restrepo, L., "Contaminant Entrainment from a Gasoline Fuel Fire," the Fall 2015 meeting of the Western States Section of the Combustion Institute in Provo, UT, USA, SAND2015-7185C. Paper 134IE-0033.
- Brown, A.L., Zepper, E., Louie, D., and Restrepo, L., "Entrainment of solid contaminants from pool fires," Proceedings of the First Pacific Rim Thermal Engineering Conference, March 13-17, 2016, Hawaii's Big Island, USA.
- Voskuilen, T.G., Pierce, F.G., Brown, A.L., Gelbard, F.E., Louie, D.L.Y., "Particle Resuspension Simulation Capability to Substantiate DOE-HDBK-3010 Data," Proceedings of the Winter 2016 ANS Meeting, November 6-10, 2016, Las Vegas, NV.
- Zepper, E.T., Brown, A.L., Pierce, F., Louie, D., and Restrepo, L., "Evaluating a Historical Airborne Release Test with Modern Modeling Methods," Proceedings of the Winter 2016 ANS Meeting, November 6-10, 2016, Las Vegas, NV.
- Pierce, F., Brown, A.L., Zepper, E.T., and Louie, D., "Contaminant Entrainment in a Liquid Fuel Fire with Multi-Component Evaporation Droplet Model," Proceedings of the Winter 2016 ANS Meeting, November 6-10, 2016, Las Vegas, NV.
- Pierce, F., Brown, A.L., Louie, D. Y.L., and Zepper, E.T., "Multicomponent Evaporation Effects on Particulate Release in a Liquid Fuel Fire," Proceedings of the 2nd Thermal and Fluid Engineering Summer Conference, April 2-5, 2017, Las Vegas NV, USA TFEC-IWHT2017-17668.
- Zepper, E.T., Brown, A.L., Pierce, F., Voskuilen, T., and Louie, D. Y.L., "Contaminated Fuel Fires: Parametric Sensitivity of Resuspension and Boiling Particle Evolution," Proceedings of the 2nd Thermal and Fluid Engineering Summer Conference, April 2-5, 2017, Las Vegas NV, USA, TFEC-IWHT2017-17709.
- Louie, David L.Y., Alexander L. Brown, Fred Gelbard, John Bignell, Flint Pierce, Tyler Voskuilen, Salvador B. Rodriguez, Remi Dingreville, Ethan T. Zepper, Pierre Juan, San Le, and Lindsay N. Gilkey, "NSRD-11: Computational Capability to Substantiate DOE-HDBK-3010 Data," SAND2016-12167, 2016.
- Koo, H., Brown, A.L., Voskuilen, T., and Pierce, F., "Rubble Fire Multi-Phase Model Development," SAND 2017-9463, June 2017.
- Koo, H., Brown, A.L., Voskuilen, T., Pierce, F., "Numerical study of pyrolysis and combustion of a carbon fiber-epoxy composite," Paper 2FI-0244, 10th US National Combustion Meeting, College Park MD, USA, 2017.
- Brown, A.L., Koo, H., Voskuilen, T., and Pierce, F., "Modeling a rubble fire consisting of comingled liquid and solid fuel," Proceedings of The JANNAF Interagency Propulsion Committee Meeting, 4-7 December, 2017, Newport News, Virginia, USA. SAND2017-12318C.

Why Want to Substantiate Handbook?

Sandia National Laboratories

- Safety analysts at DOE complex rely heavily on the data provided in this Handbook to determine the source term (ST)
- Five Factor Formula
  - $\mathrm{ST} = \mathrm{MAR} \cdot \mathrm{DR} \cdot \mathrm{ARF} \cdot \mathrm{RF} \cdot \mathrm{LPF}$
    - MAR - material at risk, DR – damage ratio, ARF – airborne release fraction, RF – respirable fraction & LPF – leak path factor
- More often, analysts simply take the bounding values to perform ST calculations to avoid regulatory critique
- Derived data (i.e., ARF & RF) from Handbook:
  - Very limited table-top and bench/laboratory experiments
  - Engineering judgement which may not have adequate bases
  - Actual situation may not be represented

HPC Platforms

Sandia National Laboratories

- As of April 2018, 237,978 processors are available within Sandia network across 10 machine platforms
  - Provides more than 2B CPU hours per year
  - High-end computing capacity: 2.1-2.7GHz with 3.5-4GB per processor
  - Ample storage: more than 50PB with high-speed access from computational processors
  - Only 2.5 years old in average; 5 of them are launched in 2017 or later
  - Not included are jointly funded machines that are located outside Sandia (ex> Trinity)

Outline

- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

NW Philosophy

- Safety starts with a theme
- STS (stockpile to target sequence) defines scenarios
  - These are abstractions
- Probabilistic use of simulation and testing to define risks
  - Test as much as possible
  - Mod/sim fills gaps, uses statistical representations
- Walsky criterion (10^{-6}) probability of failed safety theme
  - This number was a simplifying assumption
- Panel oversees continuing safety assessments
  - Annual review

Outline

- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

Munition Demonstrated Safety

Sandia National Laboratories

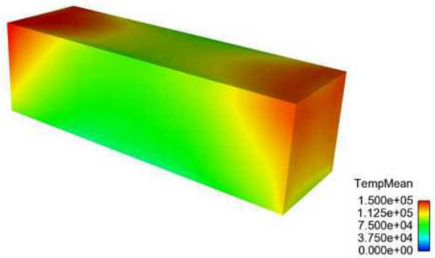
- Munitions and fires don't mix well, can be very hazardous
- It is impossible to eliminate the potential for fire environments
- Standards exist, and numerous documents (below) describe requirements
- Fast and slow heating test scenarios are typically required

Document	Title/Description	Relevance
MIL-STD-2105C	Hazard Assessment Tests for Non-Nuclear Munitions	Section 5.2, Insensitive Munitions Tests
STANAG 4240	Liquid Fuel/External Fire, Munition Test Procedures	Section 20, Test Requirements for Engulfing Munitions in a Fire
STANAG 4382	Slow Heating, Munitions Test Procedures	Section 11, Test Requirement for Slow Heating Tests
STANAG 4439	Policy for Introduction and Assessment of Insensitive Munitions (IM)	Definition of what qualifies as an "Insensitive Munition"
AOP-39E(3)	Guidance on the Assessment and Development of Insensitive Munitions (IM)	Page C-1 #2, simplified categories for thermal environment tests
TB 700-2	Department of Defense Ammunition and Explosives Hazard Classification Procedures	Section 5-7, UN test series 6, External Fire section

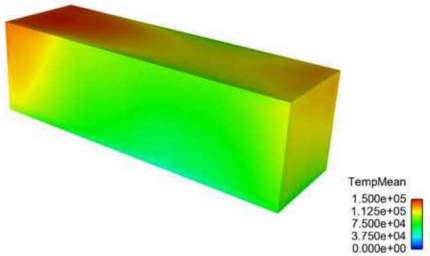
Munition Philosophy

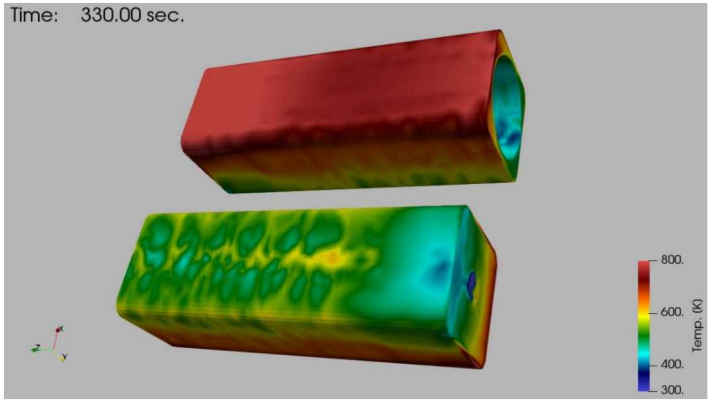
- Demonstrated failure in representative risk environments
- Approvals based on response to tests

A. Coarse mesh

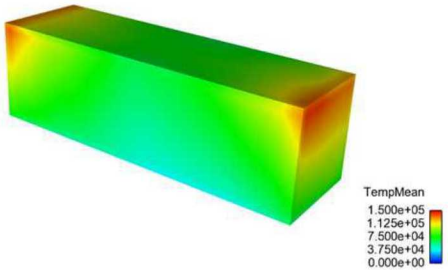


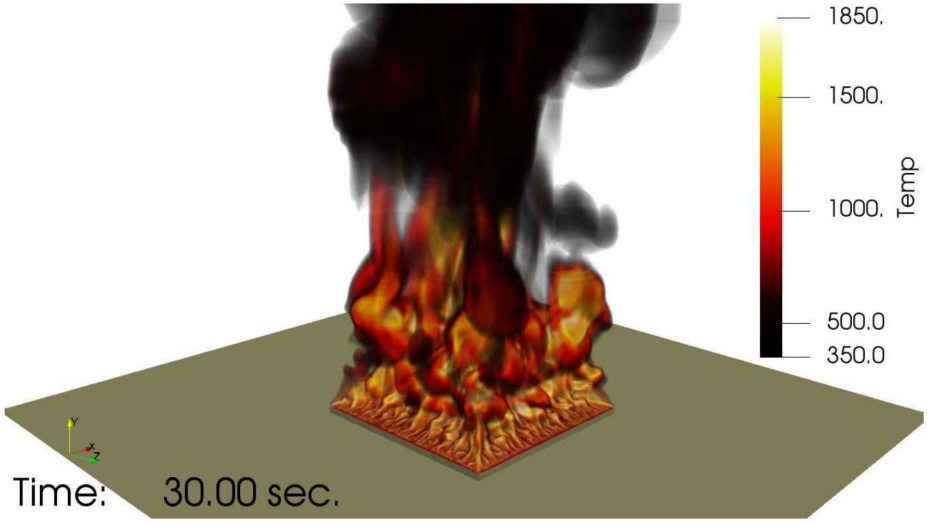
B. Medium mesh





C. Fine mesh



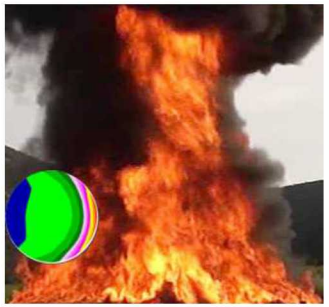


Outline

- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

Radioactive Material Transportation Regulations

- Transportation of hazardous material is regulated by the Department of Transportation in the Code of Federal Regulations, Title 49, Parts 171-178 (49CFR171-178).
- For radioactive materials, regulations from the Nuclear Regulatory Commission (NRC) in 10CFR71 also apply.
- The regulations provide increasing levels of rigor depending on the form and quantity of material being transported.
- For large quantities (known as Type B), packages must be accident resistant.



Regulatory Hypothetical Accidents
10 CFR 71.73

- Test sequence must be conducted so that the cumulative effect is the most damaging to the package.
- Individual tests are conducted with the package in the most damaging orientation.
- Test initial conditions regarding ambient temperature, internal heat load, and internal pressure must also be the most unfavorable.
- Following the accidents, the package must be leak tight, limit the external radiation dose rate, and be subcritical assuming the contents are in their most reactive credible configuration.

Nuclear Materials Philosophy

- Demonstrated failure in representative risk environments
- Iterative package design
- Approvals based on response to tests

Outline

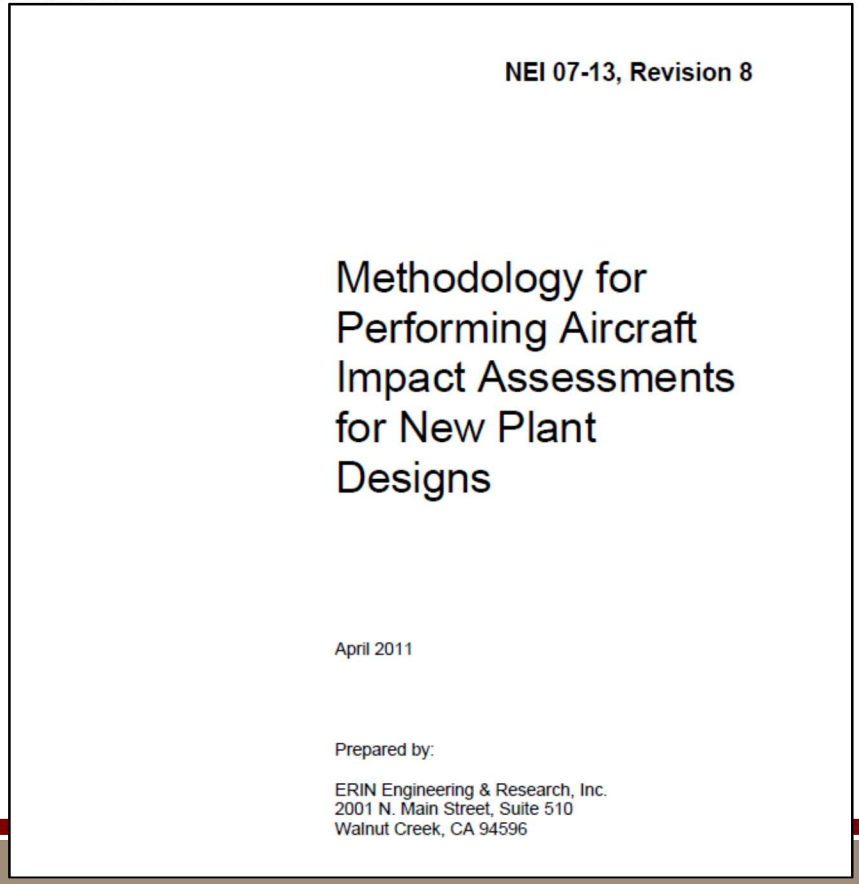
- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

Nuclear Power Plants

Sandia National Laboratories

- Each plant conducts/maintains a PRA, Probabilistic Risk Assessment document

- New US plants are assessed for aircraft impact (per 10 CFR 50.150)
  - NEI 07-13 provides guidance on approved methods
- Full assessment very costly
  - Creates simplified abstractions
  - Designs are altered to meet safety themes
- Assessments made to simplified rules
  - Full coverage not guaranteed
  - Provides some



NEI 07-13, Revision 8

Methodology for Performing Aircraft Impact Assessments for New Plant Designs

April 2011

Prepared by:

ERIN Engineering & Research, Inc.
2001 N. Main Street, Suite 510
Walnut Creek, CA 94596

Nuclear Power Plant Philosophy

Sandia National Laboratories

- Probabilistic assessments for plant operations and system functions

- Aircraft impact
  - Uses committee approved abstractions
  - Simplifications for fire made by conservative approximations
  - Results in some over-design of facilities (I'm OK with that)

Outline

- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

Fire Safety

- Usually managed by fire safety engineers
- Lots of regulations, tools
- Commercial testing for safety (UL listing)
- Facility sprinklers, alarms
- Response teams constant training

Outline

- Introduction to Safety
- Overview of High Hazard Safety Approaches
- Case Studies
  - NW Weapon System Safety
  - Military System Safety Fire
  - Nuclear Materials Packaging and Shipping
  - Nuclear Power Plants
  - Fire Safety (US regulatory)
  - Launch Safety
- Summary

Space Launch Philosophy

- Some probes require hazardous power source for longevity, heat, power, etc.
- ~99% of launches are successful
  - What about the 1%?
- Presidential approval required prior to launch
  - Approved software and tools
  - Data collected where necessary (meteorology)
  - Statistical assessments made
  - Advisory committee and accepted documents maintained
  - Testing performed to inform hazard classification