SANDIA REPORT
SAND2014-20064
Unlimited Release
Printed November 2014

Pantex Falling Man - *Independent Review Panel Report*

L. Bertolini, N. Brannon, J. Olsen, B. Price, M. Steinzig, R. Wardle, & M. Winfield

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-2087
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/help/ordermethods.aspx#online

SAND2014-20064
Unlimited Release
Printed November 2014

Pantex Falling Man
Independent Review Panel Report

Louis Bertolini
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

Nathan Brannon
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0483

Jared Olson, Bernard Price, and Robert Wardle
ATK Aerospace Group
PO Box 707
Brigham City, UT 84302

Mike Steinzig
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

Michael Winfield
Atomic Weapons Establishment
Aldermaston, Reading, RG7 4PR, United Kingdom

Executive Summary

Consolidated Nuclear Security (CNS) Pantex took the initiative to organize a Review Panel of subject matter experts to independently assess the adequacy of the Pantex Tripping Man Analysis methodology (13385-ANL-2, referred to as just 13385 through the rest of this SAND Report). The purpose of this report is to capture the details of the assessment including the scope, approach, results, and detailed Appendices. Along with the assessment of the analysis methodology, the panel evaluated the adequacy with which the methodology was applied as well as congruence with Department of Energy (DOE) standards 3009 and 3016. The approach included the review of relevant documentation, interactive discussion with Pantex staff, and the iterative process of evaluating critical lines of inquiry. Since 13385 was designed to be part of a larger hazards analysis process, the panel found it very difficult to evaluate in isolation. Only until the panel was exposed to broader factors of the operations, tool design, and hazard analyses, was the panel able to make an assessment of 13385. The panel determined that the methodology as defined in 13385 is an adequate baseline, along with its application to tool designs. The panel also determined that the methodology is congruent with regulatory requirements. For example, Pantex has used a statistical distribution (as opposed to a deterministic) method for input parameters (e.g., 95th percentile Pantex male weight) to 13385. The panel found several features of the methodology and application that render the assessment of adequacy unnecessarily cumbersome. Weaknesses in the methodology and recommendations for improvement are included in this SAND Report. The panel was unanimous with respect to the conclusions and recommendations. Key recommendations for improvement are:

1. Provide data from an updated Falling Man model to Design Agencies (DAs) for a representative sample of Falling Man scenarios to evaluate the change in predicted weapon response compared to the current revision of 13385.
2. Learn to apply the notion of continuous improvement for methods such as 13385. The analysis was originally a *static* analysis. The panel strongly urges that this analysis have regular reviews and updates to make use of new and additional information so that this analysis is *not* just a static endeavor, (e.g., the justification for not including the conversion of the Falling Man's potential to kinetic energy is insufficiently documented).
3. Revise 13385 to describe the document as a design guide and clearly explain the proper use of the guide.
4. Determine whether all the possible load cases have been considered and add to the design guide as necessary. For example, it is believed that Atomic Weapons Establishment (AWE) is considering a purely vertical load case. Pantex operations should consider such a scenario as well.
5. Determine why Sandia National Laboratories (SNL) and Lawrence Livermore National Laboratory (LLNL) use a different Falling Man methodology. It seems highly desirable for Pantex and the DAs to be using a common approach. Work with the DAs to develop this methodology and make it consistent across the board with all DAs and other agencies.
6. Engage the broader range of expertise in the domains of Human Factors and Biomechanics to improve the technical basis. Significant research continues to occur in this area, since the release of 13385, that is relevant.

7 Improve the application of concurrent engineering so less technical gaps exist among DAs and Production Agencies (PAs). In addition, greater concurrent engineering would reduce the inordinate decision authority that rests on tooling engineers at Pantex.
8 Further study of the available energy from a Falling Man and what proportion this could be possibly transferred to a second body.
9 Continued observation and evaluation of walking/work flow and how to improve the overall flow.
10 Perform a dynamic analysis of insult loads.
11 Conduct a sensitivity study of the Falling Man model using the 99^{th} and 50^{th} percentile of Pantex males.

ACKNOWLEDGMENTS

The panel would like to thank Terry Montgomery (CNS/Pantex) for facilitating this review. Terry made every effort to accommodate the panel before, during, and after visits to Pantex. In addition, Terry was diligent in providing reference material necessary for the panel to make informed assessments.

CONTENTS

1. Introduction..11
   1.1. Scope..11

2. Approach..12
   2.1 Lines of Inquiry..13
   2.2 Benchmarking..13

3. Results..13
   3.1 Lines of Inquiry..13
      3.1.1 Question 1: Is the Physical Application of 13385 Satisfactory?..13
      3.1.2 Question 2: Is the Practical Application of 13385 Satisfactory?..18
   3.2. General Observations..19
      3.2.1 Noted Strengths..19
      3.2.2 Noted Weaknesses..21
   3.3 Benchmarking..22
      3.3.1 AWE..22
      3.3.2 ATK..22
   3.4 Congruence with Regulatory Requirements..22
   3.4 Physicality..23
      3.4.1 Suitability of Linear Approximation..24
   3.5 Assessment of Conservatism..24
   3.6 Process Inputs and Outputs..25

4. Conclusions..26

5. References..28

Appendix A: Requirements Verification Matrix..29

Appendix B: ATK Requirement Example from the ATK Hazards Analysis Guidelines..34
   Phase 2 Analysis..38

Appendix C: Comparison of Methods..47

Appendix D: Falling Man Analysis Inputs and Outputs..57

Appendix E: Panel Members..58

FIGURES

Figure 1. Graphical Representation of Operator Velocity vs. Distance Walked 17

TABLES

Table 1. Conservatisms and Non-Conservatisms 24
Table 2. Hazards Summary (Risk Assessment)..45
Table 3. Tripping Example (Hazard Summary) 46

NOMENCLATURE

AB	Authorization Basis
AHAT	ATK Hazards Analysis and Testing
AHOPS	ATK Hazardous Operations Standard
AWE	Atomic Weapons Establishment
CNS	Consolidated Nuclear Security
Cp	Containment Probability
DA	Design Agencies
DBAs	Design Basis Accidents
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DSA	Documented Safety Analysis
EM(s)	Energetic Material(s)
Ep	Event Probability
ESD	Electrostatic Discharge
F	Frequency
FM	Failure Mode
FMEA	Failure Modes and Effects Analysis
Fp	Fire Probability
HA(s)	Hazard(s) Analysis
HAR	Hazards Analysis Report
HE	High Explosive
HERC	Hazards Evaluation and Risk Control
HEVR	High Explosive Violent Reaction
IND	Inadvertent Nuclear Detonation
Ip	Initiation Probability
LBF	Pound-Force
LLNL	Lawrence Livermore National Laboratory
LOIs	Lines of Inquiry
LOPA	Layers of Protection Analysis
MPH	Miles per Hour
NDI	Non-Destructive Inspection
NEO	Nuclear Explosive Operations
NNSA	National Nuclear Security Administration
NPH	Natural Phenomenon Hazards
PE	Potential Energy
PHA	Primary Hazard Analysis
PPC	Production Plant Contractor
PPCB	Plant Processor Control Board
PT(s)	Production Technician(s)
PRS	Periodic Review of Safety
PSM	Process Safety Management
SACs	Specific Administrative Control
SAR	Safety Analysis Report
SC	Safety Class

NOMENCLATURE

SME(s)	Subject Matter Expert(s)
SNL	Sandia National Laboratories
Sp	Sustained Burn Probability
SSCs	Structures, Systems, and Components
TIL	Threshold Initiation Level
Tp	Transition Probability
TSRs	Technical Safety Requirement
UV	Ultra Violet
Xp	Explosion Probability

1. INTRODUCTION

Consolidated Nuclear Security (CNS) Pantex (referred to as just Pantex through the rest of this SAND Report) took the initiative to organize a Review Panel (the terms *Falling Man Review Team, Review Panel*, *Review Team* and *panel* are interchangeable terms through the rest of this SAND Report) of subject matter experts (SMEs) to independently assess the adequacy of the Pantex Falling Man Analysis methodology (13385). The purpose of this SAND Report is to provide the details of the assessment including the: scope, approach, results, and Appendices (which contain the detailed review process data) to the general public for review.

The panel included individuals that possessed relevant knowledge and provided independent perspectives. Panel members were both internal and external to the National Nuclear Security Administration (NNSA), refer to Appendix E: Panel Members for additional information. Pantex did not have any panel members participate in this study so that the conclusions would not be biased. The only Pantex participation was done specifically and only to facilitate the study and the review. A representative from the Defense Nuclear Facilities Safety Board (DNFSB) was present during all onsite meetings as an observer.

1.1. Scope

The Review Team derived three main sub-questions to address the scope, which consisted of the following:

1. Is 13385 satisfactory?
2. Is the application of 13385 satisfactory?
3. How congruent is 13385 with the regulatory requirements?

The independent Falling Man Review Team was provided all of the available documentation associated only with the development and application of the 13385 model. The documents were provided along with open technical exchanges with the Pantex Engineering staff. In addition, walk downs were performed allowing the panel to appreciate the context in which Nuclear Explosive Operations are performed. The Review Team was not provided prior evaluations, critiques or any current on-going experimental work so that the study could focus on the current methodology. The Review Team did learn about the existence of similar external data and evaluations while preforming their evaluation, but these studies were not in the scope of the review requested by Pantex.

2. APPROACH

There were a number of actions for the panel members to address including:

1. Benchmark the calculations against existing methods from AWE, and ATK.
2. Read/interpret the regulations and identify relevant requirements, then make a judgement against compliance.
3. Determine whether or not 13385 is physically satisfactory by determining:
    a. If possible, determine if the linear calculation method used is suitable to model the non-linear situation and
    b. if 13385 is adequately conservative and
    c. generate/interpret sensitivity studies to determine significance of assumptions.
4. Read and understand the Special Tooling Design Manual (MNL293130, Issue 6), with emphasis on the context of 13385 and judge if its application is satisfactory.
5. Produce a flowchart showing all of the possible inputs and outputs of 13385.

The independent review at Pantex was performed as a collaborative, multi-pronged effort. The Review Team reviewed multiple documents and met with key engineering, safety, and operations personnel. Methods used in the industry for evaluating accident scenarios in explosive operations were reviewed, and Nuclear Explosive Operations were observed. The Review Team also independently reviewed the technical basis of assumptions including the:

1. 13385 analysis, and
2. application of 13385 for accident scenarios with inadvertent nuclear detonation (IND) and high explosive (HE) violent reaction (HEVR) consequences identified during the Documented Safety Analysis (DSA) and the Hazards Analysis Report (HAR) process. Lines of Inquiry (LOIs) were then developed by the Review Team and submitted to Pantex. Pantex reviewed the LOIs and submitted responses back to the Review Team that were analysed and reviewed.

The Review Team meetings occurred at Pantex, with DNFSB and Pantex Engineering representatives present, on 16-18 Sep 2014 and 28-30 Oct 2014. The Review Team meetings occurred via teleconference, without DNFSB and Pantex representatives present, on 15 Oct 2014, 22 Oct 2014, 12 Nov 2014 and 19 Nov 2014.

The following applicable Department of Energy (DOE) standards, the Pantex Falling Man/Tripping Man Engineering Analysis, Pantex Engineering Analyses, Design Requirements Documents, drawings, and the Basis of Calculations Documents were reviewed:

- 13385-ANL-2 Tripping Man Analysis, Feb 2004
- DOE-NA-STD-3016-2006 “DOE Limited Standard, Hazard Analysis Reports for Nuclear Explosive Operations,” May 2006
- DOE-STD-3009-94, “DOE Standard, Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses,” March 2006
- 000-2-1472-ANL-02 Workstand Engineering Analysis, Jul 2008
- 000-2-1472-DRD-07, Workstand Design Requirements Document, Sep 2013
- 000-2-1472 Rev C Workstand Drawing, Oct 2005

- 000-2-1472 SDS No. 14040-06 Workstand Support Data Sheet, Sep 2014
- 061-2-0835-ANL-02 Transfer Cart Engineering Analysis, Mar 2014
- 061-2-0835-DRD-04 Transfer Cart Design Requirements Document, Jul 2014
- 061-2-0835 Rev B Transfer Cart Drawing, Jul 2013
- 061-2-0835 SDS No. 14872-01 Transfer Cart Support Data Sheet, Nov 2013
- Description of the Falling Man Scenario, Aug 2014
- DSA Input-Review of Falling Man, Aug 2014
- Tripping Man Standard, Tooling and Machine Design, Nov 2010
- MNL-293130-006 Special Tooling Design Manual
- SB-CAL-369058 95th Percentile Man Calculation, Jan 2012
- SB-CAL-941386 Basis for Tripping Man Probability, Dec 2008
- SB-CAL-941694 Basis for Tripping Man Probability – Operational, Jun 2011
- Special Tooling Design Presentation, Mar 2010

2.1 Lines of Inquiry

In order to systematically examine the central questions, the panel identified LOIs. The LOIs allowed specific panel members to investigate topics relevant to the review. Many LOIs were identified that were later determined to be irrelevant and/or non-value added. These LOIs are not discussed in this SAND Report.

2.2 Benchmarking

The task of assessing the adequacy of 13385 is fundamentally a relative judgment. Along with principles captured in references such as dynamics or biomechanics literature, the panel sought the perspective of panel members from organizations outside of NNSA. Members from ATK and AWE were asked to determine how they would analyze the Falling Man hazard for their high consequence operations, particularly involving energetic hazards.

3. RESULTS

3.1 Lines of Inquiry

3.1.1 Question 1: Is the Physical Application of 13385 Satisfactory?

- *How are trips systematically prevented/minimized?*

  One of the inputs to 13385 is the likelihood of the trip event. 13385 generally uses industry data to derive this likelihood. The likelihood is used to determine the safety factors required in related tooling designs.

  Industry data is an abstract source and the likelihood of the trip event is significantly influenced by the design of the resources in the work facility. The design of the work area has been and will continue to be dynamic. New tooling designs for new processes are inevitable yet the likelihood of the tripping event for 13385 is a relatively fixed number.

It was not evident to the panel what systematic design efforts were being made to analyze and control design features that influence the likelihood of tripping. Towards the end of the panel's efforts to collect data, the panel was notified of another Review Team evaluating the design of work processes to determine ways to reduce the likelihood of tripping. This Review Team included most notably Human Factors Engineers. Clearly the decision to commission such an effort is a step in the right direction.

An initial response to this line of inquiry noted that all Pantex employees will be required to receive "Falling Man Awareness training." Awareness training along with other "try harder" and "pay attention" programs have some transient benefits. However there are notable consequences to such programs (Dekker, 2014) and designing tools and resources that integrate the capabilities and limitations of the worker remain a far superior strategy for safe and effective work.

- *While a statistical approach for human weight is defensible, how heavy does an individual technician have to be before Pantex begins to question the adequacy of 13385 assumptions with respect to technician weight?*

  The Pantex response described the AB process. The panel reiterates the question: As a design basis, is the 280 pounds Pantex Technician a requirement? The panel recommends evaluating any sensitivity analyses that had been conducted to determine when weight gain would trigger design or requirement changes.

- *What is the technical basis for not incorporating the conversion of PE to KE due to the loss of height at the technician falls?*

  The stated goal of the 13385 analysis is to determine if a tool will tip, slide, or fail completely as a result of an impact from a Falling Man. The analysis should have a preface that describes why the chosen methodology is appropriate, and why some aspects were either not considered or ignored.

  For the tipping analysis, the kinetic energy of the Falling Man based on his walking speed is compared to the amount of potential energy required to tip over a particular tool. If this "simple energy" analysis shows that tipping is possible, the analysis proceeds to a slightly more conservative analysis that includes the inertia of the tool. In both cases, the explanation of this methodology is minimal, and makes evaluation of the analysis difficult.

  Next, the same energy is used to calculate horizontal force by dividing the energy by the length of a man's arm. This appeared to the panel to be an unusual method for performing this type of analysis, and the basis for using this methodology is not described in the 13385 document. If there is no basis for using this type of analysis, actual values should be obtained by empirical means. The vertical force used was the full weight of the 95% man. These two forces are then applied to the tools of interest. If any portion of the tool can fail from this application of force, the tool must be re-designed. The same loads are then applied to determine if the tool could slide from application of this load, and if it could slide, could it also tip over as a result of encountering some fixed object in its path.

The 13385 analysis has some conservative and some non-conservative aspects. The most important conservatism is the 4 km/hr (2.5 mi/hr) walking speed, which was based on observation, is probably greater than the actual walking speed achieved during operations in the cells or bays. It is also assumed that 100% of the kinetic energy is used in tipping the tool; at first glance this appears conservative, however there is also no consideration of flailing appendages that could in fact make use of muscle potential energy and therefore *increase* the kinetic energy of the fall and the likelihood of a tip. The most important non-conservative aspect of the analysis is that there is no consideration given to the initial potential energy of the Falling Man as a result of his center of gravity being located 41 inches above the floor. A simple analysis concludes that after falling half the distance to the floor, the velocity of the man could increase by ~ 6 miles/hour. This is a significant increase over the 2.5 mile/hour walking speed, and without the benefit of other information (empirical data from test results) it should not be ignored. This additional energy would affect all three parts of the analysis, the tipping, the damage, and the sliding.

13385 does not consider the application of the failure mode (FM) load in a dynamic sense, and how that might affect the tool's ability to retain control of the weapon components. For example, it may be possible to dislodge an object from a flat table top by the application of a purely vertical load, but this will only be ascertained by testing or the use of a dynamic model. It may be that there are few or no situations where this could be of concern, but it should still be addressed in the analysis.

Analysis using a reasonable FM scenario as described above may result in the design of tools that are so bulky they would actually hamper the safety of operations. There should be some mechanism for weighing mitigation of FM risks against increased risk due to ungainly tooling.

- *When 133385 was developed, what research was done to learn from the literature or industry practices to derive a correct and conservative approach to the Falling Man hazard?*

  Pantex has noted that the literature search used to support 13385 included: DOE standards, industry standards, human factors data, and an internet search. The list of references reinforces the panel's assessment that 13385 is a preliminary/baseline methodology (refer to Section 5. References for additional information). Panel members who did not even have a background in biomechanics performed some searches around the internet and quickly encountered a domain of research and literature associated with biomechanics that was vast, deep, and possessing a long history (Martin, 1999).

  Pantex noted that the Falling Man scenario for nuclear explosive operations has not been addressed in the literature. Certainly a collision with a nuclear explosive is a very specific circumstance. The panel agrees that a relatively larger amount of research has been performed in biomechanics to assess the impact of the environment on the human rather than the human on the environment/energetic materials (EMs). Concerns about worker safety seem to have driven the significant body of work in existence. However, the literature and subject matter expertise associated with biomechanics could be utilized to a substantially greater extent to model such high consequence operations.

- *Virginia Tech Study Report – review the test results and see how they compare to the 13385 criteria.*

  This review committee was tasked with evaluating the adequacy of the Pantex Falling Man methodology. Since LANL and Pantex thought it was worthwhile investing research funds in these studies, this review committee should have been allowed to review the results and make our own conclusions – to exclude information that could shed light on this complex problem was inappropriate.

- *What is Pantex' ability/core capability to model Falling Man scenarios?*

  During our discussion of these LOIs on October 29, 2014 Pantex responded that their engineers have the following tools available to them: CREO, ANSYS, and LS-DYNA. There was no discussion of how often these tools are employed. This question has been raised by previous NESSGs.

  Pantex has stated that tooling and machine design engineers are fully capable of modeling the Falling Man scenario. The commitment by Pantex to fund a university to support modeling efforts stands in contradiction to the assertion. Further, the assertion draws into question whether Pantex is willing to accept and acknowledge opportunities to refine and improve 13385. While Pantex tooling engineers have demonstrated the capability to model the Falling Man, the tooling engineers reasonably do not possess the scientific resources to carry out more fundamental research in support of improvements in capability and knowledge.

  Any phenomenon being modeled and simulated possesses a spectrum of uncertainty. Some factors are more deterministic and at the same time there are also factors lacking enough research to minimize or even reduce uncertainties. Many engineers could probably model relatively deterministic phenomenon to solve relatively well-understood problems. However, SMEs who live and breathe relatively complex phenomenon are necessary to correctly reduce model uncertainties. Phenomenon such as electrostatic discharge (ESD) and lightning seem to possess a spectrum of expertise across the NNSA complex and all of the workload does not rest on fully capable tooling and machine design engineers.

  During our discussion of these LOIs on October 29, 2014 Pantex responded that their engineers have the following tools available to them: CREO, ANSYS, and LS-DYNA. What was not discussed was how often these tools are employed. This question has been raised by previous NESSGs.

- *Is a risk ranking approach applied consistent with DOE STD 3009 applied at Pantex? If not elaborate why?*

  The risk ranking approach applied at Pantex is methodical and is consistent with DOE STD 3009. For any process evaluated in the DSA, there is an associated hazards analysis (HAs). The hazard events that relate to high order unmitigated consequences (IND or

HEVR) are evaluated in an accident analysis. These consequences challenge the Evaluation Guideline. The accident analysis describes the scenario and develops controls that are relied upon to prevent and/or mitigate these consequences. The hazard events that relate to consequences other than IND or HEVR may be dispositioned in the hazards analysis and not carried forward to the accident analysis. The severity of the consequences, combined with the control set relied upon in the accident analysis; provided the operational risk that is presented to NNSA Production Office for approval.

- *Characterize the available space for operations, and speed of movement* (*both issues were addressed during the onsite visit)*.

  The walking speed is related to an open floor, industrial environment with unrestricted movement. Weapon operations are performed in an engineered environment, with controlled and minimal distances between work areas.

  Tools are moved from a staging area to the operating area and the distance between stops is typically six to 10 feet. The walking speed at the staging area and the operating area should be zero; therefore, it can be assumed the technician's walking speed increases and then decreases. Refer to Figure 1 below for a graphical representation of the layout described.

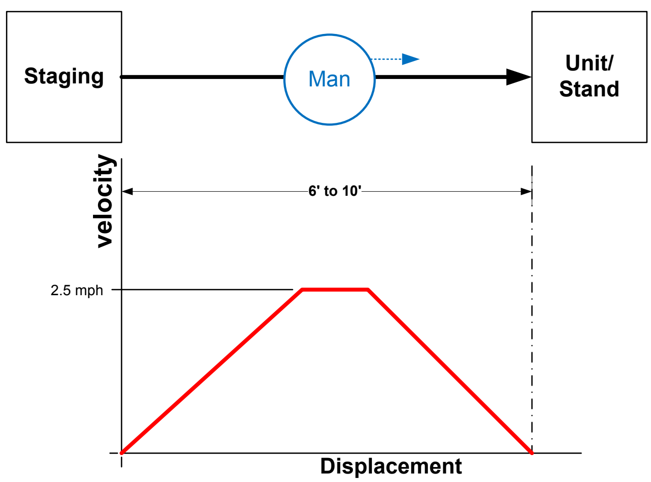


Figure 1. Graphical Representation of Operator Velocity vs. Distance Walked

The Review Team observed several processes in locations that spanned the majority of operations in the subject work area. Consistently, the space for operations was noted as adequate without undue tripping hazards. The distances are consistent with Figure 1 above. The technicians carried out their tasks in an appropriately deliberate and careful fashion. The Review Team did not observe any rushing from point-to-point. The layout reduced the travel distances needed, which further contributes to lower walking speeds.

Based on the observed distances and walking speeds, the maximum velocity used in the model of 2.5 mph (3.7 ft/sec) appears to be conservative. While the team did not specifically measuring the speed of walking from point-to-point in the process, the technicians moved in a careful and deliberate manner. When a panel member reproduced the gait, the maximum speed was estimated at 1.5 mph (2.2 fps). This suggests that the velocity used in the procedure is conservative compared to what was observed by a factor of 1.66 under actual operational conditions.

As with several factors in the Review Team's evaluation of the protocol, these are an estimate. However, this does reinforce the Review Team's general conclusion that the method is adequate to evaluate hazards with the opportunity for improved understanding of the margin. An example in this specific area would be to collect a few measurements of typical walking velocity under operational conditions. This data could then be analyzed statistically along with other previously gathered statistical data on workforce population and newer information on the force transferred from a falling human body (not an inelastic collision) to result in a more thorough understanding of the force imparted to a receiving object.

The Review Team noted that tool hand-offs were always done well away from the article when there was a larger crew and one team member was pulling tooling and delivering tooling to those executing the actual operation. It was also noted that good verbal communication of instructions and acknowledgement of instructions was observed at Pentax. There was excellent coordination on operations when two technicians needed to execute a specific action simultaneously. This matches the conclusion in the study that the dropping of a tool or mishandling of a tool can be accurately characterized as a "rare event."

The Review Team did not observe any behaviors that would be inconsistent with the maximum velocity and heights that have been described elsewhere in this study. The team believes that the maximum walking velocity to be appropriately conservative without being extreme.

3.1.2 Question 2: Is the Practical Application of 13385 Satisfactory?

- *What is the Production Plant Contractor (PPC)/DA interaction during the 13385 evaluation?*

  Refer to Appendix D: Falling Man Analysis Inputs and Outputs for a detailed analysis on the PPC/DA interactions.

- *Scope impact of increasing the design loads – Has Pantex assessed the impact of changing/increasing the design loads. Pantex has 300 tools which are subject to the Falling Man design requirements. Has Pantex done a simple examination of the factors of safety against the estimated load increase to determine how tools would have to be modified?*

  The 13385 Falling Man analysis is straightforward and methodical. Assumptions in the probability calculation of a 95th percentile male with 5th percentile arms falling and impacting a unit appear to be overly conservative. n, t_{day}, and T_{year} may be higher than actual conditions (e.g., are six Production Technician's (PTs) all working with a tool on the unit for eight hours per day, and do six PT's actually work on the unit for 360 days per year?). P_{impact} seems conservative (P_{impact} is equal to 0.10 on the assumption that a tool lies within a 36-deg arc within which an operator may fall). Relatively small adjustments to P_{impact}, n, t_{day}, and T_{year} can move P_{total} from its current baseline of 4.3E-5 to between 5E-6 and 1E-7.

Sliding and tipping man analyses may be oversimplified and conservative by assuming instantaneous transfer of energy from the Falling Man to the tool and by assuming conservation of energy between the Falling Man and the tool (i.e., in an actual fall, some losses could reasonably be expected due to friction).

3.2. General Observations

3.2.1 Noted Strengths

- Probability calculation is conservative, and exceeds 3016-2006 requirements.
- Energy calculations are conservative (no friction, assumes all Falling Man mass is at the center of mass, and etc.) except as noted below. 13385 supports HAR requirements specified in DOE-NA-STD-3016-2006 (3016-2006) by evaluating a hazard that has been identified (i.e., Falling Man).
- 13385 meets or exceeds the "reasonable level of conservatism" requirement in 3016-2006.
- 13385 exceeds 3016-2006 hazard evaluation requirements by providing a quantitative evaluation of a specific hazard.
- 13385 is comprehensive in its identification of energy imparted to a tool impacted by the 95^{th} percentile Falling Man with 5^{th} percentile arms.
- 13385 meets the 3016-2006 requirement that "Hazard scenarios must be fully developed and account for factors that influence scenario progression such as controls and physical phenomena" by including multiple Falling Man scenarios and providing a tiered approach for analyzing those scenarios.
- Grossly overestimated likelihood of occurrence is contrary to guidance of DOE STD 3016 per unit weapon operation assessment.
- The per year basis utilized and overestimated available work shift exposure result in at least a 2 order of magnitude reduction in likelihood of occurrence from 4.32 E-5 to 1E-7 or less. This may be inconsequential, given the application in the analysis is simply to bin the hazard in the rare event category.
- The low likelihood is further supported by the lack of any operational Falling Man incident history.
- Typical approach to a hazard with this level of estimated occurrence (1E-7 per operation) would be to bin it in the risk matrix approach (per MIL STD 882E or the 3X3 example of DOE STD 3009) with the lowest possible likelihood of occurrence termed per DOD requirements "so unlikely it can be assumed it will not occur" and no further mitigation would be pursued.
- The Pantex approach to the analysis process is conservative to the application of IND and HEVR consequences by ignoring the event likelihood or any site conditions or controls that would lower the event likelihood even further.

- Conservative in the general premise that absent our consideration of weapons effects that a human body, soft tissue, and/or bone and/or etc. is a credible threat to a steel/aluminum structure designed to hold/transfer a substantial/heavy product.
- Site review of live operations, tool configuration and bay layout suggest a limited necessity to approach a loaded tool with a substantial object in hand. Careful consideration of the tool assembly/disassembly processes with the judicious use of carts, handling fixtures and operational/administrative controls further control the approach to the loaded tool supporting the lack of consideration of this condition 13385.
- Falling Man maximum credible energy calculation and assumptions that it is delivered without losses is conservative. Horizontal velocity while not accounting for gravitational acceleration/potential energy as the individual begins to fall and pivot around the tipping point generating an additional horizontal velocity component (i.e., peak sometime after 45 degree arc during the fall). The walking velocity appears overestimated and would likely compensate for the falling potential energy release in the horizontal direction.
- The tip over hazard is specifically addressed in the ATK Hazardous Process Design Standard. Any tool, energetic related or not, must meet a tip over design criteria among many others related to tooling and every aspect of an energetic process. The loading force is assumed available to tip any tool regardless of mass to up to a 30 degree angle from the working plane the design must do this without "tipping" over. This is conservative for large structures but for small structures the Pantex criteria would be more conservative (i.e., there is more than enough available energy to tip over the article even though it meets the 30 degree criteria). A process HAs would invoke review of the "weapon response" and mandate mitigations depending on the response. However for the Falling Man based on the risk alone no mitigation would be mandated. There are other criteria in the standard that would not allow an article sensitive enough to be initiated from a working height drop ever being processed in the first place.
- On site observations confirm based on bay configuration, operational controls and operational cadence established by the call-recall procedure execution discipline that the walking speed established in 13385 is conservative.
- Pantex is taking prudent action to enhance and further understand the complex interactions and loading conditions with the broader biomechanics community of SMEs.
- Repeat of above takeaway from live operations review. Tool configuration and bay layout suggest a limited necessity to approach a loaded tool with a substantial object in hand. Careful consideration of the tool assembly/disassembly processes with the judicious use of carts, handling fixtures and operational/administrative controls further control the approach to the loaded tool supporting the lack of consideration of this condition 13385.
- The Pantex Team has completed a review of ~ half of the falling man credited tools and effectively doubled the loads to a 100% man configuration. The result being ~3 tools that would require any remediation to meet the now doubled rare event loading criteria supporting by my earlier assertion as to the lack of credibility of the human threat to a steel/aluminum tool designed to support substantial object with a

5 to 1 safety factor on design load. This coupled with the overall conservatism applied in the process analysis (IND, HEVR) and process design in general supports continued use of the 13385 standard for rare events.

- Max downward force of 280 pound-force (lbf) is conservative when compared to hip fracture studies which conclude worst case coupling is nominally 55% of body weight and arm bracing reaction force of ~19.5% of body weight (Robinovitch (1994)*)*. Another study (Kawalilak, et al., 2014) derives from testing a correlation of velocity of vertical impact force arriving at a linear estimate of ~ y(N)=600*x(m/s) = 600 N for 1 m/s or nominally 2.5 mph or ~135 lbf. Free fall velocity from 41 inches of 14.8 ft/sec is beyond the data set (2.5 m/s max) but extrapolating to 4.5 m/s provides ~ 2700 N or 607 lbf.
- Refer to Appendix A: Requirements Verification Matrix for additional noted strengths.

3.2.2 Noted Weaknesses

- 13385 does not account for additional energy resulting from rotation of Falling Man about tripping point (i.e., V_x may be greater than 2.5 mi/hr, and or energy from V_y does not appear to be accounted).
- Force derivation lacks conservatism with respect to the reliance upon an idealized fall counting on a nominal 12 inch "absorption" of energy to derive force.
- No accounting for the items the individual may be carrying that will constrain the ability to react over a 12-inch distance or impart an impulse or shock load via metal-to-metal contact.
- Vertical loading may or may not be underestimated.
- Applying the above referenced C. Kawalilak linear correlation of impact velocity to force in the horizontal direction at 2.5 mph walking speed suggests underestimation of Falling Man horizontal component force input to the tool (~135 lbf vs. 13385's 50 lbf) further supporting the need for additional study and experimentation.
- There appears to be many applicable biomechanics studies/tests/data (i.e., sports injury, hip injury, impulse loading of roof structures, and etc.) that could be leveraged to derive and bound maximum credible tool insult (i.e., bone stress/fracture, and impact loading)
- The integration of 13385 analyses and weapon response analyses is unclear. The DAs may or may not use results of 13385. 13385 is apparently specific to analyzing tooling, but of course the broader operation is integrated (i.e., weapon and tooling). The application of 13385 may therefore be less systematic than necessary.

3.3 Benchmarking

3.3.1 AWE

For AWE tooling, a load of 1kN (i.e., applied horizontally or vertically depending on the scenario but not both simultaneously) is used to account for operator impact. Operator impact is assumed to account for all load cases imposed by the operator including Falling Man. The basis for the 1kN figure comes from published functional anthropometric strength data, and it is judged that it often over estimates the load. The AWE methodology is under review; the draft new methodology uses a simple Force = Mass x Acceleration approach and includes an impact factor to account for the increased force under deceleration, and a further factor is included to conservatively estimate the applied force. The draft method does not currently account for initial speed of the operator, but is anticipated to be updated to account for it.

Pantex, by having an analysis method in place for falling man since before 2004 appears advanced compared to AWE who relied on applying a 1kN force. The proposed AWE method also models the non-linear situation with linear mechanics.

By performing rudimentary side-by-side calculations 13385 can be shown to be comparable to the existing and proposed AWE methods. For some impact heights 13385 gives lower forces, but generally it gives marginally higher forces. The other calculations generally take into account the mass of a carried tool, whereas 13385 does not, and this may bring it back inline.

3.3.2 ATK

In the context of the ATK methodology, 13385 is a combination of a command media requirement, much like the tooling stability requirements of the listed ATK standard bench mark section and a standard HA method (HA Guideline) for a repeated or common hazard scenario to ensure consistency in analysis of the threat. Based on the rarity of the event, and the overall plant and product sensitivity profile to the event, ATK does not have a Falling Man standard. An analogous situation for reference would be electrostatic grounding requirements also in the ATK command media coupled with the human ESD model HA guideline. Appendix B: ATK Requirement Example from the ATK Hazards Analysis Guidelines includes an example hazard analysis that maps to Pantex energetic hazards.

3.4 Congruence with Regulatory Requirements

The panel understands that the design of engineering controls (including special tooling) is regulated by two DOE standards:

1. DOE-STD-3009-94, March 2006
2. DOE-NA-STD-3016, May 2006

The panel also understands that there is no specific guidance or regulation with regard to Falling Man analyses.

The most constraining requirement comes from the following extract found in STD-3016:

*Qualitative identification of controls and **ensuring their adequacy** is the centrepiece of the safety evaluation process. In a qualitative hazard analysis, the hazard analysts are concerned with how each control may fail, how to prevent such failures, and whether redundant components, verifications, or diverse systems need to be considered to ensure adequacy of controls for each hazard/accident scenario.*

And it is the validation of adequacy of controls that 13386 is concerned with. In this context the tooling under analysis are seen as control measures against specific hazards. The panel believes that the following extract regarding engineering judgement, from STD-3016, is key in the demonstration of the above requirement:

Expert, professional, or engineering judgment refers to assessments provided by a subject matter expert. The subject matter expert's opinion or belief is based on reasoning. Expert judgments can be evaluations of theories, models, experiments, or recommendations for further research. Expert judgments can be either qualitative or quantitative. Subject matter experts are individuals recognized by their peers as authorities in a specific subject matter or topic. The weapons response process relies heavily on subject matter expert judgments and expert elicitation.

[……]

Expert elicitation may be of the greatest value and should be considered in the following situations:

- *Empirical data is not reasonably obtainable or the analysis is not practical to perform.*
- *Multiple diverse sources of applicable data must be assessed.*
- *Uncertainties are large and significant.*
- *More than one conceptual model can explain and be consistent with the available data.*
- *Technical judgments are required to assess whether calculations are appropriately conservative.*
- *Source data includes the use of unpublished, un-reviewed, or draft information.*

It is clear that many of the above identified situations which allow consideration of engineering judgement apply in the case of Falling Man calculations. The panel believes that application of engineering judgment is justified in the demonstration of a sufficient design (with respect to a Falling Man load case). As such it is not appropriate to expect the substantiation calculations to be absolute or all-encompassing in their nature.

Appendix A: Requirements Verification Matrix provides a matrix delineating prominent and relevant features of the two regulatory requirements in comparison to 13385. All features, applicable to the scope of the current assessment, appear to have been met through 13385.

3.4 Physicality

Although it is not explicitly clear in the text of 13385, the calculations have evolved from a physical basis. The omission of Potential Energy (PE) converted to Kinetic Energy as the operator loses height during a fall is not justified. The Review Team is led to believe that at one time this PE was included, but it was judged to give unrealistically high forces and thus is now omitted. While the Review Team recognizes the reasoning for this judgment it would have been more appropriate to include a component of the PE even if reduced by a significant factor (i.e., possibly to account for absorption by the human body).

The panel is of the opinion that 13385 should be treated in the wider context of generating a safety case. In that context, we believe it is possible to over emphasize the necessity for precise numerical risk evaluation, thus encourage a drive towards an unconditional calculated solution. This is not possible for such a complex system, and we believe that a model with known assumptions (which may not be wholly based on physics) can offer the necessary method for prioritizing risk reduction and implementation of controls.

3.4.1 Suitability of Linear Approximation

It is common to model a non-linear system that includes large uncertainties with linear approximations, and this is how others currently approach the Falling Man calculation. Ideally the model should be verified with dynamic models and/or empirical data. This is a difficult task due to the number of variables involved not least of which is the dynamics of the human body.

Pantex has commissioned physical experiments to verify their study, however they have not been considered in this review. Comparison between simple 2° of freedom mass/spring/damper systems and existing empirical data suggest good correlation (~80%) for the very specific situation modelled (Chiu and Robinovitch, 1998; and Nam, Chee, and Kim, 2003). This suggests that simple models can achieve at least the right order of magnitude, but the remaining uncertainty would need to be covered by additional conservatisms. It should be noted that the referenced papers extrapolate data from very small falls (1cm – 5cm drop) up to 2m, and it is unlikely that this extrapolation keeps the high level of accuracy so the output needs to be treated with due consideration.

3.5 Assessment of Conservatism

In general, the calculations are judged to be conservative due to coincidental application of pessimistic figures. However there are some needless conservatisms, and non-conservatisms included. On balance (and without in depth assessment) it is expected that, for the majority of credible cases, the calculations remain conservative.

NOTE: Table 1 is a list of conservatisms and non-conservatisms which have been identified within the calculations. Read this table in conjunction with Appendix C: Comparison of Methods due to the numbering corresponding from this table to that appendix.

Table 1. Conservatisms and Non-Conservatisms

Feature	Conservative?
1) Assumption on 95% operator weight.	Yes
2) Assumption of zero carried weight.	No
3) Assumption of operator walking speed.	Yes
4) Horizontally applied load is transferred to vertical lift. No rotation.	TBD
5) Assumption that all KE of operator is converted and applied to the tool, in	Yes

Feature	Conservative?
reality much will be directed elsewhere. Simplified assumption that entire tool is lifted linearly, rather than accounting for rotation about pivot.	
6) Assumption ignoring additional energy (conversion from PE to KE) from operator loss in height as they fall.	No
7) Inertial energy tipping could be more or less conservative than the previous calculation depending on the geometry and mass moment of inertia of the tool. If the mass moment of inertia is very low then the tool is easy to rotate and the simple calculation may be more conservative.	TBD
8) Deleted.	
9) Assumption that all KE of operator is converted and applied to the tool, much will be directed elsewhere.	Yes
10) Assumption ignoring additional energy (conversion from PE to KE) from operator loss in height as they fall.	No
11) Assumption that the CoG of the user is at 41 inches, so any impact will be purely horizontal.	Yes
12) Assumption that the arms are the only compliance is conservative, however this assumes a certain type of fall, which may not be conservative. It is a realistic scenario.	TBD
13) Assumption that the feet of the user are pinned during the fall. This appears conservative?	TBD
14) Assumption on using 5% arm length, twinned with 95% man.	Yes
15) Assumption that the applied force is constant. Plus there is no impact factor to account for the speed of the applied load.	No
16) Assumption that the CoG of the user is at 41 inches, so any impact will be both horizontal and vertical.	Yes
17) Assumption that maximum possible Fx and Fy are applied in any case, rather than calculating the vector depending upon angle of operator at impact.	Yes
18) Assumption that the applied force is constant. Plus there is no impact factor to account for the speed of the applied load.	No
19) Assumption ignoring additional energy (conversion from PE to KE) from operator loss in height as they fall.	No
20) Output from these calculations will be used in further detailed checks. The forces are applied as point loads, and peak values of stress are compared to the allowable figures.	Yes

3.6 Process Inputs and Outputs

Appendix D: Falling Man Analysis Inputs and Outputs shows a symbolic representation of the HA process, and how 13385 sits within that process. It is not exhaustive, and concentrates on the nuclear explosive operations rather than facilities.

4. CONCLUSIONS

The Pantex approach to Falling Man scenarios is probabilistic in nature and a tool forming part of a broader process. As such, panel members felt that it was difficult to evaluate the Pantex Falling Man Design Criteria (13385) in isolation. Having reviewed the criteria and having viewed representative tools used in typical operations t panel has concluded that the greater Pantex tooling methodology supports safe operations. The 13385 document by itself leaves something to be desired, but its execution within the total design and fielding processes at Pantex appears to produce effective tools that are implemented safely for bounding conditions. The panel was unanimous with respect to the conclusions and recommendations.

The panel's specific recommendations are:

1 Provide data from an updated Falling Man model to DAs for a representative sample of Falling Man scenarios to evaluate the change in predicted weapon response compared to the current revision of 13385.

2 Learn to apply the notion of continuous improvement for methods such as 13385. The entire analysis was originally just a *static endeavor*. The panel recommends that this endeavor have regular reviews and updates to make use of new and additional information so that is *not* just a static endeavor, (e.g., the justification for not including the conversion of the Falling Man's potential to kinetic energy is insufficiently documented).

3 Consider revising the 13385 to describe the document as a design guide and clearly explain the proper use of the guide.

4 Determine whether all the possible load cases have been considered and add to the design guide as necessary. For example, it is believed that AWE is considering a purely vertical load case. Pantex operations should consider such a scenario as well.

5 Determine why SNL and LLNL use a different Falling Man methodology. It seems highly desirable for Pantex and the DAs to be using a common approach. Work with the DAs to develop this methodology and make it consistent across the board with all DAs and other agencies.

6 Engage the broader range of expertise in the domains of Human Factors and Biomechanics to improve the technical basis.

7 Improve the application of concurrent engineering so less technical gaps exist among DAs and PAs. In addition, greater concurrent engineering would reduce the inordinate decision authority that rests on tooling engineers at Pantex.

8 Further study of the available energy from a Falling Man and what proportion this could be possibly transferred to a second body.

9 Continued observation and evaluation of walking/work flow and how to improve the overall flow.

10 The dynamic analysis of insult loads was not addressed in the methodology application.

11 Conduct a sensitivity study of the Falling Man model using the 99^{th} and 50^{th} percentile of Pantex males.

12 Identify a highly stressed tool for analysis. Execute the 13385 analyses using absolute worst case operator weight with all other variables (i.e., speed, CoG, arm length and etc.)

at realistic/nominal values. Repeat changing the variable selected as absolute worst case. Compare results with current method.

13 The panel determined that 13385 cannot be evaluated in isolation; it must be treated in the wider context of generating a safety case. In that context, the panel believes it is possible to overemphasize the necessity for precise numerical risk evaluation, thus encourage a drive towards an unconditional calculated solution. This is not possible for such a complex system, and the Review Panel believes that a model with known assumptions (which may be empirical in nature, i.e., not wholly based on physics) can offer the necessary method for prioritizing risk reduction and implementation of controls. The panel has judged that 13385 provides the baseline for such a model, but that Pantex should not become complacent in its use. The limitations of 13385 have been highlighted many times, but a greater understanding of what happens when those limits are reached or breached would create a safer design (this would be achieved by following the Review Panel recommendations).

5. REFERENCES

Chiu, J. & Robinovitch, S. (1998). Prediction of Upper Extremity Impact Forces during Falls on the Outstretched Hand. *Journal of Biomechanics*, 31(12), pp. 1169-1176.

Dekker, S. W. (2014). The Bureaucratization of Safety. *Safety Science, 70*, pp. 348-357.

DOE-STD-3009-94, DOE Standard, *Preparation Guide for U.S Department Of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, March 2006.

DOE-NA-STD-3016-2006, DOE Limited Standard, *Hazard Analysis Reports For Nuclear Explosive Operations*, May 2006.

Kawalilak, C., Lanovaz, J., Johnston, J., & Kontulainen, S. (2014). Linearity and Sex-Specificity of Impact Force Prediction During a Fall onto the Outstretched Hand using a Single-Damper-Model. *Journal of Musculoskeletal and Neuronal Interactions, 14*(3), pp. 286-293.

Nam, J, Chee, W., & Kim, K. (2003). Identification of Falling Human Body Dynamics, *Proceedings of the American Control Conference*, Denver Colorado.

Martin, R. B. (1999). A Geneology of Biomechanics. *23rd Annual Conference of the American Society of Biomechanics (Presidential Lecture)*. University of Pittsburgh: Pittsburgh PA.

Pantex (2004). Tripping Man Analysis. Engineering Analysis, 13385-ANL-2. B&W Pantex Plant: Amarillo, TX.

Pantex (2014). Special Tooling Design Manual. MNL293130, Issue 6. B&W Pantex Plant: Amarillo, TX.

Robinovitch, S.N. (1994). *Hip Fracture and Fall Impact Biomechanics*. Massachusetts Institute of Technology: PhD Dissertation. September 1994, Massachusetts Institute of Technology.

APPENDIX A: REQUIREMENTS VERIFICATION MATRIX

I.D.	Source	Title	Specific Rqt	Meets Rqt?	Comments
1	DOE-NA-STD-3016-2006 sec. 3	Included Hazards	The HAR shall consider all hazards that could lead to Inadvertent Nuclear Detonation (IND), High Explosive Violent Reaction (HEVR), and radioactive or other hazardous material dispersal, and adverse Worker Safety (WS) effects from a weapon assembly.	Y	13385-ANL-2 quantifies the design requirements for scenarios that have been identified as having Falling Man hazards
2	DOE-NA-STD-3016-2006 sec. 6	Approach to Hazard and Accident Analysis	Information that supports the documentation used in the preparation of the HAR shall be complete and accurate in all material respects as required by 10 CFR 830 Subpart B, Appendix E, Paragraph 2.	Y	Assumes data from the 13385 analysis, which are included in the tool analysis, are also included in the HAR
3	DOE-NA-STD-3016-2006 sec. 6	Conservatism in Engineering Judgment	DOE/NNSA expects a reasonable level of conservatism using engineering judgment throughout HAR development.	Y	13385-ANL-2 appears to exceed the "reasonable level of conservatism" requirement
4	DOE-NA-STD-3016-2006 sec. 6.1	Intended Results of Hazards Analysis	The process of hazard evaluation is qualitative in nature and intended to result in effective controls for prevention or mitigation of consequences.	Y	13385-ANL-2 appears to exceed this requirement by providing a quantitative evaluation of a specific hazard
5	DOE-NA-STD-3016-2006 sec. 6.1	Identification of Meaningful Hazards	The hazard evaluation must be comprehensive in its identification of the physically meaningful hazard scenarios (i.e., determined to be non-negligible contributors to accident scenario probabilities) and potential controls.	Y	13385-ANL-2 is comprehensive in its identification of energy imparted to a tool impacted by the 95th percentile Falling Man
6	DOE-NA-STD-3016-2006 sec. 6.1	Scope of Evaluation	Hazard scenarios must be fully developed and account for factors that influence scenario progression such as controls and physical phenomena (e.g., sufficient voltage, capacitance).	Y	13385-ANL-2 includes multiple Falling Man scenarios and provides a tiered approach for analyzing those scenarios
7	DOE-NA-STD-3016-	Scope of Evaluation	This evaluation should include the generation of energy, possible ways to apply the energy to the weapon with consideration of potential controls, and	Y	13385-ANL-2 calculates the energy generated in a Falling Man

I.D.	Source	Title	Specific Rqt	Meets Rqt?	Comments
	2006 sec. 6.1		then the application of energy to a sensitive component that could lead to undesired consequences.		event and possible ways to apply the energy to the weapon
8	DOE-NA-STD-3016-2006 sec. 6.1	Scope of Evaluation	The first two elements of the analysis are developed by the PPC (in consultation with the Design Agencies (DAs) as appropriate), to define the weapon environment, while the DA weapon response determines the last element.	Y	The PPC's application of 13385-ANL-2 defines the weapon environment in detail and the DA provides a weapon response based on that specific, detailed environment
9	DOE-NA-STD-3016-2006 sec. 6.2	Weapon Response	Hazards and associated weapon configuration combinations that cannot result in a weapon response are identified in a screening table issued by the DA. The screening tables must be accompanied with bases information that includes the weapon configuration and the screening rationale with reference to appropriate and defensible documentation. The screening tables should be approved by the applicable DAs for use in a time frame to support the hazard analysis development. The weapon configurations, hazards, and parameters for scenarios (that cannot be screened utilizing the screening tables) are documented in a formal weapon response request prepared by the PPC utilizing the Engineering Authorization System or equivalent. Weapon response requests must be forwarded to the appropriate DAs. Weapon response consequences shall be categorized into consequence categories of IND, HEVR, Material Dispersal, and Worker Safety as a minimum.	NA	The DA provides a weapon response
10	DOE-NA-STD-3016-2006 sec. 6.3	Probability Calculations	The specific operations covered by a HAR run for a limited duration of weeks or months. Therefore, the HAR accident sequence likelihood estimations should be represented in units of probability per single unit weapon operation (e.g., assembly, disassembly).	Y	13385-ANL-2 provides a probability calculation for a 95th percentile Falling Man with 5th percentile arms impacting tooling, represented in

I.D.	Source	Title	Specific Rqt	Meets Rqt?	Comments
					units of probability per year. This is conservative compared to units of probability per single unit weapon operation.
11	DOE-NA-STD-3016-2006 sec. 7	Evaluation Requirements	The HAR must evaluate all hazards that could impact the NEO and must serve as the final safety basis integration document. Another DSA (e.g., a SAR) may provide analysis and resulting controls for hazards that are relevant to the NEO. However, the HAR must verify the analysis and controls are adequate for the hazard.	Y	13385-ANL-2 is the evaluation tool for a specific (Falling Man) hazard
12	DOE-NA-STD-3016-2006 sec. 8	Probability Estimates	Probability estimates for weapon responses, safety function failures, and intermediate events as part of an accident sequence should: a) Provide reasonably approximate, order-of-magnitude point-estimates commensurate with the secondary role that estimation of accident scenario probabilities play in the safety basis documentation,	Y	13385-ANL-2 provides a probability calculation for a 95th percentile Falling Man with 5th percentile arms impacting tooling, represented in units of probability per year.
13	DOE-NA-STD-3016-2006 sec. 8	Probability Estimates	Probability estimates for weapon responses, safety function failures, and intermediate events as part of an accident sequence should: b) Characterize the degree of uncertainties from the range of variability in supporting information that was used to develop the point-estimate probability,	Y	13385-ANL-2 provides a probability calculation for a 95th percentile Falling Man with 5th percentile arms impacting tooling, and accounts for the degree of uncertainties in the range of variability in supporting information by incorporating a high degree of conservatism (such as assuming 6

I.D.	Source	Title	Specific Rqt	Meets Rqt?	Comments
					operators are working on one weapon at the same time for 8 hours per day for 360 days per year).
14	DOE-NA-STD-3016-2006 sec. 8	Probability Estimates	Probability estimates for weapon responses, safety function failures, and intermediate events as part of an accident sequence should: c) Be reasonably conservative	Y	13385-ANL-2 provides a probability calculation for a 95th percentile Falling Man with 5th percentile arms impacting tooling, and accounts for the degree of uncertainties in the range of variability in supporting information by incorporating a high degree of conservatism (such as assuming 6 operators are working on one weapon at the same time for 8 hours per day for 360 days per year).
15	DOE-NA-STD-3016-2006 sec. 8	Probability Estimates	Probability estimates for weapon responses, safety function failures, and intermediate events as part of an accident sequence should be associated with properly and thoroughly defined events.	Y	
16	DOE-STD-3009-94 3.3	HA Requirements	Hazard identification and evaluation provide a thorough, predominantly qualitative evaluation of the spectrum of risks to the public, workers, and the environment due to accidents involving any of the hazards identified.	Y	13385-ANL-2 exceeds this requirement by performing a quantitative evaluation of the Falling Man event
17	DOE-STD-3009-94 3.3	HA Requirements	The evaluation identifies preventive and mitigative features, including identification of expected operator response to incidents (e.g., accident mitigation actions or evacuation) and	NA	13385-ANL-2 evaluates the Falling Man event

I.D.	Source	Title	Specific Rqt	Meets Rqt?	Comments
			provisions for operator protection in the accident environment		
18	DOE-STD-3009-94 3.3.2.3	Hazard Evaluation	Hazard evaluation presents potential accidents in terms of hazards, energy sources, causes, preventive and mitigative features, consequence estimates, and frequency estimates.	Y	13385-ANL-2 treats the Falling Man event as an "energy source"
19	DOE-STD-3009-94 A.3.1	Design Basis Accident Calculation	Once a set of SC SSCs has been identified, accident consequences can be estimated in a DBA calculation, which represents the accident scenario progression where SC SSCs successfully perform their intended safety function.	NA	13385-ANL-2 evaluates the Falling Man event and quantifies the energy imparted to tooling; the DA provides a weapon response via separate analysis

APPENDIX B: ATK REQUIREMENT EXAMPLE FROM THE ATK HAZARDS ANALYSIS GUIDELINES

Below are applicable excerpts from ATK command media with regard to tooling, facility, operational and risk management requirements. Following the requirement example section are excerpts from the ATK HAs Guidelines with a brief example case of a tripping scenario analyzed. The parenthetical letter references map-to-hazard categories used by ATK.

Tooling Requirements Examples

4.1.4.1 (A,B,C) The method used to secure small parts in the security zone should be visible for inspection. If a thread locking compound cannot be seen, the fastener shall be identified with ink, utilization of ultra violet (UV) sensitive thread locking compound, or otherwise identified as having thread locking compound applied.

4.1.5 (A,B,C,D) When a potential static hazard exists, a means shall be provided to eliminate or minimize static hazards.

4.1.6 (A,B,C,D) In the design of all tooling, the hazard of tipping shall be minimized by keeping centers of gravity low, choosing proper size and configurations of wheels and casters, utilizing stable supporting arrangements or providing stabilizing tie bars, framing, outriggers, and etc. A minimum tipping angle (i.e., angle at which a fixture will overturn) of 30° degrees should be used.

4.6.4 (A,B,C,D,O,NH) Material to be used in the fabrication of tooling shall be selected to retain adequate physical characteristics and dimensional integrity under operational conditions (i.e., taking into consideration such factors as shock), vibration, temperature cycling, abrasion, aging, embrittlement, curing, subsequent coating, liquid absorption and/or decontamination operations.

4.1.3 (A,B,C) Items shall be designed to prevent improper installation of parts that are assembled or disassembled during a normal operational cycle that could cause a malfunction jeopardizing personnel, property, or product. Color coding or match marking is a less desirable, but acceptable, method to prevent improper installation.

4.1.4 (A,B,C,O) The use of small parts should be minimized. If fastening devices, such as nuts, washers, pins, or other devices must be used, they are located in the security zone and shall be secured. The plant process control board or designated representative shall approve the securing methods. Examples include:

- Safety wiring,
- Staking of threads,
- Tack welding,
- Thread locking compounds, and

- The use of self-locking fasteners such as Ny-lock nuts.

CAUTION: Potting compounds such as RTV are not acceptable thread locking compounds, but may be used for preventing the contamination of parts.

CAUTION: Avoid welding on high strength bolts.

4.5.6 (A,B,C,D,O,NH) Tooling subjected to cyclic loading and designed for infinite life shall be designed for stress amplitudes 25 percent greater than the maximum expected operating stress amplitudes. A Non Destructive Inspection Plan shall be implemented for applications where failure would create a safety hazard.

4.5.7 (A,B,C,D,O,NH) For bolted joints, the safety factor shall be calculated based on applied load. A bolted joint shall be able to withstand five times the applied load for lifting equipment and four times the applied load for all other equipment. Bolt preload should be calculated to minimize joint separation and maximize joint friction during use. Critical torques shall be specified and verified.

4.2.1 (A,B) Tooling shall be so designed that during and after fabrication all welded joints shall be accessible for surface examination per requirements of the Inspection and Acceptance document.

4.2.2 (A) Tooling shall be so designed that during and after fabrication all welded joints shall be accessible for 100 percent subsurface radiographic examination per requirements of the Inspection and Acceptance document.

4.5.5 (A,B,C,D,O,NH) The safety factor of commercial items used in the design of tooling shall be equal to or greater than the overall safety factor of the tool. In the event that the safety factor of the commercial item cannot be determined, then a safety factor of 2.5:1 of ultimate strength shall be assumed and the item is to be downgraded accordingly.

4.5.4 (A,B,C,D,O,NH) Tooling and equipment other than lifting equipment and coded pressure vessels (refer to AHOPS 2.4.1.8), shall be designed with a minimum safety factor of 4:1 on ultimate, 2.5:1 on yield strengths, and 2.5:1 on critical buckling strength.

4.4.1 (A,B) The design of a tool should minimize levels of friction and/or impact that could be applied to explosive materials by use of shields, gaskets, washers, bushings, grommets, nonmetallic or soft materials, and etc.

4.3.1 (A,B,C,D,O,NH) All controls shall be designed to be fail-safe in the event of an actuating medium failure.

4.3.2 (A,B) All manual and automatically controlled steps of an operation should be interlocked when these steps must occur in a particular sequence to avoid a potentially hazardous condition.

4.3.3 (A,B,C,D,O,NH) Emergency override controls should be located at the operator stations and at convenient locations near the tooling for emergency shutdown.

4.3.4 (A,B) Control systems used to operate tooling, should be integrated into fire protection systems so that sprinkler actuation will override and shut down the control system and the tooling, except in cases where it can be shown that tooling should remain in operation.

6.1 (A,B) Prototypes of newly designed units shall be tested under simulated operating conditions using operating procedures with inert material prior to release for production operations.

6.2 (C,D,O,NH) Functional testing shall be accomplished according to the end use of the item.

Facility Requirements Examples

5.7.1 (L,S) The choice of a specific floor construction or covering material shall be based upon operational requirements. Such items as source of contamination, projected use, amount of traffic, explosive processes, cost, hazard analysis studies, and etc., shall be considered before a. material is selected. Epoxy coatings should be considered in lieu of lead floors for conductive/anti-static floors.

4.4.2 When an operation, facility, or piece of equipment is of a critical nature or has been subjected to a hazards analysis, all improvements shall be subjected to an additional hazards analysis prior to implementation of the improvement.

Operational Requirements Examples

7.5 Personnel shall handle all tools in a manner which will minimize impact and friction.

7.6 Any tool or object which must be handled over an open container of liquid explosives shall be provided with an approved means of securing against falling into the container (e.g., leather thongs on flashlights). Any tool or object which must be handled over solid explosives, fuels or oxidizers should be secured.

7.7 Desiccators shall be protected by location or other means from being struck by falling or moving objects.

10.1.1 Free fall of explosives, liquid or solid, should be minimized and shall be restricted to safe distances as determined by Hazard Analysis (HA).

10.2.3.1 Vessels containing liquid explosives should not be lifted or suspended from overhead lifting devices.

10.2.3.3 Liquid explosive vessels other than molds, under pressure or vacuum, shall not be moved. Pressurized molds should not be moved.

10.3.1 Whenever lifting energetic material, the process shall be designed to minimize lifting heights, and safety devices should be provided to prevent dropping. HA shall assess the hazard of dropping the material. The risk level determined by HA may require PPCB/Review Board/Standards Board approval per ATK Hazardous Operations Standard (AHOPS) 5-1 requirements.

12.3.2 The manual addition to or removal of explosives from a unit on cure shall not be permitted.

12.4.4 Initial loosening of cores and mold parts in contact with explosives shall be remotely controlled or as remote operation based on hazards analysis.

Risk Management Requirement Examples

5.5.5 Where the potential effect for a failure is documented with a hazard severity of 1 or 2, the safeguards preventing the occurrence of the failure should not be solely administrative safeguards. An independent engineering safeguard should be incorporated to do at least one of the following:

- Reduce the chance that the initiation energy will be present at the event site.
- Reduce the chance that the EM will be present at the event site.
- Reduce the chance of sustaining a reaction if initiation occurs.
- Reduce the effect of the event through means such as a remotely controlled operation.

Hazard Analysis Process

Process Analysis Setup:
The analysis must provide a review of the process from three distinct viewpoints:

- Facility level (macro view)
- Production/operations (equipment/operator level)
- Ancillary operations/ human hazards (training, production support operations, maintenance activities, clean-up operations, and etc.)

Facility level review is the macro view of the process. This macro view of the process should address the following issues:

- The effect on other processes
- How other process can affect the process under analysis
- Building structural concerns
- Equipment structural concerns
- Interaction between transportation of materials and process activities
- Analysis of the transportation of materials and
- Other macro view items.

Facility incidents include interactions between the operation and the building surrounding the operation under review. These failures can include building collapse, sink holes,

support failure, floor failure, building electrical rating, snow loading, and etc. This section is also used to identify interaction between operations such as facility siting issues; these can be addressed in the analysis or referenced out to the Facility Siting Report.
The production or operational level analysis is the typical analysis that follows the process flow during normal process modes. This analysis details the operations, equipment, and sub-components. Production/operations incidents include the equipment, human error, and processing failures. This is the typical section where most analyses are focused.

The analysis of ancillary operations and human hazards involve analyzing other activities that interface with the operation at times other than the when the process is in the normal operational mode. This analysis reviews the maintenance activities, clean-up operations, and other support operations such as training requirements and procedural detail. Evaluate ancillary operations for the potential for leaving the system in an unsafe state and being performed with the energetics present. The following are examples of operations that should be analyzed under this section:

- Routine machine adjustments
- Filter bag change-out
- Clean-up methods such as vacuum
- Clean-up of the equipment/tooling used in the process
- Tooling change-out and
- Preventative maintenance activities.

Ancillary operations incidents include but not limited to clean-up, maintenance modes, start-up, setup, emergency shutdown, and other operations that are related to the operation under review. This section also is used to analyze other administrative control systems such as hot work permit program, production pressures, change control program, and etc.

An efficient method to organize the analysis into these three viewpoints as well as to organize the analysis for identification of distinct analysis methodology selection is to use the logic diagram. Ideally, the logic diagram will be an extension of the location logic diagram. The specific process logic diagram begins by stating “major incident due to operation of the XXX operation”. Three major headings are included below the top incident:

1. Incident due to operation of the facility,
2. Incident due to production/operations, and
3. Incident due to ancillary operations (production support).

If the analysis is only addressing a specific piece of equipment then, the analyst will reference that branch of the logic diagram that this analysis is intended to cover. The logic diagram should be developed to a point where specific pieces of equipment or specific operations are performed. Further development of the logic diagram may be performed but is not required.

Phase 2 Analysis

Methodology Selection

The ATK Hazards Analysis and Testing (AHAT) method does not require the same type of analysis or methodology as was done for the ATK analysis. For example: a "What-If" analysis may be appropriate for addressing a tank farm; and an Failure Modes and Effects Analysis (FMEA) can be used for analyzing a pump or valve. A description of the selected methodology or methodologies shall be provided in this SAND Report. The following is a guide for methodology selection when analyzing energetic processes:

- **Checklist:** This is not allowed on an energetic process.
- **"What-If" Analysis:** Generally used for simple non-automated processes; however, an analyst experienced in performing PHAs and energetic processing may be able to apply sufficient detail in a What-If analysis to be an acceptable methodology in many applications.
- **FMEA**: the preferred methodology for energetic processes. This method is ideal for mechanical and batch type operations.
- **Hazardous Operation:** the preferred methodology for chemical type processes or processes that are continuous and automated.
- **Fault Tree:** Detailed identification of probability of failure. The fault tree must be accompanied with a table that references source of probabilities, safeguards, and listing corresponding recommendations.
- Many other types of analysis are available that match the detail required for the complexity of the process. A discussion these Primary Hazard Analysis techniques can be found in a number of resources (e.g., the System Safety Analysis Handbook refer to the International System Safety Society website for additional information (http://www.system-safety.org/).

It is recognized that many times the hazards analysis must be started with minimal design information. If the analysis must be started before acquiring all of the information identified in Phase 1, then the recommendations should be generated requesting the information at this point. The combination of the recommendations and the information acquired provides a record of the information used to generate the HA.

Any HAs performed on processes with EMs shall be performed with the intent of identifying the following information under normal and abnormal conditions:

- Identify the scenarios where the process delivers energy to the EM.
  For each scenario, document the comparison between the (potential and normal) process energy and the minimum energy required to initiate the material.
- Identify the potential situations that may result in out of place EM.
- Identify the potential situations that will introduce foreign objects into the system.
- Identify the potential for chemical reactions with other materials.
- Determine the reactivity/propagation characteristics for the EM in the process configuration(s).

The depth to which each section of the analysis is taken will be determined by the hazards analyst through a series of iterative judgments. Factors involved in the process include the complexity of the process, the sensitivity of the materials, the potential result of a failure, and other factors.

All analysis techniques used for energetic processes involve the identification of failures. These failures are documented in the analysis by using a form of a question, failure mode, or guideword. When analyzing an energetic process the failure documentation should conform to the following:

- **EMs:**
  - ESD Initiation
  - Friction Initiation
  - Impact Initiation
  - Impingement Initiation
  - Shock Initiation
  - Thermal Initiation including material compatibility
  - Propagation of reaction (critical height/critical diameter/deflagration vs. detonation/dust explosion)
  - Out of place EM
  - Foreign objects
  - Stress incident(s)
  - Other failure modes for EMs are specific to the process such as cracks/voids in a cast motor, equipment/facilities, or ergonomic issues.
  - Failure modes for non-EMs include vapor/liquid release, material release, thermal reaction, chemical reaction, high/low pressure, rupture of vessel, and etc.
- Others such as human hazards, personnel exposure, ergonomic, and etc.
- **Potential cause/description of failure:** provide a brief description of the failure such as metal on plastic movement with EM present. The potential cause description(s) does not follow a specific format because the nature of the descriptions should be tailored to the failure. Keep in mind that the cause should be very specific to one failure only **NOT** a series of failures. For example: ESD occurs during the mixing cycle. This description is not specific to the event. The full description of ESD during mixing may be several individual failures such as: ESD between the shaft bearing and shaft, ESD between bowl and blade, and etc.

- **Effect of the Failure Scenario (Potential Effects):** A description of the potential consequences of the failure scenario needs to consider the effects on the material (such as initiation, fire, and etc.), the effects on personnel (injury severity), the effects on equipment/tooling under analysis, and the effects on the facilities. Using the generic descriptions provided below enables the analyst to accurately assign a severity for the qualitative assessment (Hazard Category).
  Material potential effects include:
  - Initiation of material
  - Minor fire
  - Major fire requiring suppression system to extinguish
  - Explosion
  - Detonation
  - Release of toxic materials (vapor/fume)
  - Out of place EM

Personnel related Potential effects include:

- Minor injury/ illness
- Injury/ Illness
- Severe injury/ illness
- Death or loss of life

Equipment, Tooling, Operation, and facility potential effects include:

- Minor equipment damage
- Minimum facility damage
- Minor damage resulting in damage to less than 10% of production capability and requiring no more than 3 days to repair.
- Major facility damage resulting in more than 10% loss of production capability and requiring more than 3 days to repair.
- Facility loss
- Propagation to other areas (describe area)
- Propagation of reaction to other operations
- Propagation of reaction to other facilities
- Incidents requiring the evacuation of the facility
- Incidents that may have off-site consequences

Safeguards or Design Safety – Safeguards are engineering and/or administrative controls that are physically in existence at the time of the analysis. These safeguards should be identified and retained in the process safety information. Any item listed in the safeguard column is considered critical to the safety of the operation. Safety critical items shall have a means to be verified (maintain the integrity of the interlock, PM, checklist, procedure, and functional check). In addition, the verification method should be referenced in the safeguard column. The following are examples of administrative and engineering safeguards:

- Administrative safeguards:
  - Written procedural steps
  - Other written documentation
  - Documented training to perform the action
- Engineering safeguards:
  - An interlock either separates the EM from energy levels that are unacceptable or the interlock keeps the available energy below the Threshold Initiation Level (TIL) of the material.
  - Available energy in the system is below the threshold of initiation level for the EM (during normal and abnormal conditions).
  - The system is designed to keep the reaction to a deflagration and fire suppression is provided.

Recommendations: The best recommendations are worded in a way that states the problem or issue and the potential hazard then suggest potential solutions to the problem. This allows the engineer to find appropriate solutions to the problem rather than stating that there is only one way to correct the problem.

The recommendation needs to mitigate the hazard to an acceptable level. Perform a hazards evaluation of the recommendation implementation (hazard category table on to the right of the recommendation).

Recommendation tracking system: All recommendations shall be tracked to closure. Each location must define a tracking system for recommendation closure. This system shall satisfy the management of change requirements for Process Safety Management (PSM) and AHOPS.

Hazards Risk Rating (Hazard Category) – Each identified failure should be evaluated using the qualitative method. Three qualitative evaluations can be made for each failure scenario.

1. The first evaluation meets Occupational Safety and Health Administration PSM's requirement for a qualitative evaluation without considering any safeguards or recommendations implementation.
   NOTE: A written description of the potential failure can be substituted for a qualitative evaluation without the safeguard present.
2. The second evaluation can be made with the safeguards present but without implementation of the recommendations.
3. The third evaluation can be made with safeguards and recommendations implemented.

A minimum of one qualitative evaluation is required by AHAT methodology. In addition, if the safeguard does not lower the hazard risk rating to an acceptable risk level then process modification and/or recommendation is required; refer to AHOPS 5-1 for acceptable risk levels.

3.1.2.5 HERC or LOPA Analysis Introduction

A quantitative probabilistic hazards and risk evaluation requires that a probability be determined for each identified initiation mode of the system being analyzed. Possible initiation modes include impact, friction, electrostatic discharge, impingement, and thermal initiation.

This section describes type and form of data developed in the engineering analysis and material response phases of the analysis, and how these data are applied in this and/or other forms of this conditional probability model. The methodology for determining each of the probability terms in the model will be described with illustrative examples.

The Hazards Evaluation and Risk Control (HERC) or Layers of Protection Analysis (LOPA) method of analysis provides a detailed analysis of a failure scenario within a system. The concept behind HERC and LOPA is that a series of events must occur for the failure scenario to be realized. These events are distinct and identifiable. If any one of the events in this chain of events is prevented then the failure scenario is not realized. So by assuring that all of the layers of protection are in-place will mean that there are multiple systems present preventing the one failure scenario from being realized. The following chain of events must occur to have a major incident involving EMs:

- Energy must be present though a normal or a failure event.
- EM must be present at the energy site though a normal or a failure event.
- The energy input to the material must result in an initiation event.
- Upon initiation will the conditions allow for transition to a burning reaction?

- Upon sustaining a burning reaction will the conditions allow for transition to an explosion?

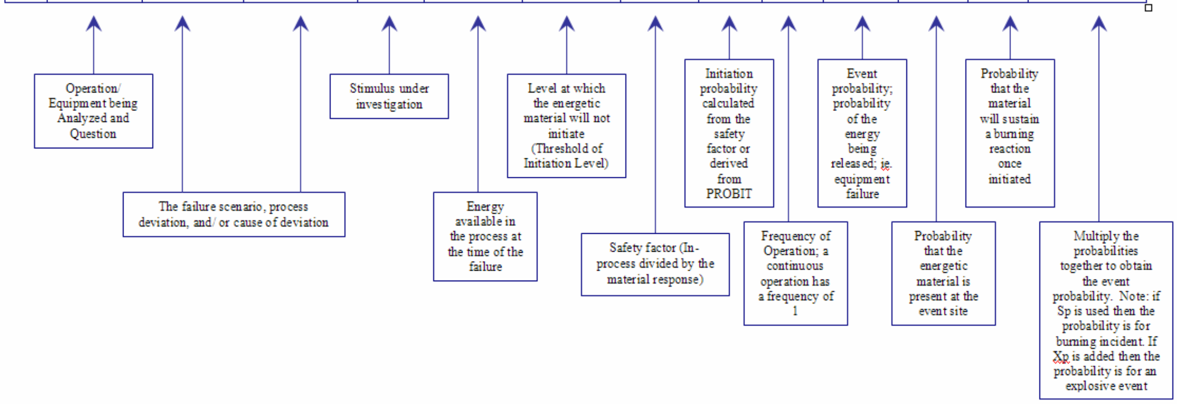
The HERC/LOPA analysis for an energetic event analyzes each of the conditions listed above. A probability is assigned to the following layers or events.

- **Initiation Probability (Ip)** – Comparison between an energy input and the material response. Probability is determined though the ATK modified PROBIT method or Safety Factor method.
- **Event Probability (Ep)** – The probability that the equipment will input the energy identified in the failure scenario. For normal events, the probability is one and for abnormal events, the probability is determined by the reliability of the equipment.
- **Contamination Probability (Cp)** – The probability that the EM will be at the site where the energy is present in the failure scenario. For normal events, this probability is one and for abnormal events, the probability is based on the scenario of migrating EM to the event site.
- **Frequency (F)** – The probabilities must be normalized to a specific time frame such as per event or per operation. This allows for the determination of the probability of the incident occurring on a per year or per shift basis.
- **Sustained Burn Probability (Sp)** – The probably that conditions will be favorable for an initiation event to propagate to a fire. This can be determined empirically or by predicting the material condition.
- **Transition Probability (Tp)** – The transition from a fire to an explosion may take milliseconds or microseconds but under some conditions this transition may be difficult. The Tp is the probability that the conditions will be favorable for an explosion or detonation to occur as a result of initiation and fire. The probability can be determined empirically or by predicting the material condition and equipment conditions.

When Ip, Ep, Cp, F, and Sp are multiplied together, the probability for a fire is realized or Fire Probability (Fp). When the probability of a fire (Fp) is multiplied with Tp, the probability for an explosion is realized (Xp). Table 2 provides an example of a HERC/LOPA analysis commonly documented in a table called "Hazards Summary/Risk Assessment".

Table 2. Hazards Summary (Risk Assessment)

Ref No.	Item	Failure Mode	Failure Cause	Stim.	In-Process Potential (Units)	Material Response (Units)	Safety Factor	Init. (Ip)	Freq. (F)	Event (Ep)	Cont. (Cp)	Sust. (Sp)	Probability Of Incident Per Operation
	Primer Cup	ESD initiation due to separation of bowl lid from bowl	Non-conductive lid on conductive bowl with dry primer mix present	ESD	0.3 Joules	0.002 Joules	0	1	1	1.00E-02	1.00E-03	1	1.00E-05
	Propellant Loader	Friction initiation due to rotation of the dial loader	Propellant migrates to location where contact is made with dial mechanism	Friction	60 Kpsi @ 4.8 ft/s	60 Kpsi @ 8 ft/s	1.67	3.00E-02	1	1	1.00E-03	1	3.00E-05
	Propellant Loader	Friction initiation due to closure of slide gate	Metal on metal contact with propellant present; normal operation	Friction	60Kpsi @ 0.33 ft/s	60 Kpsi @ 8 ft/s	24	1.00E-06	1	1	1	1	1.00E-06



The justification for each probability is documented in a companion "Hazards Summary Reference" table (which is not shown in this SAND Report).

Table 3 provides another example of a HERC/LOPA analysis which consists of a “Tripping Example/Hazard Summary.

Table 3. Tripping Example (Hazard Summary)

TABLE 2

HAZARDS SUMMARY [redacted]

LINE NO.	ITEM	FAILURE MODE	FAILURE CAUSE	COND	STIM.	COMB. MAT.	UNITS	IN-PROC. POT	MAT RESP	SF	INIT (Ip)	FREQ (f)	EVENT (Ep)	COMB (Cp)	SUST (Sp)	FIRE (Fp)	RISK INDEX	MEET [redacted]
	[redacted] Tank	Shock initiation of [redacted] during [redacted]	Operator hits [redacted] Tank	A	Shock	[redacted] 100%	ft lb$_f$	30 ft lb$_f$	1.53 ft lb$_f$ thin wall vessel	0.05	1	1	1E-4 Trip & Fall	1	1	E-4	1C	NO
									5 ft lb$_f$ estimate ¼” thick wall vessel	0.17	1	1	1E-4 Trip & Fall	1	1	E-4	1C	NO
	[redacted] Tank	**(Implementing Safety Action Request SAR [redacted])**	**Using 1” Pink Poly Foam** on [redacted] Tank **(SAR [redacted])**	A	Shock	[redacted] 100%	ft lb$_f$	30 ft lb$_f$	40 ft lb$_f$ 1” PPE Foam thin wall 100% [redacted] (1/2 90% [redacted] data)	1.3	8E-3	1	1E-4 Trip & Fall	1	1	8E-7	1E	YES
	[redacted] Tank	**Twice the Pink Poly Foam Thickness as recommended**	**Using 2” Pink Poly Foam** on [redacted] Tank	A	Shock	[redacted] 100%	ft lb$_f$	30 ft lb$_f$	80 ft lb$_f$ 2” PPE Foam thin wall 100% [redacted] (1/2 90% [redacted] data)	2.7	2E-5	1	1E-4 Trip & Fall	1	1	2E-9	1E	YES

The justification for each probability is documented in a companion “Hazards Summary Reference” table (which is not shown in this SAND Report).

APPENDIX C: COMPARISON OF METHODS

NOTE: Read this appendix with in conjunction with Table 1. Conservatisms and Non-Conservatisms because the numbering corresponding from this appendix to that table. Also please note the legend of highlighted colours below to determine methods used for this appendix.

Interpretation/Observations of Pantex 13385-ANL-2

This document duplicates the most pertenent calculations used in 13385-ANL-2, and has been annotated with comments, and alternative methods.

In general the calculations are in the same order as they appear in 13385-ANL-2, so they should be relatively easy to follow if familiar with 13385-ANL-2.

Key to highlight colours:
- original calculation
- note
- conservative
- unconservative
- unclear if conservative or not
- Additional checks/calcs with alternative method
- Proposed MENSA Approach

Input Data

Operator weight	$W_{man} := 280lbf = 1.246 \times 10^{3} N$	1) Conservative assumption on 95% operator weight (conservative but not bounding)
Operator Mass	$M_{man} := \frac{W_{man}}{g} = 280 \cdot lb$ $\quad M_{man} = 127.006\,kg$	
Operator CoG height	$Height_{CoGMan} := 41in$	
Arm length	$\delta_{arm} := 12.6in$	14) Conservative assumption on using 5% arm length, twinned with 95% man (for force calcs only, doesn't effect topple)
Carried item weight	$W_{carry} := 0lbf$	2) non-conservative assumption on zero carried weight
Carried item mass	$M_{carry} := \frac{W_{carry}}{g}$	
Tool weight	$W_{tool} := 100lbf = 445N$	guess an approximate tool weight for the sake of getting an answer
Tool mass	$M_{tool} := \frac{W_{tool}}{g} = 45\,kg$	
Initial Operator travel velocity in X	$V_{xman} := 2.5mph$	3) Conservative assumption on operator speed. This is a square relationship
Tool CoG height	$Y_{eg} := 1m$	guess an approximate tool CoG height for the sake of getting an answer
Tool base diameter	$D := 1m$	guess and approximate tool base diameter for the sake of getting an answer

note
Unclear if conservative or not

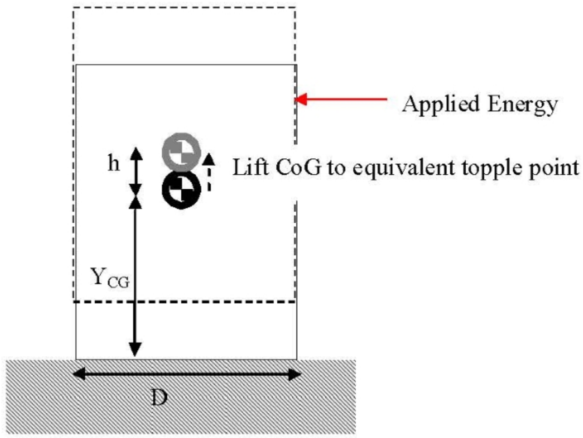
Mass moment of inertia around CoG $I_{tool} := 200\text{kg}\cdot\text{m}^2$

guess. Note: must be about axis of pivot, not CoG

Simple energy tipping (first pass analysis)

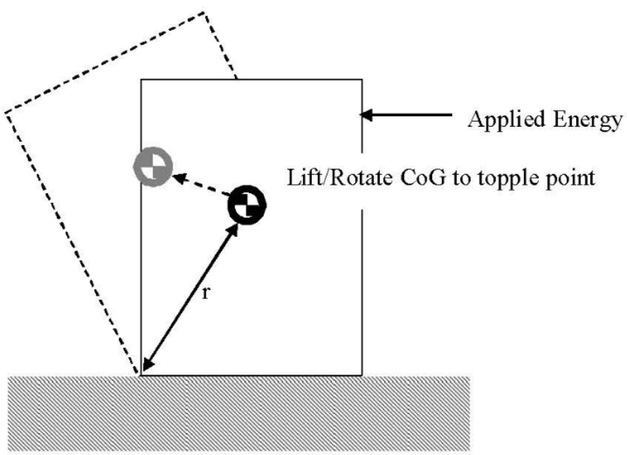
(lift CoG past toppling point)

This is a diagram of the modelled situation:



4) Assumes horizontally applied load is transferred to vertical lift. No rotation.

This diagram shows the more complex model, but is also helpful here to define r, which in turn defines h.



Stability Ratio $R_{stab} := \frac{Y_{eg}}{D} = 1$

Radius from pivot to CoG $r = \sqrt{Y_{eg}^2 + \left(\frac{D}{2}\right)^2}$

Original calculation

note
conservative
unconservative
Additional checks/calcs with alternative method

$$r := \sqrt{Y_{eg}^2 + \left(\frac{D}{2}\right)^2} = 1.118\,m$$

Distance to lift CoG to topple $h_{tip} = r - Y_{eg}$

$$h_{tip} := r - Y_{eg} = 0.118\,m$$

For convenience write h.tip in terms of D and R

re-define $h_{tip} := \left[\sqrt{Y_{eg}^2 + \left(\frac{D}{2}\right)^2} - Y_{eg}\right] = 0.118\,m$

re-define for convenience $h_{tip} := D\cdot\left(\sqrt{R_{stab}^2 + \frac{1}{4}} - R_{stab}\right) = 0.118\,m$ (see working to get to this point in pantex document)

Calculate energy needed to reach tipping point

$PE_{tool} = KE_{man}$

5) Conservative assumption that all KE of operator is converted and applied to the tool, in reality much will be directed back in to the operator.
Simplified assumption that entire tool is lifted linearly, rather than accounting for rotation about pivot.

$PE_{tool} = m\cdot g\cdot h_{tip}$ $KE_{man} = \frac{1}{2}\cdot m\cdot v^2$

$PE_{tool\_simple} := W_{man}\cdot h_{tip} = 147.012\,J$ $KE_{man} := \frac{1}{2}\cdot M_{man}\cdot V_{xman}^2 = 79.3\,J$

These two numbers (PE_{tool_simple} and KE_{man}) need to be compared to check if there is enough energy available to topple the tool.

6) non-conservative assumption ignoring additional energy (conversion from PE to KE) from oprator loss in height as he falls.

Additional Energy (from lost PE) could be as much as -

$$E_{manAdditional} = PE_{lost}$$

$$PE_{lost} = m\cdot g\cdot h$$

$$PE_{lost} := M_{man}\cdot g\cdot Height_{CoGMan} = 1297\,J$$

This is a significant amount of energy not accounted for if the CoG drops significantly, a more accurate figure (and the H and V componants) could be calculated for any given impact height.

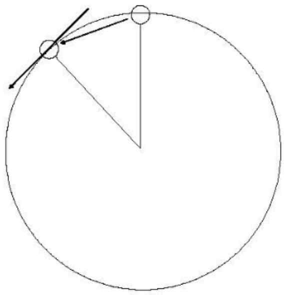
For toppling horizontal is the only important factor:

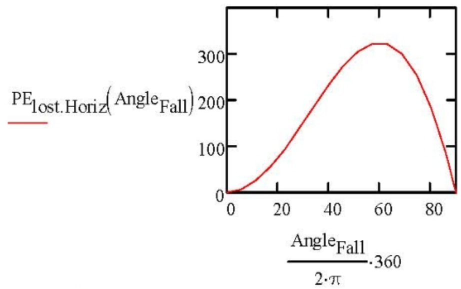
Drop for a given angle $Drop(\theta) := Height_{CoGMan} - Height_{CoGMan}\cdot\cos(\theta)$

$$PE_{lost.Horiz}(\theta) := M_{man}\cdot g\cdot Drop(\theta)\cdot\cos(\theta)$$

Original calculation

Additional checks/calcs with alternative method





$\theta := 55°$ first guess

Given

$\theta < 1°$

$\theta > 90°$

$Q := Maximize(PE_{lost.Horiz}, \theta) =$ ▮

$Maximize(PE_{lost.Horiz}, \theta) = 60\cdot°$

$PE_{lost.Horiz}(60°) = 324\,J$

So the maximum possible additional horizontal energy from drop in CoG is approxiamtely 330J at 60deg angle. Again, we shouldn't assume that the whole of this energy is transferred to the tool.

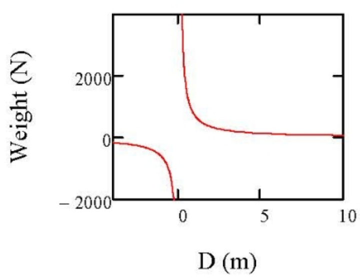
$PE_{tool} = W_{tool}\cdot h_{tip}$

$PE_{tool} = KE_{man}$

Tool weight $W_{tool} = \frac{KE_{man}}{h_{tip}}$

Tool weight function $W_{tool\_fn}(D) := \frac{KE_{man}}{\left[D\cdot\left(\sqrt{R_{stab}^{2} + \frac{1}{4}} - R_{stab}\right)\right]}$

Plot Weight vs D:



Using this graph, or the function which defines it, the designer can select the required D based on the Weight of the tool to prevent topple. R can also be modified to give a different curve.

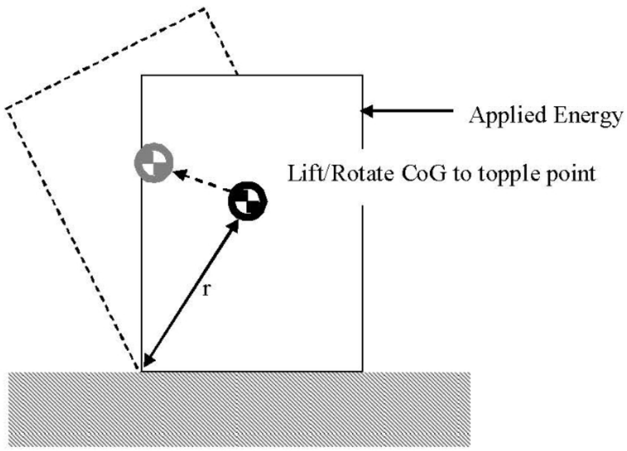
$W_{tool\_fn}(1000mm) = 671.985\,N$

$W_{tool\_fn}(1000mm) = 151.068\cdot lbf$ (agrees with pantex charts)

Unclear if conservative or not

conservative

Inertial energy tipping (Second pass analysis)



7) This could be more or less conservative than the previous calculation depending on the geometry and mass moment of inertia of the tool.
If the mass moment of inertia is very low then the tool is easy to rotate and the simple calculation may be more conservative.

Conservation of momentum:

$$Mom_{RotTotalAtImpact} = Mom_{RotTotalAtTopple}$$

~~8) Deleted~~

$$Mom_{RotTotalAtImpact} = M_{man\_1} \cdot v_{man\_1} \cdot Y_{eg} + I_{tool} \cdot \omega_{tool\_1}$$

$$Mom_{RotTotalAtTopple} = M_{man\_2} \cdot v_{man\_2} \cdot Y_{eg} + I_{tool} \cdot \omega_{tool\_2}$$

$$M_{man\_1} \cdot v_{man\_1} \cdot Y_{eg} + I_{tool} \cdot \omega_{tool\_1} = M_{man\_2} \cdot v_{man\_2} \cdot Y_{eg} + I_{tool} \cdot \omega_{tool\_2}$$

assume $v_{man\_2} := 0$ and $\omega_{tool\_1} := 0$

$$M_{man\_1} \cdot v_{man\_1} \cdot Y_{eg} = I_{tool} \cdot \omega_{tool\_2}$$

$$\omega_{tool\_2} = \frac{M_{man\_1} \cdot v_{man\_1} \cdot Y_{eg}}{I_{tool}}$$

Assuming pivot about 1 point,

$$KE_{ToolRotational} = PE_{ToolLinear}$$

9) Conservative assumption that all KE of operator is converted and applied to the tool, much will be directed

elsewhere.

$$\frac{1}{2}\cdot I_{tool}\cdot\omega^2 = M_{tool}\cdot g\cdot h_{tip}$$

$$\frac{1}{2}\cdot I_{tool}\cdot\left(\frac{M_{man}\cdot v_{xmanx}\cdot Y_{eg}}{I_{tool}}\right)^2 = M_{tool}\cdot g\cdot\left[\sqrt{Y_{eg}^{\;2}+\left(\frac{D}{2}\right)^2} - Y_{eg}\right]$$

$$\frac{1}{2}\cdot I_{tool}\cdot\left(\frac{M_{man}\cdot v_{xmanx}\cdot Y_{eg}}{I_{tool}}\right)^2 = \frac{1}{2}\cdot M_{man}\cdot v_{xmanx}^{\;2}$$

Need to find speed of impact of the man to cause toppling

Solving for the required man velocity velocity to satisfy the above equality v_{xmanx}

$$v_{xmanx} := \frac{\sqrt{2}\cdot\sqrt{I_{tool}}\cdot\sqrt{M_{tool}}\cdot\sqrt{g}\cdot\sqrt{Y_{eg}-\sqrt{\frac{1}{4}\cdot D^2+Y_{eg}^{\;2}}}\cdot i}{M_{man}\cdot Y_{eg}} = -1.141\,\frac{m}{s}$$

$$v_{xmanx} := -\frac{\sqrt{2}\cdot\sqrt{I_{tool}}\cdot\sqrt{M_{tool}}\cdot\sqrt{g}\cdot\sqrt{Y_{eg}-\sqrt{\frac{1}{4}\cdot D^2+Y_{eg}^{\;2}}}\cdot i}{M_{man}\cdot Y_{eg}} = 1.141\,\frac{m}{s}$$

the only real, positive solution. Agrees with Pantex formula.

pantex formula:

$$\sqrt{\frac{2\cdot M_{tool}\cdot g\cdot\left(\sqrt{Y_{eg}^{\;2}+\frac{D^2}{4}}-Y_{eg}\right)\cdot I_{tool}}{M_{man}^{\;2}\cdot Y_{eg}^{\;2}}} = 1.141\,\frac{m}{s}$$

Energy required

$$KE_{man} = \frac{1}{2}\cdot m\cdot v^2$$

Energy required to tip the tool considering conservation of momentum:

10) non-conservative assumption ignoring additional energy (conversion from PE to KE) from oprator loss in height as he falls.

$$KE_{man\_inertial} := \frac{1}{2}\cdot M_{man}\cdot v_{xmanx}^{\;2} = 82.68\,J$$

This depends heavily on the mass moment of inertia of the tool.

This should be compared against the total amount of energy ($KE_{man} = 79.317\,J$) that the man has to see if toppling will occur.

Maximum Exerted Force of a Tripping Man

Impact **above** 41 inches

Original calculation

unconservative
Additional checks/calcs with alternative method
Unclear if conservative or not
Proposed MENSA approach

11) assumption that the CoG of the user is at 41 inches, so any impact will be purely horizontal

Maximum energy of man $KE_{man} = 79.317\,J$

Make the assumption that the only coimpliance in the system is the users arms, of length δ_{arm}.

12) Assumption that the arms are the only compliance is conservative, however this assumes a certain type of fall, which may not be conservative. It is a realisitc scenario.

13) Assumption that the feet of the user are pinned during the fall.

$$Force = \frac{Energy}{Distance}$$

15) non-conservative assumption that the applied force is constant. Plus there is no impact factor to account for the speed of the applied load. Plus the extra energy from falling CoG is not included.

$$F_x := \frac{KE_{man}}{\delta_{arm}} = 247.835\,N \qquad F_x = 55.715 \cdot lbf$$

An alternative approach would be at assume a natural frequency for the human (and infinite stiffness for the tool) to calculate an impact duration.......

deceleration time $time_{decel} := 0.1 s$ $\qquad \frac{1}{time_{decel}} = 10 \cdot Hz$

MENSA MER-001-144394-R-02-S01 DRAFT Approach - assumes body is completley rigid and uses impact factor and conservatism factor.

$$Force_{Resultant.MENSA} = M_{man} \cdot I_{Factor} \cdot g \cdot Height_{CoGMan} \cdot \frac{\sin(\theta) \cdot \lambda_{conservatism}}{Reach_{Height}}$$

Arbitrary conservatism $\lambda_{conservatism} := 1.1$

Height of shoulders $Reach_{Height} := 1580mm$

Impact Factor $I_{Factor} := 1.4$

Conservative impact factor and conservatism factor

Non conservative - not taking initial speed in to account

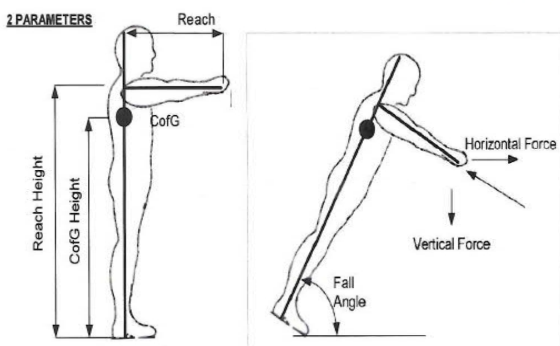


Figure 1 Standing Position Figure 2 Falling

Original calculation

Proposed MENSA approach

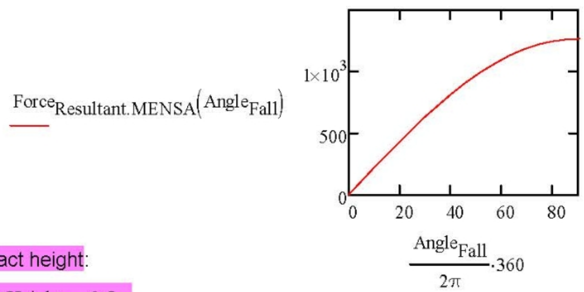
conservative

$$Force_{Resultant.MENSA}(\theta) := M_{man} \cdot I_{Factor} \cdot g \cdot Height_{CoGMan} \cdot \frac{\sin(\theta) \cdot \lambda_{conservatism}}{Reach_{Height}}$$

$$Force_{Resultant.MENSA}(90°) = 1264\,N$$

$$Force_{Resultant.MENSA}(45°) = 894\,N$$

$$Force_{Resultant.MENSA}(90° - 31.6 \cdot °) = 1077\,N$$



Calculate force for any given contact height:

$$ContactHeight := 0.5m$$

$$Reach := 975mm$$

$$InitialAngle := atan\left(\frac{Reach}{Reach_{Height}}\right) = 31.678 \cdot °$$

$$hypotinuse := \frac{Reach}{\sin(InitialAngle)} = 1857 \cdot mm$$

$$RemainAngle := asin\left(\frac{ContactHeight}{hypotinuse}\right) = 15.623 \cdot °$$

$$FallAngle := \frac{\pi}{2} - RemainAngle - InitialAngle = 42.699 \cdot °$$

$$Force_{Resultant.MENSA}(FallAngle) = 857\,N$$

Maximum Exerted Force of a Tripping Man

Impact **below** 41 inches

16) assumption that the CoG of the user is at 41 inches, so any impact will be both horizontal and vertical

$$F_x = 248\,N$$

$$F_y := M_{man} \cdot g = 1246\,N$$

$$Force_{Resultant.MENSA}(90° - 31.6 \cdot °) = 1077\,N$$

17) Conservative assumption that maximum possible Fx and Fy are applied in any case, rather than calculating the vector depending upon angle of operator at impact.

unconservative
conservative

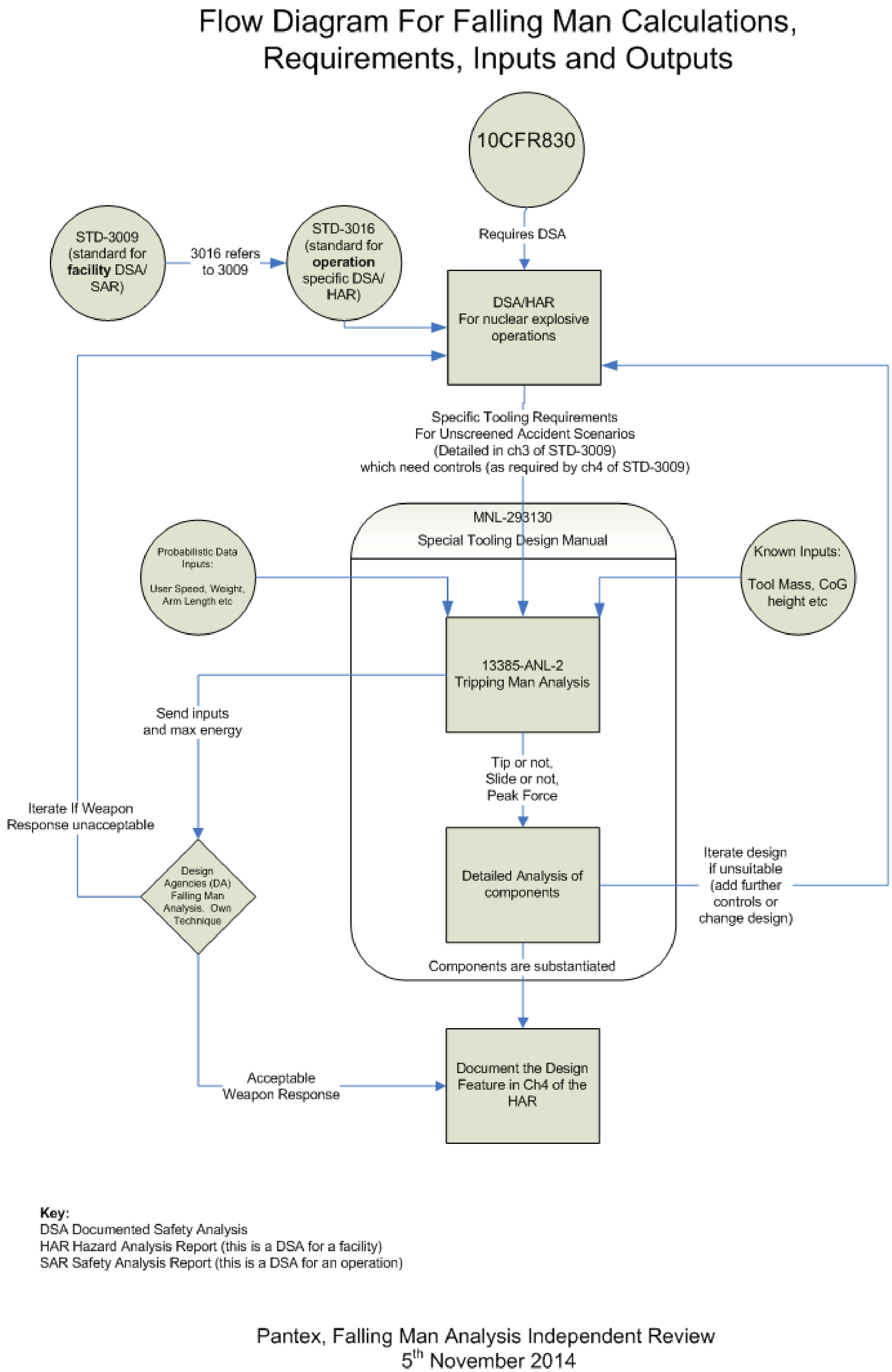
18) non-conservative assumption that the applied force is constant. Plus there is no impact factor to account for the speed of the applied load.

19) non-conservative assumption ignoring additional energy (conversion from PE to KE) from oprator loss in height as he falls.

(Skip the Sliding, Gait and Hoisted calculations to concentrate on more frequently used calculations)

20) Output from these calculations are used in further detailed checks. The forces are applied as point loads, and peak values of stress are compared to the allowable figures.

APPENDIX D: FALLING MAN ANALYSIS INPUTS AND OUTPUTS



APPENDIX E: PANEL MEMBERS

Louis Bertolini, is a member of the management staff at the LLNL. For the last two years Lou has served as the Defense Technologies Engineering Associate Division Leader for Operations. In this role, he has been responsible for overseeing the Environmental, Safety and Health and Security compliance of the engineering personnel supporting LLNL Weapons and Complex Integration activities. He chairs LLNL Significant Finings Investigation and Weapons Response Peer Reviews. He is responsible for the conduct of internal LLNL technical reviews. Prior to joining the Weapons Program, Lou served for 12 years as a design engineer and later as an Associate Program Leader at the LLNL National Ignition Facility. He has been a staff mechanical engineer at LLNL for 36 years serving in a variety of programs and projects. Lou earned his B.S. in Engineering from California Polytechnic State University at San Luis Obispo, California.

Nathan G. Brannon, Ph.D., is a Distinguished Member of the Technical Staff at Sandia National Laboratories. For the last four years Nathan has served as the W78 Weapon System Lead. Prior to the W78 program, Nathan was an Annual Assessment Red Team Chair coupled with responsibilities for the Independent Nuclear Weapon Assessment Team research program. Nathan was detailed to the National Nuclear Security Agency Headquarters, Office of Nuclear Surety as a technical advisor where he published three Department of Energy directives. For ten years Nathan worked in the Human Factors Department at Sandia supporting a variety of programs including process engineering at Pantex (Seamless Safety for the 21st Century), weapon development programs, and Work for Others (WFO) research and development programs. His primary technical area of expertise is computational modeling of cognition to support systems engineering. Nathan holds a patent for Human-Machine Interactions (US 7,526,465 B1). He has published several journal articles related to cognitive modeling, pilot spatial orientation and most recently with respect to human interaction with sensor fusion algorithms. Nathan earned a B.S., M.S., and Ph.D. in Human Factors Engineering from Wright State University in Dayton, Ohio.

Jared K. Olson, Ph.D., is a Program Manager at ATK Aerospace Group with responsibility for Specialty Materials. Jared has over 12 years' experience in propellant and explosives manufacturing, composites manufacturing, specialty chemicals manufacturing, and research and development. Experience includes roles as a Research Scientist, Hazards Analyst, and Program Manager. Jared has over 30 publications and four patents, which include patents for the prevention of initiation of explosive devices (US Patent 7,810,421) and measuring electrical properties of energetic materials (US Patent 7,609,073). Jared earned B.S. and M.S. degrees in Physics from the University of Utah, an MBA from Westminster College, and a Ph.D. in Physical Chemistry from Utah State University.

Bernard Price, ATK Aerospace Group – Propulsion Systems

MS Physics, University of Utah
BS Physics, University of Utah
MBA/MIS, Westminster College
25 years Explosives/ Semiconductor/ Composite Mfg. Experience
Areas of Expertise:

- Team Management
- ESE/ESD, RF, Lightning
- Demil, Fuze Safety

Experience spans composite, semiconductor and explosives manufacturing industries in diverse rolls such as industrial engineering, environment science, manufacturing engineering, product development and safety. Currently the Director of Safety and Plant Protective Services at ATK, with responsibility for Hazards Analysis, Industrial Safety, Radiation Safety, Industrial Hygiene, Security, Fire and Medical Services in compliance with the Department of Defense, NASA and other federal agency regulations.

Industry Committee Experience:

- Principal Member, National Fire Protection Association Technical Committee on Static Electricity, 2014 NFPA 77 Re-write
- Founding Chairman, Working Group Committee 31, Institute of Environmental Sciences (Currently IEST), "Outgassing Performance Criteria for Cleanroom Materials".
- Member, Working Group Committee, Institute of Environmental Sciences (Currently IEST), "Automotive Issues Group on Vibration Data Analysis and Test Methodology".

Michael Steinzig, PE, PhD., is a system engineer in the Weapons System Engineering group at LANL. Mike is currently responsible for product definition of the W88 nuclear warhead, and has supported the Navy nuclear warheads (W76 and W88) at LANL since 2005. From 1999-2005 he worked for a company specializing in ultra-stable platforms and composite structure design, and interferometric diagnostic techniques. He worked in the power industry and conducted performance testing on heat recovery steam generators from 1990-1995 prior to graduate study. Mike's graduate work focused on computational fluid dynamics and material modeling. In the last 10 years, he has developed significant expertise in the measurement and analysis of residual stresses. He received his BA in Physics from Colorado College in 1987. Mike received his PhD in Mechanical Engineering from New Mexico State University in 1999.

Robert Wardle, PhD., is the Director of Technology Programs at ATK Aerospace Group. In this role, he leads the IR&D Program as well as contracted R&D efforts for the Group. Prior to this role, Robert has:

- ran the Research and Development Laboratories within ATK.
- published over 100 technical papers in forums from JANNAF to Journal of Organic Chemistry.
- inventor of 40 granted U.S. Patents in the broad area of propulsion, explosives and pyrotechnics.
- served on numerous national boards and panels including for the National Academy of Sciences and the National Academy of Engineering.
- served on an external review panel for LANL for 6 years.
- also done relevant work has been on the manufacture, handling and processing of explosive materials.
- developed novel processes for the manufacture of CL-20, BDNPA/F and TEX.
- led the effort to design and commission new explosives processing facilities at ATK including for loading of warheads and explosives.

Michael Winfield, CEng, IMechE, is a Senior Mechanical Design Engineer with AWE in the Mechanical Compliance Team (2013 to present). His current position revolves around ensuring adequate substantiation and legal compliance of new mechanical designs for conventional and nuclear related equipment. He has a background in engineering substantiation and consultancy covering:

- Nuclear Safety Case for British Energy power stations and AWE lifting equipment,
- Time history and response spectrum analyses on high temperature oxygen, chlorine and titanium dioxide production plant piping,
- Dynamic and modal analyses of 'vertical turbine' firewater pumps used on oil drilling platforms,
- Static piping analyses with fully non-linear supports, complex thermal gradients and pressure cycles,
- He has designed, developed, tested and sold bespoke devices including a tool to spin and tighten a nut on to an un-retained and inaccessible bolt,
- Tubular space frame design for a large lorry based x-ray scanner,
- Explosion, wind and snow loading calculations on large panel structures.

Distribution

1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories