Department of Energy's

An Introduction to Current Practices at DOE

James O'Brien
DOE / HSS

Workshop on Risk Assessment and Safety Decision Making Under Uncertainty

September 2010

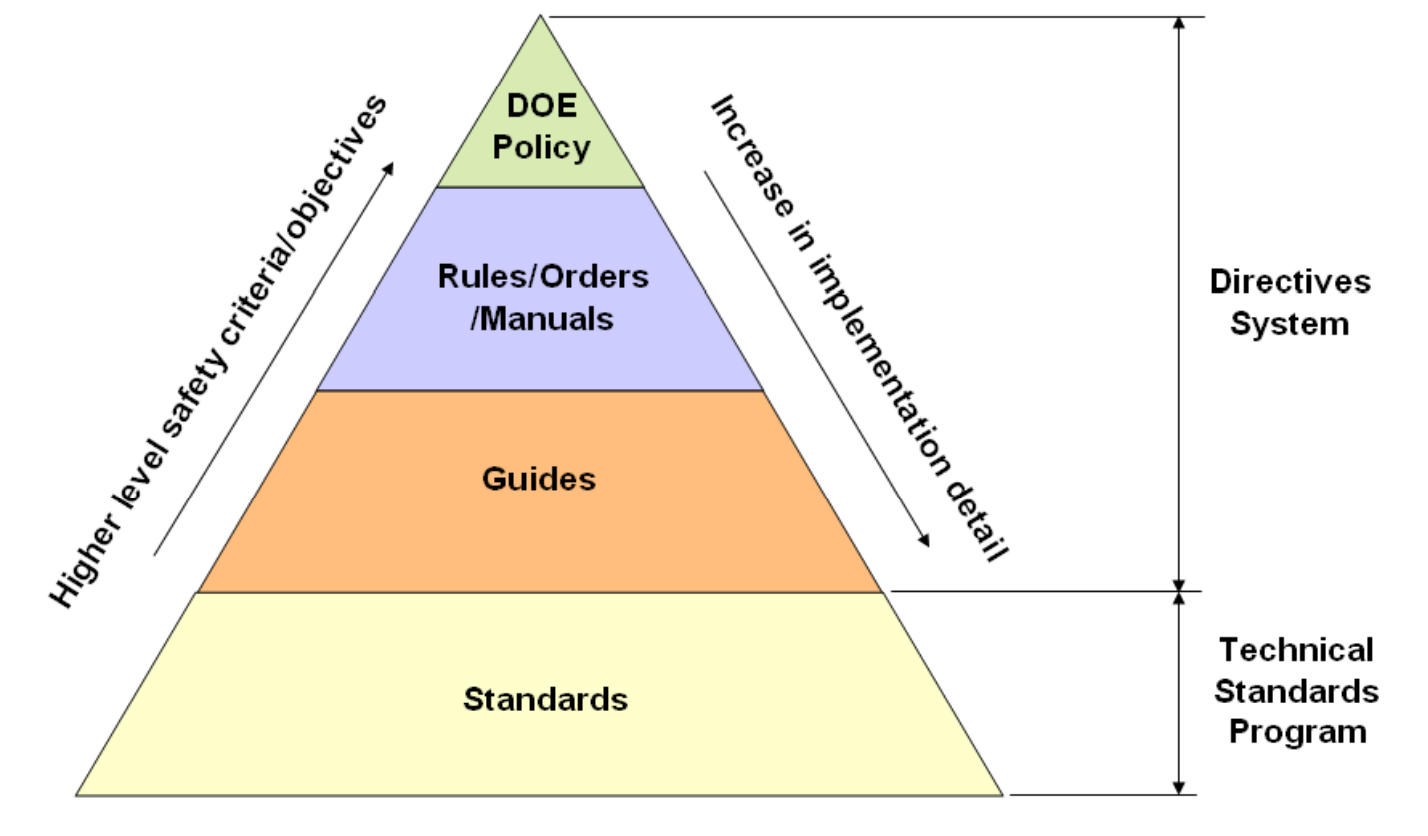
HSS
Office of Health, Safety and Security

DOE Nuclear Safety Framework

- A hierarchical set of governing documents:
  - Starts with Policies (sets high level expectations)
  - Rules and Orders (provide requirements)
  - Guides and Standards (provide acceptable methods and criteria)
- Framework defined in:
  - DOE Order 251.1C, *Departmental Directives Program*
  - DOE Order 252.1, *Technical Standards Program*

Current DOE Nuclear Safety Framework (continued)

DOE Directives and Technical Standards Hierarchy



Current DOE Nuclear Safety Framework (continued)

POLICY	**SEN 35-91**	
	"DOE facilities will be designed, constructed, operated, and decommissioned to assure the protection of the public, workers, and the environment."	
REGULATIONS	**10 CFR 830, Subpart A** ***Quality Assurance***	**10 CFR 830, Subpart B** ***Safety Basis***
	"Establish and Implement QA Plan"	"Establish, Maintain and Work IAW Safety Basis"
ORDERS	DOE Order 414.1, *Quality Assurance*	DOE Order 420.1B, *Facility Safety* DOE Order 425.1C, *Startup and Restart of Nuclear Facilities* DOE Order 433.1B, *Conduct of Maintenance* DOE Order 426.2, *Conduct of Training* DOE Order 422.1, *Conduct of Operations* DOE Order 5480.30, *Nuclear Reactor Safety Design Criteria* DOE Manual 442.1-1, *Differing Professional Opinions Manual*
GUIDES AND STANDARDS	DOE Guide 414.1-1B, *Management and Independent Assessment* DOE Guide 414.1-2A, *Quality Assurance Management System* DOE Guide 414.1-3, *Suspect/Counterfeit Items* DOE Guide 414.1-4, *Safety Software* DOE Guide 414.1-5, *Corrective Action Program* DOE Standard 1150, *Quality Assurance* DOE Standard 1073, *Configuration Management* DOE Standard 1172, *Safety Software Quality Assurance*	DOE Guide 420.1-1, *Facility Safety Design* DOE Guide 420.1-2, *Natural Phenomena Hazards* DOE Guide 420.1-3, *Fire Protection* DOE Guide 421.1-1, *Criticality Safety* DOE Guide 421.1-2, *Safety Analysis* DOE Guide 424.1, *Unreviewed Safety Questions* DOE Standard 1020, *Natural Phenomena Hazards* DOE Standard 1027, *Hazard Categorization* DOE Standard 1104, *Safety Analysis Review* DOE Standard 1189, *Safety in Design* DOE Standard 3006, *Operational Readiness Reviews* DOE Standard 3009, *Safety Analysis Preparation*

Nuclear Safety Policy
SEN 35-91

Top Level Policy Statement

- *It is the policy of the Department of Energy (DOE) that the general public be protected, such that no individual bears significant additional risk to health and safety from the operation of a DOE nuclear facility above the risks to which members of the general population are normally exposed.*

- *The purpose of this document is to establish the basic nuclear safety policy from which specific safety Rules, Orders, Standards, and other requirements shall follow.*

- *DOE facilities will be designed, constructed, operated, and decommissioned to assure the protection of the public, workers, and the environment.*

Nuclear Safety Policy
SEN 35-91

Key Elements for Implementing the Policy

- Management
- Technical Competence
- Safety Goals
- Independent Oversight
- Safety Culture

Nuclear Safety Policy
SEN 35-91

Safety Goals (paraphrased)

- The risk to an average individual in the vicinity (1 mile) of a DOE nuclear facility for prompt fatalities should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatalities resulting from other accidents to which members of the population are generally exposed.

- The risk to the population in the area (10 miles) of a DOE nuclear facility for cancer fatalities should not exceed one-tenth of one percent (0.1%) of the sum of all cancer fatality risks resulting from all other causes.

- Aiming points for performance

Draft
Update of Nuclear Safety Policy

- Minor Clarifications
- Reflect DOE's Use of Integrated Safety Management
- Address Use of Quantitative Risk Assessments

  Ensuring that quantitative and probabilistic risk assessments is only used to supplement qualitative hazard assessment and hazard control development processes when allowed by DOE directives and to the extent supported by industry practices and availability of risk data [current proposed draft]

10 CFR 830
Nuclear Safety Requirements

- Subpart A, *Quality Assurance Requirements*
- Subpart B, *Safety Basis Requirements*
  - Hazard Category 1,2, and 3
  - Documented Safety Analysis
  - Change Control

DOE Order 420.1B
Facility Safety

Addresses Five Important Facility Safety Areas

- Nuclear Safety and Explosive Safety Design
- Fire Protection
- Natural Phenomena
- Criticality Safety
- System Engineering (Configuration Management)

Establishes Key Nuclear Safety Design Criteria -- Defense in Depth

- Remote Siting
- Minimize Hazardous Material
- Design Margin
- Multiple Barriers
- Rigorous Operations

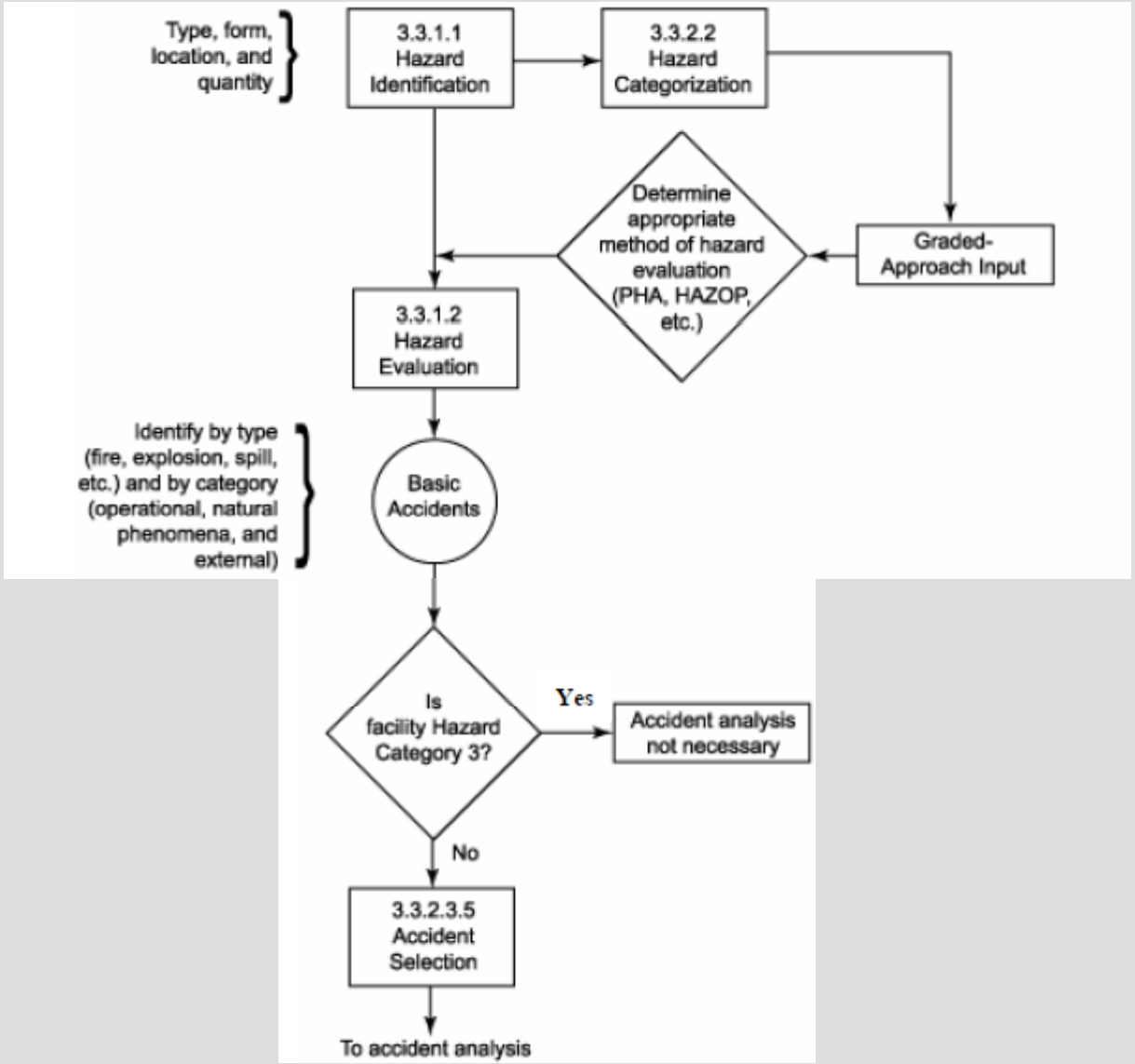
Implementing Guides and Standards

- Key Standards and Guides
  - DOE Standard 1027 – Facility Hazard Categorization
  - DOE Standards 3009 and 1189 – Safety Analysis Development
  - DOE Handbook 3010 – Airborne Release Fraction
  - DOE Guide 420.1-1 – Facility Safety Design
- Standards can be found at: https://www.directives.doe.gov/
- Guides can be found at: http://hss.doe.gov/nuclearsafety/ns/techstds/

Current Use of Risk Assessments to Support Safety Decision Making

- Facility-Specific Hazard Assessments based upon Center for Chemical Process Safety Guides
- Primarily Qualitative Assessment of Impacts to In-facility Workers, Co-located Workers, and Public
  - Includes Conservative Quantitative Calculation of Unmitigated Accident Calculation
  - Comparison Against “Evaluation Guide”
- Establish “Safety Significant” Controls for
  - Protection of Workers
  - Significant Defense in Depth protection of Public
- Establish “Safety Class” Controls for Protection of Public

Hazard/Accident Analysis Overview

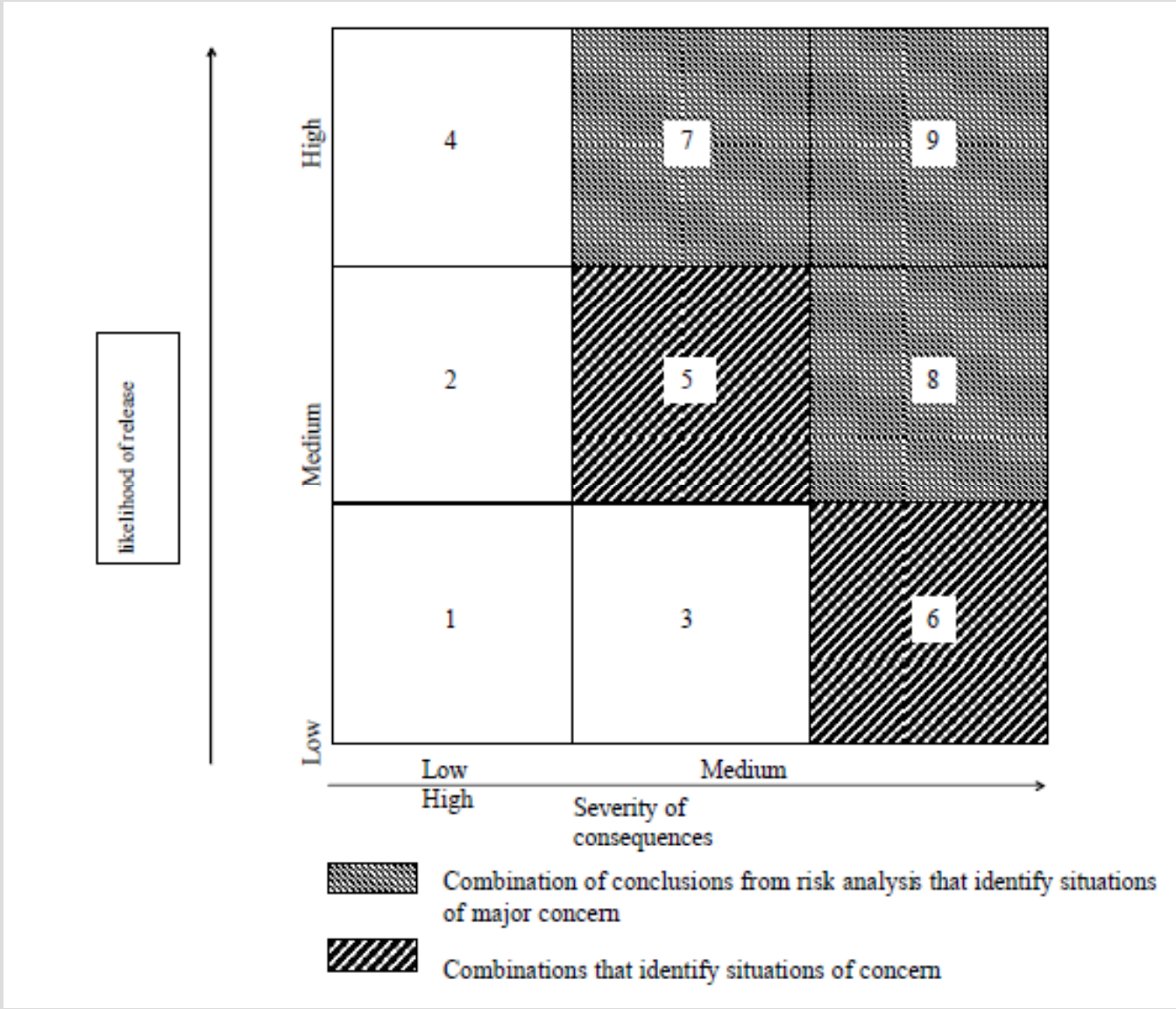


Example of Process Hazard Analysis in DOE Standard 3009

Facility: Example Refinery Date: 04/07/90 Page 3 of 30
Area: HF Alkylation
Unit: Unloading HF from Supply Tanker

Hazard	Cause	Protection and mitigative systems	Consequence	Frequency	Ranking	Action item/ Comment
(1) Anhydrous HF, 5,000 gallons. (2) <100 psi potential energy from nitrogen blanket.	(1) Leak at connection point. (2) HF hose ruptures. (3) HF hose ruptures, flow not immediately shut off. (4) Truck relief valve fails open. (5) Truck relief valve opens; over-pressure conditions. (6) Tanker failure from over-pressure. (7) N_2 hose ruptures.	(A) Operators in chemical suits with respirators for emergency use. (B) Specific procedures, trained operators. (C) HF detectors. (D) HF line remote shutoff valve on truck. (E) Emergency relief valve capping kit available. (F) Two N_2 pressure regulators. (G) Check valve on N_2 gas line. Maximum N_2 pressure less than tanker design pressure. (H) Emergency water deluge system.	(1) Minor operator exposure – **LOW.** (2) Minor operator exposure off site <ERPG-2 – **LOW.** (3) Operator exposure, possibly ERPG-2 off site – **MEDIUM.** (4) Typically (a) **LOW** if capped. Possibly (b) **MEDIUM** if not capped and no deluge. (5) Typically (a) **LOW** if short duration. Possibly (b) **MEDIUM** if longer and no change. (6) Possible operator fatalities and ERPG-3 off site – **HIGH.** (7) N_2 leak– **LOW.**	(1) **HIGH** (2) **MEDIUM** (3) **LOW** (4) (a) **MEDIUM** (4) (b) **LOW** (5) (a) **LOW** (5) (b) **LOW** (6) **LOW** (7) **MEDIUM** (8) See #5 frequency (9) **HIGH**	4 2 3 2 3 1 3 6 2 See item #5 4	(1) Verify that procedures provide consistent leak-check on fitting. (2) Verify that procedures provide appropriately defined interaction between plant personnel and truck operators. (3) Area should be roped off and access controlled during unloading. (4) Specific evacuation routes for operators should be defined in procedures.

Risk Ranking and Binning



Ranking and Binning (cont)

- Designed to separate the lower risk accidents that are adequately assessed by hazard evaluation from higher risk accidents that may warrant additional quantitative analysis if the phenomena involved are not simplistic.

- Ranking should use broad bins.
  - frequency bins should typically cover two orders of magnitude.

- Binning is essentially qualitative, analysts can use a simple numerical basis for judgments to provide consistency.

Ranking and Binning Schemes

- Simple methodology for frequency binning
  - a probability of 1 to non-independent events,
  - 0.1 to human errors,
  - and 0.01 to genuinely independent failures.

- Another methodology would be to use a summary historical data.

- A conservative Gaussian plume estimation of the amount of material needed outside the building to cause a certain dose might be performed to aid in defining thresholds of significance.

Control Hierarchy

- Passive or Active
- Preventative or Mitigative
- Closest to Hazard
- Engineered
- Administrative

Control Reliability

- Quality Assurance
- Configuration Management
- Technical Safety Requirements
- Single Failure (for Safety Class Active Engineered Controls)

Risk Assessment Information Notice

- Defines Risk Assessment
- Identifies Risk Assessments Applications at DOE
- Discusses Quality Assurance for Nuclear Safety Applications
- Promotes use of Risk Assessment Technical Expert Group

Risk Assessment Information Notice (cont)

- DOE uses risk assessments and risk management processes in numerous ways
  - to support project management decisions
  - selection between alternative safety systems,
  - supporting an unreviewed safety question determination,
  - compliance with established performance objectives
- Risk assessment tools are employed they must be used appropriately in a technically sound manner
- Their use in nuclear safety applications is subject to theDOE quality assurance requirements as well and line management and independent oversight

Risk Assessment Information Notice (cont)

- Risk assessments can be used to inform nuclear safety decisions, but are not a substitute for complying with nuclear safety requirements.

- Department's approach does not require or expect the level of detail analysis necessary for a quantitative or probabilistic risk assessment

Next Steps/Challenges

- Identifying Application (e.g., defining nuclear safety application)
- Communications
  - Risk Assessment Terms
    - Qualitative
    - Probabilistic Risk Assessment
    - Semi-quantitative
    - Deterministic
  - Risk Assessment Results

DOE Challenges with increase use of QRA/PRA

- Ensuring Appropriateness and Adequacy of Tools
- Ensuring Adequacy of Data
- Developing Standards/Guidance for
  - Performance of QRA
  - QA of QRA
  - Peer Review of QRA
- Establishing Appropriate Support Infrastructure

Benefits/Costs with increase use of QRA/PRA

- Benefits
  - Higher level of safety assurance
  - Use of Quantitative Risk Assessments to Preventative Controls versus Mitigative Controls
  - Understanding importance of controls
  - Defining Design Basis Accidents
- Costs
  - Cost (time, money, resources) of development
  - Cost of maintenance
  - Over reliance on output
- Ensure right application

Information Sources/Contact

Information

- Overview of DOE Nuclear Safety: http://hss.doe.gov/nsrf/
- Office of Health, Safety and Security: http://www.hss.doe.gov/
- U.S. Department of Energy: http://energy.gov/

Contacts

- James O'Brien, Director Office of Nuclear Safety Policy and Assistance (HS-21): james.o'brien@hq.doe.gov
- Andrew Wallo, Deputy Director Office of Nuclear Safety, Quality Assurance and Environment (HS-20): andrew.wallo@hq.doe.gov