SAND2014-17182PE

Exceptional service in the national interest

Operational Safety at US Repositories

Probabilistic and deterministic approaches, and technical vulnerabilities

E.L. Hardin, Sandia National Laboratories

G.-H. Nieder-Westermann, DBE TEC GmbH

Sandia National Laboratories

Verantwortung für Generationen
Responsibility for Generations
DBE TEC
DBE TECHNOLOGY GmbH

PTKA
Project Management Agency Karlsruhe
Karlsruhe Institute of Technology

U.S. DEPARTMENT OF ENERGY

NNSA
National Nuclear Security Administration

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. SAND NO. 2011-XXXXP

Operational Safety at U.S. Repositories

Outline

- Deterministic vs. Probabilistic (finding balance)
- Deterministic Safety Analysis at U.S. Department of Energy (DOE) Facilities (e.g., Waste Isolation Pilot Plant, WIPP)
- Overview of Yucca Mountain Preclosure Safety Analysis (PCSA)
- Current German Approach for Licensing of Repositories
- Technical/Regulatory Vulnerabilities
- Summary and Outlook

Probabilistic vs. Deterministic
Finding Balance for Operational Safety Analaysis

- **U.S. Repositories for HLW/SNF (deterministic ↔ probabilistic)**
  - **Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (10 CFR Part 63, U.S. Nuclear Regulatory Commission)**
    - Aggregated repository worker dose (10 CFR Part 20, U.S. NRC)
    - Dose at or beyond site boundary (10 CFR Part 63, U.S. NRC)
- **German Repositories (deterministic ↔ probabilistic)**
  - **Safety Requirements Governing the Final Disposal of Heat-Generating Radioactive Waste (Sicherheitsanforderungen)**
    - Requires both deterministic and probabilistic assessment
    - Requires implementation of nuclear power plant requirements for operational safety

Deterministic Safety Analysis
U.S. DOE Nuclear Facilities (1/4)

- **Hazards to workers, the public, and the environment**
- **Transuranic Waste (DOE, not NRC regulated)**
- **Deterministic (DOE Order 5480.23 - SAR)**
  - Similar to civilian power plant licensing (NRC 10CFR Part 50)
  - Design basis (normal, accidents, events)
- **Facility Nuclear Hazard Category (complexity and inventory)**
  - Risk Category 1: Potentially significant off-site consequences (e.g., reactor)
  - Risk Category 2: Potentially significant on-site consequences (e.g., WIPP with >80 Ci Pu-239 per container)
  - Risk Category 3: Localized (facility) consequences (e.g., accelerator)

Deterministic Safety Analysis
U.S. DOE Nuclear Facilities (2/4)

- Graded Approach for Each Credible Hazard Identified (DOE STD 5506-2007)
  - Magnitude of hazards, complexity of facilities, life-cycle state
  - Example: WIPP Documented Safety Analysis

ACCIDENT/EVENT DOSE CONSEQUENCE GUIDELINES*

Consequence Level	Maximally Exposed Offsite Individual	Co-Located Worker (at 100 m)	Facility Worker
High	Approaching 25 rem	>100 rem	Safety Significant (DOE STD 3009)
Moderate	≥1 rem	≥25 rem	Qualitative; no threshold
Low	<1 rem	<25 rem	Qualitative; no threshold

ACCIDENT/EVENT RISK CLASS*

Consequence Level	Beyond Extremely Unlikely $<10^{-6}$/yr [A]	Extremely Unlikely 10^{-4} to 10^{-6}/yr	Unlikely 10^{-2} to 10^{-4}/yr	Anticipated 10^{-1} to 10^{-2}/yr
High	III	II	I	I
Moderate	IV	III	II	II
Low	IV	IV	III	III
[A] Probability of 10^{-6} calculated conservatively, or 10^{-7} calculated realistically.				

* Not to be construed as regulatory acceptance criteria, per DOE STD 5506-2007.

Deterministic Safety Analysis U.S. DOE Nuclear Facilities (3/4)

- Hazard/Accident Analysis → Material-at-Risk →
  Hazard Evaluation (prevention, mitigation) → Design Basis
- "Hazard Evaluation" → Technical Safety Requirements
  - Identify Safety-Significant systems, structures and components
  - Administrative controls
- Develop Prevention/Mitigation Controls
  - Examples: waste loading, waste transport, etc.
- Identify Representative Hazards for Further Analysis as Design Basis Events (DBEs)
- Analyze Beyond-Design-Basis Events
  - Low-probability, high consequence

Deterministic Safety Analysis U.S. DOE Nuclear Facilities (4/4)

- **Example: WIPP Risk Ranking**
  - Contact-handled waste, underground events

Event #	Description	Frequency (mitigated)	Consequence (mitigated)			Risk Class		
			MOI [A]	Co-Located Worker	Facility Worker	MOI [A]	Co-Located Worker	Facility Worker
CH-UG-1-001a	Single-vehicle fire underground during waste transport	10^{-4} to 10^{-6}/yr	M	M	L	III	III	IV
CH-UG-1-002a	Collision of 2 vehicles and fire underground during waste transport	10^{-4} to 10^{-6}/yr	L	M	L	IV	III	IV
CH-UG-1-003a	Single-vehicle collision, fire under-ground at waste face	10^{-4} to 10^{-6}/yr	H	H	L	II [B]	II	IV
CH-UG-6-001a	Internal deflagration in CH waste container underground	10^{-2} to 10^{-4}/yr	L	L	H	III	III	I

[A] MOI = Maximally Exposed Off-Site Individual [B] Risk class of I may be unacceptable and II may be marginally acceptable, for the MOI. Source: *WIPP Documented Safety Analysis*, DOE/WIPP 07-3372 Rev. 4

Overview of YM PCSA (1/4)
Probabilistic Approach (YM, Part 63)

- "What can go wrong?"
  - A set of scenarios or event sequences
- "How likely is it?"
  - Compile available evidence including historical records, engineering analysis (e.g. fragility, reliability) and expert judgment
  - Use event sequence diagrams to estimate the probability of unlikely scenarios, with uncertainty
- "What are the consequences?"
  - PCSA Consequences: Directly calculate dose to off-site public, dose to on-site workers and public, criticality
  - Explicit dose limits are defined by decision-makers (e.g., U.S. NRC regulations: 10 CFR Part 63 for YM)

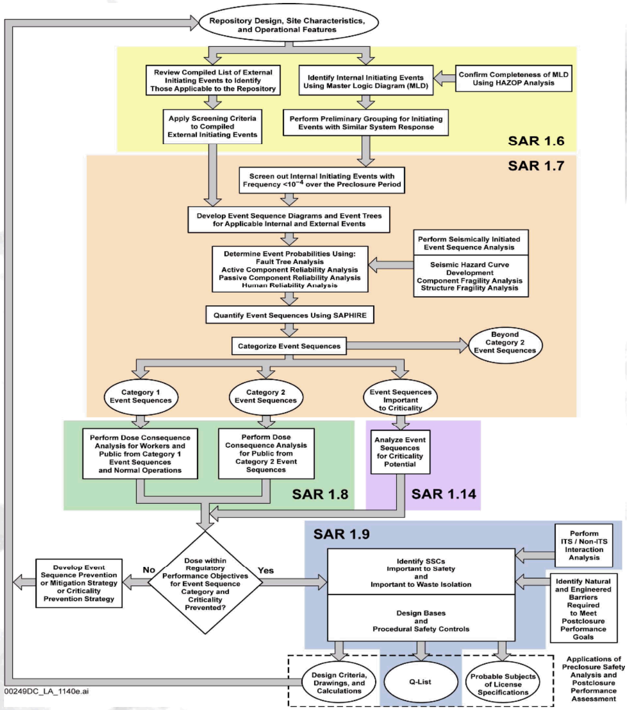
Overview of YM PCSA (2/4)

Some Differences Using 10 CFR 63 Compared to Previous, Deterministic Nuclear Power Plant Licensing:

- Category 1 (expect $\geq$ 1 over ~100 years) dose limits for public
  - Aggregated over normal operations and all Category 1 events*
  - Onsite dose: 100 mrem/yr (5 rem/yr for workers; see 10 CFR Part 20)
  - At site boundary: 15 mrem/yr* or 2 mrem/hr
  - Beyond site boundary: 100 mrem/yr or 2 mrem/hr
- Category 2 (expect < 1 but $\geq 10^{-4}$ over ~100 years)
  - Event sequences categorized <u>individually</u> on probability only, not risk*
  - At or beyond site boundary, for each sequence: 5 rem (workers or public*)
  - Onsite dose: Not regulated*
- No criticality allowable for Category 1 and 2 event sequences
- No consequence analysis needed for “Beyond Category 2“

Overview of YM PCSA (3/4)

- **Initiating Events**
  - Internal (process diagrams, hazard/operability)
  - External (experiential)
- **Event Sequences**
  - Screen on probability of initiating events
  - Logic diagrams, hazard analysis, fault trees
  - Simulate hazards, fragilities, etc.
  - Quantify event sequences (SAPHIRE)
  - Categorize (1, 2 and/or Important to Criticality)



- **Dose Consequence Analysis**
  - Normal + Category 1, aggregated (workers and public)
  - Category 2, individual events *p* > 10^{-4} in ~100 years (public)
- **Design Interface**
  - Identify items "Important to Safety" ("Q-List")
  - Develop as-low-as-reasonably achievable (ALARA) requirements for normal operations and Category 1
  - Develop design basis (iterate on design)

Overview of YM PCSA (4/4)

- **Preclosure Dose Summary for YM PCSA**
  - Aggregated for normal operations + Category 1 (expect ≥1 in ~100 years)
  - Each Category 2 event sequence analyzed individually

Category	Standard	Limits	Results
Public onsite	Normal operations + Category 1	100 mrem/yr TED [A]	78 mrem/yr
Public at site boundary	Normal operations + Category 1	15 mrem/yr TED	0.05 mrem/yr
Public beyond site boundary	Normal operations + Category 1	100 mrem/yr TED	0.11 mrem/yr
Radiation workers	Normal operations + Category 1	5 rem/yr TED	1.3 rem/yr
Public at site boundary	Any Category 2 event sequence	5 rem TED	0.01 rem
Public beyond site boundary	Any Category 2 event sequence	5 rem TED	0.03 rem

[A] TED = Total Effective Dose Equivalent (see Parts 20 and 63 for individual organs. Peak dose rate limits or results, and airborne emissions of radioactive material to the environment, are not shown.
Source: *Yucca Mountain Repository Safety Analysis Report,* DOE/RW 0573 Rev. 1. Table 1.8-36.

Current German Approach to Repository Operational Safety Analysis

- **Probabilistic Safety Analysis is Used in Germany to Identify/ Quantify Event Sequences**
  - Initiating events that cannot be controlled by design
  - Supplement deterministic safety assessments
  - Analyze high-consequence events
  - Sensitivity analysis; effectiveness of prevention/mitigation measures
- **PSA is Required for Repository Licensing to Supplement Deterministic Assessments, But Limits Have Not Been Defined**
- **Guidelines for Implementing PSA in Nuclear Power Plant Operational Reviews Were Developed in 2005 (BfS)**
- **Similar PSA Provisions Specific to a HLW Repository Will Likely Be Incorporated After Codification of the Site Selection Decision (by 2031, per the Site Selection Act of July, 2013).**

Regulatory Vulnerablities

- **Larger Repositories**
  - Factor of 2 to 3 range in waste inventory is possible
- **Longer-Operating Repositories**
  - 50 years operation vs. → 150 years
- **More Waste Packages**
  - YM (~11,000) vs. all U.S. SNF (up to 90,000)
- **Completeness of Initiating Events/Sequences**
- **Feedback to Design & Operations**
- **Methodological**
  - Disaggregation
  - Representational Accuracy

Disaggregation Dilemma Caused by Probabilistic Approach (10 CFR 63)

- Level of Aggregation (resolution) of Initiating and Pivotal Events Represented in a Sequence Can Determine Categorization Probability, esp. Internal Events
- More Aggregation → Higher Probability Event Sequence
- More Resolution (less aggregation) → Lower Probabilities → More Analysis/Licensing Effort
- Example: Impact and Breach of Canister
  - Should a single event sequence include all drops of all types of canisters from all possible sources in all facilities?
- Important for Risk Management (feedback into design & operations):
  - Hardware reliability requirements
  - Operations/procedures

Representational Accuracy

- Criterion for level of aggregation is representational accuracy
- Separation into different event sequences warranted because of variations of:
  - Facility configuration and operations (leading to different challenges, e.g. lift heights, number of lifts, residence time)
  - Equipment (although some equipment is similar across facilities,the complement of equipment is different for each facility)
  - Waste forms and containers (variation in robustness over different casks and canisters and variation in source terms because of different fuel/form of fuel)
- Disaggregation should represent different waste processing functions, waste forms, containers and facilities
  - For example: receipt, preparation, transfer, welding, load-out, transport, and emplacement

Summary and Outlook

- Deterministic vs. Probabilistic, in Transition (finding balance)
- Accumulating Experience with Nuclear Safety Analyses
- Periodic Updates for Operating Facilities
- Regulatory Developments are Iminent in Germany & the U.S.
  - Siting process, conceptual design and suitability determination
  - Re-promulgation of generic repository regulations
- New Systems Important to Nuclear Safety, and Supporting Analyses
  - Conveyances, packaging, etc.
- International Cooperation is Vital to Confidence Building
  - Events/sequences
  - Feedback to design & effective operations
  - Methodology

BACKUP SLIDES

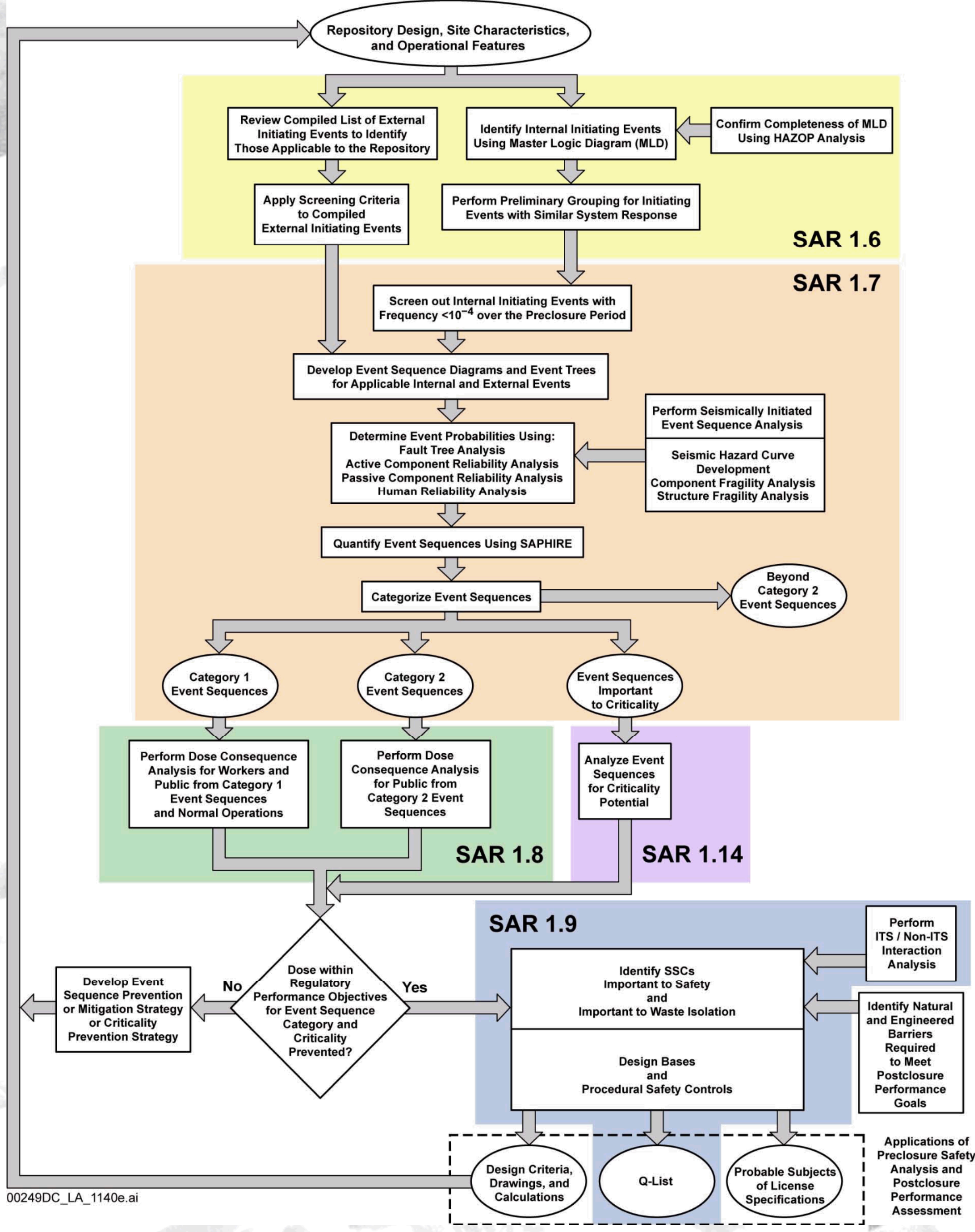
Concept of an Event Sequence

Initiating Event → "Pivotal" Events → End State

A perturbation from normal operation that might, with other events, lead to a dose consequence

Represents system, facility, human response to the initiating event

Consequence of interest: radionuclide release, direct exposure, criticality



Internal & External Initiating Events

Event Sequences and Hazard/Fragility Analysis

Overview of YM PCSA (2/6)

Dose Consequence & Criticality

Important-to-Safety
Important-to-Waste-Isolation
Design Bases

Overview of YM PCSA

YM Bounding Category-2 Event Sequences

Event #	Waste Form or Canister	End State
2-01	LLW Facility inventory	Seismic event → LLWF collapse and failed HEPA filters
2-02	5 HLW canisters	Breach of sealed HLW in a sealed transport cask
2-03	5 HLW canisters	Breach of sealed HLW in an unsealed waste package
2-04	2 HLW canisters	Breach of sealed HLW during xfer (one drops on another)
2-05	4 PWR or 9 BWR assemblies	Breach of bare CSNF in a sealed truck transport cask in air
2-06	4 PWR or 9 BWR assemblies	Breach of bare CSNF in a sealed truck transport cask in pool
2-07	36 PWR or 74 BWR assemblies	Breach of a sealed DPC in air
2-08	36 PWR or 74 BWR assemblies	Breach of a sealed DPC in pool
2-09	21 PWR or 44 BWR assemblies	Breach of a sealed TAD canister in air
2-10	21 PWR or 44 BWR assemblies	Breach of a sealed TAD canister in pool
2-11	2 PWR or 2 BWR assemblies	Breach of bare CSNF in pool (one drops onto another)
2-12	1 PWR or 1 BWR assembly	Breach of uncanistered CSNF in pool
2-13	Combustible LLW	Fire involving LLWF inventory
2-14	4 PWR or 9 BWR assemblies	Breach of a sealed bare fuel transport cask due to fire

TAD = transport-aging-disposal canister; DPC = storage-transport canister; CSNF = commercial SNF
Source: *Yucca Mountain Repository Safety Analysis Report,* DOE/RW 0573 Rev. 1. Table 1.8-26.

Overview of YM PCSA

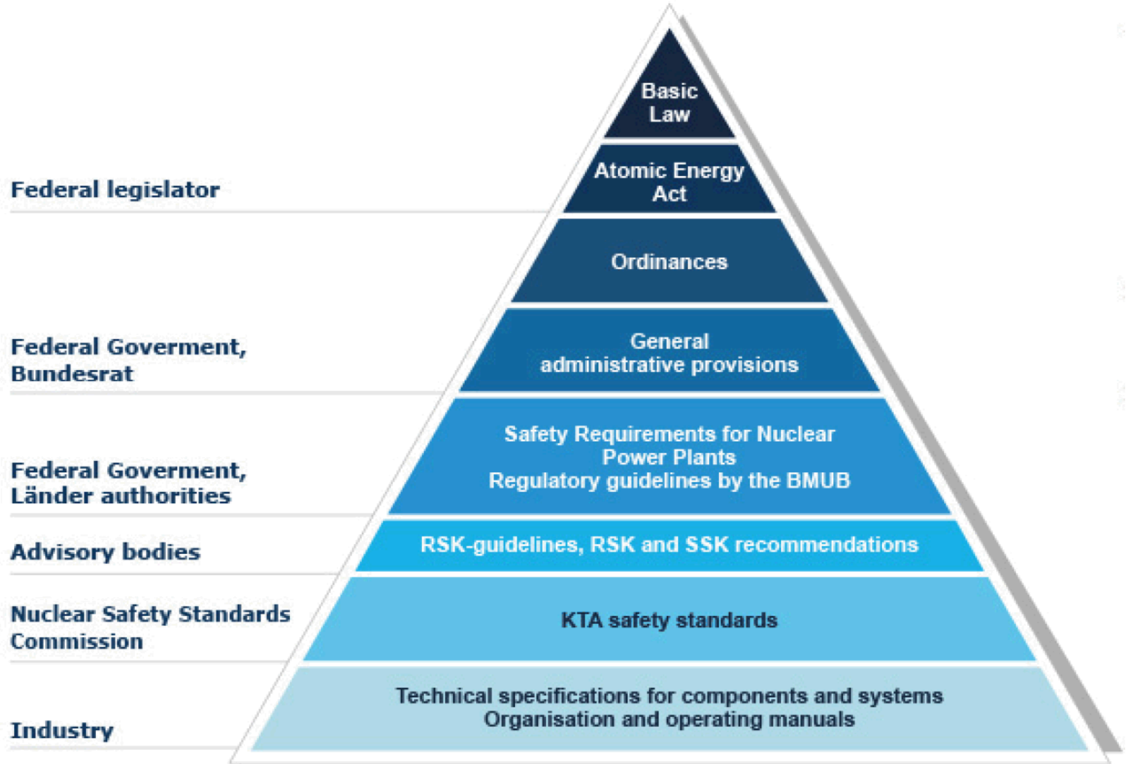
Potential Onsite Public Dose from Normal Operations + Category 1 Event Sequences (aggregated)

Area #	Onsite Location	Direct Radiation TED [A] (mrem/yr)	Airborne Release TED [A] (mrem/yr)	Total (mrem/yr)
Construction Locations				
17P	Aging Pad 17P	10.0	0.28	10.0
200	Receipt Facility	0.5	0.25	0.7
070	Canister Receipt and Closure Facility 2	1.5	0.21	1.7
080	Canister Receipt and Closure Facility 3	1.8	0.20	2.0
620	Administration Facility	0.1	0.11	0.2
71A	Craft Shop	0.1	0.13	0.2
30C	North Perimeter Security Station	9.7	0.08	9.8
Other Onsite Public Areas				
220	Heavy Equipment Maintenance Facility	1.5	0.16	1.7
240	Central Control Center Facility	7.0	0.12	7.1
230	Warehouse and Non-Nuclear Receipt Facility	17.0	0.11	17.0
25A	Utilities Facility	0.5	0.10	0.6
30A	Central Security Station	0.1	0.11	0.2
27A	Switchyard	36.0	0.18	36.0
780	Lower Muck Yard	78.0 [B]	0.09	78.0 [B]

[A] TED = Total Effective Dose Equivalent, rounded. [B] Exposure to waste transport railcar and truck buffer areas.
Source: *Yucca Mountain Repository Safety Analysis Report,* DOE/RW 0573 Rev. 1. Table 1.8-28.

Current German Approach to Repository Operational Safety Analysis: Statutes, Regulations & Guidance

- **Mining Law**
- **Atomic Energy Act (2013)**
  - Radiation Protection Ordinance (BfS, 2012)
  - Safety Requirements Governing the Final Disposal of Heat Generating Radioactive Waste (BMU, 2010)
- **Additional Requirements and Guidance:**
  - Site Selection Act (2013)
  - Guide to Probabilistic Safety Analysis for Nuclear Power Plants (BfS, 2005)
  - Verständnis der Sicherheitsphilosophie (RSK, 2013)



Regulatory Pyramid - Germany
http://www.bmub.bund.de/en/topics/nuclear-safety-radiological-protection/nuclear-safety/legal-provisions-technical-rules/

Current German Approach to Repository Operational Safety Analysis: Safety Levels and Associated Dose Limits

- ***Safety Requirements Governing the Final Disposal of Heat Generating Radioactive Waste*** **promulgated in 2010 (BMU) Requires Consideration of 4 Safety Levels:**
  - **Level 1: Normal operation (*Radiation Protection Ordinance*)**
  - **Level 2: Anomalous operation**

< 1 mSv/yr (total); 0.2 mSv/yr (effective)	**Public (§ 46-47)**
< 20 mSv/yr + <400 mSv/lifetime	**Workers (§ 55-56)**

  - **Level 3: Design Basis Accidents (generally internal events; cannot be excluded on low probability)**

< 50 mSv worst case accident	**Both (§ 49)**

  - **Level 4: Beyond Design Basis Accidents (generally external events)**

    No threshold identified
  - **Additional: Very low-probability, catastrophic accidents including criticality accidents**

Current German Approach to Repository Operational Safety Analysis: Probability Ranges for Safety Levels

- **Reactor Safety Commisison (RSK) *Verständnis der Sicherheitsphilosophie* (December, 2013)**
- **Recommended Probability Ranges for Safety Levels**
  - **Normal Operation (Level 1): Expected**
  - **Anomalous Operation (Level 2): > 10^{-2}/yr**
  - **Design Basis Accidents (Level 3): > 10^{-5}/yr and < 10^{-2}/yr**
  - **Beyond Design Basis Accidents/Events (Level 4): < 10^{-5}/yr**
- **Lower limit of design basis event probability may be extended (e.g., to 10^{-7}/yr) for certain applications**

Overview of VSG Assessment
Probabilistic Operational Safety Analysis

- Focus on Site Suitability (Bollingerfehr et al. 2013)
- Compilation of Significant Events
- Limited Probabilistic Safety Assessment:
  - Ventilation failure
  - Power supply system failure
  - Rock mechanical impacts
  - Inflow of brine and natural gases (H_2, CH_4)
  - Fire in facilities
  - Derailment of a loaded waste package transport
- Prevention/Mitigation Strategies Available for: Ventilation, Power Supply, Fire, Derailment, and Rock Mechanical Impacts
- Brine and Gas Inflows Must Be Assessed
- Demonstration Tests and Preliminary Analysis of Other Events