SAND2013-9979C

QRA Tools Workshop
Washington, DC
June 11-12, 2013

Development of Risk-Informed Approach to Hydrogen Safety

Jeffrey LaChance[1] and Andrei V. Tchouvelev[2]

[1]Distinguished Member of Technical Staff, SNL

[2]President, AVT and HySafe

Andrei

Jeff

Objectives of Hydrogen Risk Assessment Activities

- Understand the risk associated with hydrogen facilities
- Provide a safe infrastructure for the use of hydrogen through risk management
- Provide risk-informed basis for development of uniform model codes and standards

We can't measure risk – we have to evaluate it using models:

- Models do not always address all contributors and failure mechanisms
- Data is often sparse
- Uncertainties can be large

Therefore, risk should be used in conjunction with other information when making decisions! This is called RISK-INFORMED APPROACH.

History of Risk-Informed Approach

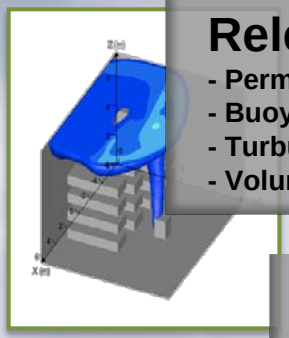
- **Risk-informed approach originated in nuclear industry:**
  - ✓ **Terms like RIDM (risk-informed decision making) and IRIDM (integrated risk-informed decision making) were introduced in the late 1990-s.**
- **NRC SECY-98-0144 definition for RIDM reads:**
  - ✓ **A "risk-informed" approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to health and safety.**
- **Today NRC defines *risk-informed* as "… a decision-making approach that uses risk insights, engineering judgment, safety limits, and other factors …."**

History of Risk-Informed Applications to Hydrogen

- **Use of risk assessment for establishing H2 C&S mentioned at ICHS 2005 in joint paper by SNL and NREL** (Ohi, Moen, Keller, and Cox)
- **Risk-informed approach for NFPA codes endorsed by Fire Protection Research Foundation in 2007** ("Guidance Document for Incorporating Risk Concepts into NFPA Codes & Standards")
- **Risk-informed process for permitting hydrogen fueling stations outlined in paper at 2nd ICHS in 2007** (LaChance, Tchouvelev, and Ohi)
- **First risk-informed application established separation distances in NFPA 55 (2009)**

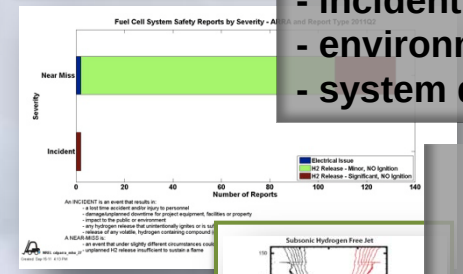
Risk-Informed Approach

Use of validated simulations, field data and expert input to determine risk through quantitative risk assessment.



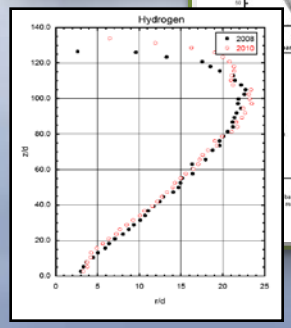
Release Probability
- Permeation
- Buoyant creeping flow
- Turbulent jet
- Volumetric rupture

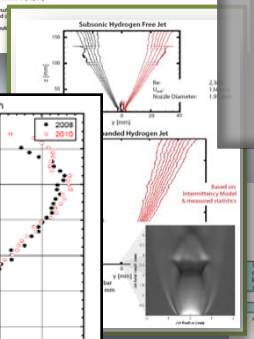
Informed Input
Code development groups, industry, regulators and code enforcers



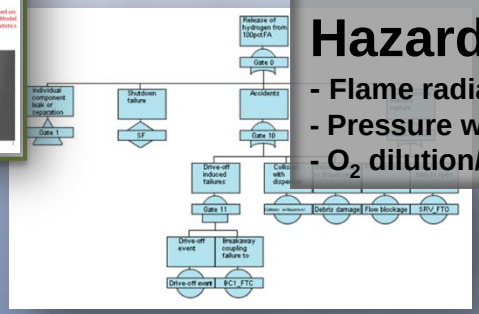
Field Data Input
- incident data,
- environmental/human factors,
- system design/mitigation

QRA





Ignition Probability
- Ignition mechanism
- Mixture ignitibility
- Ignition delay/location
- Sustained light-up



Hazard Probability
- Flame radiation
- Pressure wave (deflagration/detonation)
- O_2 dilution/depletion

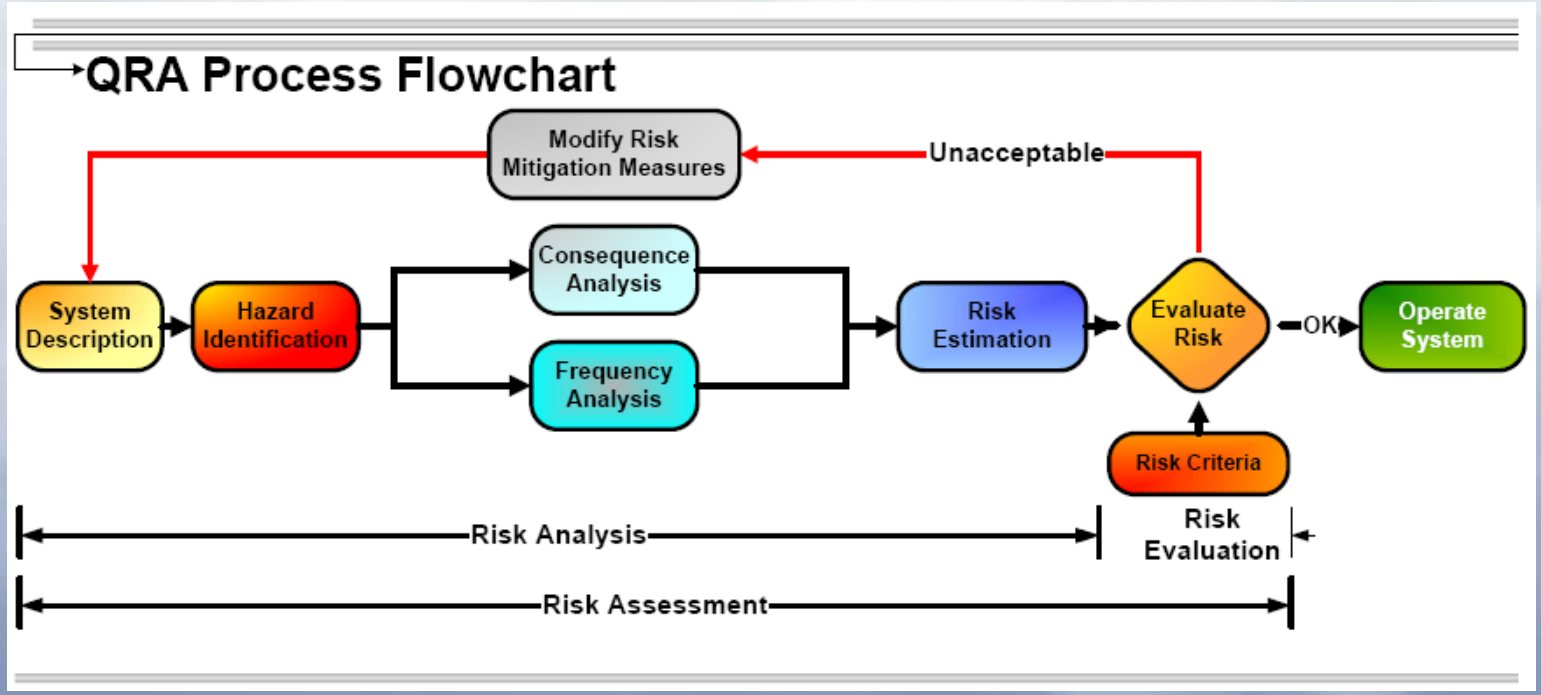
Harm Probability
- Burns
- Lung damage
- Shrapnel wounds
- Building collapse

Evidence-Based, Risk-Informed Process to Ensure Safety

- **Good science and engineering best practices should always be utilized to establish C&S requirements and to design and operate facilities**
- **Risk information can also be utilized (risk-informed process) when needed:**
  - ✓ **Results combined with other considerations to establish minimum code and standard requirements needed for an established risk level**
  - ✓ **Can include defense-in-depth and safety margins in design to address uncertainties**

Risk Management

- **Definition from ISO/IEC Guide 73: 2002:**
  - ✓ ***"coordinated activities to direct and control an organization with regard to risk. Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication"***
- **QRA process to improve safety:**



Essential Definitions

- **It starts with a hazard:**
  - ✓ No Hazard, No Risk
- **Definitions / explanations:**
  - ✓ Hazard – potential source of harm (ISO/IEC Guide 51)
  - ✓ Risk (unofficial) – probability of realization of a hazard
  - ✓ Risk (official) – combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51)
  - ✓ Risk (origin) – *risicare* (Italian) "to dare"
  - ✓ Risk is a *technical* construct – it can be calculated
  - ✓ Risk is a measure of *safety*, which is a *social* construct and cannot be calculated other than through risk
  - ✓ Safety is freedom from unacceptable risk (ISO/IEC Guide 51)
  - ✓ Risk criteria – terms of reference by which the significance of risk is assessed (ISO/IEC Guide 73)

"This is a potential hazard", says Thomas Jordan

Approach for Utilizing Risk Insights for Ensuring Safety of Hydrogen Facilities

- **Identification of the type and frequency of potential hydrogen releases**
- **Generate the experimental and analytical basis for evaluating the behavior and consequences of hydrogen releases**
- **Use of Quantitative Risk Assessment (QRA) to evaluate resulting risk, identify important risk drivers, and evaluate risk-reduction potential of accident prevention and mitigation features and actions**
- **Utilize risk insights to help establish code and standard requirements and improve design and operation of facilities**

What can go wrong?

What are the consequences?

Is the risk acceptable?

How can we reduce risk and, thus, increase safety?

Hazard Identification Methods

- Hazard Identification (HAZID)
- Hazard and Operability (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Failure Modes and Effects Criticality Analysis (FMECA)
- WHAT-IF Analysis

Hazard and Exposure

Courtesy of Thomas Jordan, KIT

Criticality Ranking

Risk Matrix

Severity	Frequency (/yr)				
	A (<0.001)	B (0.001-0.01)	C (0.01-0.1)	D (0.1-1.0)	E (>1.0)
1 (Catastrophic)	H	H	H	H	H
2 (Severe Loss)	M	H	H	H	H
3 (Major Damage)	M	M	H	H	H
4 (Damage)	L	L	M	M	H
5 (Minor Damage)	L	L	L	L	M

Risk Level	Description
High (H)	High risk, not acceptable. Further analysis should be performed to give a better estimate of the risk. If this analysis still shows unacceptable or medium risk redesign or other changes should be introduced to reduce the criticality.
Medium (M)	The risk may be acceptable but redesign or other changes should be considered if reasonably practical. Further analysis should be performed to give a better estimate of the risk. When assessing the need of remedial actions, the number of events of this risk level should be taken into consideration.
Low (L)	The risk is low and further risk reducing measures are not necessary.

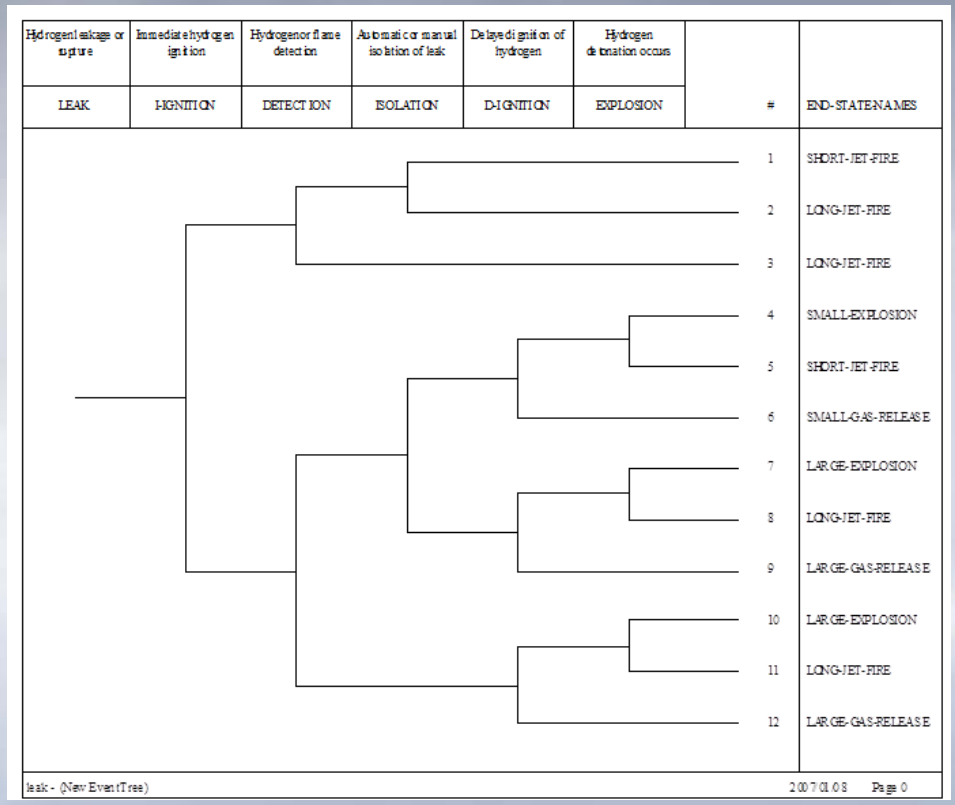
Developed by DNV as part of RRR – Rapid Risk Ranking methodology within EIHP2 project (1998-2003)

Hydrogen Hazards

- For hydrogen systems, hazards usually consist of hydrogen leakage or rupture events
  - ✓ Full spectrum of leak sizes needs to be analyzed (e.g., small, medium, large leak)
  - ✓ Can include events that result in system breach (e.g., transient that leads to over pressurization)
- Accidents that lead to hydrogen explosions (e.g. air ingress into hydrogen compressor)
- Others – any event that can lead to harm (e.g., chemical release from electrolyzer)

Event Tree Analysis

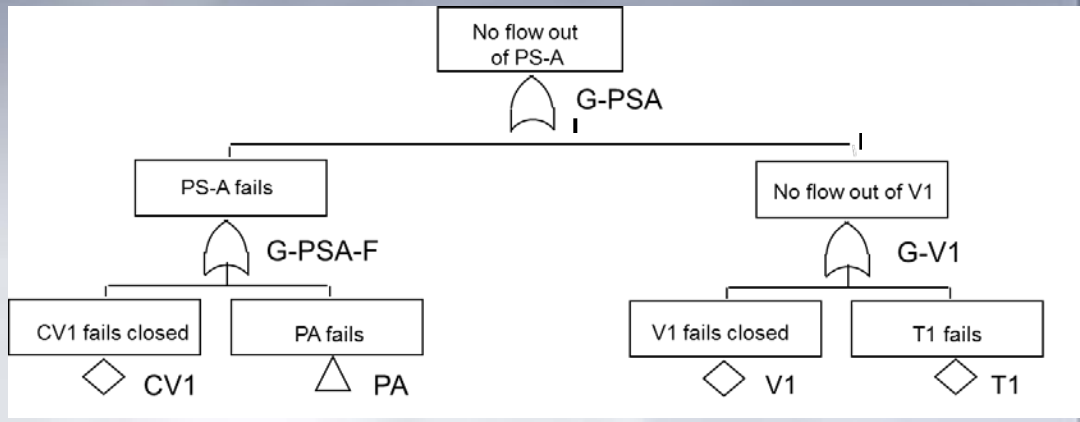
- Typically used to model the response to an accident initiator
- Features:
  - ✓ Identifies systems/functions required for mitigation
  - ✓ Identifies accident sequence progression
  - ✓ End-to-end traceability of accident sequences leading to undesired outcome
- Primary use
  - ✓ Identification of accident sequences which result in some outcome of interest (for hydrogen facilities, usually jet fires, flash fires or explosions)



Basis for evaluating accident sequence frequencies

Fault Tree Analysis

- Deductive analysis tool (event trees are inductive)
- Starts with undesired event definition
- Used to estimate system unreliability (can also be used to identify accident initiators)
- Identify ways in which a system can fail
- Explicitly models multiple failures



- **Models can be used to find:**
  - ✓ System "weaknesses"
  - ✓ System unreliability (failure probability)
  - ✓ Interrelationships between fault events

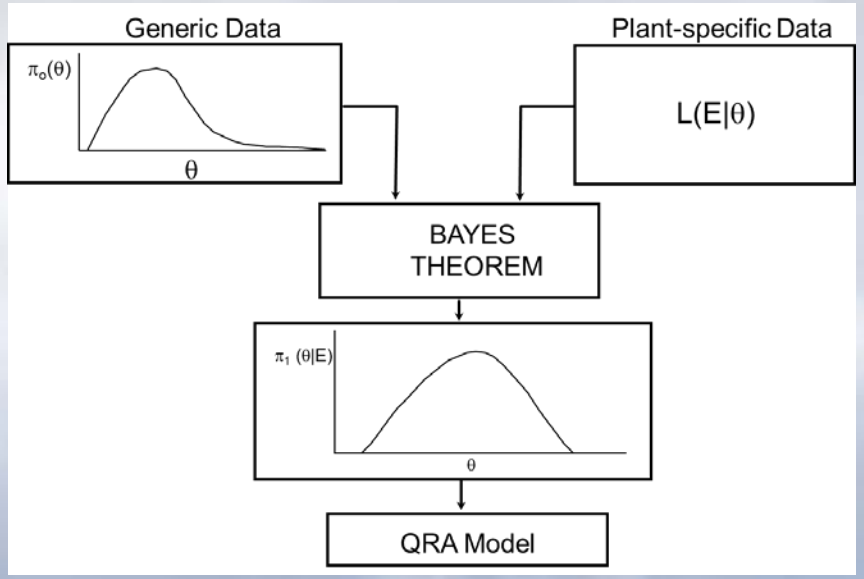
System unreliability used in accident sequence frequency evaluation

Data Requirements

Data needed to quantify accident sequence models:

- ❑ Initiating Event Frequencies
- ❑ Component Event Probabilities
  - ✓ Hardware
    - ❖ Component reliability (fail to start/run/operate/etc.)
    - ❖ Component unavailability (due to test or maintenance)
  - ✓ Common Cause Failures
  - ✓ Human Errors
- ✓ Conditional events (e.g., ignition)

Bayesian Analysis



Used to generate failure probabilities when data is sparse

Human Error is a Significant Contributor to Risk

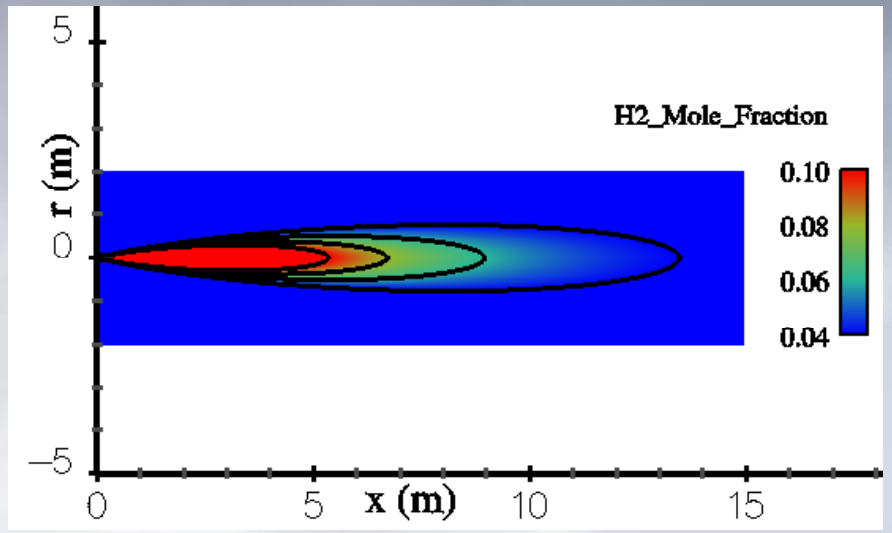
Accidents at Sea	90%
Chemical Industry	80-90%
Airline Industry	60-87%
Commercial Nuclear Industry	65%

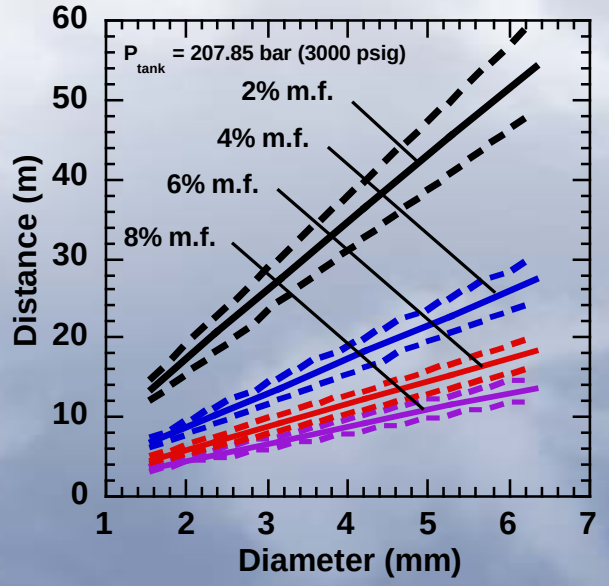
Regardless of the domain, there seems to be general agreement that 60-90% of all system failures could be attributed to erroneous human actions.

Human error probabilities can be identified through data analysis and/or by the performance of a Human Reliability Analysis

Consequence Evaluation

- **Required to determine consequences of accident scenarios:**
  - **Explosion overpressure**
  - **Radiation and convective heat flux**
  - **Cryogenic effects**
  - **Asphyxiation**



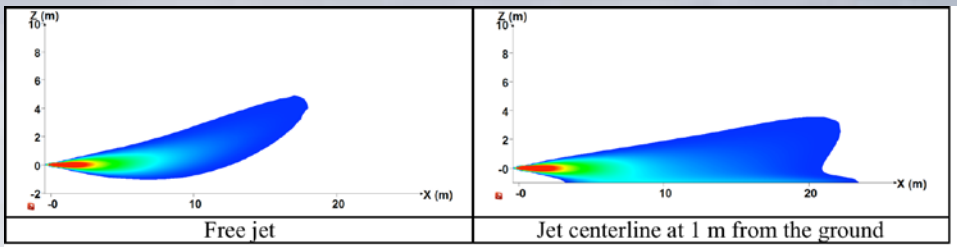


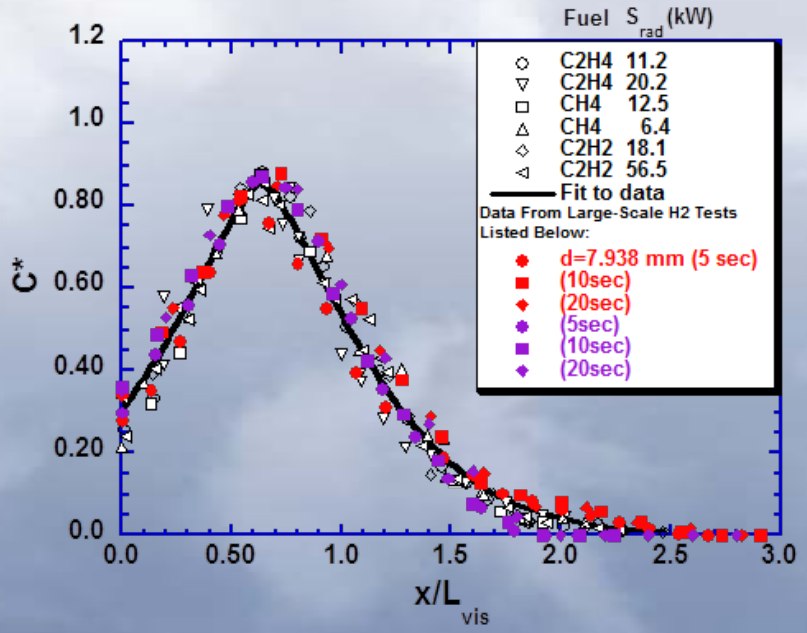
Analysis Process

- Characterising the source of the release of material or energy associated with the hazard being analysed
- Measuring (through experiments) or estimating (using models and correlations) the transport of the material and/or the propagation of the energy in the environment to a target of interest
- Identifying the effects of the propagation of the energy or material on the target of interest
- Quantifying the health, safety, environmental, or economic impacts on the target of interest

Consequence Modeling

- **Computational Fluid Dynamic (CFD) models**
  - ✓ CFD models are complex and require expert users
  - ✓ Accuracy of CFD simulation dependent upon number of factors including time step size, mesh size, choice of physical models, and boundary conditions
- **Simple 1D engineering models**
  - ✓ Quick and easy to use
  - ✓ Because they are based on correlation, they have limited applicability





Harm Criteria

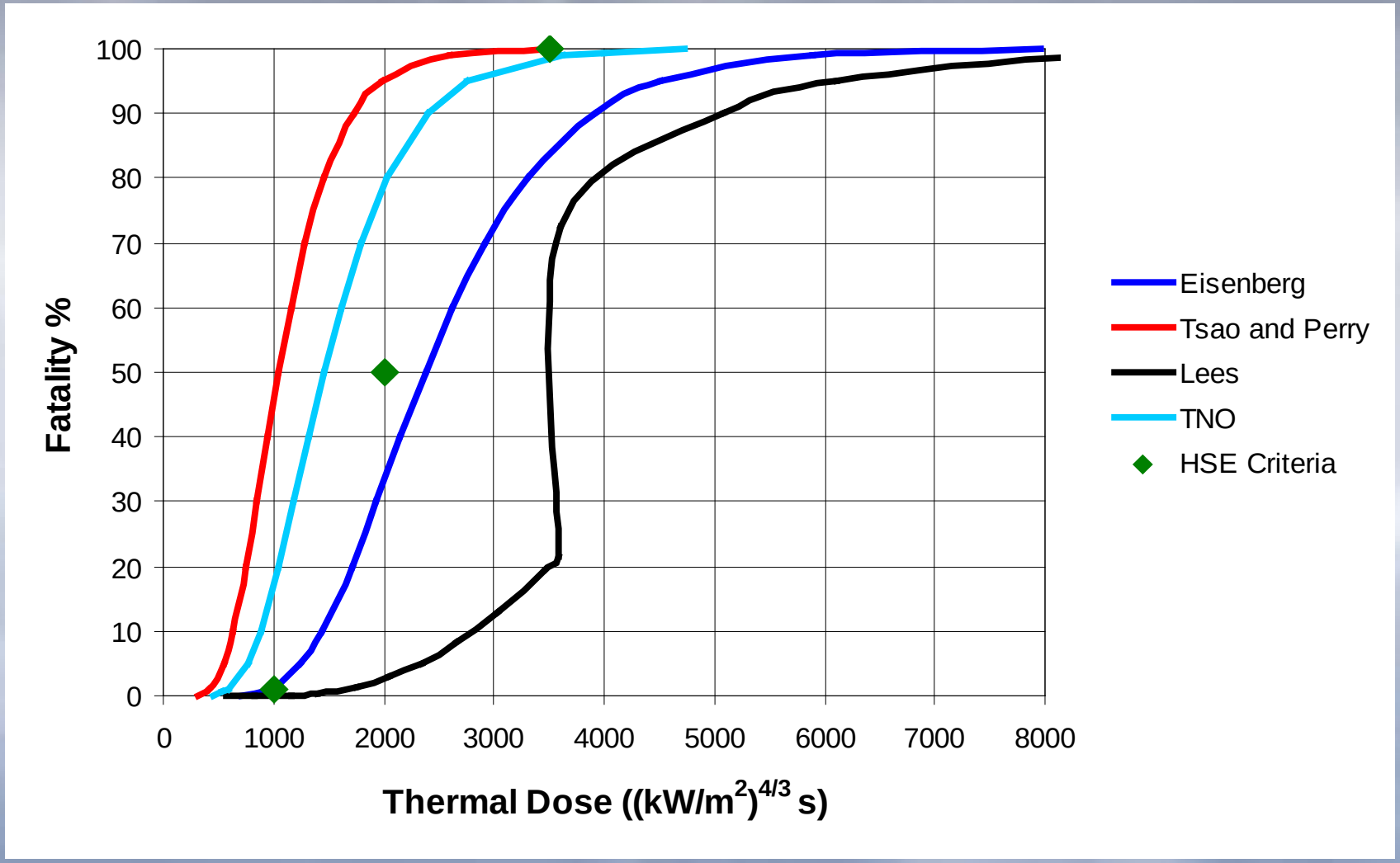
A harm criterion is used to translate the consequences of an accident, evaluated from deterministic models, to a probability of harm to people, structures, or components.

- **Harm criteria are required for full range of accidents modeled in QRA**
  - ✓ **Jet fires, flash fires, pool fires, vapor cloud explosions (VCEs), and Boiling Liquid Expanding Vapor Explosion (BLEVE)**
- **Accident consequences**
  - ✓ **Thermal effects (direct flame contact, high air temperatures, and radiation heat flux)**
  - ✓ **Overpressure effects (direct and indirect)**
  - ✓ **Others (asphyxiation, cryogenic)**
- **Primary interest is human harm criteria but also need to consider equipment and structures**
  - ✓ **For people, harm criteria can be expressed in terms of injury or fatalities**

Types of Harm Criteria

- **Single criteria (e.g., thermal radiation)**
  - ✓ Specified heat flux level and exposure time
  - ✓ Specified thermal dose ($I^{4/3}t$)
  - ✓ Use of a single criteria is generally used in deterministic evaluations and is not easily utilized in the probabilistic evaluations in QRAs
- **Continuous criteria**
  - ✓ Probit functions – translates hazard measure into probability of injury, fatality, or facility damage
  - ✓ Probit functions are particularly useful in QRA since they can provide harm probabilities for the range of accidents included in the risk assessment

Examples of Probit Functions



Risk Measures

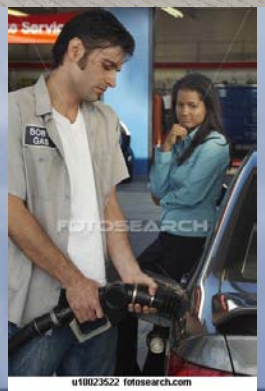
- **Human injury or fatality**
  - ✓ **Individual risk – probability that an average unprotected person, at a certain location, is killed or injured due to an accident**
  - ✓ **Societal risk – probability that multiple people within an area are killed or injured due to an accident (typically represented on an FN curve)**
- **Others**
  - ✓ **Economic loss – typically expressed in terms of loss value (lost income and replacement cost)**
  - ✓ **Environmental damage – can be expressed in terms of time required to recover damage to ecosystem**

Exposures or Parties

- **First party:**
  - ✓ Workers / employees – most trained and have most knowledge about hazards and related risks – ***highest acceptable risk***
- **Second party:**
  - ✓ Customers – knowingly take risk
  - ✓ Note: customer becomes 1st party when self-servicing
- **Third party:**
  - ✓ Public – may not be aware of hazards and risks, i.e. unknowingly takes risk – ***lowest acceptable risk***

Third Party – Public

Customer becomes 1st Party when self-refueling

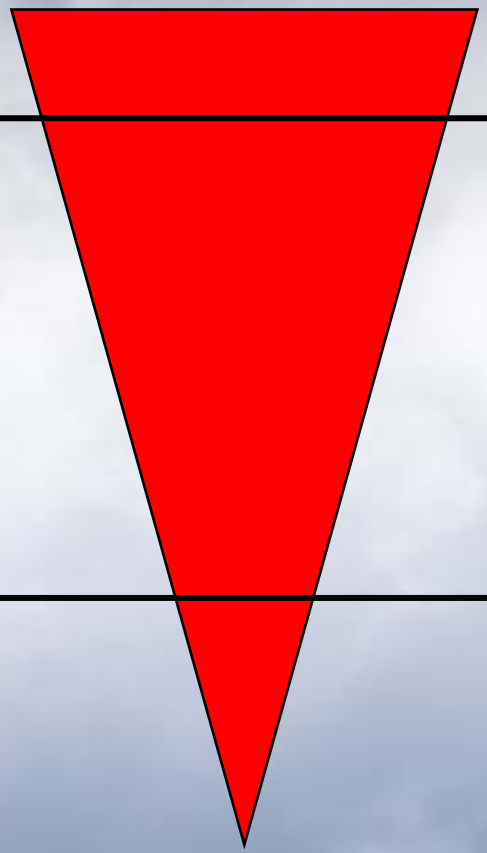


Attendant – 1st Party
Customer watching – 2nd Party

As Low As Reasonably Practicable (ALARP)

- There are no zero risk situations
- Managing risk to a reasonable level is achievable
- The ALARP principle is that the residual risk should be As Low As Reasonably Practicable – risk can be tolerated if additional risk reducing measures are feasible and their costs are not larger than the benefits
- Tolerable risk represents the level below which an investment will not be made to reduce risk
  - ✓ There is no minimum in some versions of ALARP - continuous improvement in safety using best available technology
  - ✓ Some versions have target levels
- The minimum risk level that must be obtained, regardless of cost is referred to as the intolerable risk

ALARP Concept – Individual Risk



Unacceptable Region

Risk must be reduced regardless of cost unless there are extraordinary circumstances

ALARP or Tolerability Region

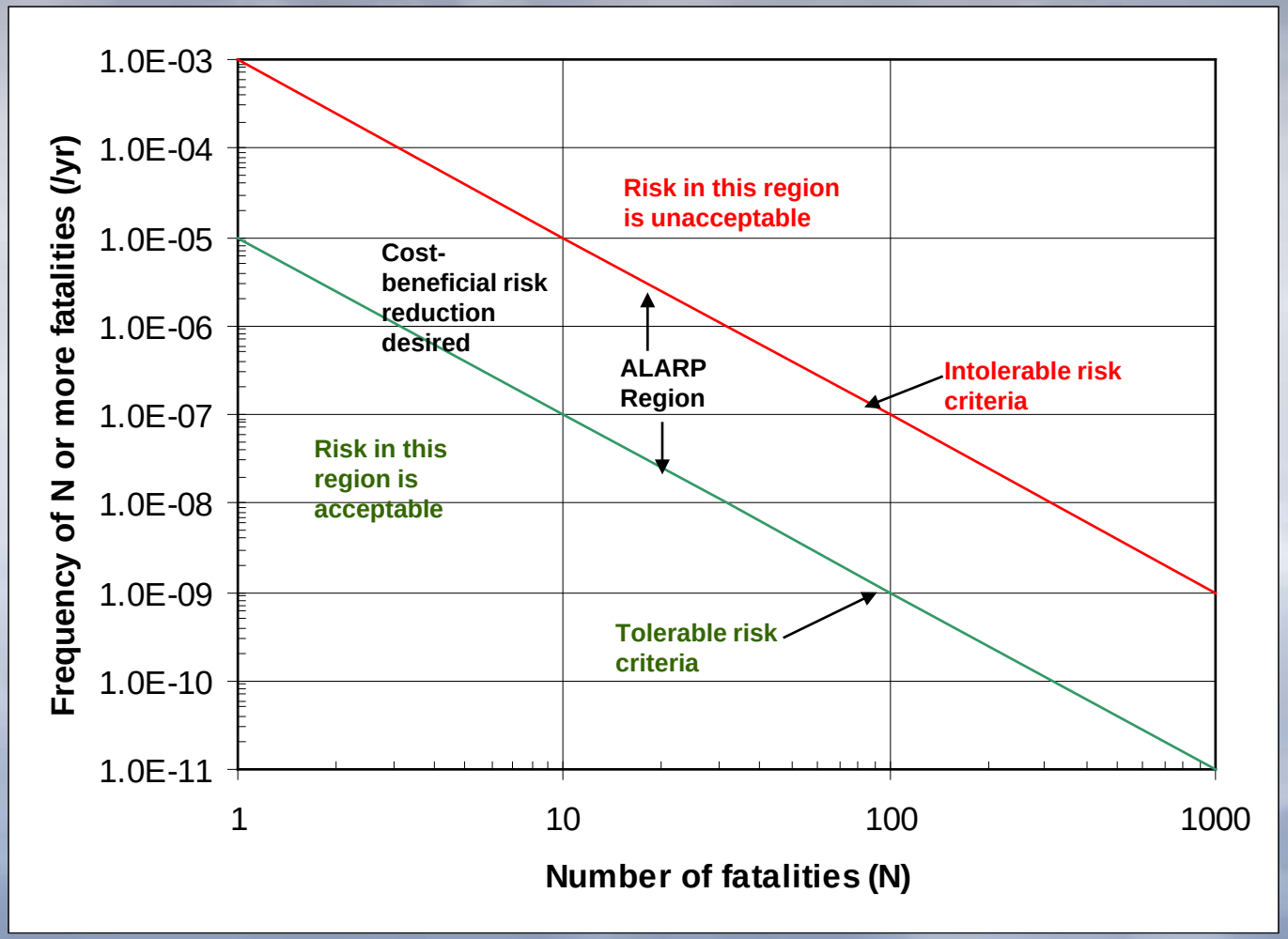
Risk tolerable if reduction cost exceeds improvement achieved

Acceptable Region

Necessary to maintain assurance that risk remains at this level and/or reduced further if reasonably practical

Negligible Risk

ALARP Concept – FN Curve



Suggested Guidance on Public Risk Criteria

- **Individual Risk – ALARP with following criteria:**
  - ✓ **Unacceptable risk level -1x10^{-5}/yr**
    - ❖ **Basis – Comparative risk to gasoline stations, 10% of risk to society from all other accidents, representative value used by most countries**
  - ✓ **Acceptable risk level – 1x10^{-7}/yr**
    - ❖ **Basis – Representative of most countries**
- **Societal Risk – Adopt EIHP ALARP FN curve**
  - ✓ **Basis – risk aversion factor of 2 and with a pivot point for 100 fatalities of 1 x10^{-5}/yr for unacceptable risk curve and 1x10^{-7}/yr for acceptable risk curve**
- **Customer and Worker risk – 1x10^{-4}/yr**
  - ✓ **Basis – Order of magnitude higher than the individual unacceptable risk value**

Summary
QRA Research Needs

- Need to address surface effects: does the increase in flammable extent and flame length increase risk?
- Need to develop methods and data for modeling human errors
- Need framework for addressing uncertainty in risk-informed decision making
- Need to address external hazards
- Defense-in-depth concepts should be incorporated in C&S
- QRA quality processes should be established

Q & A

THANK YOU FOR YOUR ATTENTION!