Delivering on the Promise: PRA, Real Decisions, and Real Events

Closing Plenary Speech

Ali Mosleh

Director, Center for Risk and Reliability

University of Maryland

PSAM11 - ESREL 2012

Helsinki, Finland

June 29, 2012

PRA is now a well-established discipline with growing applications in support of rational decision-making involving important technological and societal risks

- Has PRA delivered on its promise?
- How do we gage PRA performance?
- Are there disparities between what we get and what we think we are getting form PRA and its various derivatives?
- What should be our expectation, and how do we address potential gaps?

Characterizing PRA

- Common platform for technical exchanges on safety matters
  - Between regulators and industry
  - Among peers
  - Between designers and operators
  - …
- A rigorous and methodic way to steer design and operation of systems towards achieving quantitative and quantitate safety goals

A Numerical History of PRA

Nuclear Industry:

- Generic Estimate by WASH-1400
  - $5x10^{-5}$ to $5x10^{-4}$
- Experience (10,000 RY)
  - $5/10,000 = 5x10^{-4}$
- An Earlier attempt using inferior methodology:
  - 10^{-30}

A Numerical History of PRA

Space Shuttle Risk:

- Several PRA estimates:
  - 1/90 per mission
  - 1/112 per mission
- Experience
  - 2/134
- Earlier attempts using “rule of thumb”
  - 1/100,000

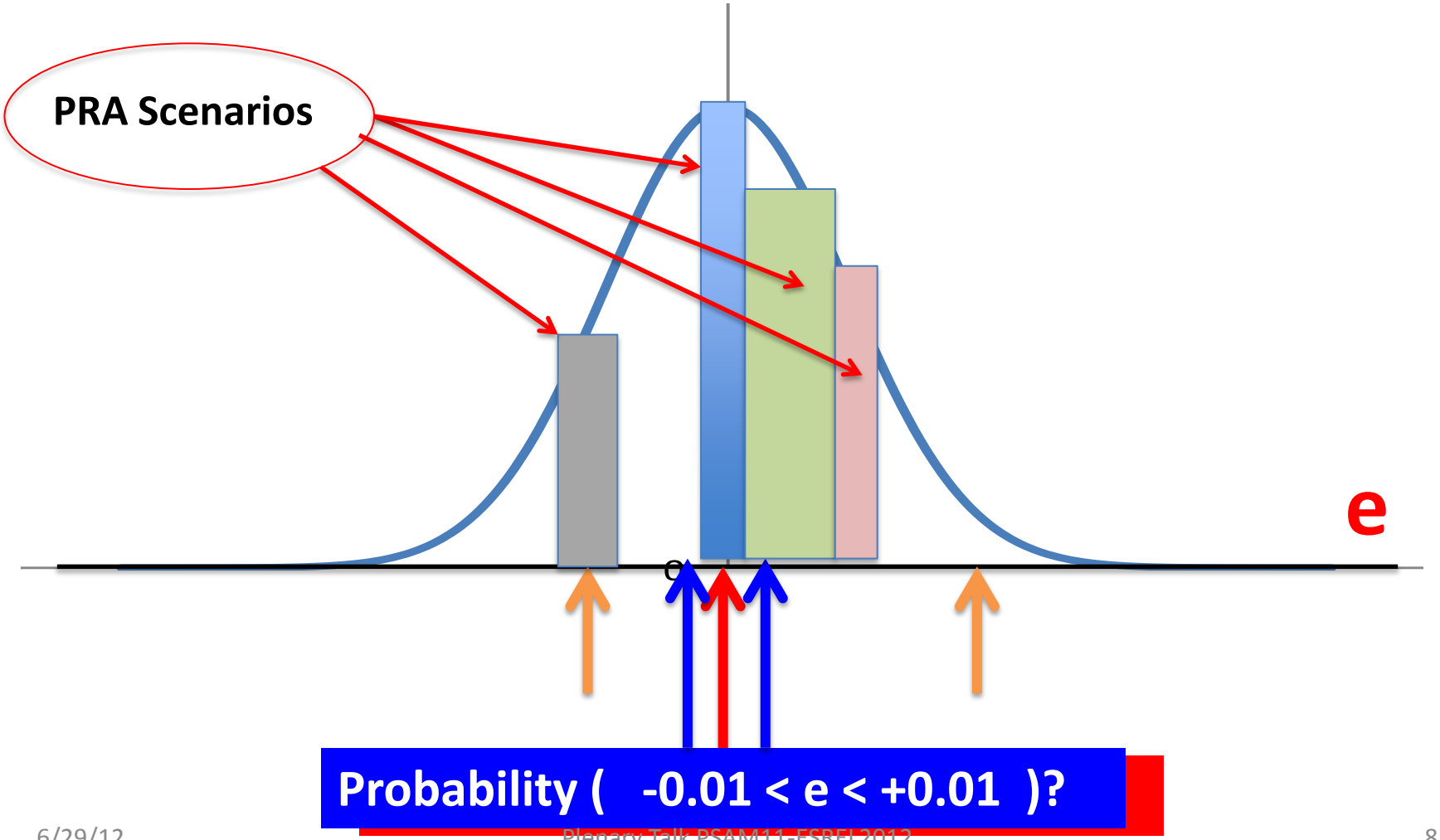
Risk Insights

- PRAs have successfully identified many vulnerabilities that were unknown, not adequately safeguarded against in the original designs, or simply viewed to be unimportant
  - WASH-1400 highlighting of importance of transients before TMI accident in 1979
  - Vulnerability to CCF, and more…
- Through ranking of risk contributors by probability and consequence, PRAs have provided a consistent basis for prioritization and implementation of many safety improvements and design decisions

Expectations

- When the reporters call after an accident:
  - "Did the PRA predict the event?"
  - "was the risk estimate correct?"
    - Meaning was it consistent with observation

Power of Binning "Reality"



Questions and Challenges

- So binning is very powerful, essential for risk analysis
- Challenges:
  - Identification (e.g., initiator/accident class)
    - Completeness
  - Proper bin size, level of resolution
    - Level of causality included
    - Fidelity of definition of basic events in FTs and ETs
    - Probability estimation
- These are the sources of all uncertainties

Questions and Challenges

- How we answer these questions is and should be a function of
  - Decision being supported by the PRA
  - State of Knowledge (level of understanding of the system and its human and physical environment
  - Availability of suitable methods and tools

What Decisions Does PRA Support?

- Use bottom-line system/site-specific risk values, in conjunction with other safety measures (e. g., defense-in depth) to meet safety goals
- Use qualitative and quantitative models (and insights they provide) to steer design and operational aspects of a plant (or system) towards higher levels of safety, in a rational and cost-effective manner
- Also used to improve operational availability and efficiency

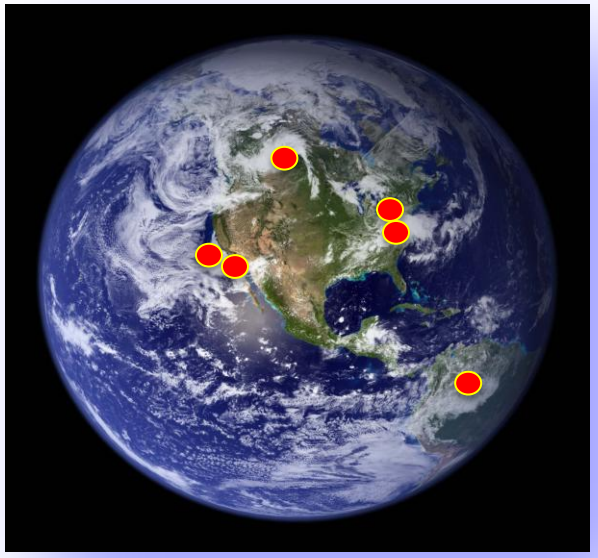
What Decisions Does PRA Support?

- More focused applications
  - Significance Determination Programs
  - Event Assessment
  - Precursor studies
  - Inspection strategies
- Design Trades (particularly important for space missions)

Bin Size Effect

Just getting the **big picture** is not sufficient for some of the PRA applications.

- **A high level, generic, global rate of accidents for a randomly selected NPP unit?**
  - $5/10{,}000 = 5 \times 10^{-4}$ events/yr
- **Generic multi-unit risk ?**
  - $\lambda_M = \beta \lambda_T$
  - $\beta = (3n_3/n_1+3n_3) = 3/5 = 0.6$
  - $\lambda_M = (0.6)\ (5 \times 10^{-4}) = 3 \times 10^{-4}$



Bin Size Effect

- Reality happens in details !
  - Robinson Event, March 28, 2010
- For every PRA application we need a level of detail that is suitable for that application

Robinson Event, March 28, 2010

- On March 28, 2010, a feeder cable failure to a 4kV non-vital bus caused an arc flash and fire. A subsequent failure of a bus-tie breaker to open and isolate the fault resulted in a loss of power to Reactor Coolant Pump (RCP) B and a subsequent reactor trip.
- Subsequent to the reactor trip, an automatic safety injection (SI) actuation occurred due to an uncontrolled reactor coolant system (RCS) cooldown.
- Plant response was complicated by equipment malfunctions and failure of the operating crew to diagnose plant conditions and properly control the plant.
- During plant restoration a relay was reset which re-initiated the electrical fault and caused a second fire.

Summary of Equipment/Operator Failures

- Equipment Failures
  - A feeder cable failure leads to an arc fault and initial fire causing the failure of the Unit Auxiliary Transformer and non-vital Bus 5.
  - Breaker 24 failed to open causing the loss of non-vital Bus 4.
  - Alternate charging valve CVC-310A opened due the Phase-A containment isolation and air leaks within the valve. This caused seal injection flow to be diverted away from the RCP seals.
  - The charging suction source failed to automatically switch-over from the VCT to the RWST due to instrumentation failure.
- Operator Deficiencies
  - Failed to control the RCS cooldown caused by the opening of the MSR drain valves.
  - Failed (initially) to recognize the closure of component cooling water (CCW) flow return valve from the RCPs.
  - Failed to recognize the RCP seal injection had become inadequate.
  - Failed (initially) to diagnose the failed charging suction switch-over resulting in a loss of charging flow.
  - NLO error caused the loss of Instrument Bus 3.
  - After the plant was stabilized, operators reinitiated the electrical fault causing a second fire because they failed to understand the current status of the electrical system and failed to followed procedures.

Important HRA Factors

- Simulator training did not match actual plant response.
- EOP procedure was deficient in regards to verifying RCP seal injection.
- Command and Control with the control room was poor.
  - Crew supervisors were distracted from oversight of the plant including the awareness of major plant parameters.
  - In addition, supervisors failed to properly manage the frequency and duration of crew updates/briefs during the early portion of the event leading to interruption in the implementation of emergency procedures and distraction the operators.
  - This negative factor affects all human actions (those that occurred or postulated).

Lessons

- Such event would never survive probability-based screening in a typical PRA
- Incredibly large number of seemingly independent contributors would push the probability of the sequence practically to zero
- Some important features of the event are not easily captured by typical PRA/HRA methods

Lessons

- PRA is basically a number-driven discipline
  - the P in PRA
- Probability ranking and screening of contributors is a key (and appealing) feature
  - But it can mask important vulnerabilities
- We need to find a way to “see” them
- We need to make sure that they do not point to new bins, undiscovered classes of vulnerability
  - The solution may be in utilizing new capabilities offered by information technology

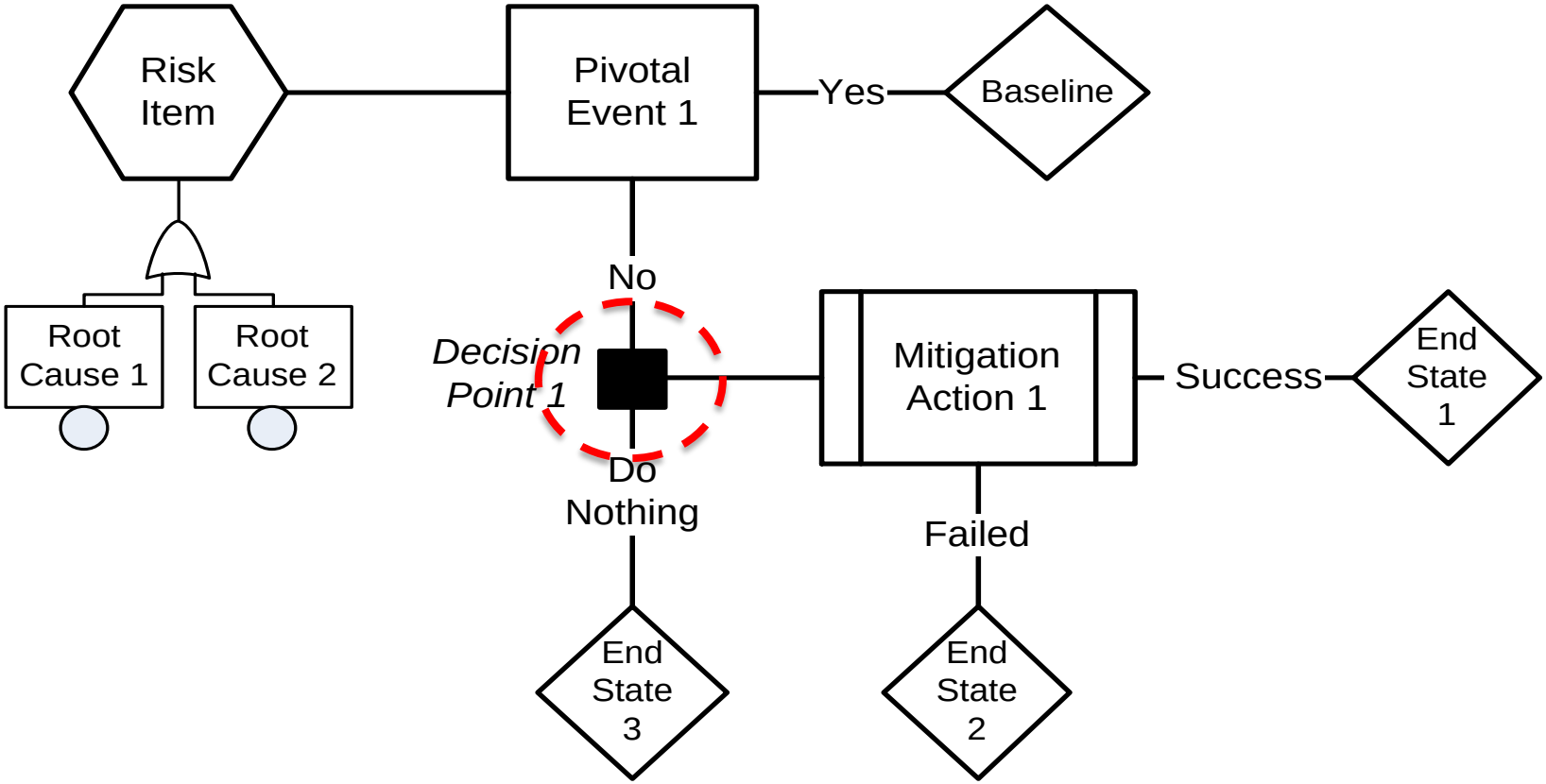
Early Screening

- Common practice, helpful but also dangerous
- In one case straight winds, not tornadoes or hurricanes, turned out to be a higher risk
  - Typical screening methods would have missed that
- So while early screening and scope reduction is a good thing, what body of information is needed to do it meaningfully?
- The question also relates to the issue of model uncertainty

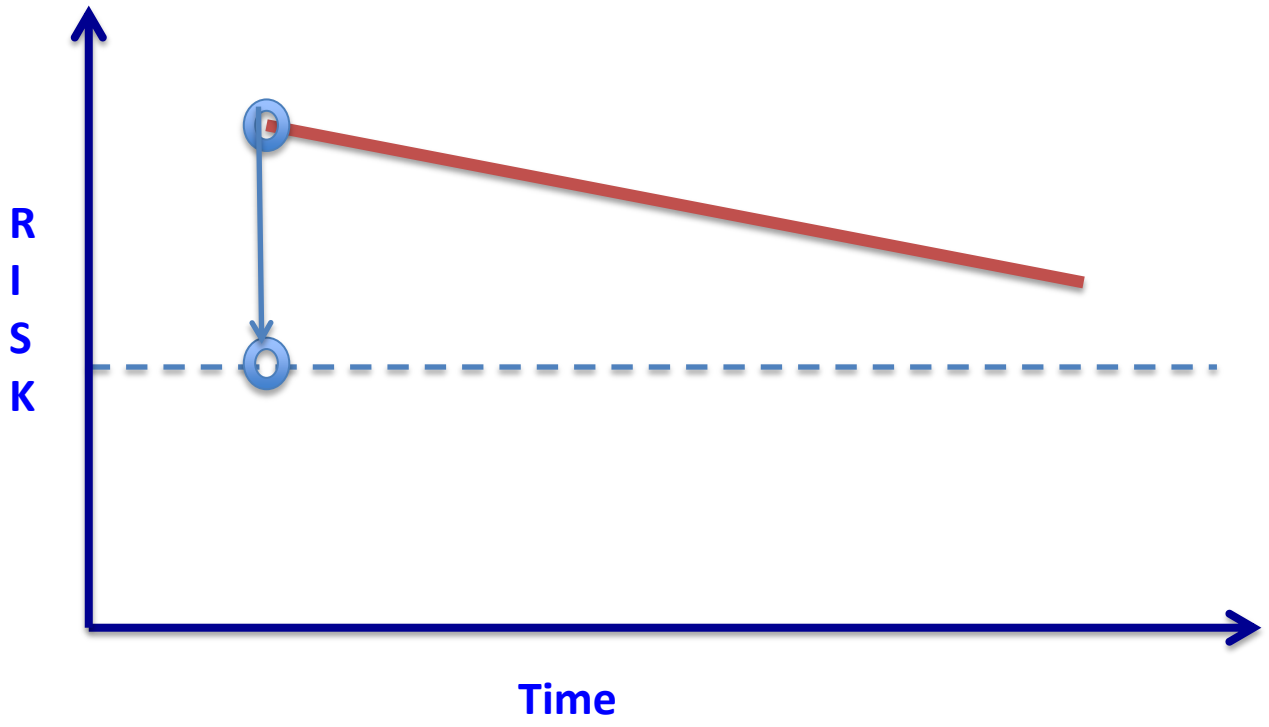
To Vent or Not To Vent …
That Was the Decision

- During major accidents “closed” systems quickly become open systems
- Causes and consequences often go beyond the physical and organizational boundaries
- For major accidents command and control and decision making changes, sometime chaotically
  - Fukushima --- prime mister’s agony: To Vent or Not To Vent …
  - FBP Gulf oil disaster
  - Fukushima---Operator interview with a reporter: “…choked with emotion when asked what was the toughest part of their job: "*You know it's our families we have left behind. I've really felt sorry for them. I want to apologize to them here and now,*" he said.”

Inserting Decision Points in the Model

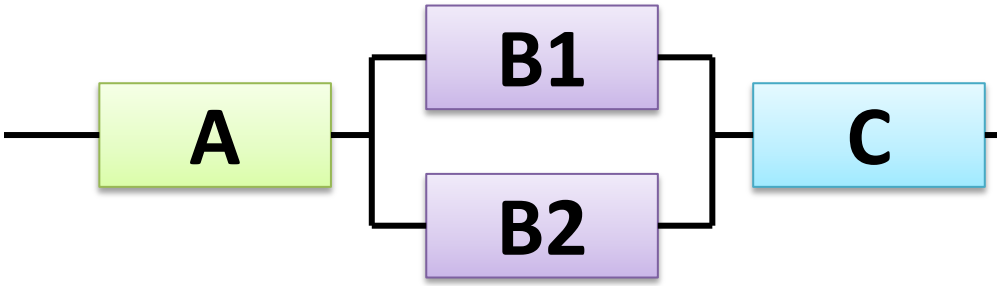


Numbers Faster Than Reality



Calculated vs Real

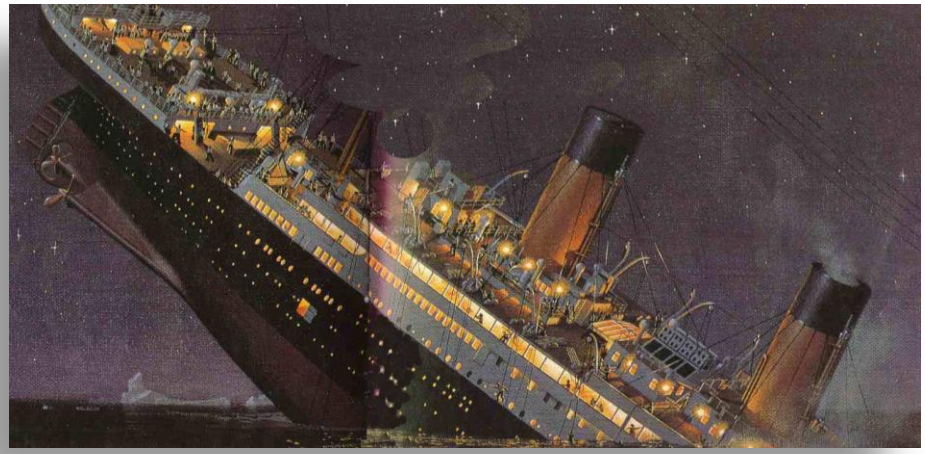
$$Q_S = Q_A + Q_B + Q_C$$



$$Q_S = Q_A + (Q_B)^2 + Q_C$$

$$Q_S = Q_A + [(1-\beta)(Q_B)]^2 + \beta\, Q_B + Q_C$$

Maritime Casualties/ Accident Rates

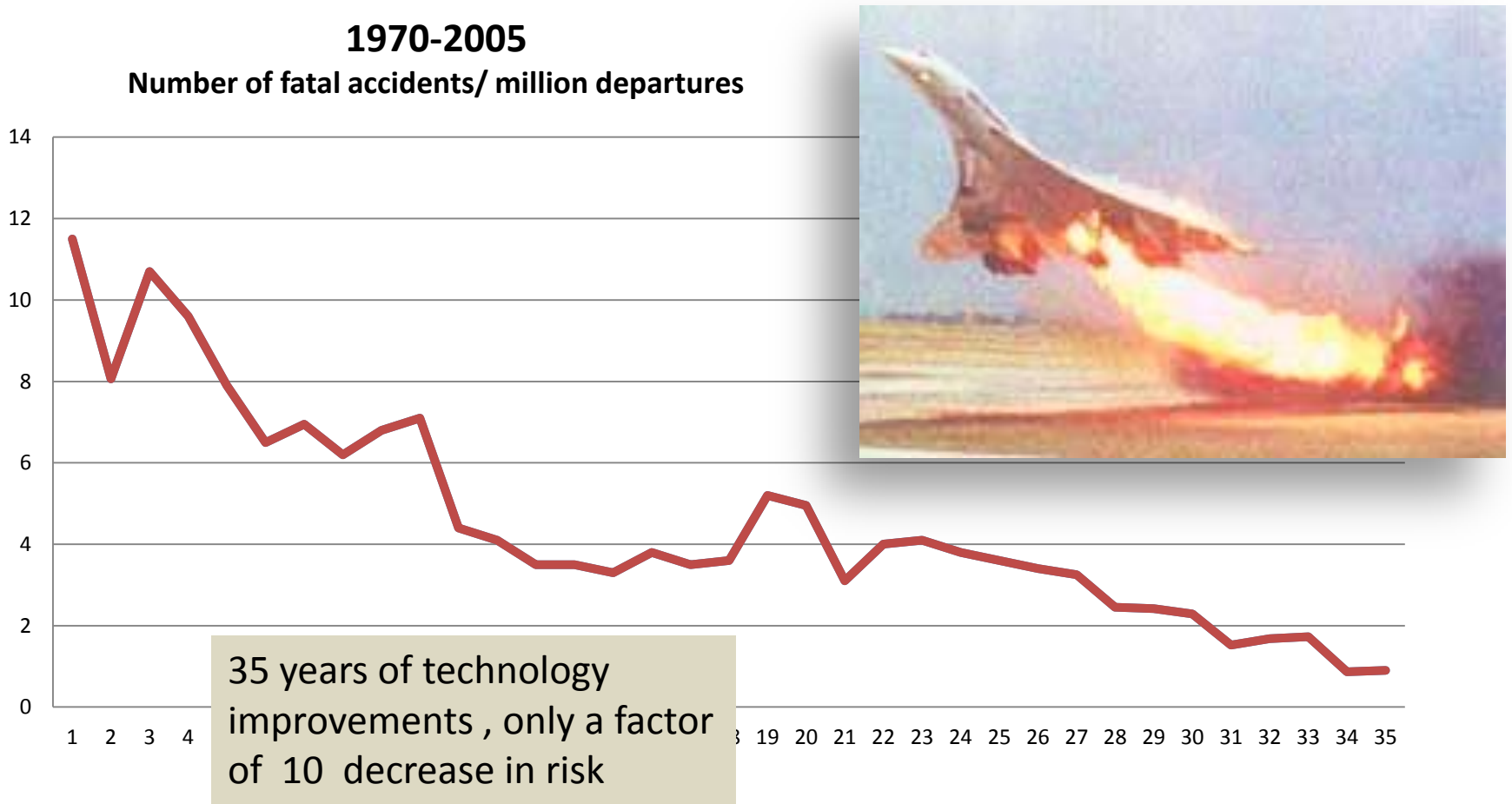


1912:
1/100

2012:
1/670

100 years of technology improvements , only a factor of 7 decrease in risk

Aviation Accident Rates



PRA Standards (ASME)

- Initially effective in improving quality of PRAs being done mostly through peer review process it required

- But as years went by, it became an impendent for advancement in the state of the art and practice
  - Meeting the standard has set a limit people aspired for
  - Does not cover LPSD, reluctance to expeditiously fill the void
  - Reluctance to change ----has become costly even for simple cases
- In hindsight push for harmonization via peer review and guidelines would have probably brought the same benefits without some of the adverse effects

A Few Suggestions

- Need to improve causal models for some applications (e.g., SDP)
- Should feed accident insights back into PRA methodology
  - One of the original objectives of precursor studies
- Better use of computer power
  - Extracting qualitative information from risk models
  - Unraveling complex interactions and dynamics through supplementary simulation
- Risk management should be also "consequence-informed"
  - Defense-in-depth is a systems implementation of this concept

A Bit of PRA History

- Fault Tree is now 50 years old
- July 1st is now declared as the birthday
  - Not knowing the exact date I used a uniform uncertainty distribution to arrive at July 1st.
  - Also because it is my birthday !

- THANK YOU !