
# A PSAM lunch time talk: Which way PRA?

June 24, 2014

Epstein & Grynblat

Lunch time is normally dedicated to... lunch, i.e. to get hopefully some good food and even more importantly, good wine. Nurturing minds and souls could be of some interest as well but ...

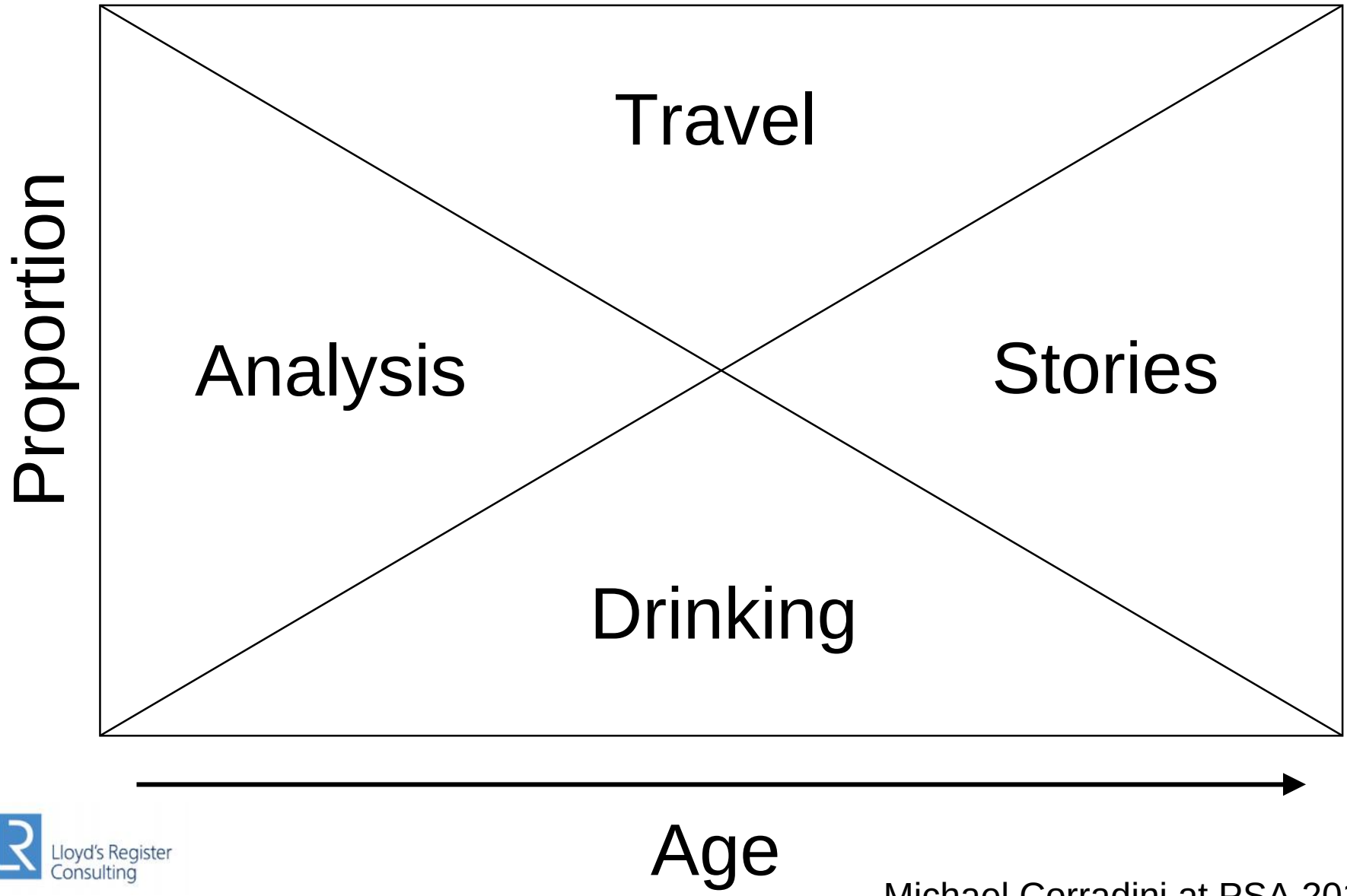
--- Antoine Rauzy, a gentleman of Paris

Lloyd's Register Consulting



Working together for a safer world

# Career Trajectory




Lloyd's Register Consulting

# She who must be obeyed.

# Woody's Career Trajectory

# What we asked:

March 11, 2011 was a wakeup call. The events of that day, and for several months afterwards, convinced many of us that to help society deal with disastrous events we might somehow have to change the way we do probabilistic risk assessment.

Impacts were not only to the Fukushima Daiichi Nuclear Power Station, but to oil and gas plants, public infrastructure, business continuity, supply chain, emergency preparedness and response, medical facilities, the understanding of extreme natural events, risk communication with the public … the 3.11 list seems endless.

How can we continue to make PRA relevant in the light of March, 11? What are your ideas and perhaps your solutions.

NOTE: We sent this to over 50 risk professionals.

Lloyd's Register Consulting

# Who responded:

Isao Kato, Tohoku Epco
Marco Cepin, Univ. of Ljubljana
Mohamed Hibti, EdF
Ali Mosleh, UCLA
Nathan Siu, US-NRC
Richard Cook, STH and KTH, Sweden
Roger Cooke, RFF
Sidney Dekker, Griffith University
Vincent Ho, MTR
Yannis Papazoglou, INTRP Greece
Jim Chapman, Scientech
Masaharu Kitamura, Univ, of Tohoku
David Tappin, BGS
Robert Geller, Univ. of Tokyo
Ola Backstrom, LRC
Curtis Smith, INL

Erik Hollnagel, Everywhere
Olivier Nusbaumer, KKL
Antoine Rauzy, ECP
B. John Garrick, Garrick Foundation
Dennis Bley, Buttonwood
Dave Johnson, ABS
Jerzy Grynblat, LRC
Anders Olsson, LRC
Michael Knochenhauer, LRC
Don Wakefield, ABS
Karl Fleming, Fleming Assoc.
George Apostolakis, US-NRC
Shunsuke Kondo, former Chairman, AECJ
Henrik Dubik, OKG
Ludivine Pascucci-Cahen, IRSN
Stefan Hirschberg, PSI
Peter Yanev, Yanev Assoc.

Lloyd's Register Consulting



NOTE: We included all opinions about PRA

# Insights (1)

Insights are more important than numbers. --- Chapman

I think finding ways to help decision makers deal with large amounts of complex, nuanced information (in the context of an analytical deliberative process) is necessary. --- Siu

Quantifying safety is actually quantifying the absence of safety. And safety is of course not the complement to the absence of safety, safety ≠ 1 - Pr(risk). --- Hollnagel

It is a mistake to focus only on what PSA can or cannot do. The question is: How do we manage hazards? --- Apostolakis

With external events (tsunami, earthquakes), there are lots of uncertainties in the inputs, and PRA will not eliminate those uncertainties. But the decision makers and the public want deterministic answers for inherently stochastic situations. Therein lies the main problem for good risk communication. --- Geller

It's puzzling to me why people refuse to understand what a risk informed (not based) approach to safety means. --- Apostolakis

Lloyd's Register Consulting

# Expert Opinion vs. Expert Evidence

| Formulation | Question | Form of answer |
|---|---|---|
| 1 | What is your best estimate for $\lambda$? | $\lambda_i$ |
| 2 | What is your state of confidence about the value of $\lambda$? | $p_i(\lambda)$ |
| 3 | What evidence and information do you have relevant to the value of $\lambda$? | $E_i$ |

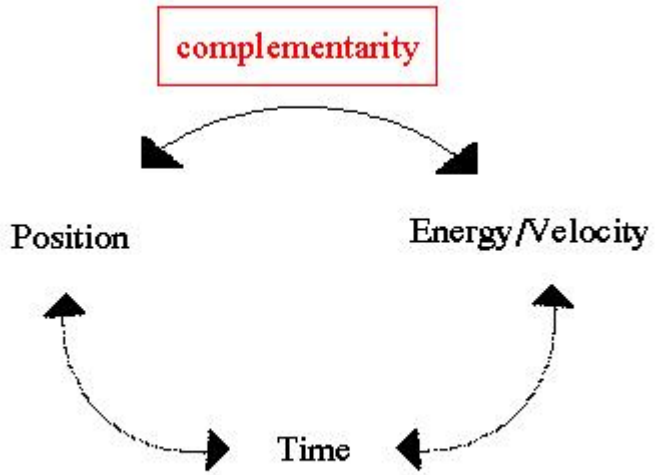
The questions of how to use expert opinion and of how to combine the opinions of different experts have generated much literature, and much debate, and there is little agreement on it even today. We are not going to answer these questions either. Rather, we are going to suggest that the way to address these issues is to bypass them by asking a different question. What makes experts 'expert', we believe, is not their opinions but their knowledge, experience, experiments, etc.; in short, their evidence. We suggest therefore that instead of asking the experts for their opinions, we ask them for their evidence.

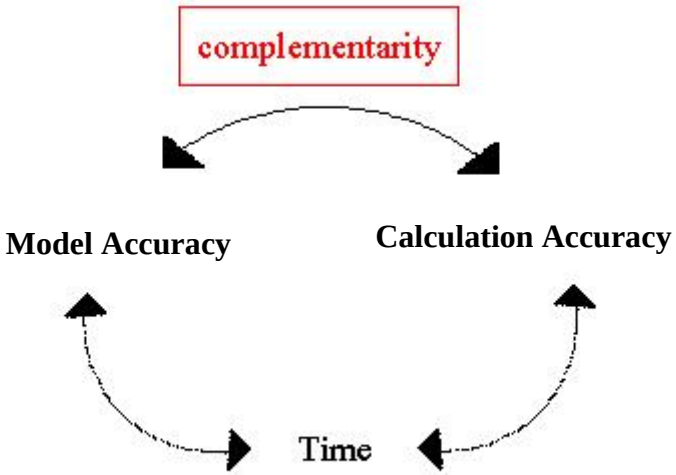
In the expert information approach, we do not ask the experts directly for their opinion about $\lambda$. Instead, we ask them what experience and information they have that are relevant to the value of $\lambda$. The PSA analyst, serving as facilitator, then leads the group in combining the different kinds of information and evidence into a consensus state-of-knowledge curve.

"The strengths and limitation of PSA: where we stand"
RE&SS, 1992
Bley, Kaplan, Johnson

Lloyd's Register Consulting

# The Cassis Uncertainty Principal



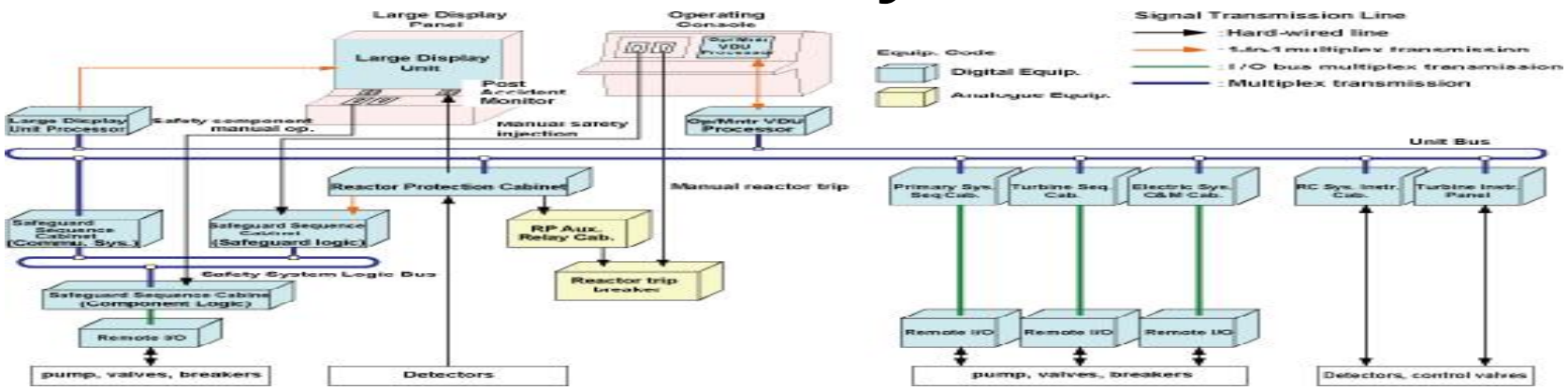

PSA calculations are provably difficult, i.e. they consume an exponential amount of resources w.r.t. the size/complexity of the model. To handle this computational complexity, tools perform approximations. The richer the model, (the more accurately it reflects the "reality"), the coarser the approximations. You cannot model a system with 100% accuracy and perform exact calculations at the same time.

There is kind of a quantum of accuracy somewhere, which is indeed relative to the amount of calculation means at hand, but those are by definition finite.

Rauzy, Epstein

Lloyd's Register Consulting

# Electrical Systems




It is important to consider that without detailed enough modeling of electrical systems, including power and I&C cabling, and aerial dependences, the PRA is of very limited value.

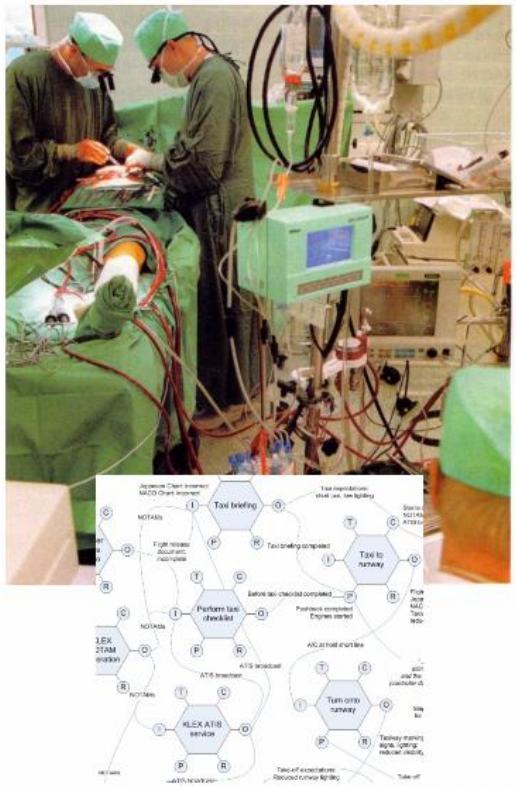
Aerial events, e.g. fire, floods and steam release, including drainage and blow-off systems are also important, especially in combination with modeling of electrical systems.

We need to represent degraded states of equipment…especially degraded electrical states…to adequately model the risk. --- Johnson

Dubik

Lloyd's Register Consulting

# Safety Version 2



Systems cannot be decomposed in a meaningful way (no natural elements or components)

System functions are not bimodal, but everyday performance is – and must be – variable.

Outcomes are determined by performance variability rather than by (human) failure probability. Performance variability is a source of success as well as of failure.

While some adverse outcomes can be attributed to failures and malfunctions, others are best understood as the result of coupled performance variability.

Risk and safety analyses should try to understand the nature of everyday performance variability and how this lead to both positive and adverse outcomes.



A new definition of safety will, however, not happen because of the efficiency-thoroughness trade-off that regulators, managers, etc like. It is so much easier to accept a numerical value than to understand what is really going on. You do, of course, get the insights by trying to understand what goes on (as a prerequisite for quantification). But unless numbers have meaning, they are useless and potentially dangerous.

Hollnagel

# Insights (2)

Politics or organizational dynamics decide the risks of concern and their acceptance level. It is very important for the PRA community to maintain its credibility. One of the key activities important for the PSAM community is to have closer ties with the standard development communities. The PSAM community may learn something through the communication. --- Kondo

We need to let utility managers understand that plant engineers must be heavily involved in PRA analysis, putting our expertise and concerns on the table. Our experiences at the plant will help produce superior PRA results leading to better AM planning. --- Kato

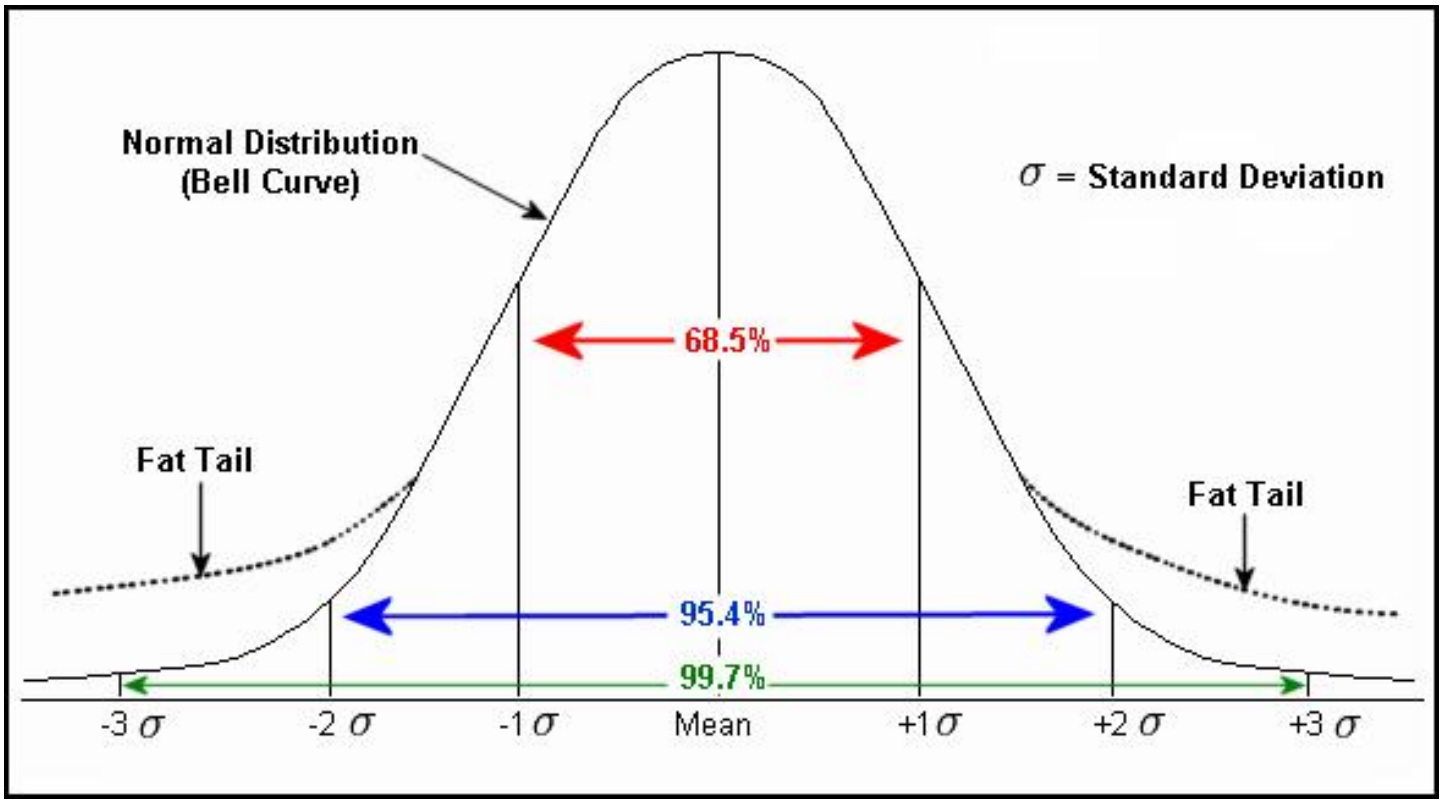
" Failure" of PRAs to "foresee" some accidents is due to lack of knowledge on the phenomenology or optimistic probability assessment. --- Papazoglou

Black swans: We must not go back to the "worst case analysis". Use of appropriate probability distributions for extreme consequences will take care of the "black swan" issue. --- Papazoglou

Full scope PSAs are still rather scarce. --- Hirschberg

Lloyd's Register Consulting

# Fat Tailed Distributions: Modeling consequences of unexpected events




A fat tail is a property of probability distributions exhibiting extremely large kurtosis particularly relative to the ubiquitous normal, or lognormal, which are examples of thin tail distributions. The term “fat tail” is a reference to the tendency of a distribution to have more observations in the tails than normal or lognormal distributions.

Cooke

Lloyd's Register Consulting

# Nuclear Refugees


The number of people displaced by nuclear accidents is a better measure of the severity of radiological consequences than the number of fatalities.

The distribution of nuclear refugees with respect to weather and release site is asymmetric and fat-tailed: unfavorable weather can lead to the contamination of large areas of land; large cities have in turn a higher chance of being contaminated.

Pascucci-Cahen

Health effects from being displaced must also be considered in our Level 3 calculations. --- Grynblat

Lloyd's Register Consulting

# Dealing with an accident

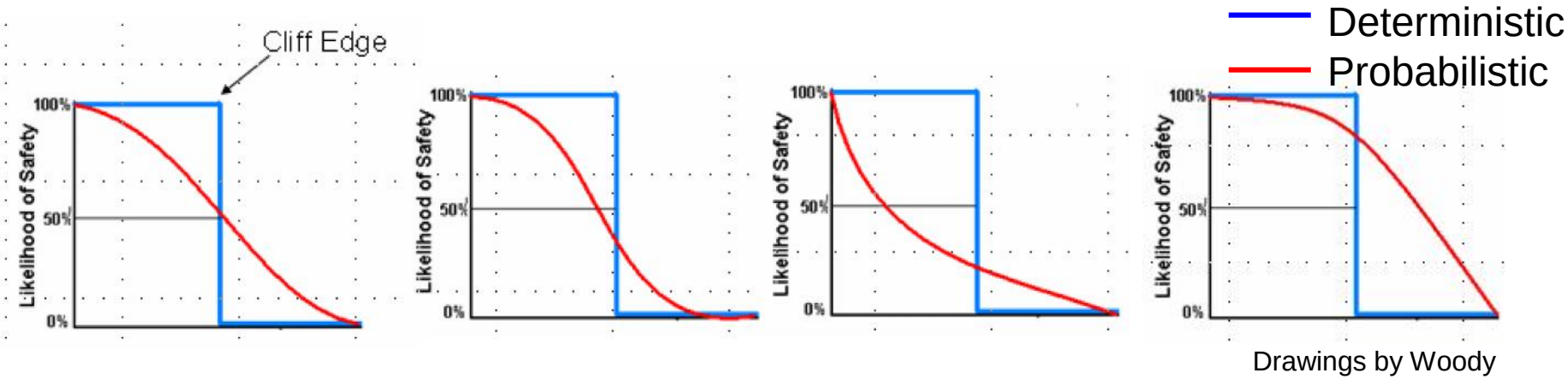

What is the likelihood of the plant staff actually dealing with the disaster on site given that they will be facing a lethal danger? What of the reports that some managers and staff at F1 self-evacuted to F2? Remember at Chernobyl, young military guys were ordered to assist with measures of suppressing the power in what was the remains of the reactor. This should be included in L3 and, maybe, also in L2 analysis.

Grynblat

Level 3 PSAs: There are not many of them and this is a major deficiency in the context of the public debate addressing the merits and drawbacks of complex systems --- Hirschberg

Lloyd's Register Consulting

# Deterministic vs. Probabilistic

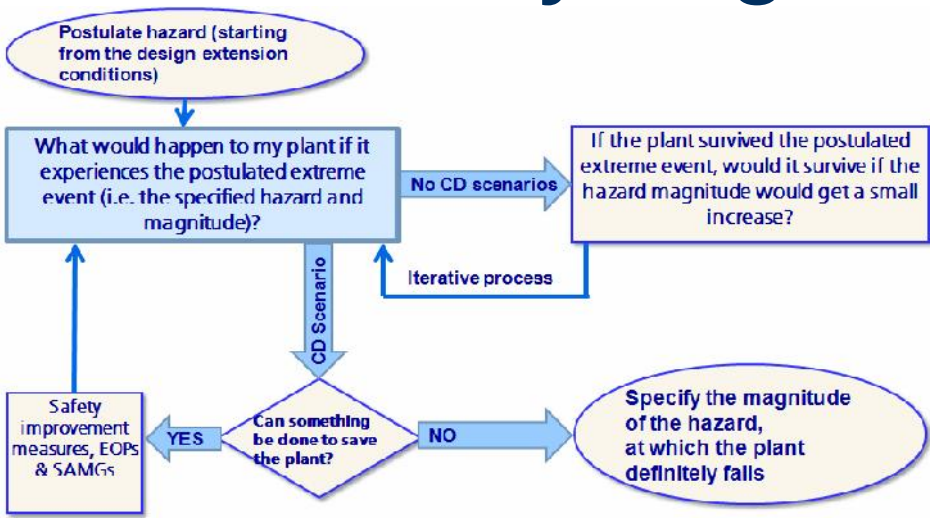



Drawings by Woody

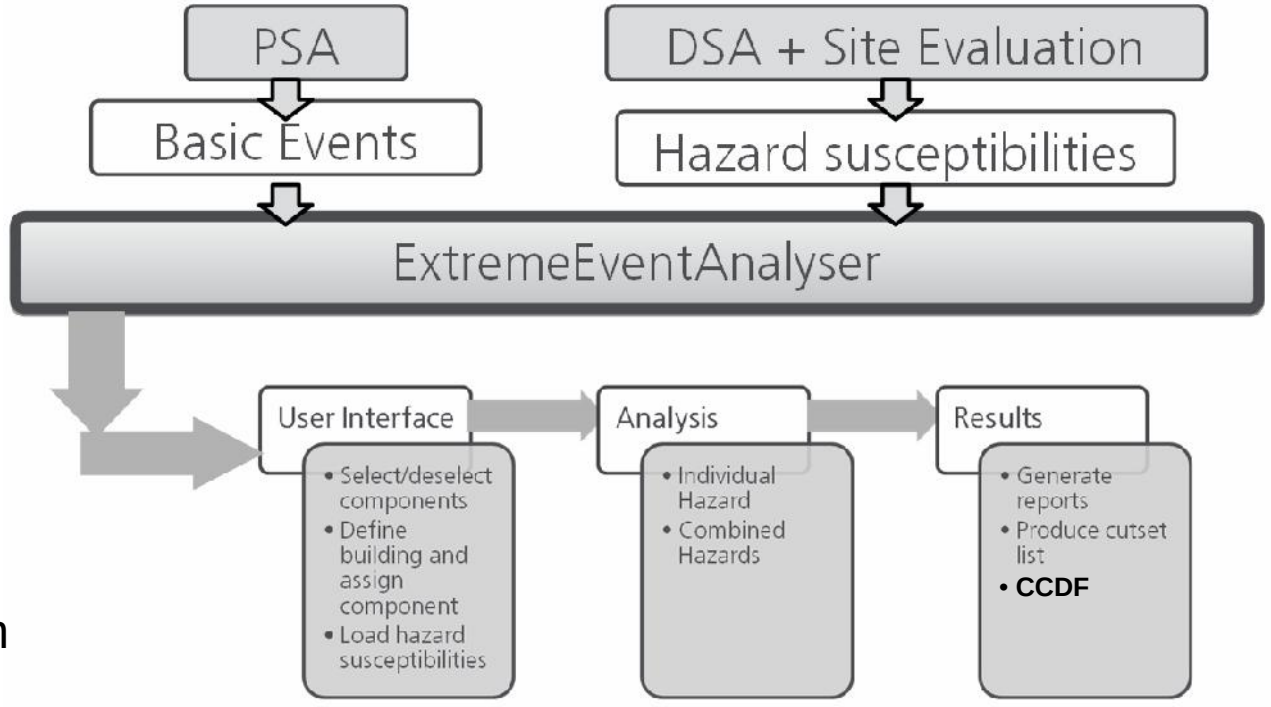
I submit that the traditional “deterministic” approach has as many, or more, problems as PSA. The right approach is to use all the tools that are available to manage risk.

There is room for PSA as there is for defense in depth and conservatism. It is in this context that benefits and limitations of all methods ought to be discussed.

# Analyzing Extreme Events




Here is a way to incorporate insights from both PSA and DSA into one analysis which evaluates the impacts of extreme events to site damage states.




Lloyd's Register Consulting Backstrom

# Identification of potential focus areas regarding development of PSA methodologies as lessons learned from Fukushima

1. External hazards screening criteria and frequency assessment
2. Consideration of correlated hazards
3. External hazard impact assessment
4. Multiple units' consideration
5. Mission time considered in Level-1 PSA
6. HRA analysis for external hazards
7. Failure possibility for qualified equipment
8. Hydrogen explosion in case of station blackout (SBO)
9. Transient explosive materials in external event conditions
10. Non-envisaged connections between plant buildings and compartments
11. Spent fuel pool and waste treatment facilities
12. Modeling of Severe Accident Management Guidelines

- Issues #1-2 are related to the hazard assessment,
- Issue # 3 relates to both categories, and
- Issues #4-12 are related to plant response modeling

Lloyd's Register Consulting

Knochenhauer and Olsson for the Nordic PSA Group (NPSAG)

# Safety differently

competition. Telling people not to have accidents, to try to get them to behave in ways that make having one less likely, is not a very promising remedy. The potential for mistake and disaster is socially organized: it comes from the very structures and processes that organizations implement to make them less likely. Through cultures of production, through the structural secrecy associated with bureaucratic organizations, and a gradual acceptance of risk as bad consequences are kept at bay, the potential for an accident actually grows underneath the very activities an organization engages in to model risk and get it under control. Even high-reliability organization (HRO)

- We need to transition from seeing people as a problem to control, to seeing people as a solution to harness;
- We need to transition from seeing safety as a bureaucratic accountability *up*, to seeing it as an ethical responsibility *down*;
- We need to transition from seeing safety as an absence of negatives to seeing it as the presence of a positive capacity to make things go right.

| **Modernist safety** | **New era safety** |
|---|---|
| People are a problem to control | People are a solution to harness |
| Safety is defined as the absence of negatives (injuries, incidents) that show where things go wrong | Safety is defined as the presence of capabilities, capacities and competencies that make things go right |
| Safety is a bureaucratic accountability directed upward in the organization | Safety is an ethical responsibility directed downward in the organization |
| Cause-effect relationships are linear and unproblematic | Cause-effect relationships are complex and non-linear |
| Vocabularies of control, constraint and human deficit | Vocabularies of empowerment, diversity and human opportunity |

Lloyd's Register Consulting

Dekker

# Lack of Power for Mitigation

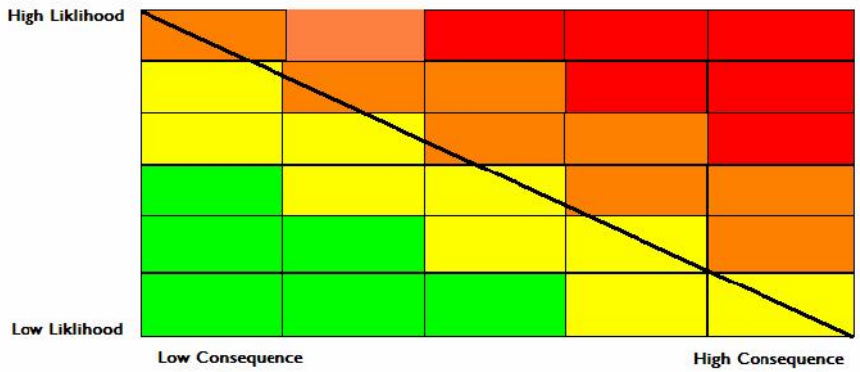
A PRA approach is acceptable when, and only when, human intervention to a target system is not so dominating. Now we have experienced the Fukushima disaster in which a wide variety of human interventions were absolutely needed. It seems obvious for me that the PRA methodology is not at all powerful enough to deal with such situations.

If TEPCO and the nuclear community of Japan were a little more sensitive to warnings of tsunami and station blackout and tried to apply a far simpler tool, such as risk matrix method, they could have prevented or mitigated the chaotic situations caused by the tsunami. Such commonsense-based risk management has nothing to do with the PRA methodology.

Lloyd's Register Consulting

Kitamura

# The Risk Matrix




A risk matrix has its own merit if used correctly and carefully, but most people do not. How can one justify picking one of the many outcomes of a hazard scenario, pick a severity class, miraculously pick a likelihood class, and then decide the risk of a scenario from a pre-made matrix without knowing the total risk of the scenarios or whether the risk class they pick is the dominating risk outcome.

But everyone is using it and worshipping it like a religion. Some companies even have only one risk matrix for all their business across the world when their businesses clearly have different risk exposures, risk appetites, and tolerance levels.

Lloyd's Register Consulting

Ho

# The need for leadership from the top

A requirement of such leadership is the need to buy into the tools, processes, and procedures necessary to enable effective decision-making during the course of a severe threat to the plant that does not allow time to receive offsite support.

Since the Fukushima Daiichi event made clear the need for additional safeguards and stronger utility leadership, there has been no more opportune time for the operating companies to step forward and lead the way to not only take appropriate corrective actions, but to exemplify the culture necessary for assuring nuclear safety in the future.

What is needed is a plan that builds public confidence that those benefits can be realized without the fear of another Fukushima Daiichi event.  And of course the plan must provide a level of scientific evidence concerning nuclear plant safety beyond what is currently available.

Lloyd's Register Consulting

Garrick

# The Good, the Bad, and the Ugly

## Earthquake Predictions and Hazard Maps

il Buono

We have methods for making earthquake predictions and hazard maps.

il Brutto

These methods haven't been verified.

il Cattivo

The predictions and hazard maps don't agree with the data.

VALIDATION! Any model or theoretical analysis – is just that until supported by observational data. --- Tappin

Lloyd's Register Consulting

# The Ulitimate Shake Table

- The Onagawa NPS was the ultimate shake table test for structures, systems and components for a nuclear plant

•The March 11, 2011 earthquake was the largest earthquake ever experienced at a nuclear plant.

- Engineering design demonstrates that plants can survive large earthquakes without significant damage or loss of function.

- We can demonstrate to the public, the governments, and the regulators that the Japan 3/11 earthquake is an earthquake engineering success which can be used to demonstrate robustness of existing designs.

- The Onagawa NPS, particularly the non-safety related parts, show large margins of safety. We need to quantify those margins and use them to support restart of other NPS if they have the same margins of safety.

- Onagawa in many ways is a typical nuclear plant. Use that knowledge to save on un-needed analyses and upgrades.

Lloyd's Register Consulting

Yanev

# PSA Technology Challenges Revealed by 3.11

- Extending the PSA Scope
- Treating Feedback Loops
  - Level 3 feedbacks to Levels 1 or 2
  - Multi-units: Unit 2 feedbacks to Unit 1
- Reconsidering “Game Over” Modeling/Conservatism
  - Termination of accident sequences early
  - Risk-significant sequences are masked
  - Responders can be unaware of mitigating activities
- Treating Long Duration Scenarios
- Improving and Expanding External Hazards Analysis
- Improving HRA
- Characterizing Uncertainty in Phenomenological Codes
- Increasing the Emphasis on Searching (vs. Screening)

Lloyd's Register Consulting

Siu, et. al.

# Suggestions for the Future

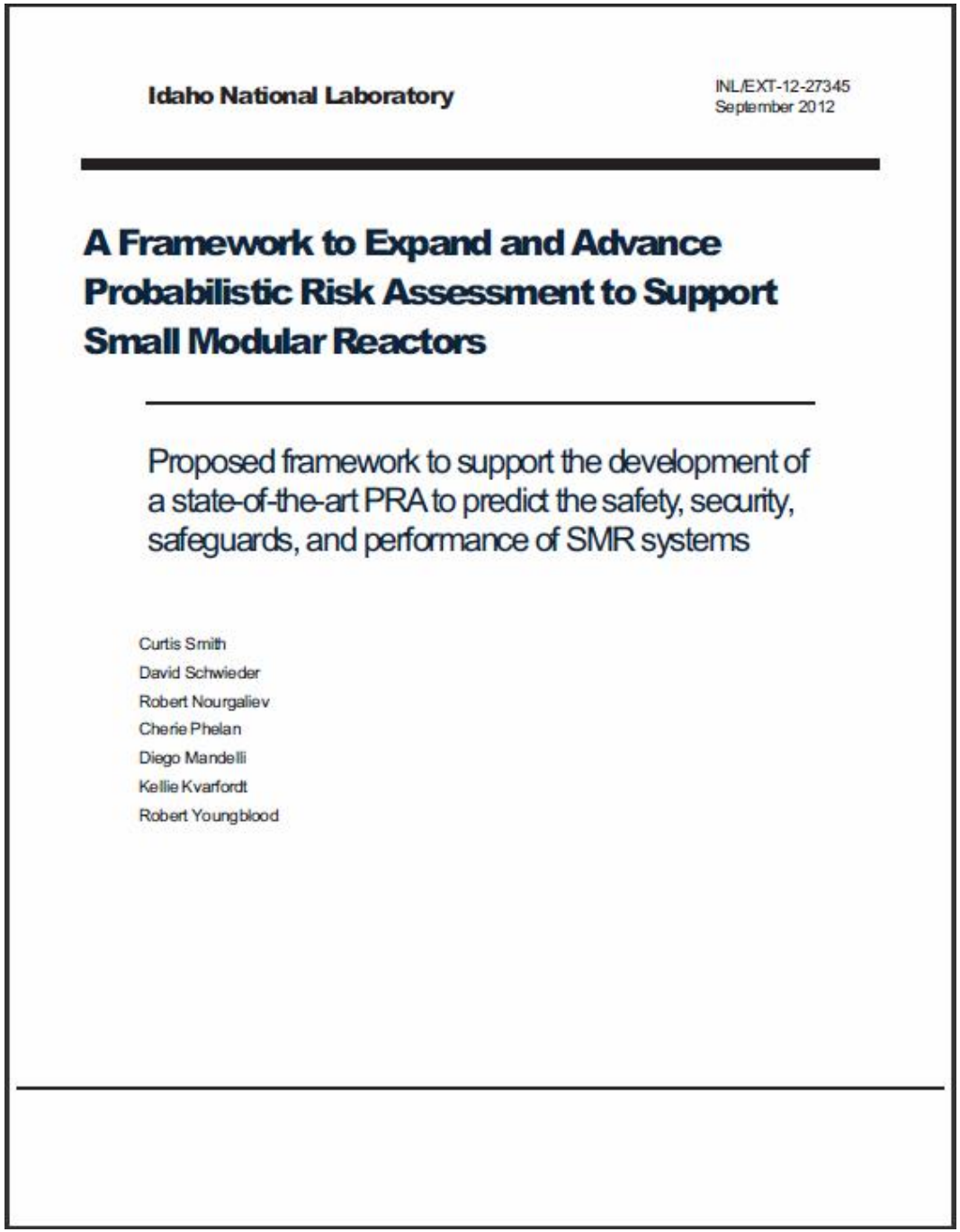
- For every PRA application we need a level of detail that is suitable for that application.
- Screening which does not mask important vulnerabilities: The Robinson event (2010).
  - Such events would never survive probability- based screening in a typical PRA.
  - Incredibly large number of seemingly independent contributors would push the probability of the sequence practically to zero.
- We need to find a way to “see” the vulnerabilities irrespective of the numbers.
- Should feed accident insights back into PRA methodology, one of the original objectives of precursor studies.
- Only a small fraction – very small fraction- of methodological solutions find their way into the practice of PRA
  - Need to fill the gap between research and application

# The need for multi-unit site PRA

- Most reactor sites are multi-unit.
- Deterministic and probabilistic risk assessments are performed on each reactor independently.
- Accidents considered on each unit assume the other units are safe.
- Accidents involving multiple units are not included in the PRA.
- A single unit accidents that could affect other units are not considered.
- Risk metrics (CDF, LERF, …) do not capture multi-unit effects.

Lloyd's Register Consulting

Fleming, Garrick



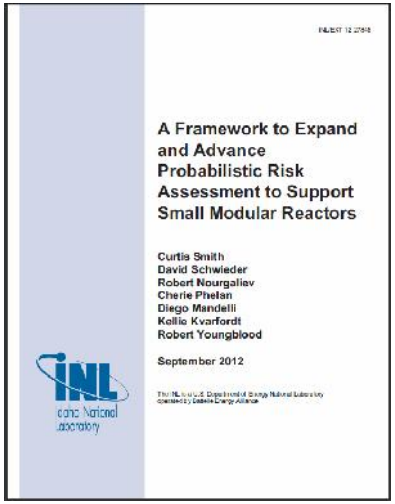
Idaho National Laboratory

INL/EXT-12-27345
September 2012

# A Framework to Expand and Advance Probabilistic Risk Assessment to Support Small Modular Reactors

Proposed framework to support the development of a state-of-the-art PRA to predict the safety, security, safeguards, and performance of SMR systems


Curtis Smith
David Schwieder
Robert Nourgaliev
Cherie Phelan
Diego Mandelli
Kellie Kvarfordt
Robert Youngblood


Smith, et. al.

# A look into the future …

As PRAs become more and more complex and incorporate more information, and because more detailed risk-informed applications are expected in always shorter and shorter time spans, it has become essential that models and tools evolve. We need platforms that will allow us to visually develop module-based PRAs. --- Nusbaumer

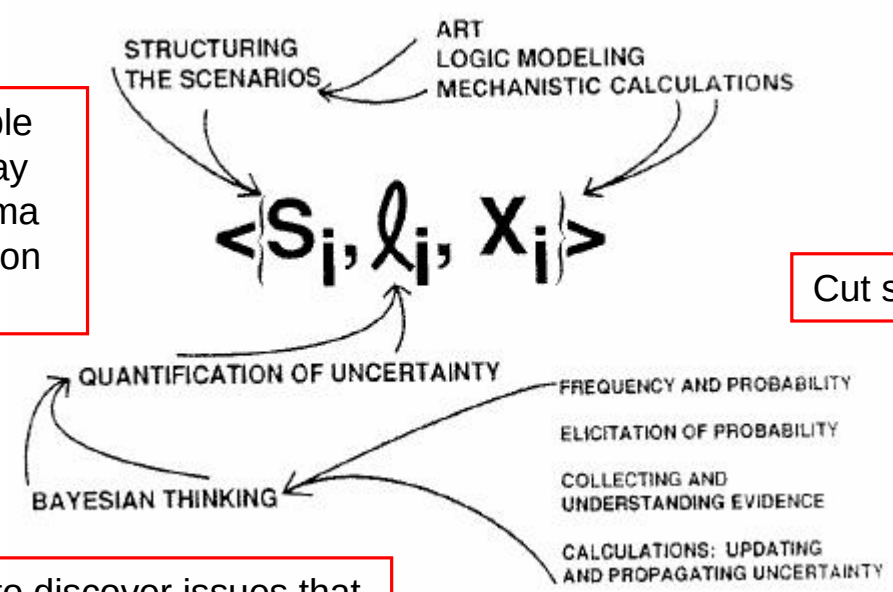
The greatest visible challenge to PRA is NOT, the Network Of Things. And it is highly likely that we will see critical infrastructure become part of this network and be challenged by the implementers to estimate the reliability of parts of that infrastructure. To do so and have some confidence in the accuracy of the result will require different tools than currently exist. --- Cook

We need really to implement a new visual thinking on our complex systems and make it ”simplex”. Addressing visual complexity should be done not by simplifying, but by finding solutions whose processes, although they can sometimes be complex, will allow us to act in the midst of complexity and uncertainty. --- Hibti

Lloyd's Register Consulting

# Return to the scenario approach to PRA

… our models should be able to represent (important) relay races…such as at Fukushima unit 1 that resulted in isolation of the IC.




Cut sets are not sequences.

Add depth to sequences to discover issues that may have been overlooked. But watch out for artificial fracture.

We should capture the sequence timing in a more robust and rigorous manner.

Where have all the success branches gone? Long time passing.

We should not be happy having software limitations dictate any issue. Nor computer power.

PSA, then, is building the complete list of triplets; i.e. the set of all $S_i$, $\ell_i$, and $X_i$: $\langle\{S_i, \ell_i, X_i\}\rangle$. Identifying the full set of triplets requires the analyst to structure the scenarios in a way that is complete and is organized to facilitate the analysis. Structuring the scenarios is both an engineering art requiring experience and a nice sense of analysis, and a process drawing on the techniques of logic modeling and traditional engineering and scientific mechanistic calculations.

Johnson, Wakefield, Epstein

Lloyd's Register Consulting

# In conclusion …..

"I often say that when you can measure what you are speaking about, and express it in numbers, then you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the *beginning* of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever that may be.

--- Lord Kelvin, 1891

"If you are sure that you have measured the risk, then suspect there is something you are missing.

--- Woody Epstein, 2011

Lloyd's Register Consulting

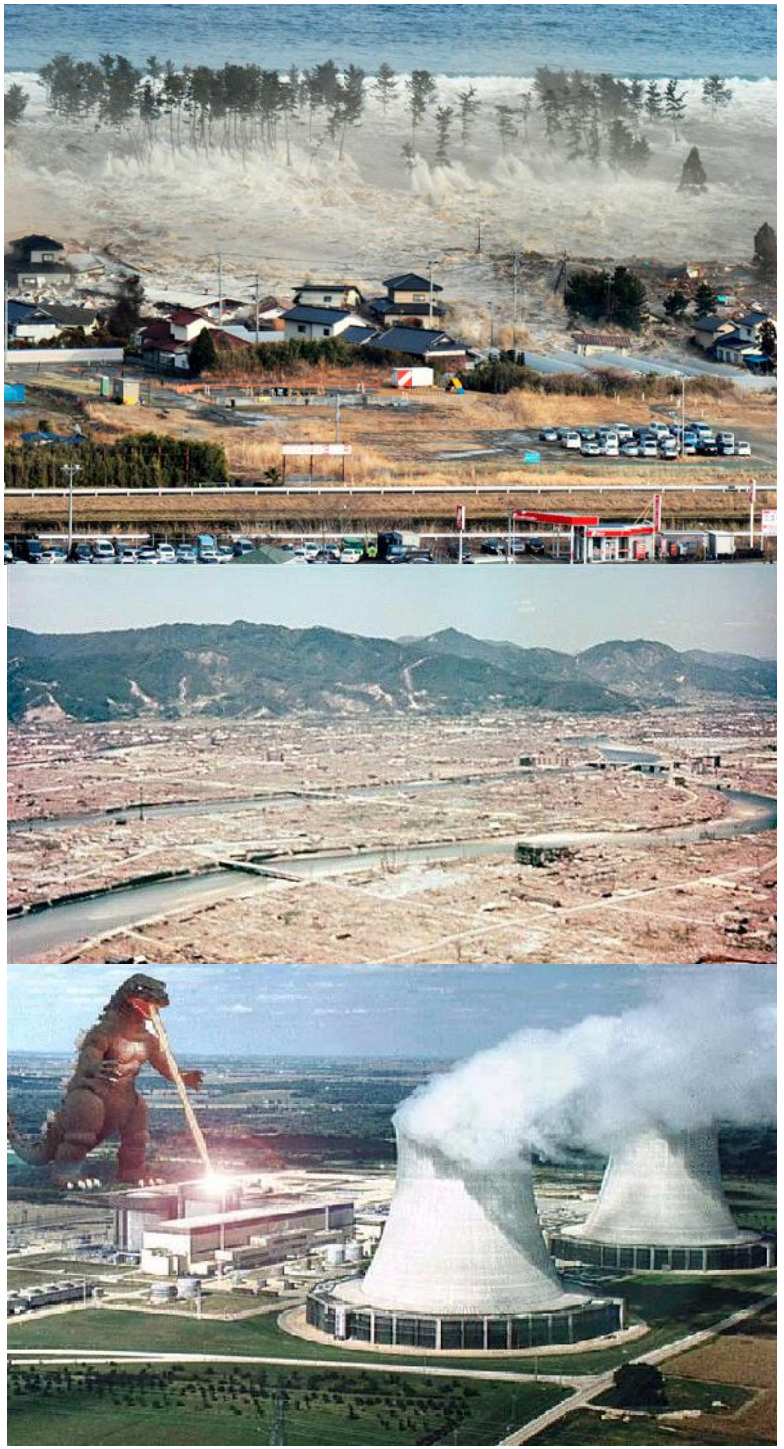
**Woody Epstein**
**Lloyd's Register Consulting**
**Manager Risk Consulting, Japan**

+81 (0)80-4401-5417
woody.epstein@lr.org

**Jerzy Grynblat**
**Lloyd's Register Consulting**
**Nuclear Business Director, Global**

+46 7077-306-33
jerzy.grynblat@lr.org

If you would like a copy of this presentation, and a free USB, please come to our booth in the exhibition area.



Lloyd's Register Consulting