

I gave this presentation at the second Resilience Engineering Symposium on November 6th, 2006. The accompanying article was included in the book, Resilience Engineering: Remaining Sensitive to the Possibilities of Failure, E. Hollnagel, et. al, editors (Ashgate Press), 2007, under the title “Unexampled Events, Resilience, and PRA”.

The words of the presentation have remained the same, but for the changing of “unexampled” to “unforeseen”, and “PRA” to “risk assessment”; the example given in slide #32 has been changed from the Storm King Mountain fire to the hydrogen explosion at Fukushima Daiichi Unit #1.

I have changed the images to reflect the recent events in Japan.

Woody Epstein, April 10th, 2011

A lovely spring night
suddenly vanished while we
viewed cherry blossoms.

Basho

March 11, 2011

Unforeseen Events, Resilience, and Risk Assessment

"Why isn't it loaded? Are you afraid of shooting yourself?"

"Of course not. These weapons don't go off accidentally. You have to do five things in a row before they'll fire, and an accident can seldom count higher than three ... which is a mystery of probability that my intuition tells me is rooted at the very base of physics. No, it's never loaded because I am a pacifist."

-- Field Marshall Strassnitzky of the First Hussars of the Belvedere during WW I

The Ghost of Risks to Come

The Focus Will be on Well-Tested Systems (WTS)

In the design and operations of a WTS there is a very high degree of reliability of equipment, workers and managers are vigilant in their testing, observations, procedures, training, and operations, with well trained staff, enlightened management, and good operating procedures in place.

Unforeseen Events

想定外

... and an accident can seldom count higher than three ...



#1 Earthquake



#2 Tsunami

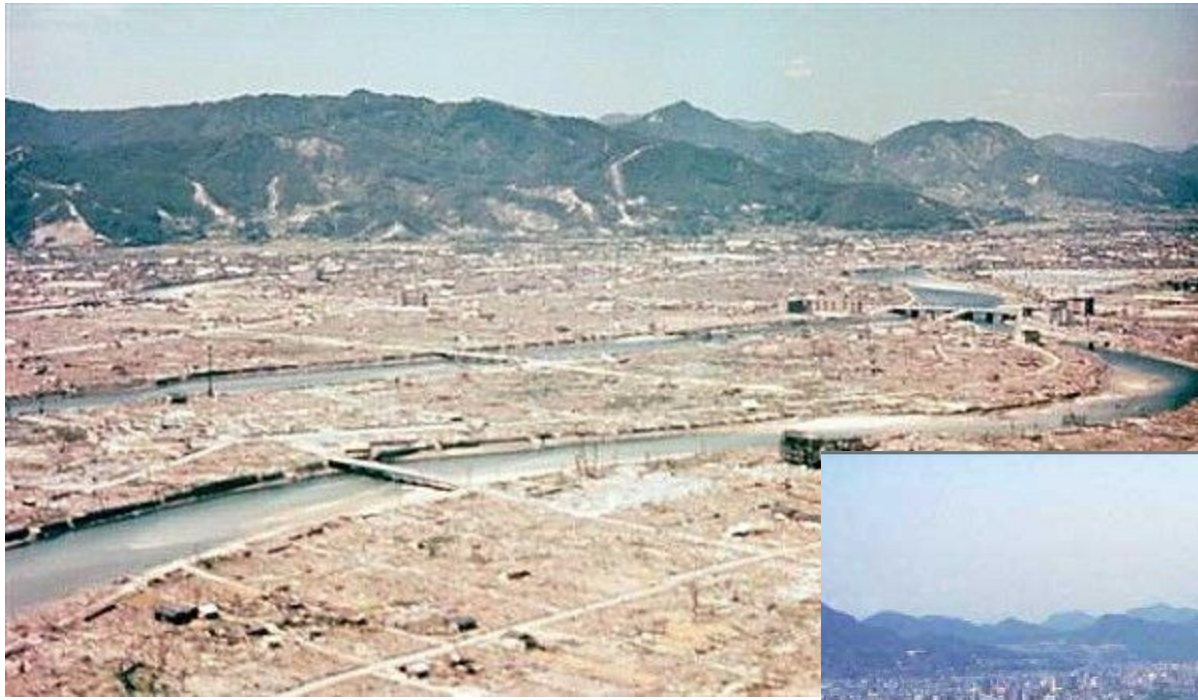


#3 Loss of cooling

Resilience

彈

Hiroshima,
August 6th, 1945



Hiroshima,
August 6th, 1995



And Risk Assessment



Fuku-1 Hydrogen Explosion

Unforeseen Events



#1 Earthquake



#2 Tsunami



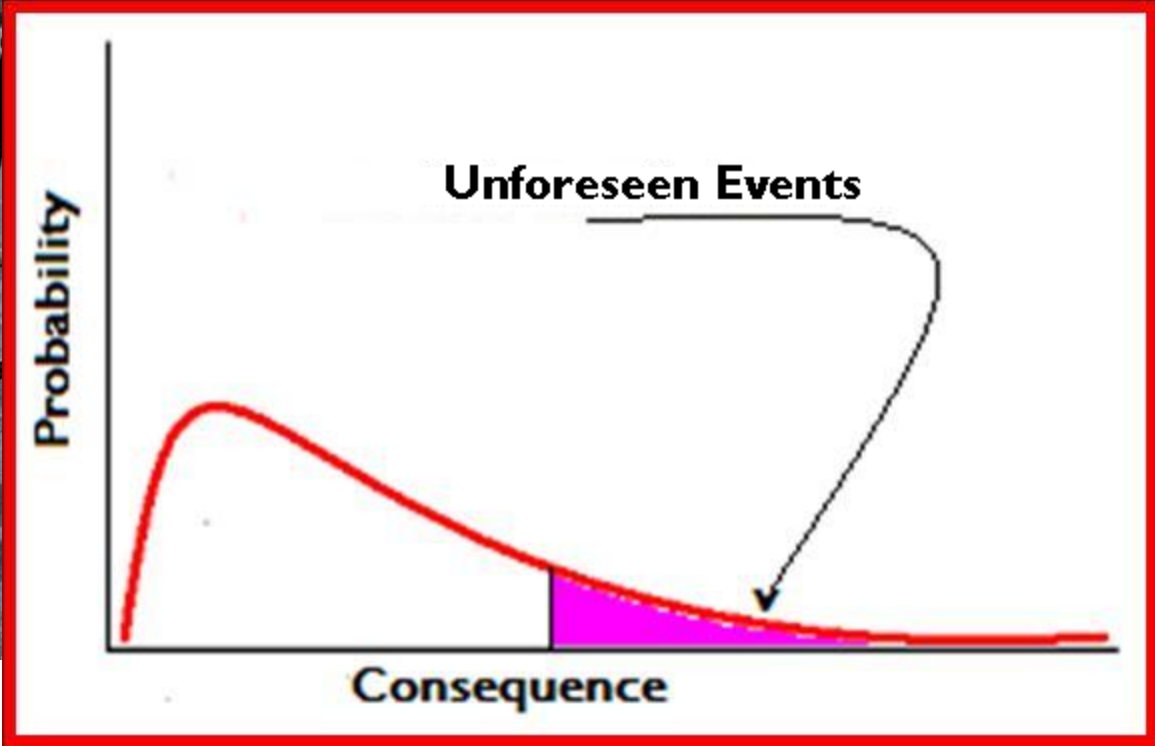
#3 Loss of cooling



#1 Earthquake



#2 Tsunami



#3 Loss of cooling



When hitherto seemingly disparate events are juxtaposed in new and unique ways, startling consequences can result.

tsunami

#1 Earthquake



#3 Loss of cooling



#1 Earthquake



#2 Tsunami

Extraordinary, never before thought of, challenges to the normal daily flow of a system.



#3 Loss of cooling



#1 Earthquake



#2 Tsunami

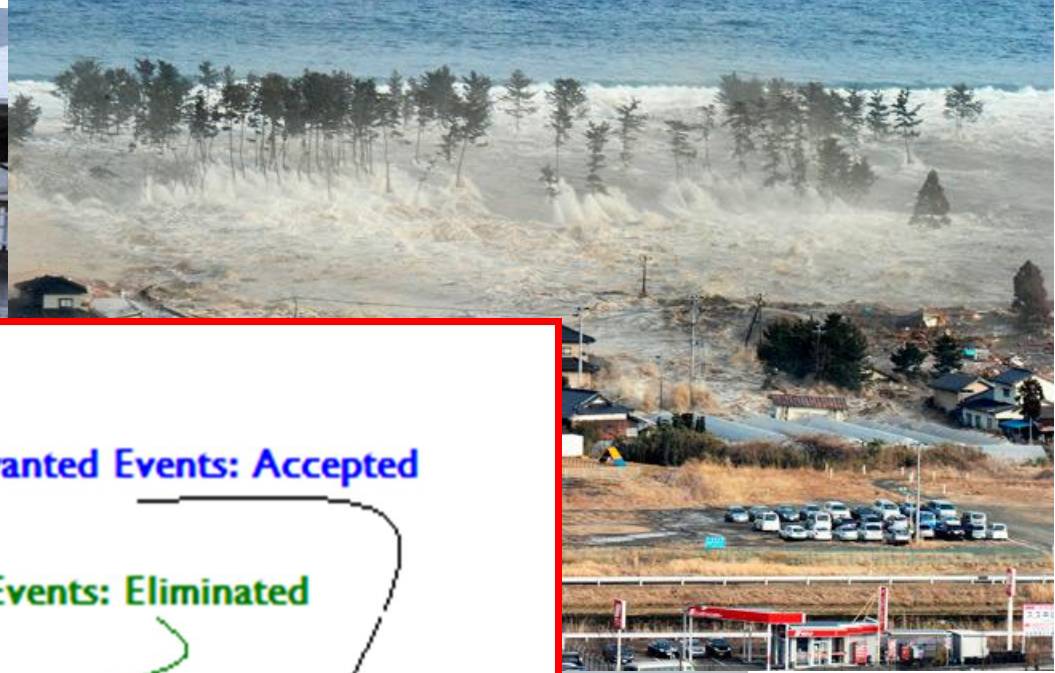
Events with such low probability that they are dismissed as not necessary to guard against.



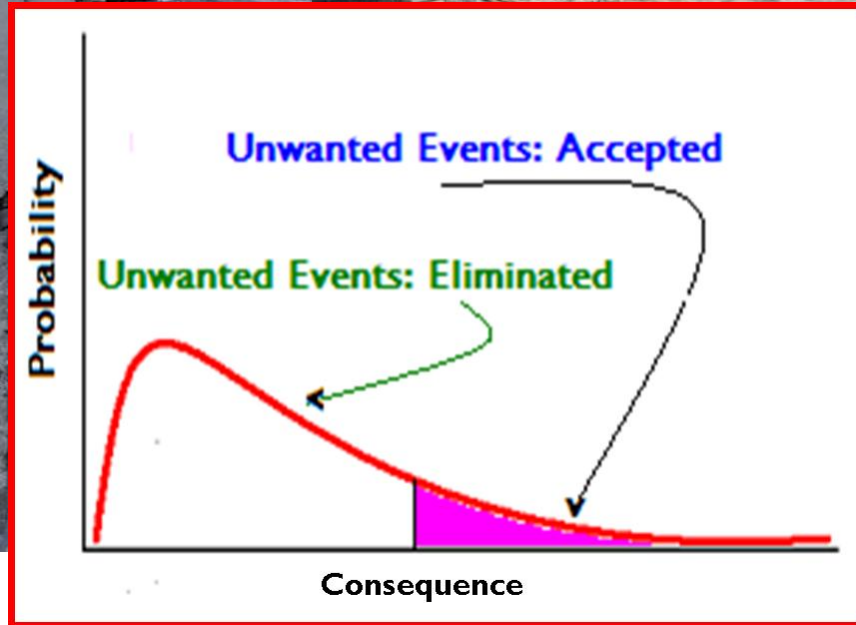
#3 Loss of cooling



#1 Earthquake



#2 Tsunami



#3 Loss of cooling

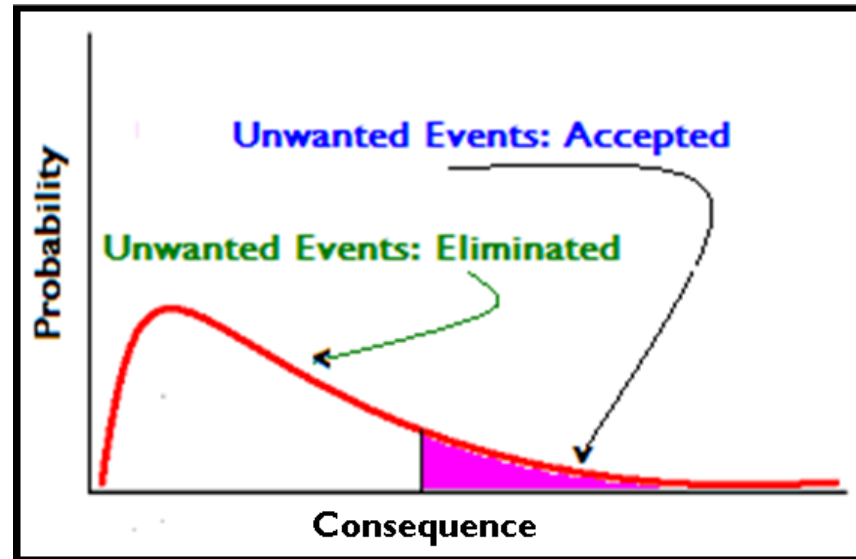


But does eliminating high probability risks and accepting very low probability risks inherently make a facility safe? Consider the following.

1. In well-tested systems, rarely executed code has a higher failure rate than frequently executed code;
2. consequences of rare event failures in well-tested systems are more severe than those of other failures;
3. given that there is a failure in a well-tested system, significantly more of the failures are caused by rare events;
4. inability to handle multiple rare conditions is a prominent cause of failure in well-tested systems.

Hecht: "Rare Events – an Important Cause of Software Failures"
[1993]

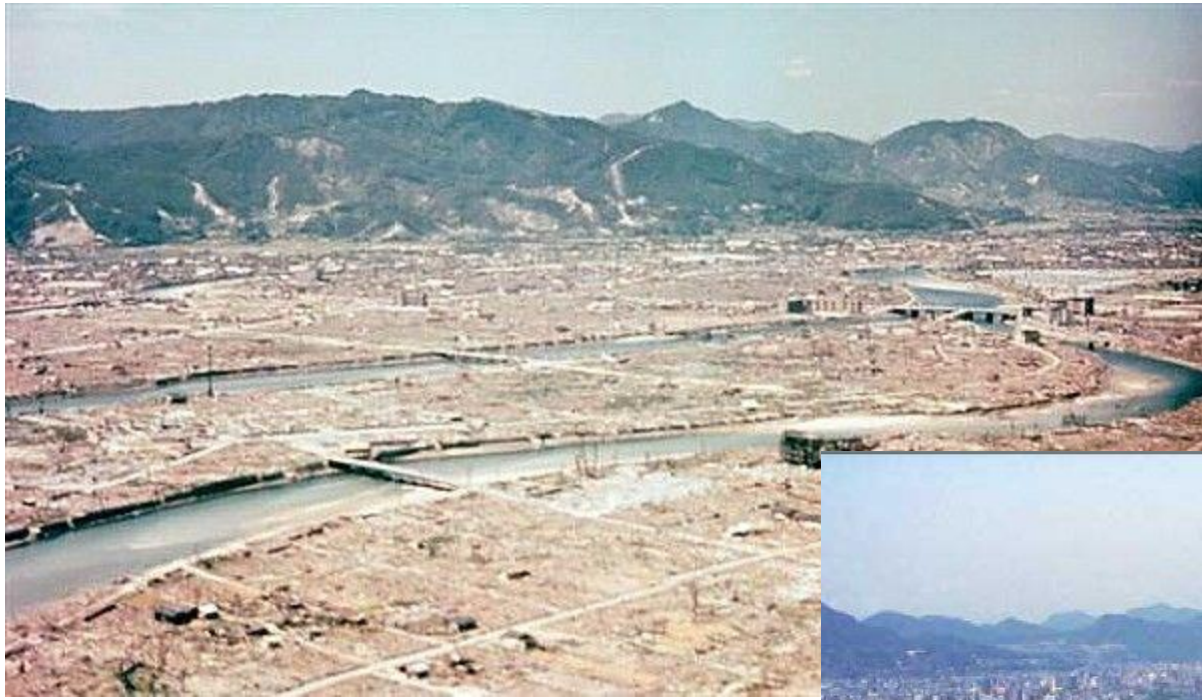
What do Hecht's Observations Tell Us About Well Tested Facilities?



The white area represents the unwanted events that a facility wants to entirely eliminate.

By exceptional planning, maintenance, reliability of equipment, human factors engineering, training, and organizational development skills, the facility is successful. The known and the thought of problems are vanquished.

What is left are the events in the magenta area, the accepted risks, the unforeseen, rare events. So if there is a failure, chances are the failure is an unforeseen event.



Resilience

彈

resilience

Pronunciation

Etymology

Quotations

Date chart

[ad. L. type **resilientia*: see [RESILIENT](#) and [-ENCE](#), and cf. It. *resilienza*.]

1. The (or an) act of rebounding or springing back; rebound, recoil. (See also quot. 1656.)

1626 [BACON](#) *Sylva* §245 Whether there be any such Resilience in Eccho's. **1656** [BLOUNT](#) *Glossogr.*, Resilience, a leaping or skipping back, a rebounding; a going from ones word. ?**1799** [COLERIDGE](#) *Hymn to Earth*, Mightier far was the joy of thy sudden resilience. **1843** [CARLYLE](#) *Past & Pr.* (1858) 79 The Heaviest..has its deflexions..nay at times its resiliences, its reboundings. **1866** [J. MARTINEAU](#) *Ess.* I. 41 The heart does not always propel without resilience.

2. Elasticity; the power of resuming the original shape or position after compression, bending, etc.; spec. the energy per unit volume absorbed by a material when it is subjected to strain, or the maximum value of this when the elastic limit is not exceeded.

1824 [TREGOLD](#) *Cast Iron* 82 The term modulus of resilience, I have ventured to apply to the number which represents the power of a material to resist an impulsive force. **1834** *Good's Study Med.* (ed. 4) I. 530 The natural elasticity or resilience of the lungs. **1867** C. T. F. [YOUNG](#) *Fouling Iron Ships* 164 To bend back again.., if the metal possesses sufficient resilience to do so. **1897** *Allbutt's Syst. Med.* IV. 470 [The skin] giving a sensation of the loss of all elasticity or resilience. **1908** E. S. [ANDREWS](#) *Theory & Design of Structures* i. 27 The work done per unit volume of a material in producing strain is called resilience. **1965** [J. A. CORMACK](#) *Definitions Strength of Materials* iii. 67 Show that resilience per cubic inch in direct tension or compression may be expressed in the form $f/2E$, where f is the intensity of stress induced and E is the modulus of elasticity. **1978** B. I. [SANDOR](#) *Strength of Materials* iv. 79 The maximum value of the elastic strain energy in a unit volume that has not been permanently deformed is called the modulus of resilience.

fig. **1893** *Independent* (N.Y.) 19 Oct., The resilience and the elasticity of spirit which I had even ten years ago.

Note:

1. Resilience is a reaction, not an action, of an object (rebounding, recoiling);
2. Resilience must be measured by experiment or experience (the maximum value of stress before breaking);
3. To measure resilience, we must know the essential properties of the material (what we are measuring).

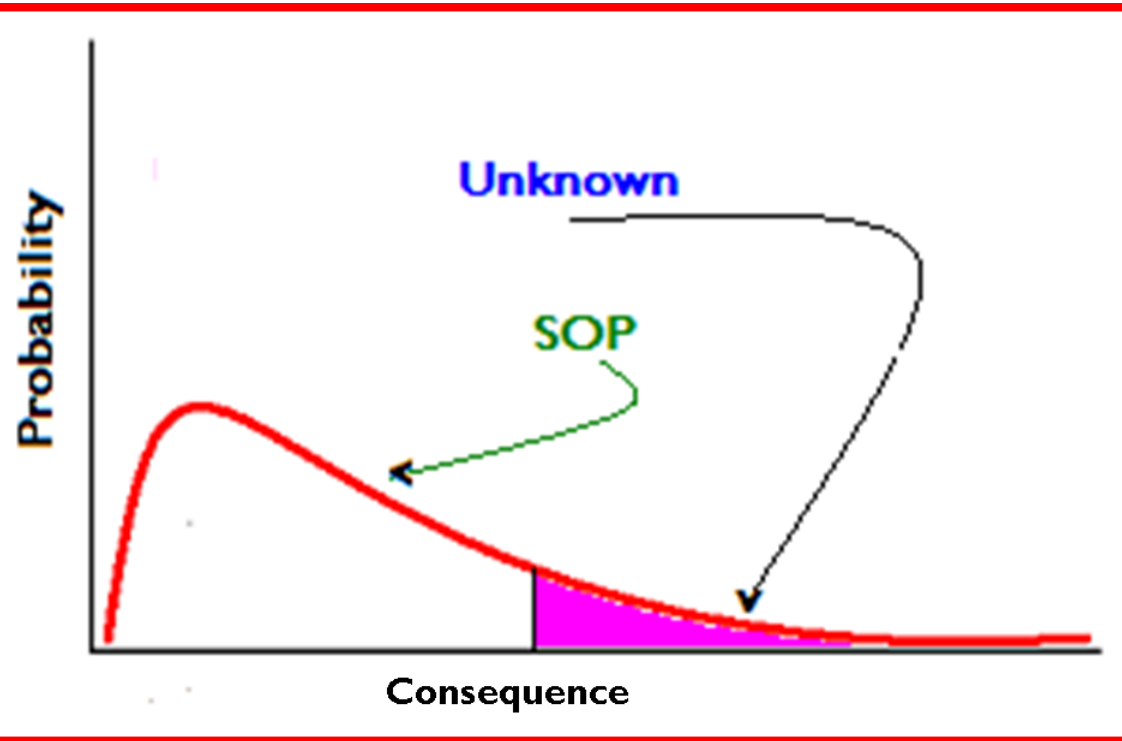
... so what is resilience in a Well Tested System?

In a WTS

...extraordinary activities eliminate unwanted events; good work rules and work habits are codified into procedures. Surveillance and technical oversight is in place.

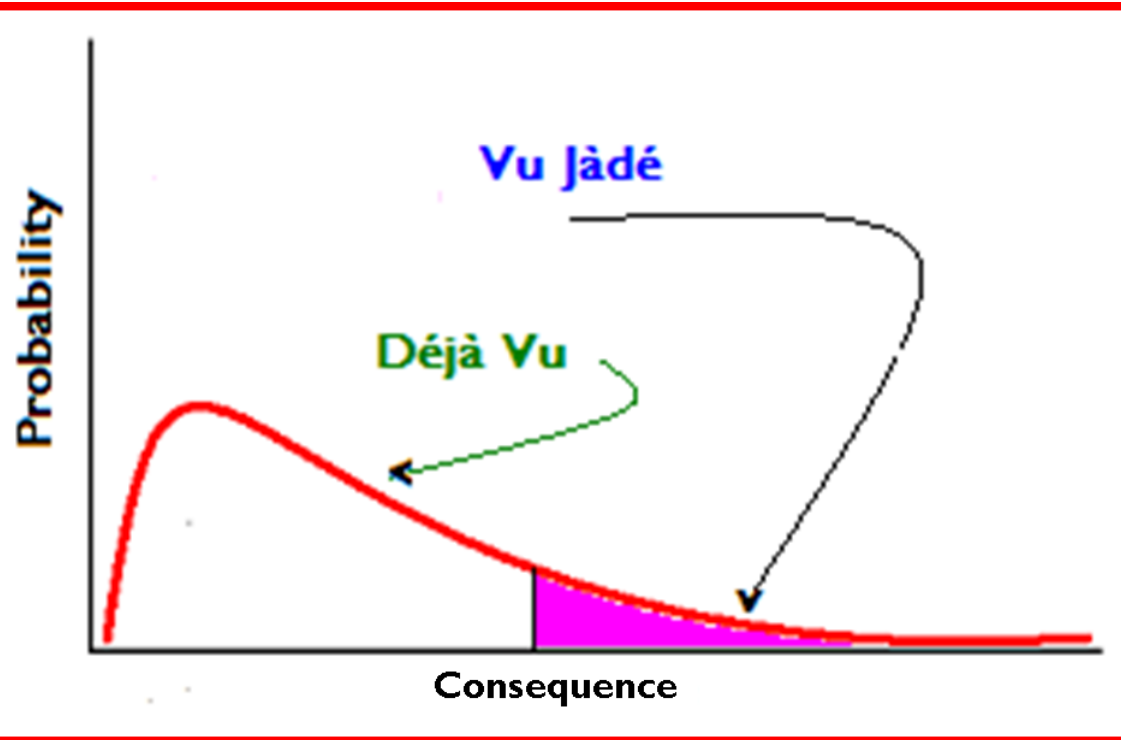
Successful reactions to known accidents are put in place as standard operating procedures.

In a WTS



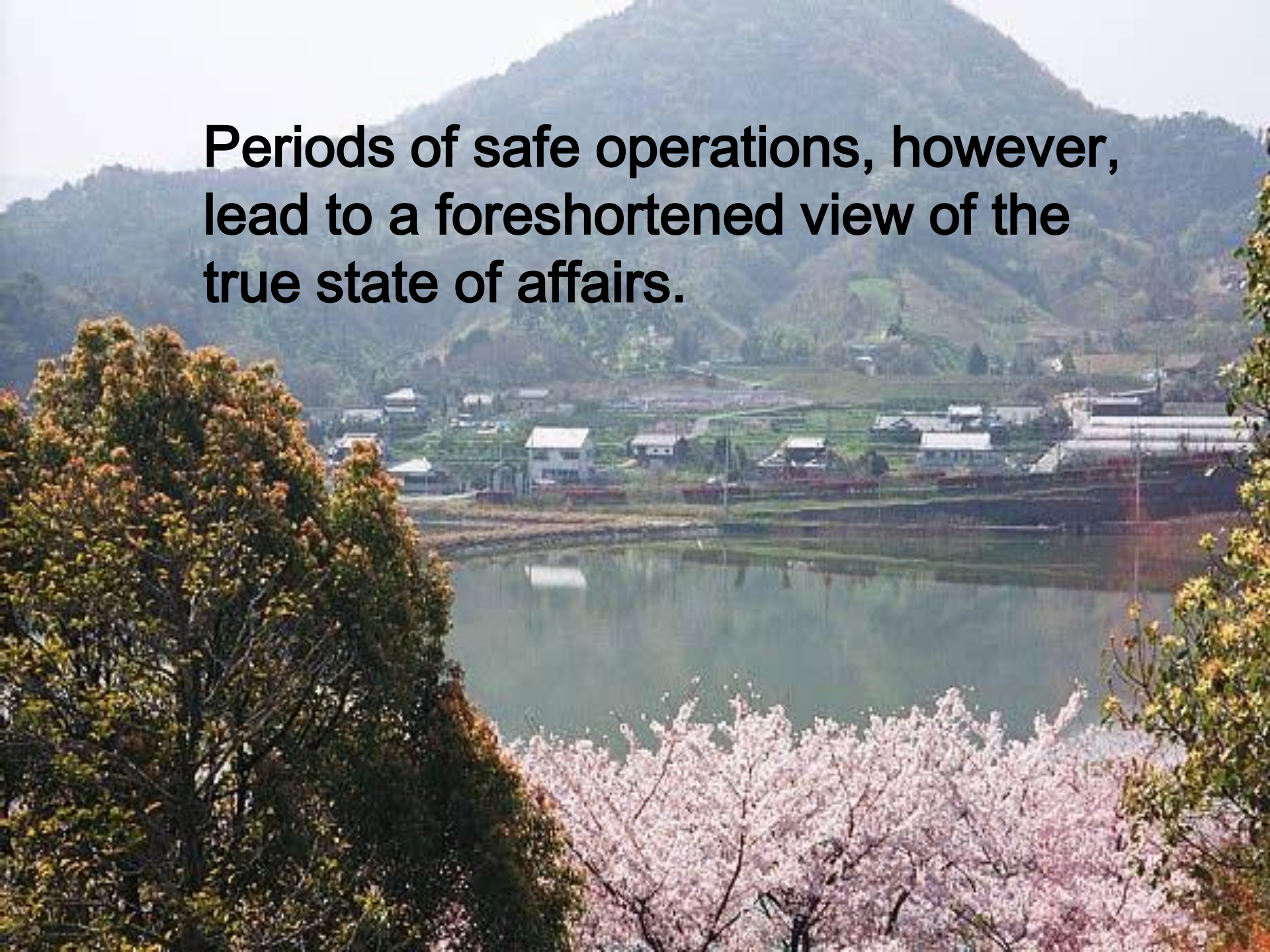
Standard operating procedures take care of known dangers ...

In a WTS

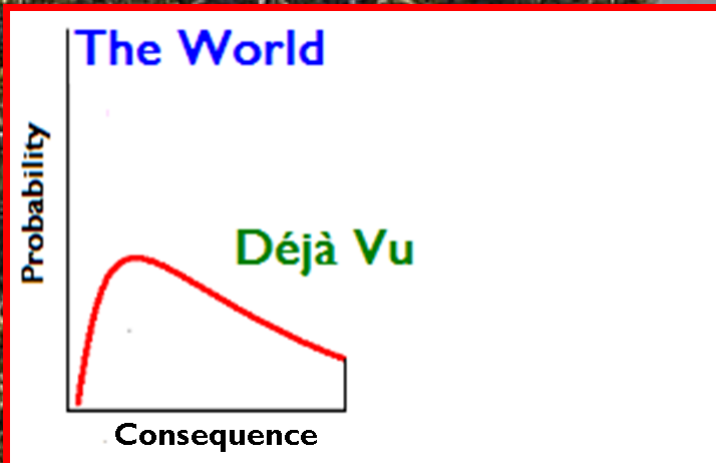


... and divide the risk into the already seen,
and the never yet seen.

Periods of safe operations, however, lead to a foreshortened view of the true state of affairs.



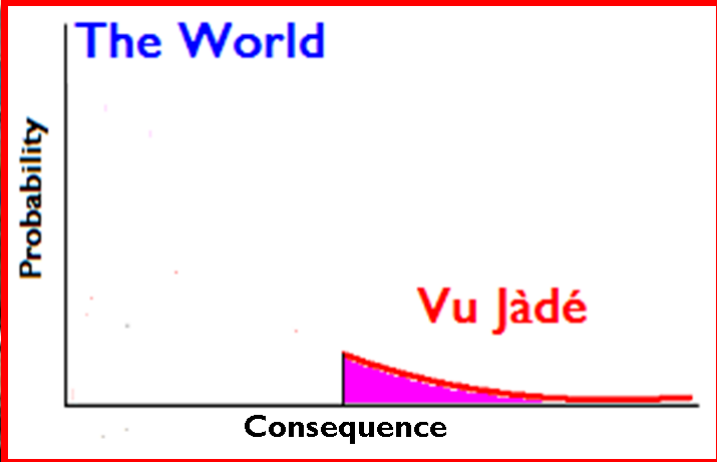
Periods of safe operations, however, lead to a foreshortened view of the true state of affairs.



**Until something unexpected happens,
and the world changes ...**



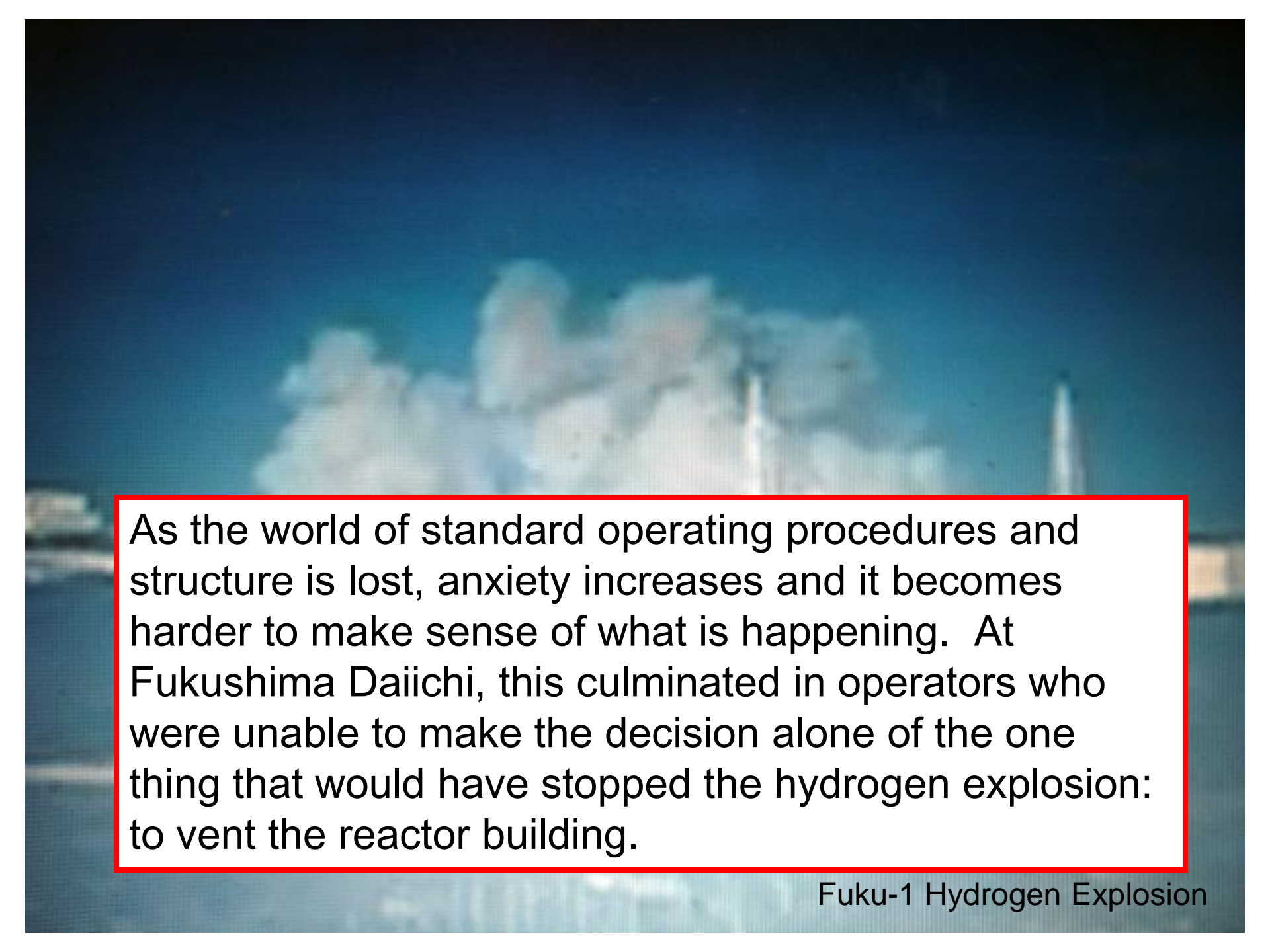
Until something unexpected happens,
and the world changes ...





**I have never been here before.
I have no idea where I am.
I have no idea which path to follow.
I have no idea who can help.**

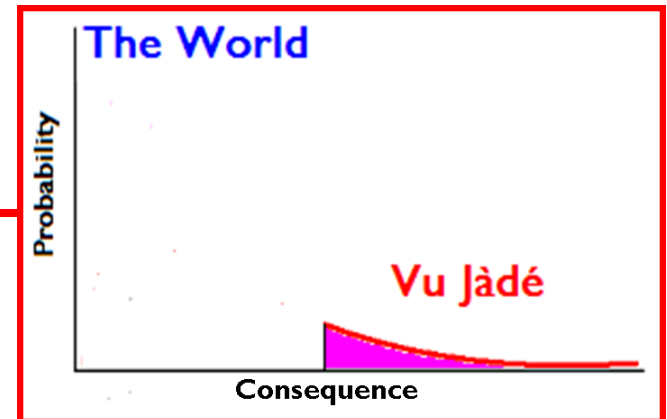
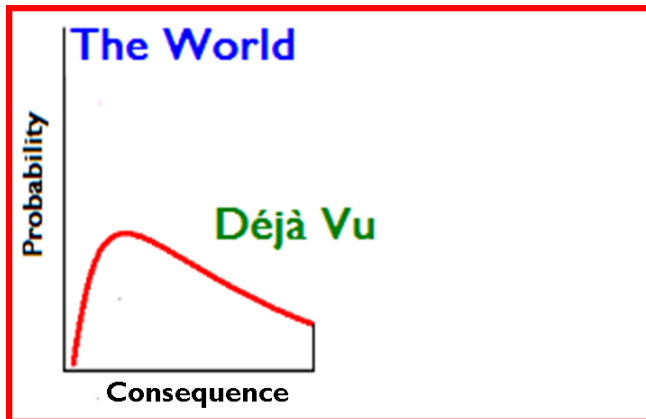




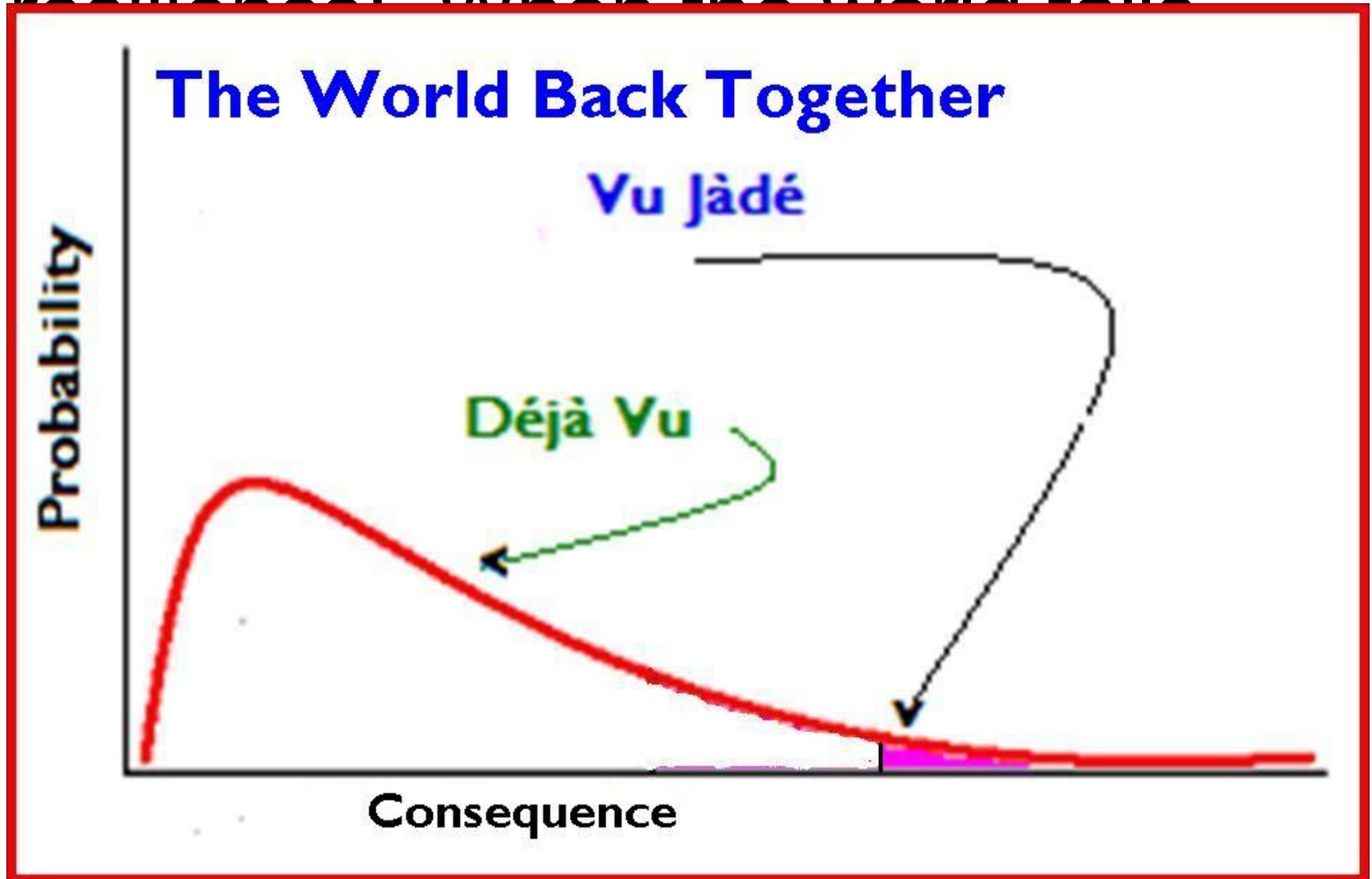
As the world of standard operating procedures and structure is lost, anxiety increases and it becomes harder to make sense of what is happening. At Fukushima Daiichi, this culminated in operators who were unable to make the decision alone of the one thing that would have stopped the hydrogen explosion: to vent the reactor building.

Fuku-1 Hydrogen Explosion

So here we find the meaning of resilience: When the world falls apart, and there seems to be no sense to the situation, resilience is the art of rebuilding some sense of what is happening and putting the pieces back together into a world.



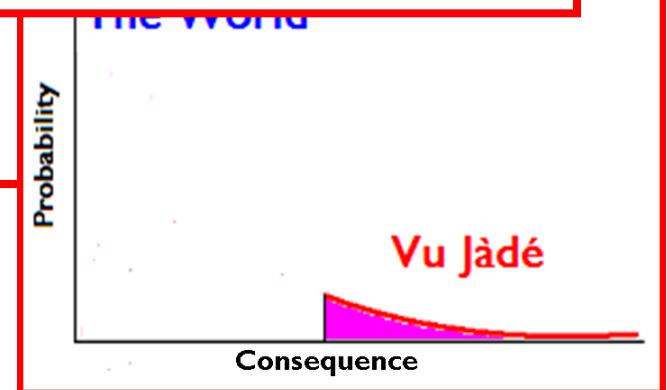
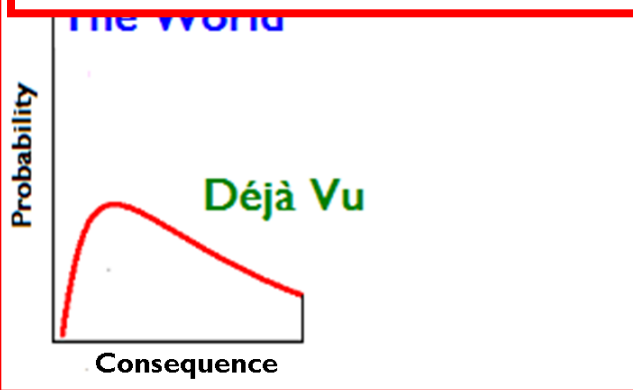
So here we find the meaning of
reciprocation. When the world falls



So here we find the meaning of resilience: When the world falls apart and there seems to be no

Resilience is rebuilding the world.
But it will not be the same world as before.

Expect the accident.
Expect to change.



The Art of Resilience

1. Having Experience
2. Questioning Experience
3. Intuition
4. Improvisation and Bricolage
5. Speaking and Listening
6. Examining Preconceptions
7. Ignorance + Knowledge = Wisdom
8. Taking Advantage of Fortuitous Events

Resilience as Adaptation





“natural selection is the claim that organisms enjoying differential reproductive success will be, on the average, those variants who are fortuitously better adapted to changing local environments, and that those variants will then pass their favored traits to offspring by inheritance”

Steven J. Gould: [The Structure of Evolutionary Theory](#) [2002]





“A new species can arise when a small segment of the ancestral population is isolated at the periphery of the ancestral range. Large, stable central populations exert a strong homogenizing influence. New and favorable mutations are diluted by the sheer bulk of the population through which they must spread. They may build slowly in frequency, but changing environments usually cancel their selective value long before they reach fixation. Thus, phyletic transformation in large populations should be very rare—as the fossil record proclaims. But small, peripherally isolated groups are cut off from their parental stock. They live as tiny populations in geographic corners of the ancestral range. Selective pressures are usually intense because peripheries mark the edge of ecological tolerance for ancestral forms. Favorable variations spread quickly. Small peripheral isolates are a laboratory of evolutionary change.”

Steven J. Gould: [The Structure of Evolutionary Theory \[2002\]](#)



“A new species can arise when a small segment of the ancestral population is isolated at the periphery of the ancestral range. Large, stable central populations exert a strong homogenizing influence. New and favorable mutations are diluted by the sheer bulk of the population through which they must spread. They may build slowly in frequency, but changing environments usually cancel their selective value long before they reach fixation. Thus, phyletic transformation in large populations should be very rare—as the fossil record proclaims. **But small, peripherally isolated groups are cut off from their parental stock. They live as tiny populations in geographic corners of the ancestral range. Selective pressures are usually intense because peripheries mark the edge of ecological tolerance for ancestral forms. Favorable variations spread quickly. Small peripheral isolates are a laboratory of evolutionary change.**”

Steven J. Gould: [The Structure of Evolutionary Theory](#) [2002]

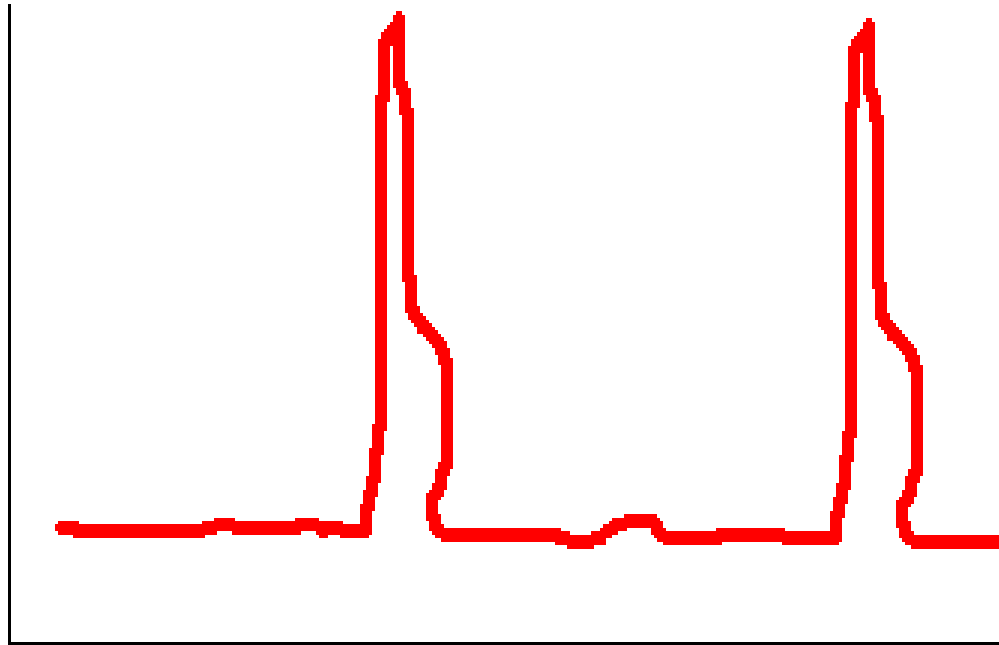
This the theory of Punctuated Equilibria

This the theory of Safety Drift



“A new species is isolated at populations are diluted by They may buy their selective transformation proclaims. But parental stock ancestral range mark the edge spread quickly

Probability of Risk



Time

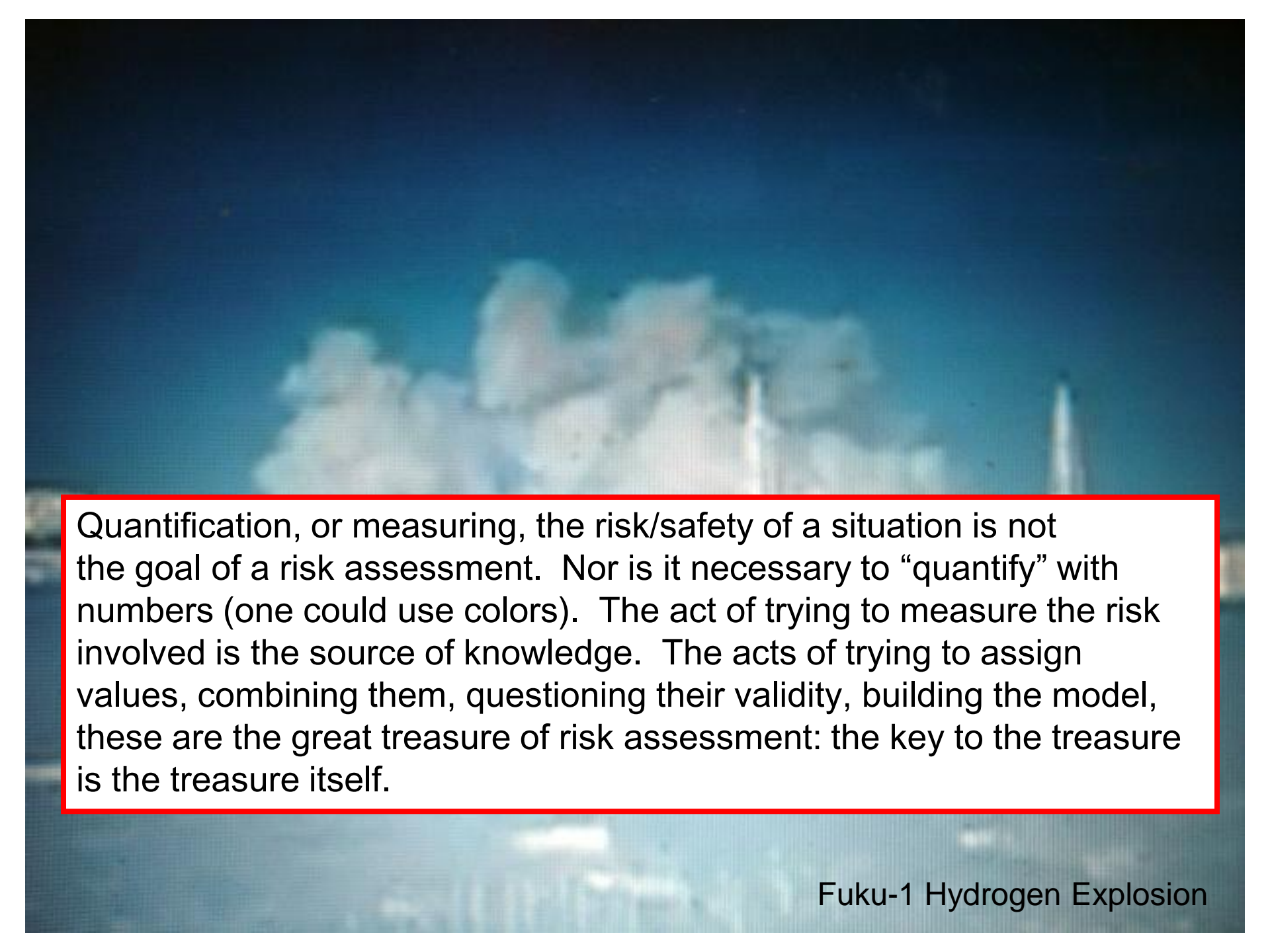
n
tations
read.
ancel
rd
ies
ions
change.”

Stephen J. Gould

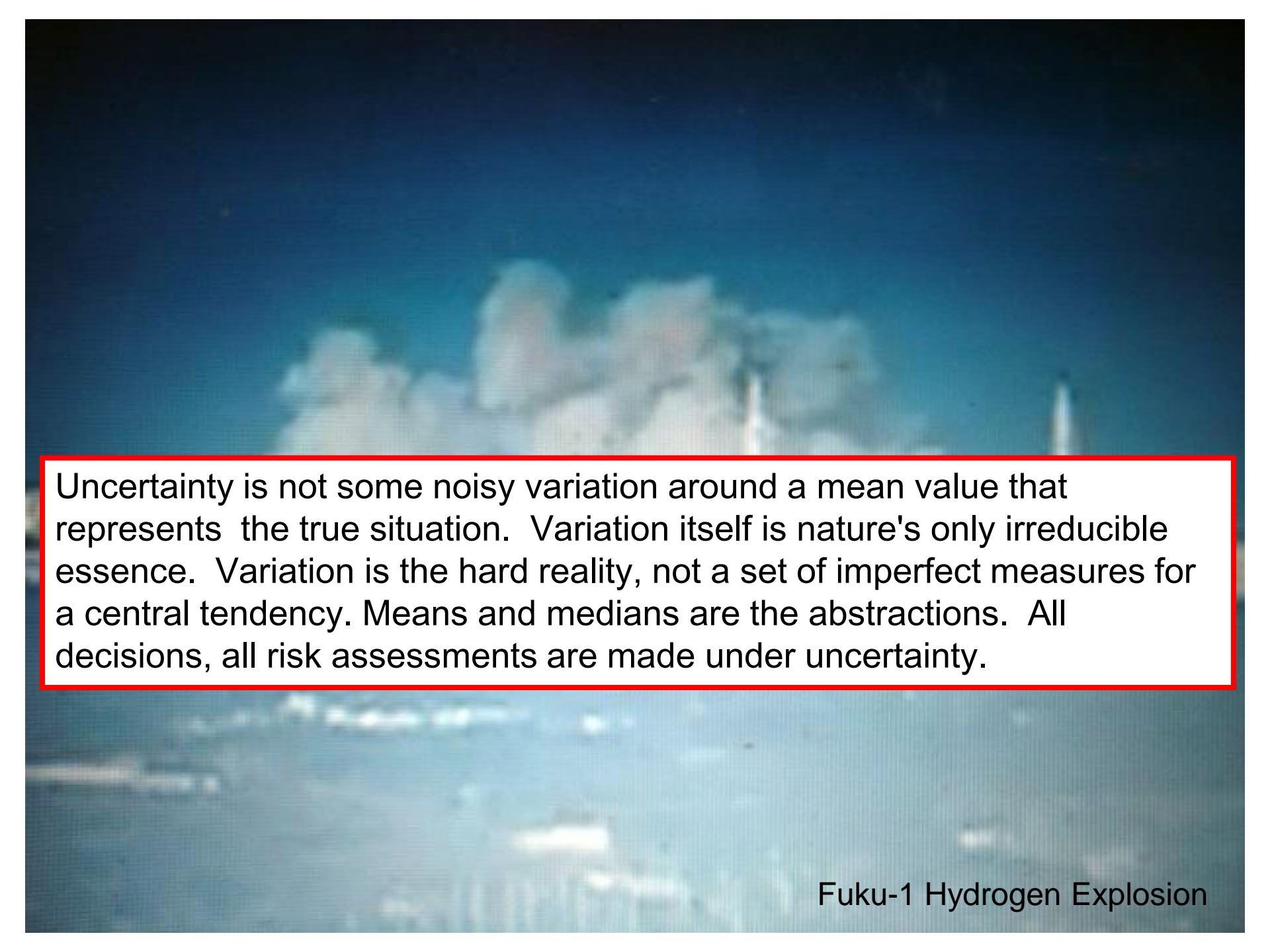


Risk Assessment

Fuku-1 Hydrogen Explosion

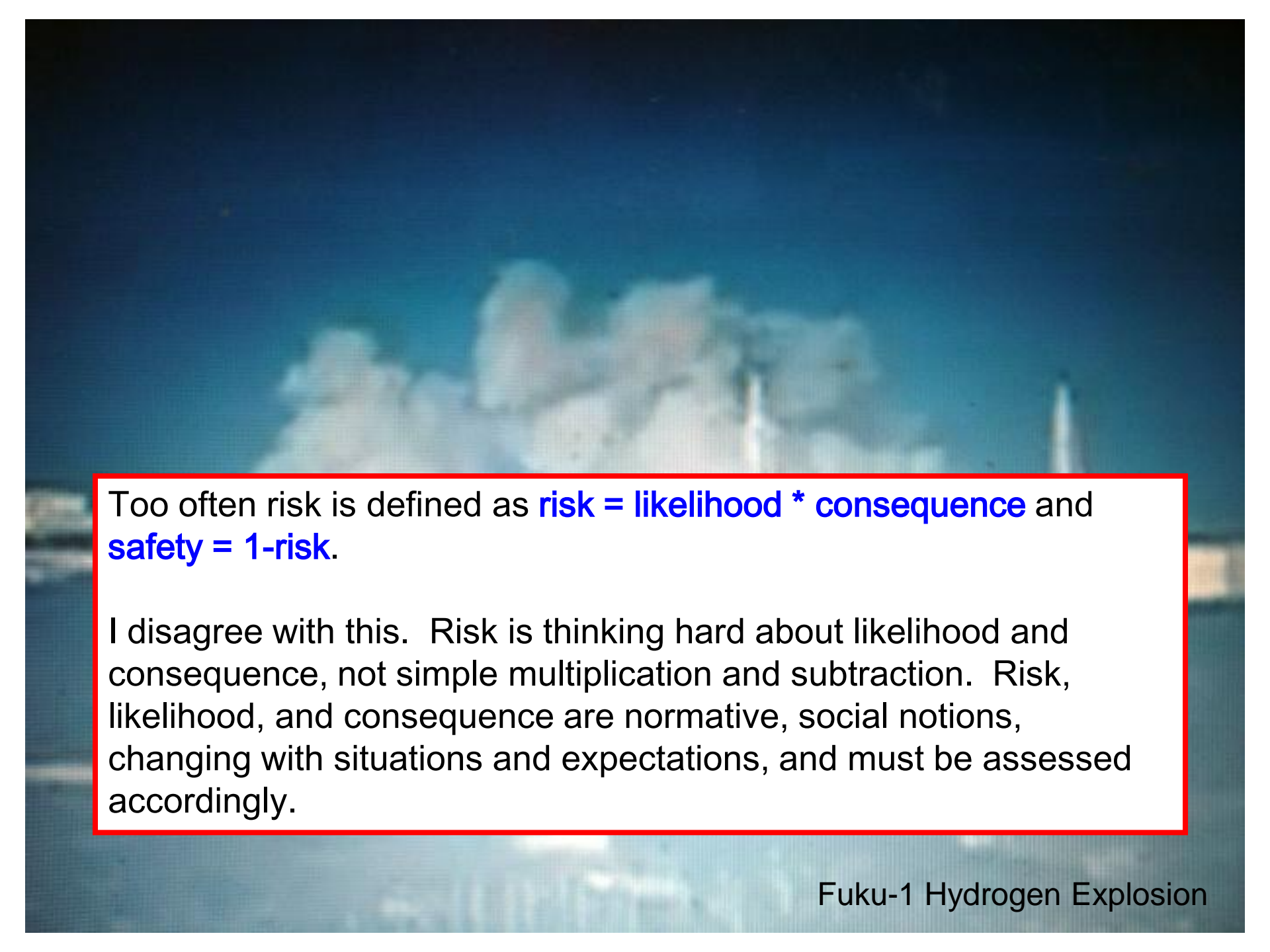


Quantification, or measuring, the risk/safety of a situation is not the goal of a risk assessment. Nor is it necessary to “quantify” with numbers (one could use colors). The act of trying to measure the risk involved is the source of knowledge. The acts of trying to assign values, combining them, questioning their validity, building the model, these are the great treasure of risk assessment: the key to the treasure is the treasure itself.



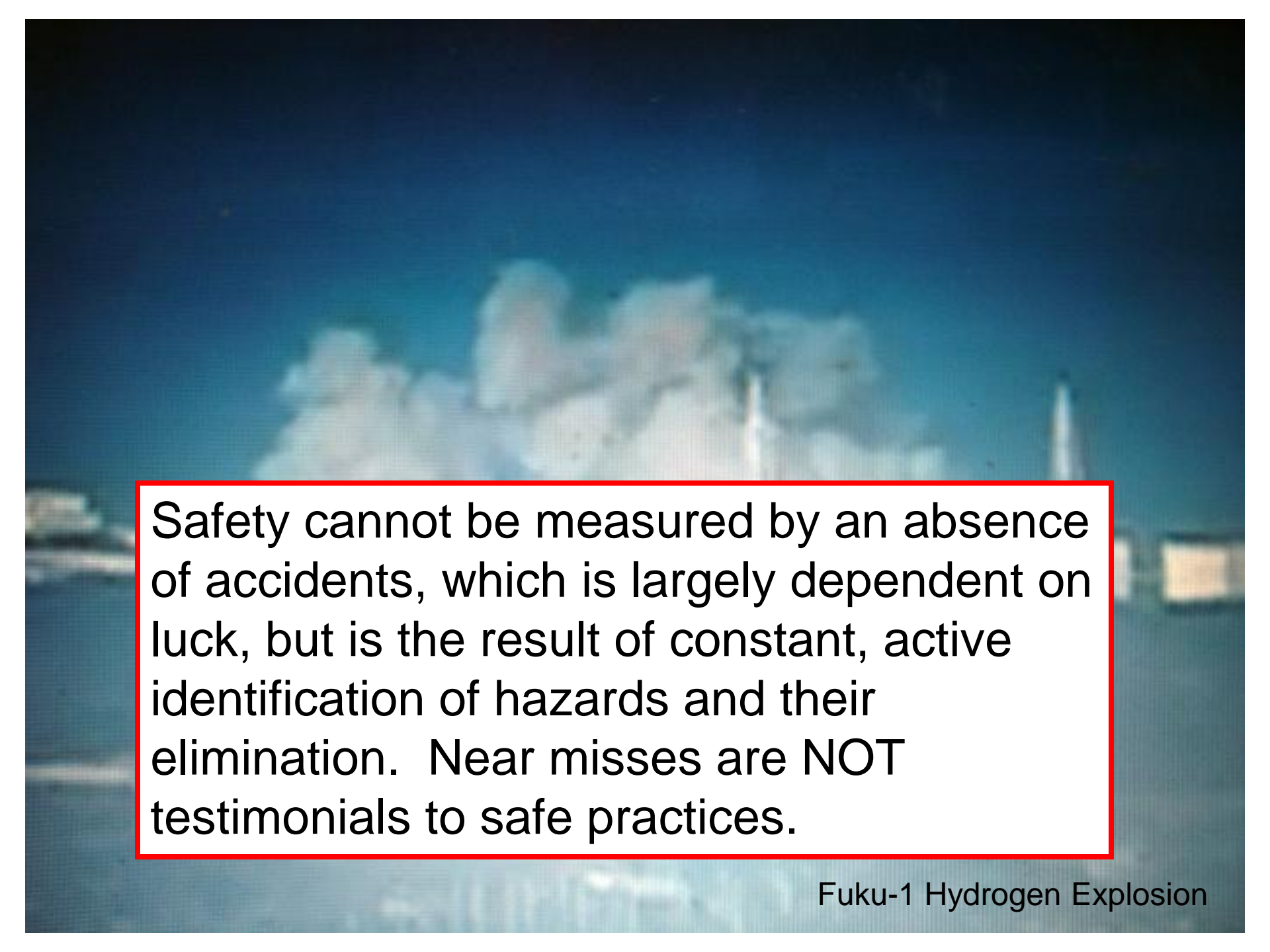
Uncertainty is not some noisy variation around a mean value that represents the true situation. Variation itself is nature's only irreducible essence. Variation is the hard reality, not a set of imperfect measures for a central tendency. Means and medians are the abstractions. All decisions, all risk assessments are made under uncertainty.

Fuku-1 Hydrogen Explosion



Too often risk is defined as **risk = likelihood * consequence** and **safety = 1-risk**.

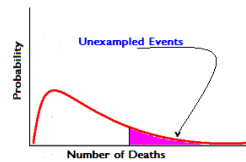
I disagree with this. Risk is thinking hard about likelihood and consequence, not simple multiplication and subtraction. Risk, likelihood, and consequence are normative, social notions, changing with situations and expectations, and must be assessed accordingly.



Safety cannot be measured by an absence of accidents, which is largely dependent on luck, but is the result of constant, active identification of hazards and their elimination. Near misses are NOT testimonials to safe practices.

The focus of WTS risk assessments is almost entirely on known system disturbances as initiating events, and static, sequential views of accident emergence and progression.

The result is that the attention of the risk analysts is not on unforeseen events.



Given that symptoms of system failure occur, attention will not be on the tail of the distributions where unforeseen events reside. There will be little experience in the organization for imagining scenarios that change critical assumptions, have slightly different symptoms, include multiple failures, or occur during times of high stress.

Moreover, the standard operational culture is focused on the procedures and rules for dealing with known disturbances and standard ways of solving problems. And rightly so, since without this focus on the checklists, procedures, and protocol, controllable situations can easily escalate out of control, and the daily safety of the facility impacted.

What we need, for lack of a better name, are **resilience engineers** to help the organization move from normal operational circumstances to emergency situations when needed.

To restate a central theme in this presentation, in WTS, given that there is an accident, chances are that the level of consequence is high and that the causes have not been modeled in the risk assessment.

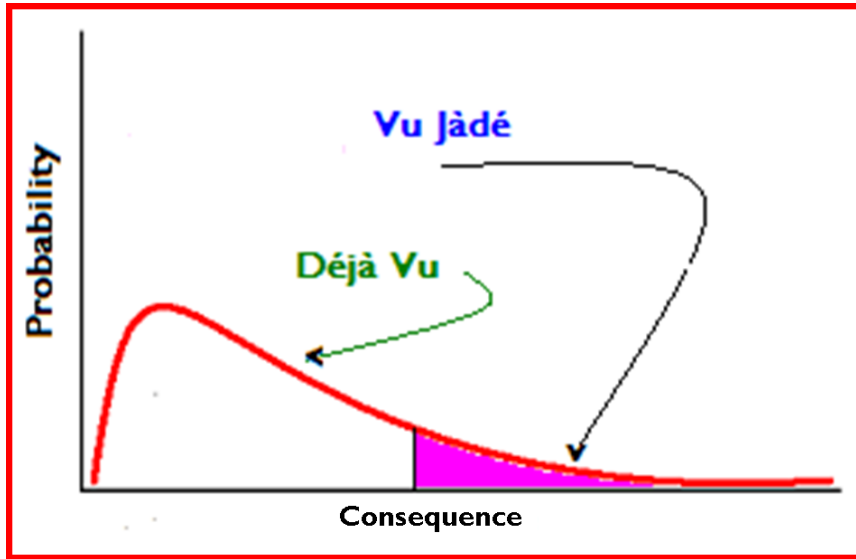
Resilience engineers, to be prepared for the unforeseen event, must constantly play with the model, question assumptions, run scenarios, and understand the uncertainty.

When there are initial indications or symptoms that a system may be going astray, resilience engineering moves the analysis away from the probable and into the possible.

Aircraft carriers, for example, have a bureaucratic hierarchical structure for normal functioning during slack times, a different structure built around expertise for "high tempo" periods of extended flight operations, and a third structure explicitly designed for emergencies.

LaPorte and Consolini (1991) describe a high tempo structure on carriers this way: "Contingencies may arise that threaten potential failures and increase the risk of harm and loss of operational capacity. In the face of such surprises, there is a need for rapid adjustment that can rarely be directed from hierarchical levels that are removed from the arena of operational problems. As would be expected, superiors have difficulty in comprehending enough about the technical or operational situation to intervene in a timely, confident way. In such times, organizational norms dictate noninterference with operators, who are expected to use considerable discretion."

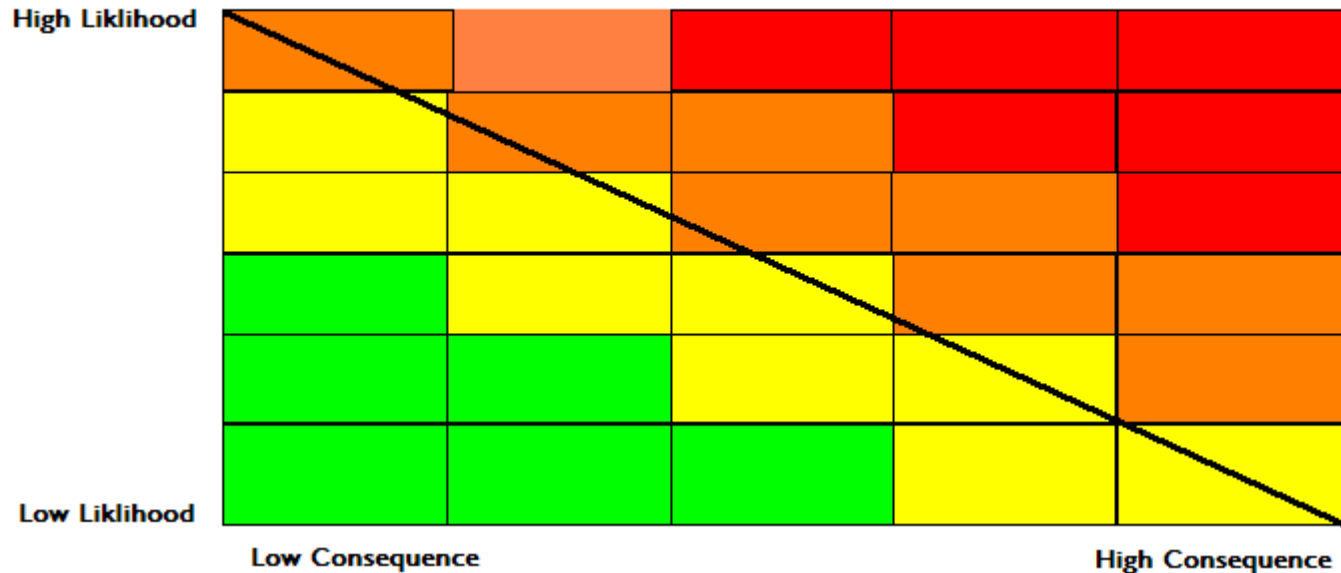
A Caveat: Resilience Engineers are different.



- The Art of Resilience
1. Experience
 2. Question Experience
 3. Intuition
 4. Improvisation
 5. Communication
 6. Examine Preconceptions
 7. Think Outside of the Box
 8. Take Advantage of Fortuitous Events

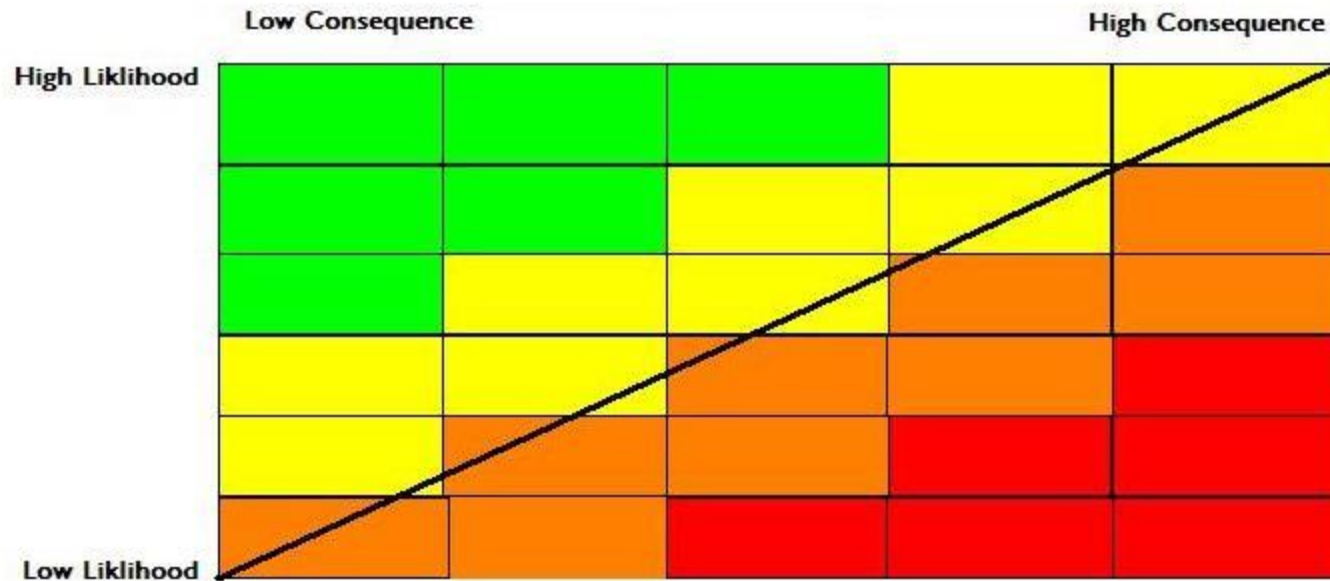
Individuals or groups that showed the traits enumerated above, are much different than individuals or groups whose work entails following strict protocols, procedures, and rules. In critical situations there may be clashes of these two different cultures. Resilience in an individual may meet with no internal resistance, however in a group, those who follow a rule, and those who improvise a tune, can often find themselves at odds.

The Standard Four Color Risk Matrix



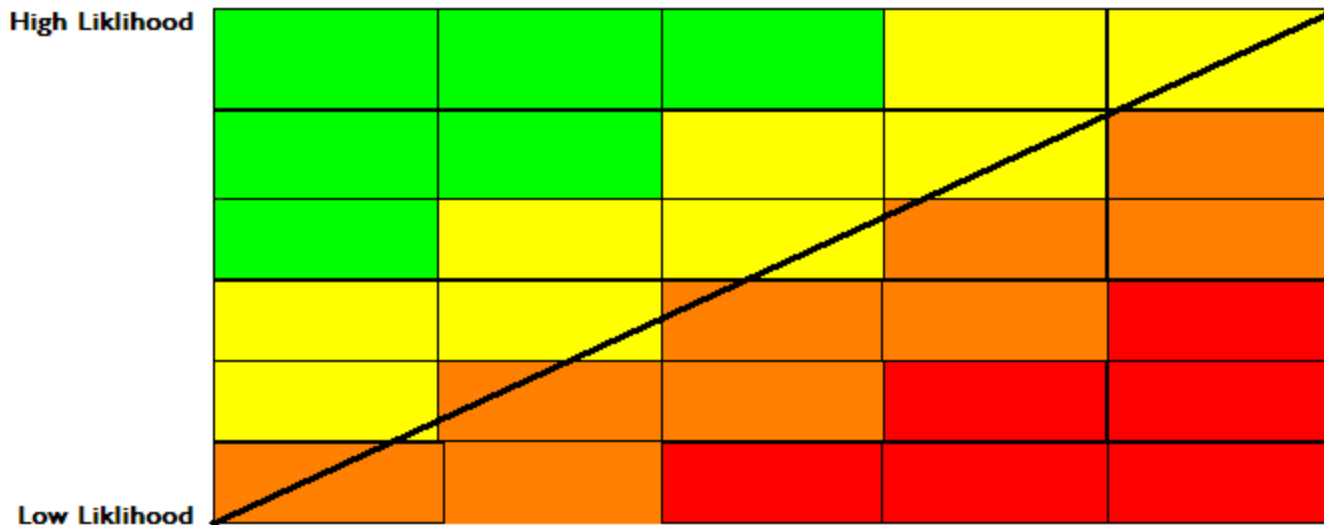
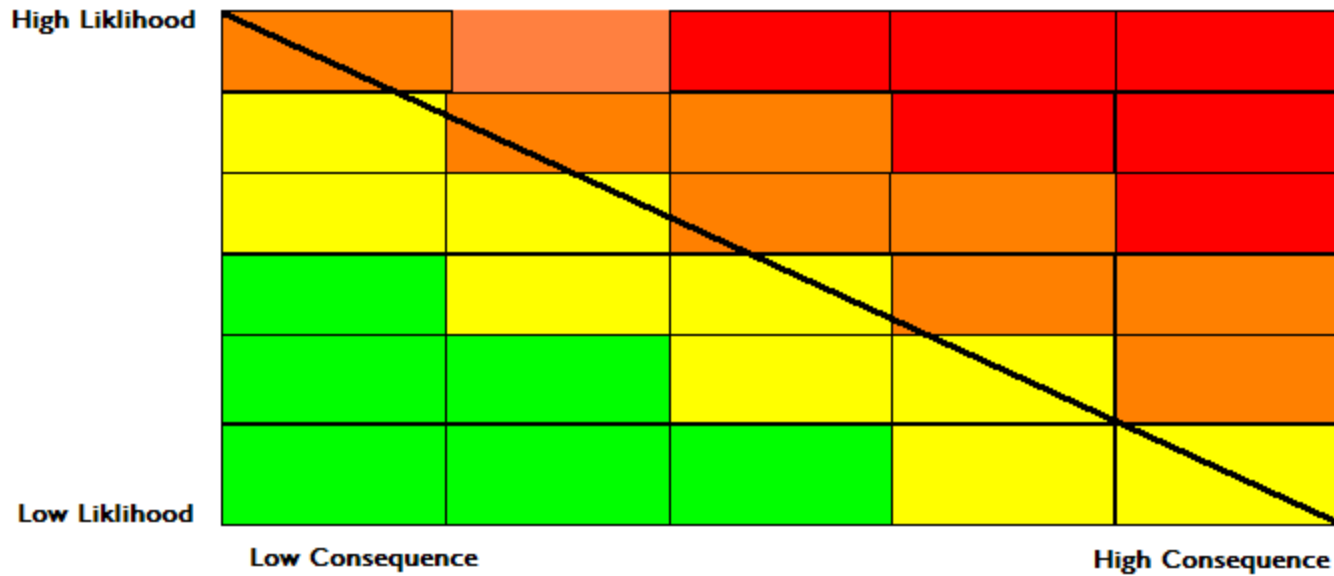
To illustrate, consider the four color matrix used by some organizations to understand where to focus resources to respond to risk.

Risk Matrix for Resilience Engineers



And here, is the mirror image of the standard matrix to illustrate where we must concentrate the resources during an emergency.

Risk Matrix for Standard Operations

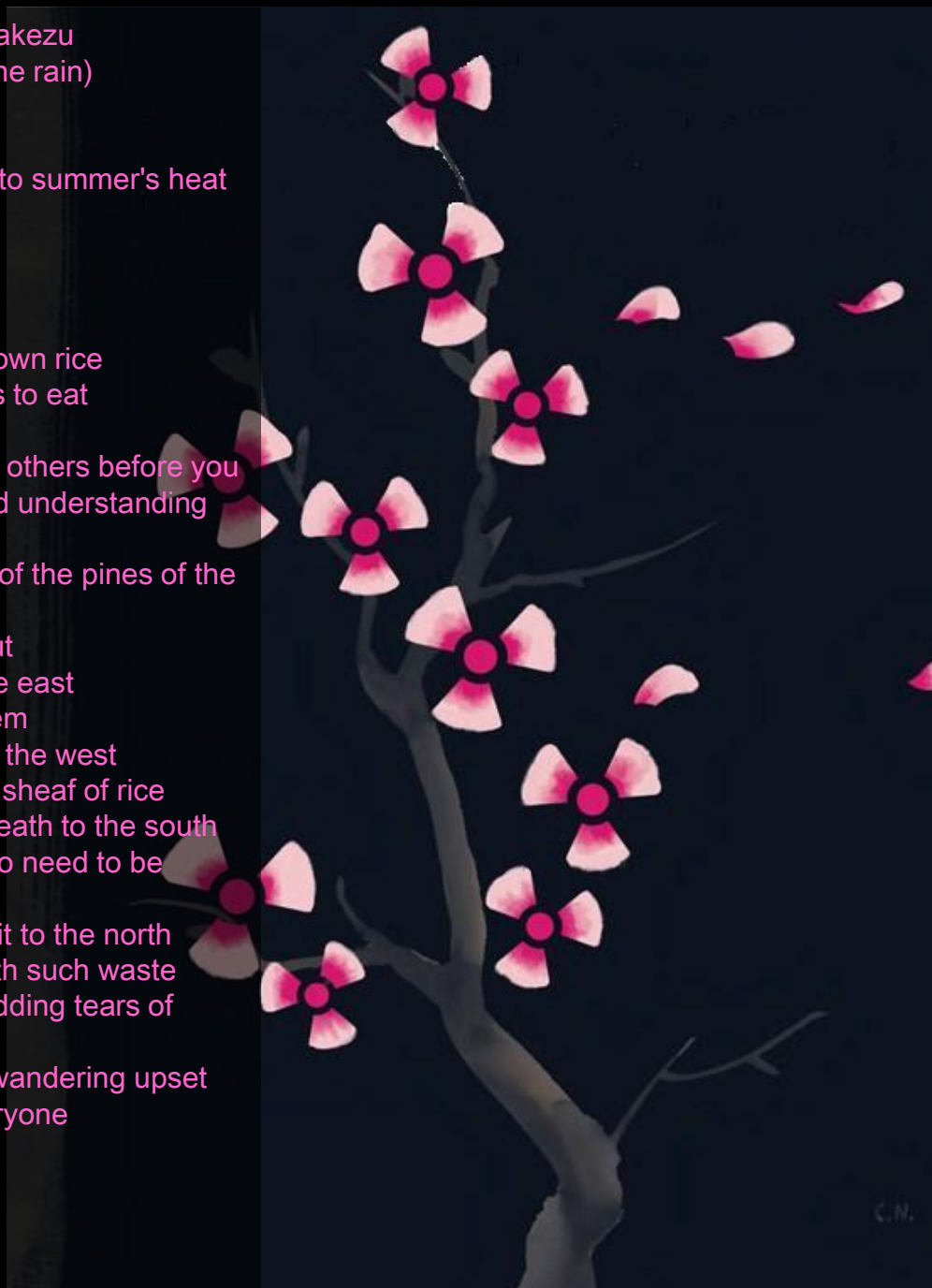


Risk Matrix for Emergencies

Can these two cultures coexist? Can one of these cultures be “proactively resilient”? I do not know the answers. But I do know, that without them both, we can be assured of future accidents with higher levels of consequence which impact lives, the environment, and the future for us all.

Ame ni mo makezu
(Not losing to the rain)

not losing to the rain
not losing to the wind
not losing to the snow nor to summer's heat
with a strong body
unfettered by desire
never losing temper
cultivating a quiet joy
every day four bowls of brown rice
miso and some vegetables to eat
in everything
count yourself last and put others before you
watching and listening, and understanding
and never forgetting
in the shade of the woods of the pines of the
fields
being in a little thatched hut
if there is a sick child to the east
going and nursing over them
if there is a tired mother to the west
going and shouldering her sheaf of rice
if there is someone near death to the south
going and saying there's no need to be
afraid
if there is a quarrel or a suit to the north
telling them to leave off with such waste
when there's drought, shedding tears of
sympathy
when the summer's cold, wandering upset
called a blockhead by everyone
without being praised
without being blamed
such a person
I want to become



Miyazawa Kenji
Poet of Tohoku
1896-1933