

Modeling the Resilience of and Risk to the Power-Grid  
Infrastructure and the Supportive Human and  
Organizations as Systems of Systems  
Presented at the

5<sup>th</sup> International Symposium  
on Resilient Control Systems

Yacov Y. Haimes, P.E., Ph.D.

[haimes@virginia.edu](mailto:haimes@virginia.edu)

L. R. Quarles Professor of Systems and Information Engineering  
and Founding Director (1987),

Center for Risk Management of Engineering Systems

University of Virginia

15 August 2012

## *Hurricane Katrina and the Nuclear Reactor Disaster in Japan*



<http://blogs.discovermagazine.com/>

### **Hurricane Katrina (August, 2005)**

- Worst natural disaster to ever hit U.S.
- Evacuation of 1 million residents
- Damage to electricity plants
- Damage to water treatment plants
- Severe losses by regional industries
- Risks augmented by institutional failure
- “Katrina was a **failure of initiative**”

### **Tsunami and Nuclear Crisis in Japan (March, 2011)**

- Earthquake and tsunami affected Fukushima Daiichi nuclear plant
- Explosion of nuclear reactors caused spread of radioactive particles
- Exclusion zone of 20 kilometers around the plant persists today
- Risks exacerbated by lack of governance
- “Catastrophe was **manmade**”



<http://beta.images.theglobeandmail.com/>

Natural disasters affect multiple entities—communities and infrastructures—not only because of the inherent interdependencies among cyber and physical infrastructures, but primarily because of the dependence of organizations on the effectiveness of humans, and on the leadership they provide to the organizations they serve and represent.

# Strategic Preparedness and Resilience

Strategic preparedness connotes a decisionmaking process and its associated actions, implemented in advance of a natural or human--induced disaster, aimed at reducing consequences (e.g., recovery time, community suffering, and cost) and/or controlling their likelihood to a level considered acceptable.

# Human-Cyber-Physical infrastructure systems

They are complex, systems of systems interconnected and interdependent cyber networks designed to achieve economies of scale, encompassing hardware, software, human involvement, protocols, connections to the Internet, culture, policies, and organizational procedures.

# Human-Cyber-Physical infrastructure as system of systems

Human-Cyber-Physical infrastructures as systems of systems, must be:

studied, modeled, its effective operation measured with appropriate data collection, and be subjected to a regular process of risk assessment, management, and communication.

# My Message

To highlight and explain the complexity of the modeling, definitions, and quantifications of the multidimensional:

vulnerability, resilience, and risk  
to

human-cyber-physical infrastructures  
as systems of systems

*Why do farmers irrigate their crops  
in non-rainy seasons?*

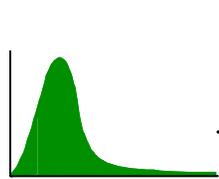
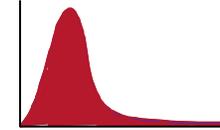
*The answer is fundamental to  
modeling and understanding the  
definitions of vulnerability and  
resilience of, and thus the risk to, a  
system.*

# **Exogenous Variables**

# **Random Variables**

*Price of fertilizer*

*Sunlight  
Precipitation*



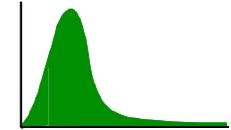
**Input**

*Water from  
upstream*



**Output**

*Crops yield*



**(Objectives)**

*Maximize profit  
Minimize soil erosion*

# **Decision Variables**

*When to irrigate and fertilize,  
And by how much?*



## Let Us Answer Basic Why-Questions:

1. Why is the question: “What is the resilience of system x is uninformative and unanswerable?”

## Let Us Answer Basic Why Questions:

1. Why is the question: What is the resilience of system  $x$  is uninformative and unanswerable?
2. Why a given immunization is effective for only specific infectious diseases?

## Let Us Answer Basic Why Questions:

1. Why is the question: What is the resilience of system x is uninformative and unanswerable?
2. Why a given immunization is effective for only specific infectious diseases?
3. Why is the question: “What is the vulnerability of system y is uninformative and unanswerable?”

## Let Us Answer Basic Why Questions:

1. Why is the question: What is the resilience of system  $x$  is uninformative and unanswerable?
2. Why a given immunization is effective for only specific infectious diseases?
3. Why is the question: What is the vulnerability of system  $y$  is uninformative and unanswerable?
4. Why is the resilience and vulnerability of a system are two sides of the same coin?

## More Basic Why-Questions:

5. Why a simple equation cannot represent the complex multidimensional the risk function?

## More Basic Why-Questions:

5. Why a simple equation cannot represent the complex multidimensional the risk function?
6. Why strategic preparedness and the resilience of a system are dual to each other?



## More Basic Why-Questions:

5. Why a simple equation cannot represent the complex multidimensional the risk function?
6. Why strategic preparedness and the resilience of a system are dual to each other?
7. Why did the criminal Osama bin-Laden and the Honorable U.S. Secretary of DHS share *seemingly* common objectives?

## More Basic Why-Questions:

5. Why a simple equation cannot represent the complex multidimensional the risk function?
6. Why strategic preparedness and the resilience of a system are dual to each other?
7. Why did the criminal Osama bin-Laden and the Honorable U.S. Secretary of DHS share *seemingly* common objectives?
8. What is the common denominator of all decisions made at all levels?

# Essential States of the System

*All decisions are made to control (retain or change as appropriate) the levels of the essential states of the system to meet specific desired outputs (goals and objectives)*

# States of a System

*Given a system's model, the states of a system are the smallest set of independent system variables such that the values of the members of the set at time  $t_0$  along with known inputs, decisions, random and exogenous variables completely determine the value of all system variables for all  $t \geq t_0$  (under certain conditions).*

# States of a System

*The selection of the appropriate number of state variables to represent the essence of the multiple perspectives of the system is among the most challenging and important tasks of systems modelers.*

# What is Vulnerability?

*Vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that if exploited by an adversary, or affected by a harmful initiating event, can result in adverse consequences to that system.*

*The vulnerability of a system is a vector that is a function of the specific initiating event (or threat) and the time frame.*

# Emergent Forced Changes

*The term emergent forced changes connotes:*

*external or internal sources of risk to a system that may adversely affect or enhance specific states of that system, and consequently, affect the system as a whole.*

# The Epistemology of Vulnerability as Manifestation of the States of the System

*Knowledge of the state (vector)  $x(t_0)$  of a system at time  $t_0$  together with the input (emergent forced changes)  $u(t)$ , for  $t \geq t_0$ , determines the vulnerability  $v(t, u)$  of the system for all  $t \geq t_0$ .*

# Vulnerability: An Example

*The human body is vulnerable to infectious diseases. Different organs are continuously bombarded by a variety of bacteria, viruses, and other pathogens.*

*However, only a subset of the human body is vulnerable to the threats from a subset of the would-be attackers, and due to our immune system (resilience) only a smaller subset of the body would experience adverse effects.*

# What is Resilience?

*The resilience of a system is also a manifestation of the states of the system. It is a vector that is time and initiating-event (or threat) dependent.*



# What Does Resilience Mean?

*Resilience represents the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable composite "cost" and time.*



# In Sum: Vulnerability and Resilience

*The questions:*

*“What is the **vulnerability** of the water system in Salt Lake City?”*

*“What is the **resilience** of the water system in Salt Lake City?”*

*These questions are **uninformative** and, thus, are **unanswerable**.*

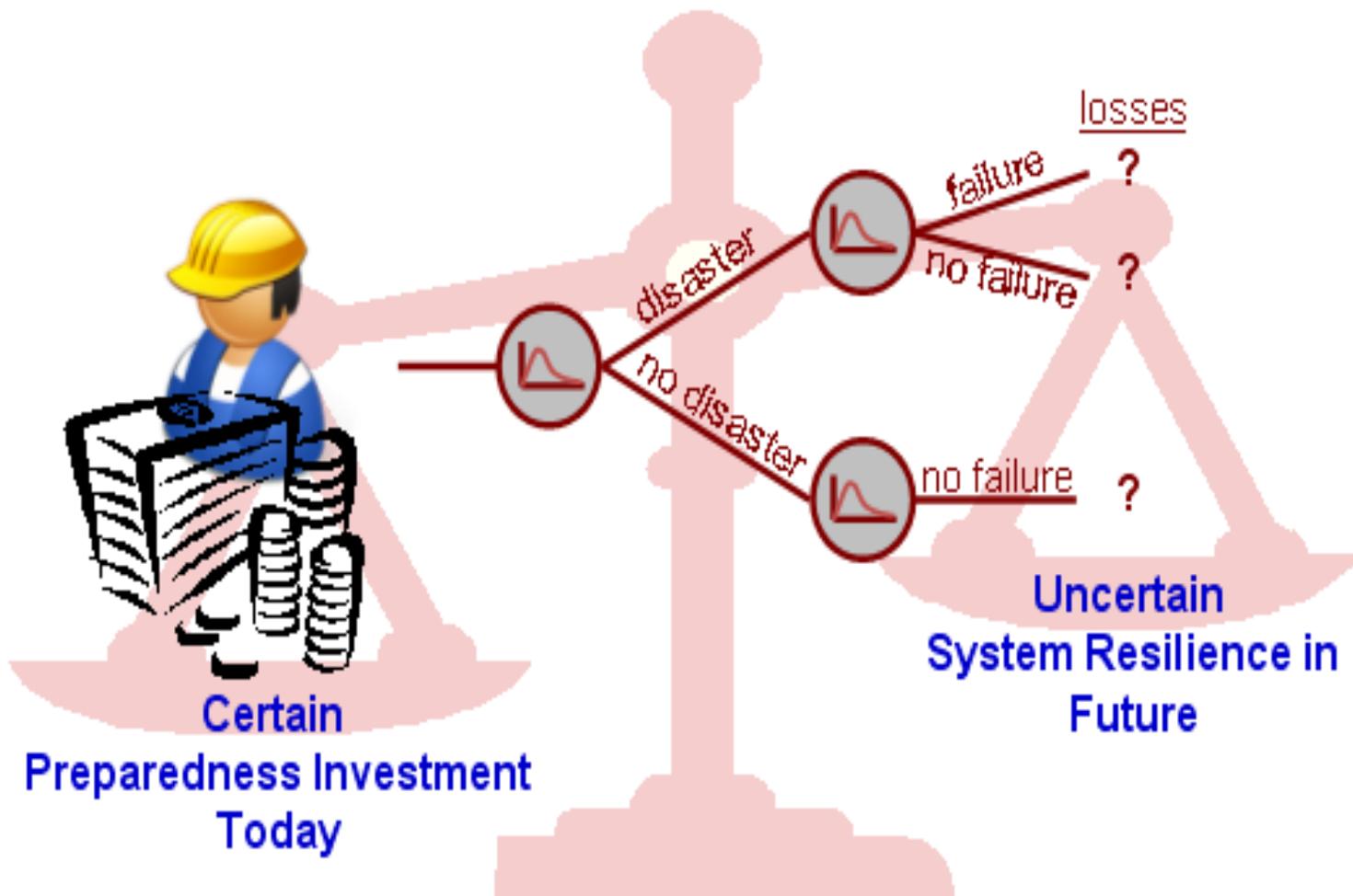
*To answer them we need to know the specific emergent forced changes (threat) and the states of the water system at time  $t$ .*



*In other words:  
The vulnerability and resilience of a  
system*

*Are both manifestations of the states  
of the systems*

*They are two sides of the same coin.*



# Emergent Forced Changes

*The term emergent forced changes connotes:*

*external or internal sources of risk to a system that may adversely affect or enhance specific states of that system, and consequently, affect the system as a whole.*



# Emergent Forced Changes

*Government agencies, the military, the private sector, and major corporations—all seek to understand the trends of risks associated with forced changes that affect the states of their systems, in order to prevent, mitigate, or prepare for undesirable future occurrences.*

# Emergent Forced Changes

*Unanticipated, undetected, misunderstood or ignored emergent forced changes, whether they originate from within or from outside a system, are likely to affect a multitude of states of that system with potentially adverse consequences.*

*Therefore, it is imperative to be able--through scenario structuring, modeling and risk analysis--to envision, discover, and track emergent forced changes.*



# William W. Lowrance

In his book: *Of Acceptable Risk* [1976], Lowrance introduce the following definition of risk:

“a measure of the *probability and severity of adverse effects*”

The following questions commonly arise:

This definition of risk can be interpreted in two ways at the same time:

(1) in terms of the probability of a threat causing adverse effects, and

(2) in terms of the probability of the *severity* of the resulting adverse effects, given a threat.

Both definitions are valid; however, each represents significantly varied conceptual and theoretical challenges.

# Consider the Following Projected Consequences from a Natural Disaster:

1. Fatalities
2. Critical Injuries
3. Homeless Communities
4. Millions of People Without Electric Power
5. Billions of Dollars Loss to Business
6. Billions of Dollars Loss to the Regional Economy

*Question: Can we augment all of the above  
with one metric? One equation?*

# Components of the Risk Function

*(i) The time frame*

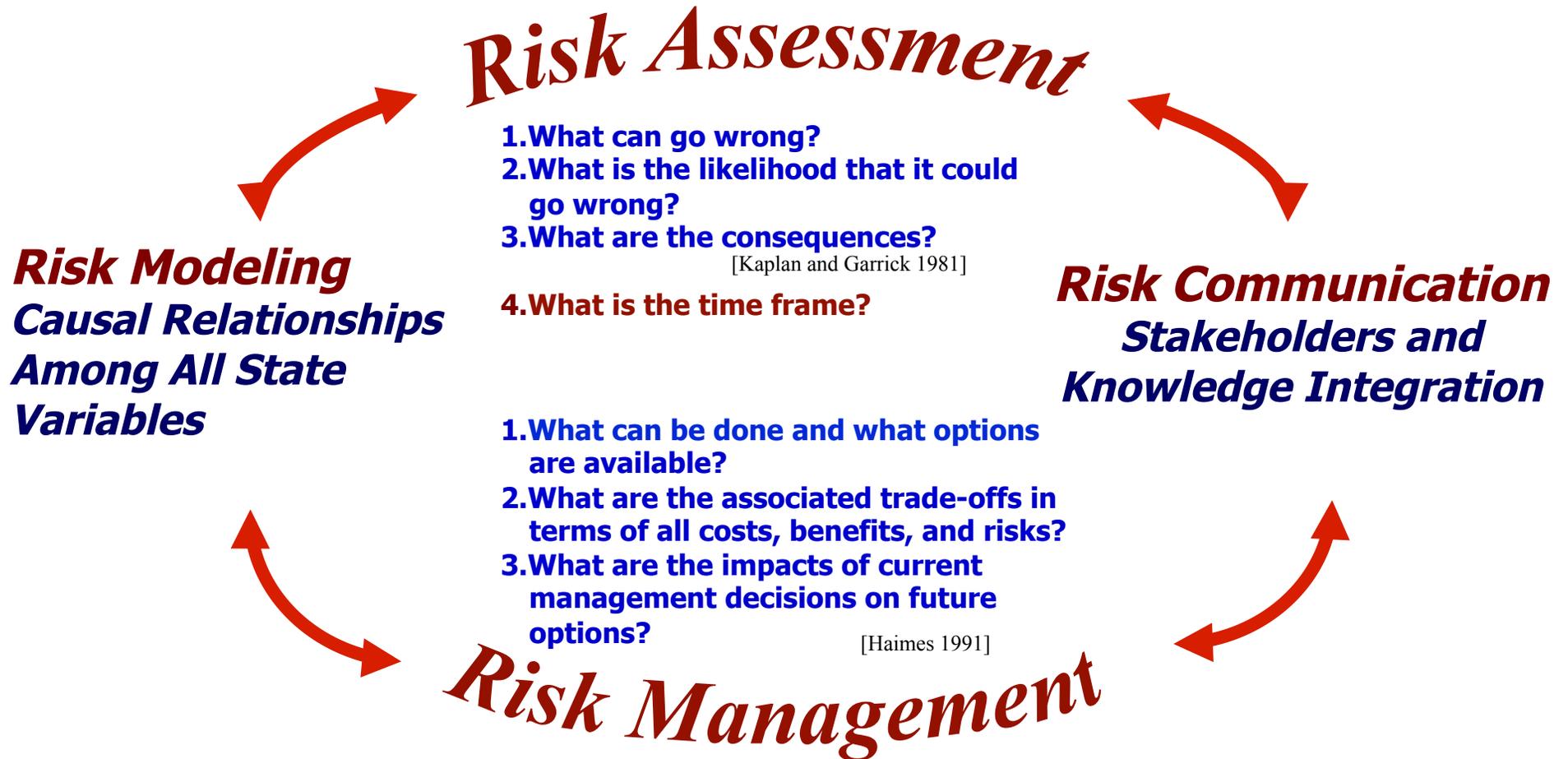
*(ii) the probability of the threat (emerging forced changes) and of its specificity (probability of the consequences)*

*(iii) the vector of the states of the system (including its performance capability, vulnerability, and resilience)*

*(iv) the vector of the resulting consequences*



# The Process of Risk Modeling, Assessment, and Management through Risk Communication



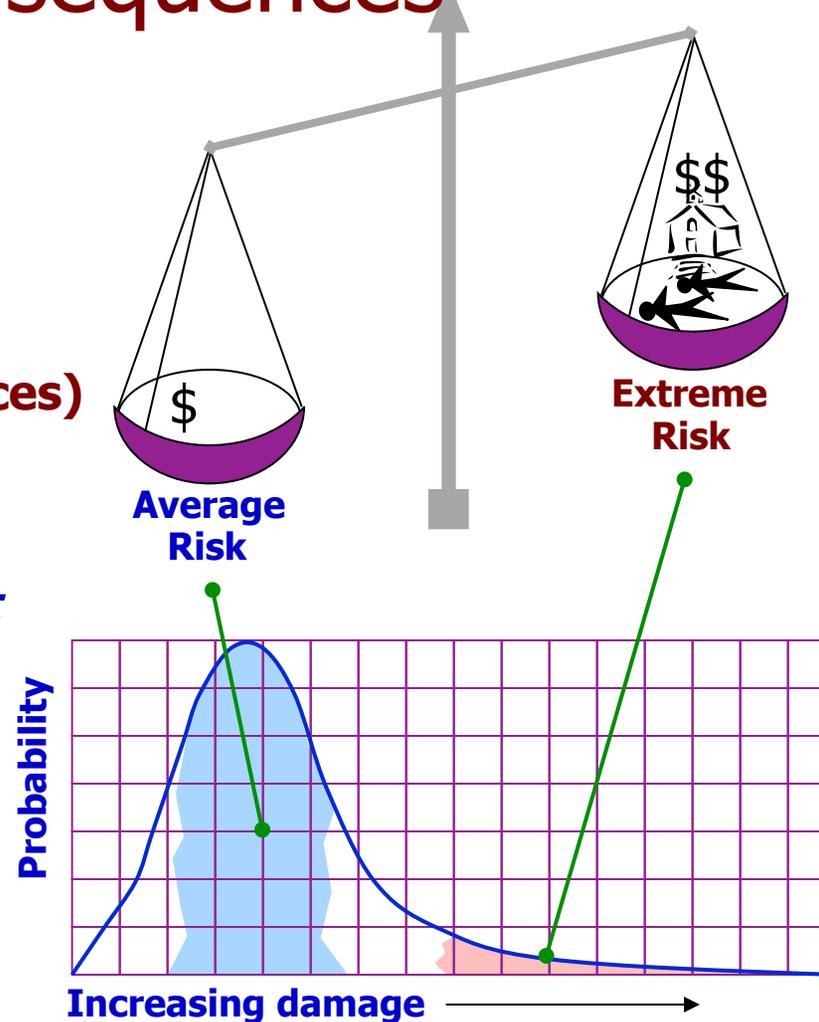
# Risk of Low Probability and Extreme Consequences

**Risk =  $f$ (Probability, Damage)**

or

**Risk =  $f$ (Likelihood, Consequences)**

*The fallacy of the expected value of risk as the sole metric for risk measurement*



# SAFETY

The level of risk that is deemed acceptable

William W. Lowrance, 1976

# A Most Challenging and Probably Unanswerable Question

*Who should decide  
On acceptability  
of what risks  
for whom,  
and in what terms,  
and why?*

*William Lowrence, Acceptable Risk, 1976*

# References

- Haimes Y. Y. Phantom System Models and the art and science of modeling systems of systems. *Systems Engineering* 2012; **15**(3): 333-346.
- Haimes Y. Y. Systems-Based Guiding Principles for Risk Modeling, Planning, Assessment, Management, and Communication. *Risk Analysis*, 2012; **32**(8):
- Haimes Y. Y. On the complex quantification of risk: Perspective on terrorism analysis. *Risk Analysis*, 2011; **31**(8): 1175-1186.
- Haimes Y.Y. *Risk Modeling, Assessment, and Management*, Third Edition. New York: Wiley, 2009.
- Haimes, Y.Y. A System-Based Approach to Preparedness for, Response to, and Recovery from Natural and Man-Made Disasters” *ASCE Leadership and Management in Engineering*, 2012.