LECTURE 9: INTRODUCTION TO RISK MANAGEMENT

Yeganeh M. Hayeri
SYS 660
Spring 2019

INTRODUCTION TO RISK MANAGEMENT

Definitions and examples of risk

Questions of risk management

Risk identification

Risk assessment

Risk prioritization

The fallacy of expected value

Risk management actions

Risk Filtering, Ranking, and Management (RFRM)

DEFINITION OF RISK

A *Risk* is defined as the probability and severity of an adverse event

Risk is fundamentally a two-dimensional metric

For example if we are considering the risk of a major earthquake in southern California we would like to know:

- How likely is a major earthquake?
- What would the consequences be of such an earthquake? Loss of life? Property damage? Lost production?

We can't assess a risk without considering both

- We wouldn't be very concerned with a high probability event that has very little consequence
- We may be very concerned with an unlikely event that has severe consequences

EXAMPLES OF RISK

Risk is measured in slightly differently ways depending on the domain

Here are just a few examples:

Finance:

- Risk as the volatility of an asset's price
- Default risk
- Systematic risk (CAPM – Capital Asset Pricing Model)

Project management:

- Schedule Risk
- Cost Risk
- Technical Risk

Risk of extreme events

- Risk of a catastrophic system failure
- Risk of a natural disaster
- Risk of a terrorist attack

QUESTIONS OF RISK MANAGEMENT

Kaplan and Garrick (1981) define the three questions of risk assessment:

1. What can go wrong?
2. What is the likelihood that it would go wrong?
3. What are the consequences?

Haimes (1991) defines the three questions of risk management:

1. What can be done?
2. What are the options available, and what are their associated trade-offs in terms of all costs, benefits, and risks?
3. What are the impacts of current management decisions on future options?

Sources: Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*, 11–27, and Haimes, Y. Y., (1991) "Total risk management." *Risk Analysis*, 11(2), 169–171.

THE CHALLENGES OF RISK MANAGEMENT

While risk management is straightforward in principle, the challenges arise in execution

Challenges of quantification:

- There are often insufficient data with which to create credible quantitative estimates of probability and consequence
- Recall the difficulties we discussed with assessing subjective probabilities
- As a result, people often resort to qualitative methods of questionable validity

Challenges of prioritizing over a two-dimensional metric

- To prioritize risks, one must make tradeoffs between probability and severity
- Different stakeholders may have very different perspectives

Challenges of agency

- Often risks are not borne equally
- A given action may be low risk to an individual or organization but increase the overall risk to society
- E.g., too big to fail

RISK MANAGEMENT IN SHORT

Different sources break out the steps of risk management in different ways, but all of them need to accomplish these four basic goals:

- Identify the risks
- Assess the risks
- Prioritize the risks
- Address the risks

In subsequent lectures, we will discuss some of the domain specific issues of risk management for

- Project risk management
- Financial risks to projects
- Risk of extreme events

For the remainder of this lecture we will consider some general purpose issues and approaches

RISK IDENTIFICATION

There are many techniques for risk identification

Often they are oriented toward a particular application domain

We will briefly cover five approaches to provide a broad sample

- Failure Modes and Effects with Criticality Analysis (FMECA)
- Fault Trees
- Event Trees
- Hazard and operability study (HAZOP)
- Hierarchical Holographic Modeling (HHM)

It should be noted that some of these techniques cover more than just risk identification

FMECA

FMECA stands for Failure Modes and Effects with Criticality Analysis

It is a very common technique in reliability engineering

First decompose the system in question into its hierarchical structure:

- Subsystem, assembly, component, part, etc.
- The depth can be varied to trade effort for thoroughness

Presumably, all of the parts of the system must work for the system to work

Identify the different ways in which each part can fail (i.e., the failure modes)

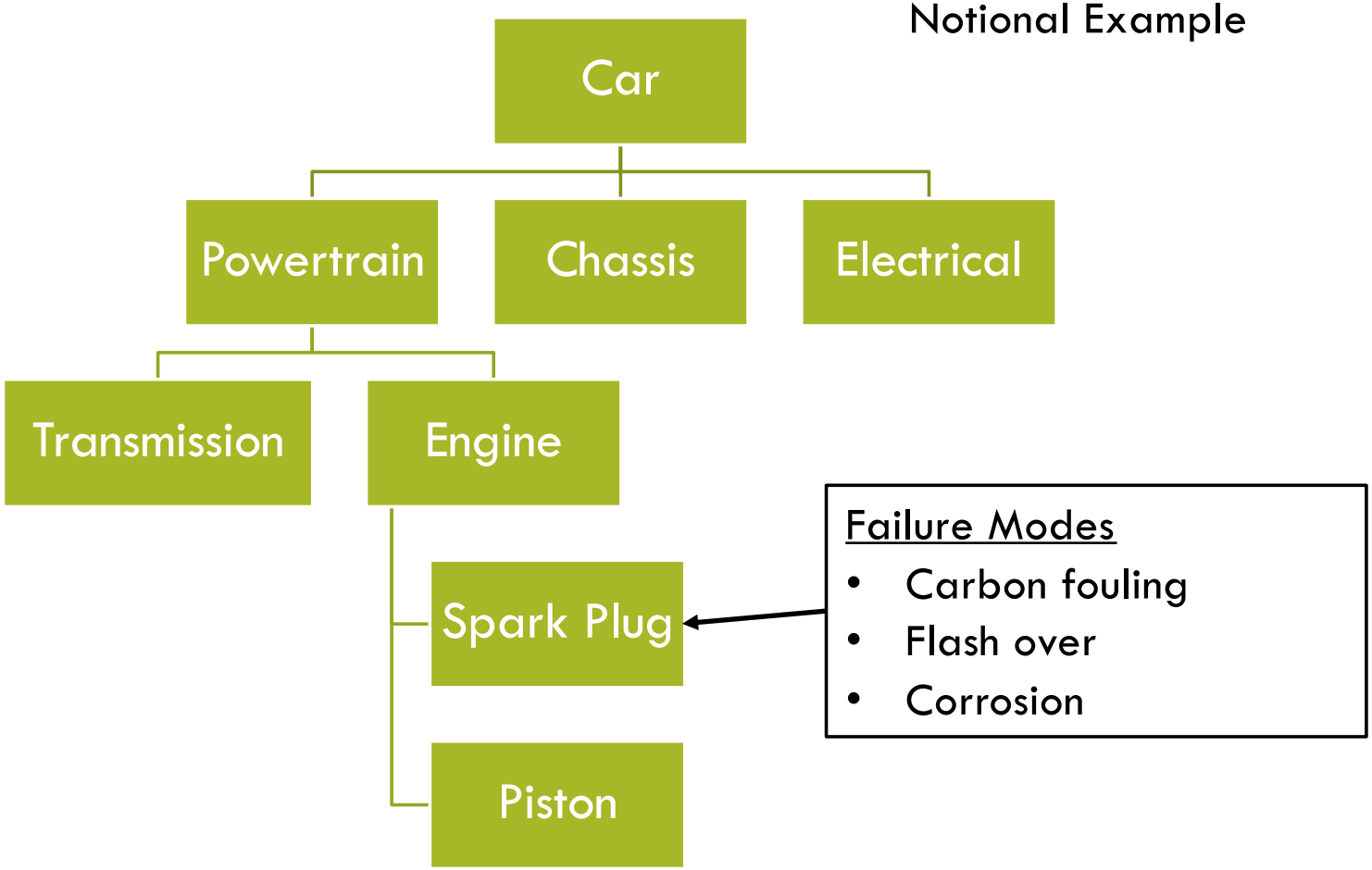
Identify the effects of each failure

Assess the probability, consequence, and detectability of each failure mode

Prioritize failure modes by these assessments

EXAMPLE: FMECA

Notional Example



FMECA

There are several different variations on FMECA

Some of these variations take different approaches as to how the risks are quantified and prioritized

This is the “criticality” portion of the assessment

A common approach is to make ordinal assessments of probability and severity and then multiply them together

- Recall the issues with multiplying ordinal numbers we discussed in the first lecture

But this does not have to be the case. Alternatives are available.

FMECA is good for generating a large number of potential failure modes but can miss system failures triggered by multiple, independent component failures

FAULT TREES

Fault trees are a classic risk analysis tool

To build a fault tree, start with the undesirable event and work backwards to determine all the different ways it could happen

- E.g. the catastrophic meltdown of a nuclear reactor

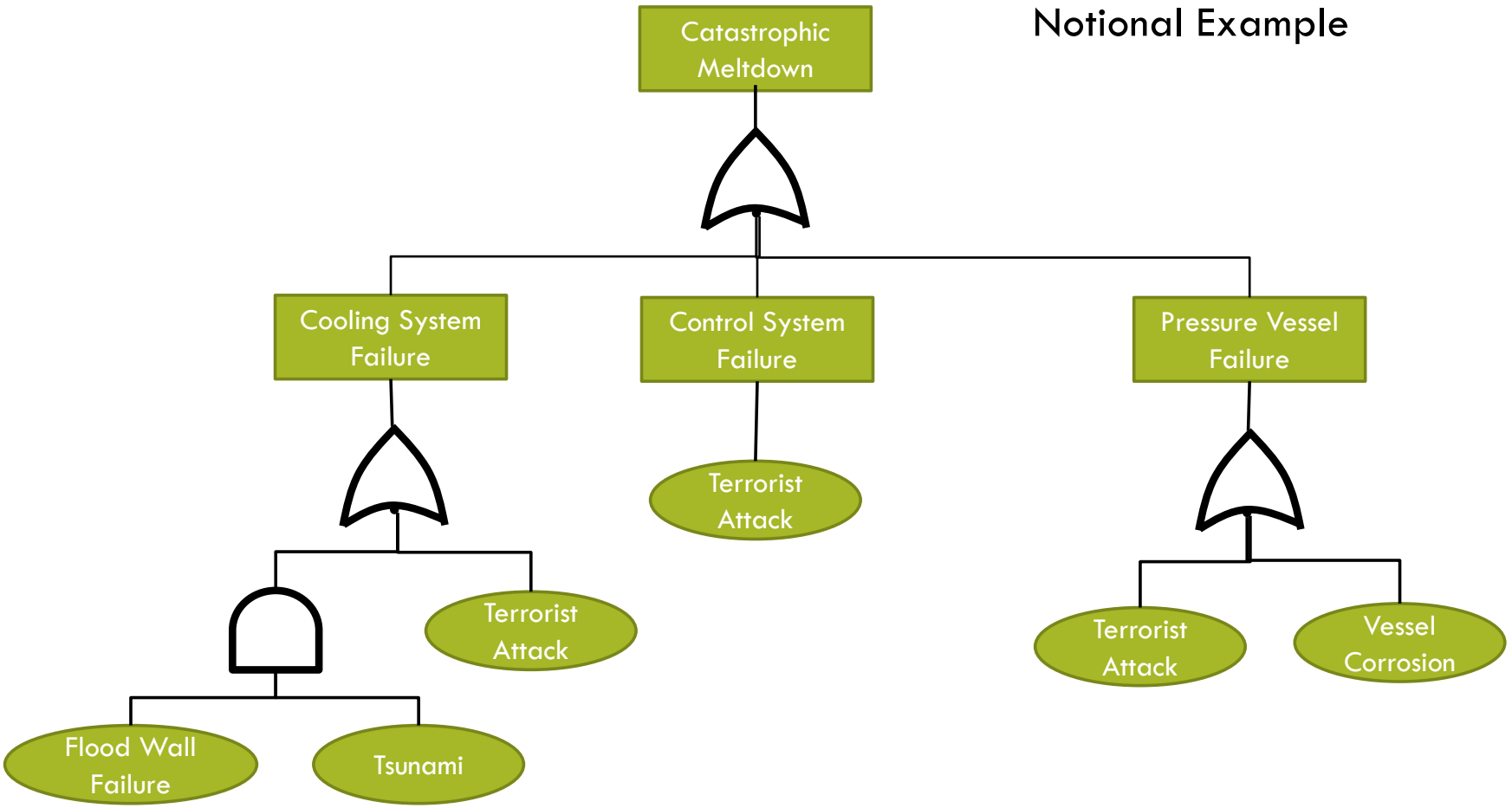
Boolean logic is used to combine lower-level events into higher-level events

This results in a tree-like structure

When probabilities are assigned to the initiating events, the probability of the top event can be calculated

Fault trees are good for identifying failure modes that result from multiple independent failures

EXAMPLE: FAULT TREES



EVENT TREES

Event trees are similar to fault trees only they start from initiating events and work the other way

We ask the question "What can go wrong" and then follow the chain of consequences to the set of possible outcomes

For example:

- What would happen if the hospital's power supply failed?
- Presumably there are backup systems and protocols in place to handle such scenarios
- We could then consider scenarios when these backups work or fail, etc.
- We might also be able to identify scenarios where there is currently no backup or redundancy to mitigate the failure

HAZOP

Hazard and Operability Study (HAZOP) is a technique that originated in the chemical industry

It analyzes a system in terms of the functions that the system provides and then asks about a deviation in each function

- For example, what if there were too much flow in this pipe?
- What are the consequences of too much flow?
- What could cause too much flow?

To think of it another way:

- Event trees start with initiating events and follow them forward in time to intermediate events to consequence events
- Fault trees start with consequence events and follow them backward in time to intermediate events to initiating events
- HAZOP starts with intermediate events and follows them forward and backward to consequence events and initiating events

HIERARCHICAL HOLOGRAPHIC MODELING (HHM)

HHM is technique for modeling a system from multiple perspectives

Originally developed by Haimes (1981) as a tool for systems engineering

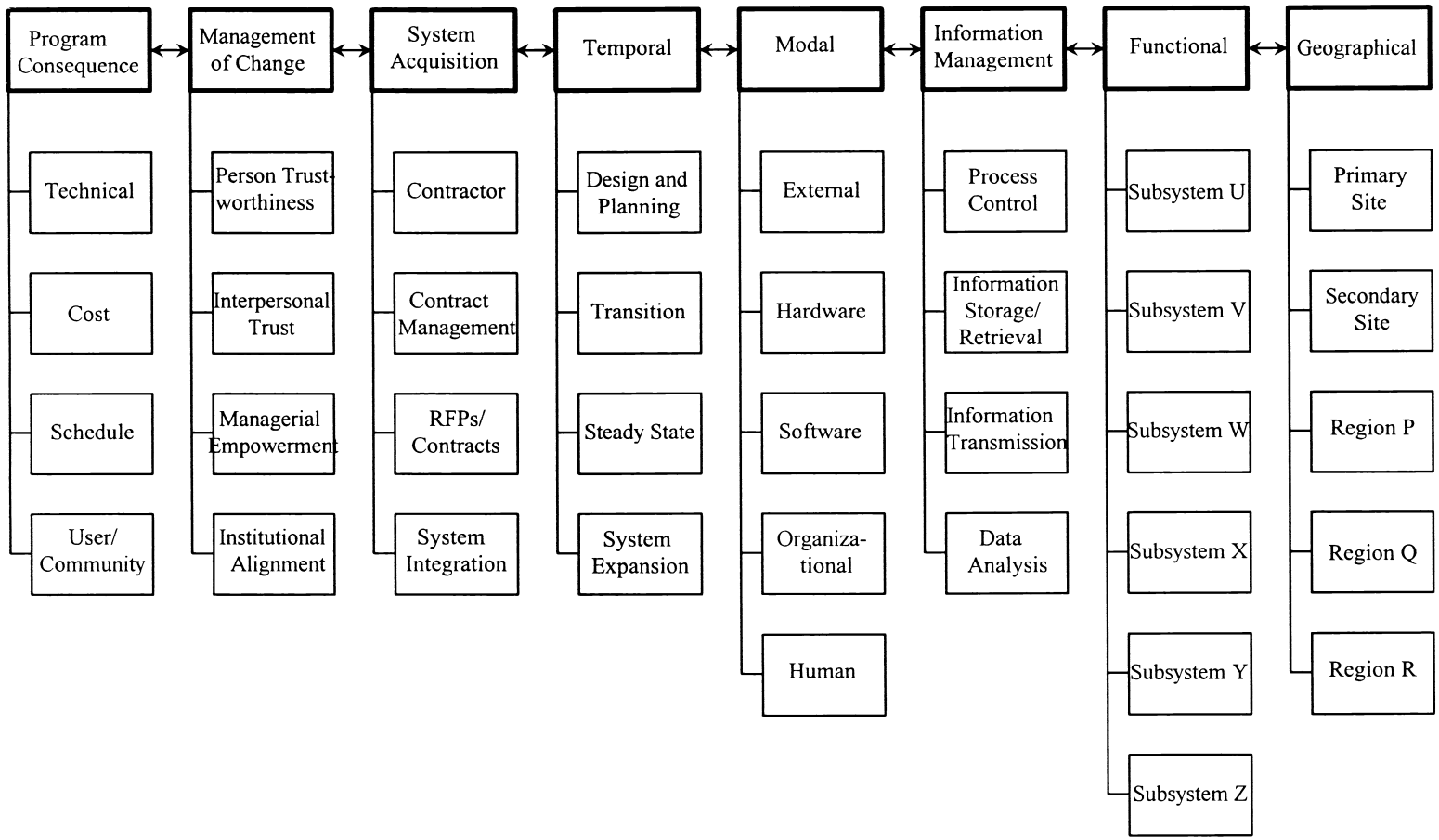
A system is modeled via multiple hierarchical structures, each from a different perspective such as organizational, physical, geographic, cost, functional, etc.

The hierarchical structure lends itself to risk identification in a manner similar to FMECA

However, since it views a system from more perspectives than just the physical, it can be used to identify more "failure modes" than FMECA

Source: Haimes, Y.Y., 1981, Hierarchical holographic modeling, *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 11, no. 9, pp. 606-616.

EXAMPLE: HHM



Source: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

RISK SCENARIOS

All of the techniques discussed are different approaches to identifying risk scenarios

Each has advantages and disadvantages depending upon the type of system and the risks of concern

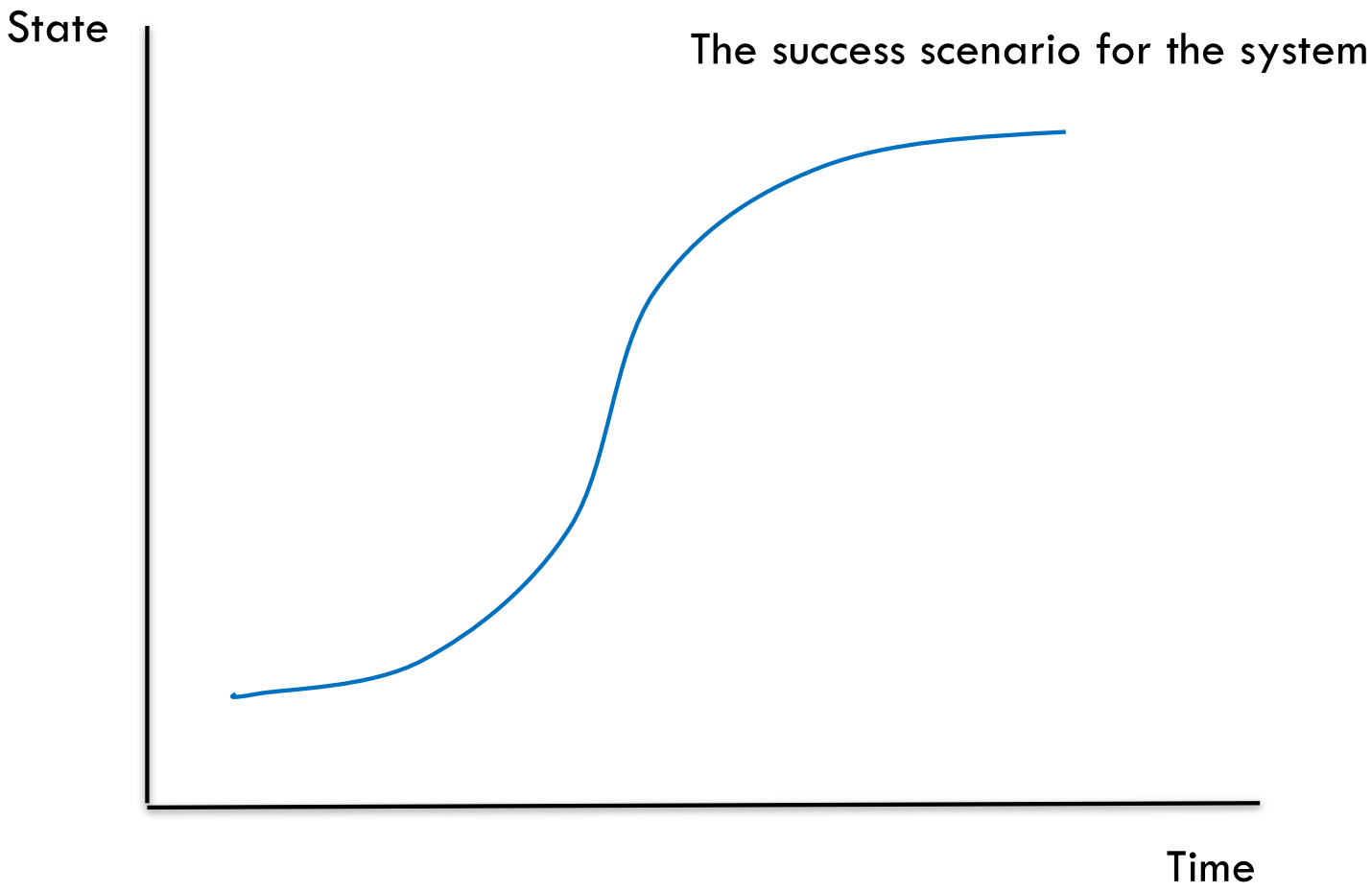
- For safety critical systems, one should use more than one technique

More broadly, identifying risk scenarios falls under the theory of scenario structuring (Kaplan, Haimes, and Garrick, 2001)*

Each of these techniques can be understood as identifying different trajectories through the state space of the system

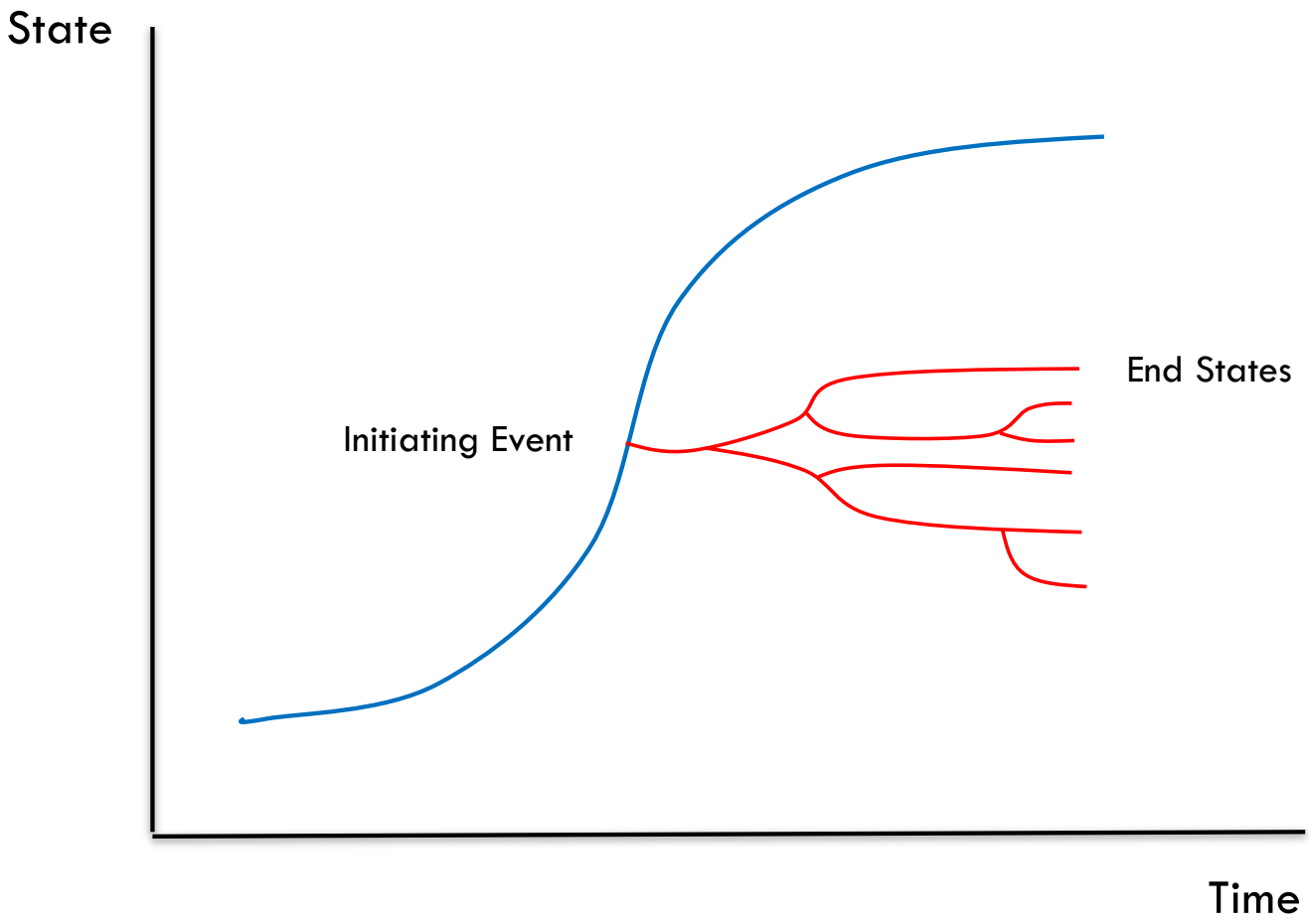
*Source: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

THE SUCCESS SCENARIO



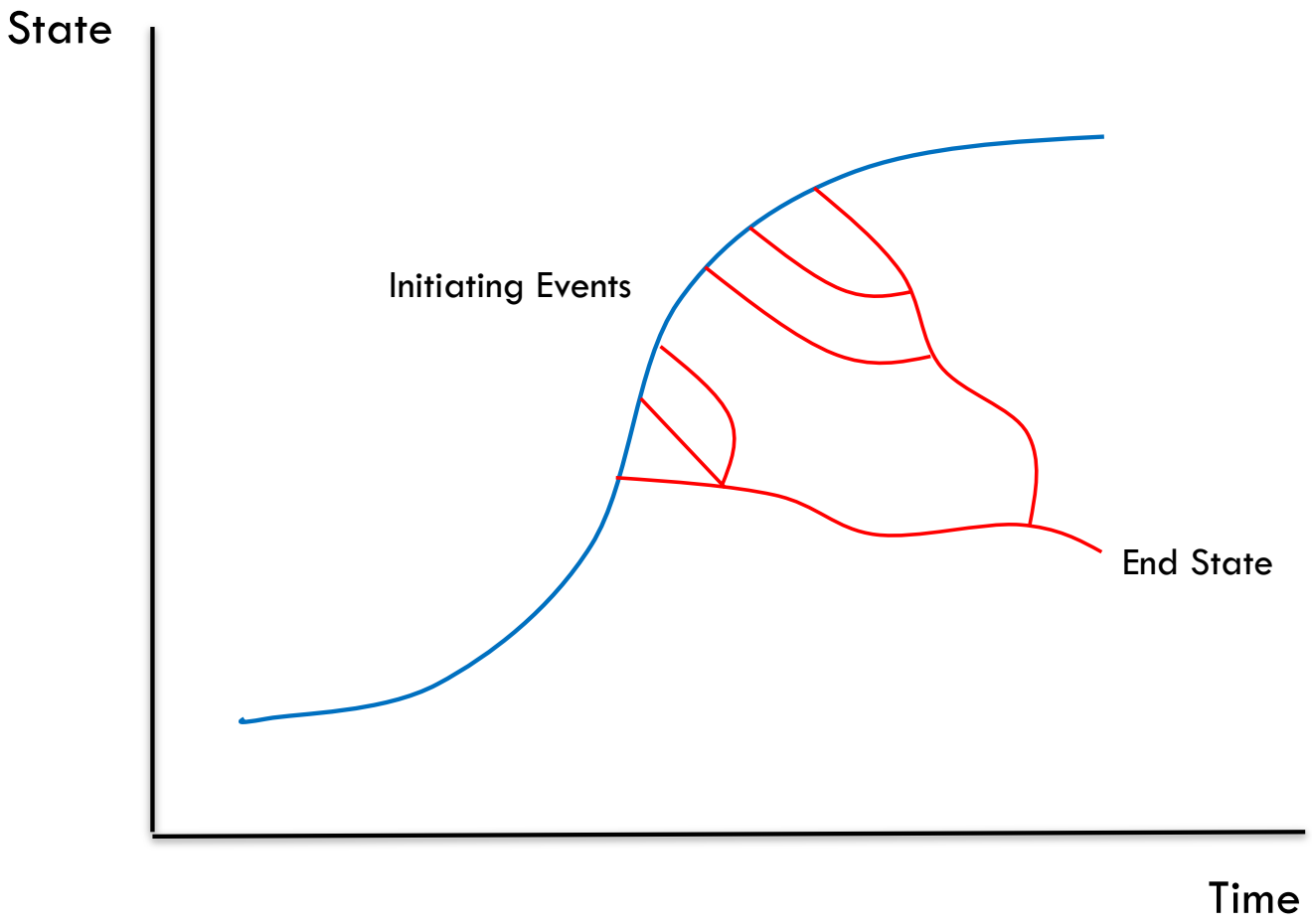
Adapted from: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

EVENT TREE AS A SCENARIO



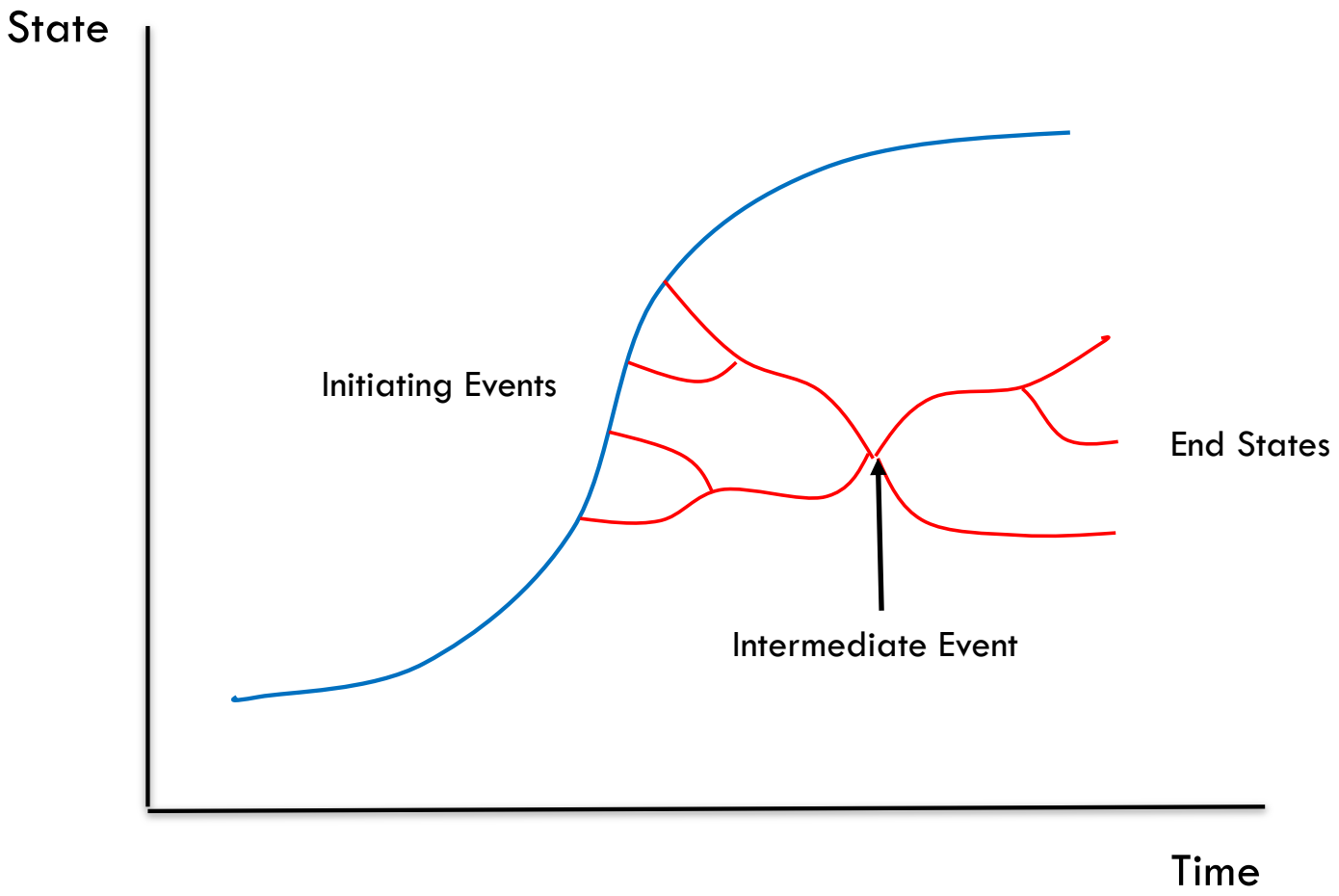
Adapted from: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

FAULT TREE AS A SCENARIO



Adapted from: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

HAZOP AS A SCENARIO



Adapted from: Kaplan, S., Y.Y. Haimes, and B. J. Garrick, 2001, Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, 21(5), 807-819.

ASSESSING RISKS

Assessing risks involves quantifying the likelihood and consequence of each identified risk scenario

- Ideally you would like a probability distribution based on empirical data

In this class, we have discussed how difficult it can be to obtain such a distribution

Common approaches include:

- Historical data
- Modeling and simulation
- Expert assessment of subjective probabilities
- Ordinal assessment of likelihood and consequence

The approach will vary depending on the circumstances

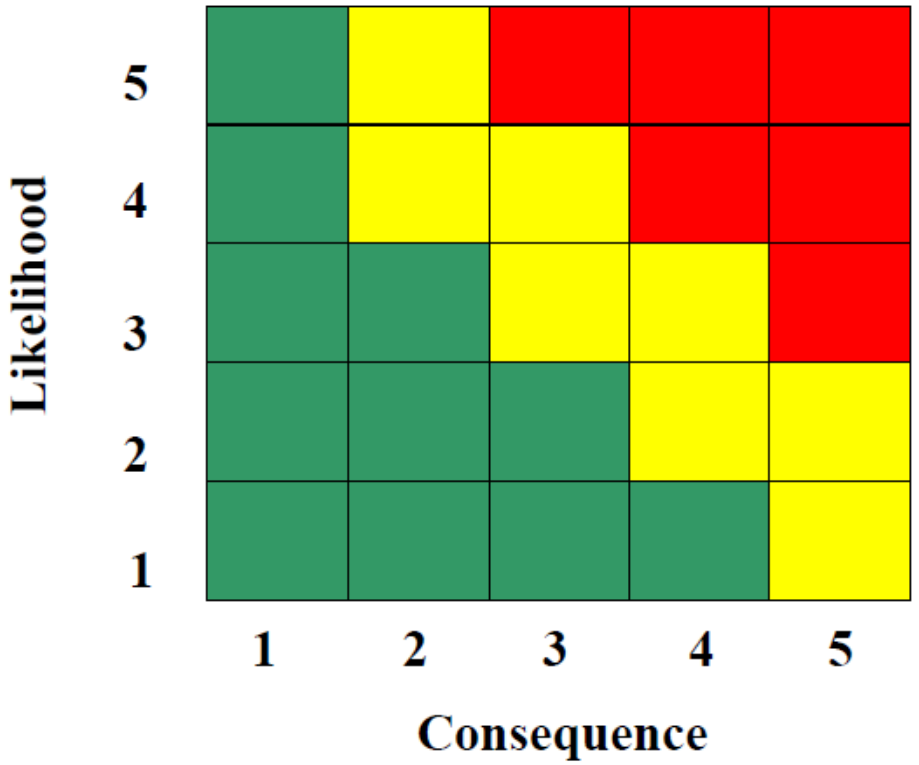
ASSESSING RISKS

A common, general purpose approach for risk assessments to use an ordinal risk matrix

We will discuss this approach more later on

To make the matrix useful, you need to assign context specific descriptions of the consequences

It should be noted that there are significant limitations to this approach that we will discuss in greater detail in the next lecture



Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

PRIORITIZING RISKS

Resources are limited, and not all risks can be addressed

Prioritization is necessarily to ensure the best possible use of scarce resources

Since risk is a two dimensional metric, risk prioritization is a multi-objective decision problem that requires making trade offs

We have spent a large portion of this class discussing how that can be done

Unfortunately, it is all too common to see risks prioritized by expected value

THE FALLACY OF EXPECTED VALUE

In many handbooks you will see risk defined as

- Risk = probability × consequence

Risks are then rank ordered by their expected value

This metric implies risk neutrality

As we discussed during our coverage of utility theory and prospect theory, most people are not risk neutral when it comes to losses

Expected value implicitly gives the same weight to low probability, high-consequence events as it does to high-probability, low consequence events

It also neglects the practical implications of variance

THE FALLACY OF EXPECTED VALUE

What would life be like if:

- Our highways were constructed to accommodate the average traffic load of vehicles of average weight
- Mass transit systems were designed to move only the average number of passengers during each hour of the day
- Bridges, homes, and industrial and commercial buildings were constructed to withstand the average wind or average earthquake
- Telephone lines and switchboards were sufficient in number to accommodate only the average number of telephone calls per hour
- Your friendly local electric utility constructed facilities to only provide the for the year-round average electrical demand
- Emergency services provided an average number of personnel and facilities during all hours of the day and all seasons of the year, or
- Our space program provided emergency procedures for only the average type of failure

Chaos is the word for it. Utter chaos [Runyon 1977].

Source: Runyon, R. P., 1977, *Winning with Statistics*, Addison-Wesley: Reading, MA.

RISK MANAGEMENT ACTIONS

While there are variations in terminology, most risk management actions fall into one of five categories:

Accept

- Simply accept the risk and its potential consequences. No further action is taken.
- E.g., A company choosing to locate its new semiconductor factory in Silicon Valley accepts the risk that it could be destroyed in a major earthquake.

Avoid

- Change the design or the structure of the program to eliminate the risk
- E.g., the fuel tank design on car model X poses a substantial risk of catching fire following a collision. The manufacturer switches to an alternative design that will not catch fire.

RISK MANAGEMENT ACTIONS

Transfer

- Share with or transfer to another party
- E.g., Most people purchase car insurance to cover damages in the event of a collision. This transfers the risk to the insurance company.

Mitigate

- Take steps to reduce the probability and/or consequences of the risk
- E.g., A company developing a new product based on a risky technology identifies a proven technology to serve as a backup in the event that the risky technology fails

Monitor

- Take no action for now but monitor the situation to see if the probability or consequence of the risk increases over time
- E.g., a particular bridge is approaching its end of life, but appears to be in serviceable condition. The state DOT decides to monitor condition of the bridge each year in case it unexpectedly begins to deteriorate

RISK, FILTERING, RANKING, AND MANAGEMENT

RFRM was developed by Haimes, Kaplan, and Lambert [2002]

The purpose of RFRM is to deal with two issues:

- One can often identify a very large number of risks for a given system
- It can require a great deal of effort to quantify each risk

Consequently, RFRM applies a phased approach that imposes increasingly rigorous filters such that the most effort is expended on assessing the most important risks:

1. Scenario Identification
2. Scenario Filtering
3. Bi-criteria Filtering and Ranking
4. Multi-Criteria Evaluation
5. Quantitative Ranking
6. Risk Management
7. Safeguarding Against Missing Critical Items
8. Operational Feedback

Source: Haimes, Y.Y., S. Kaplan and J. H Lambert, 2002, Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397.

1. SCENARIO IDENTIFICATION

Scenario identification begins by building an HHM of the system in question

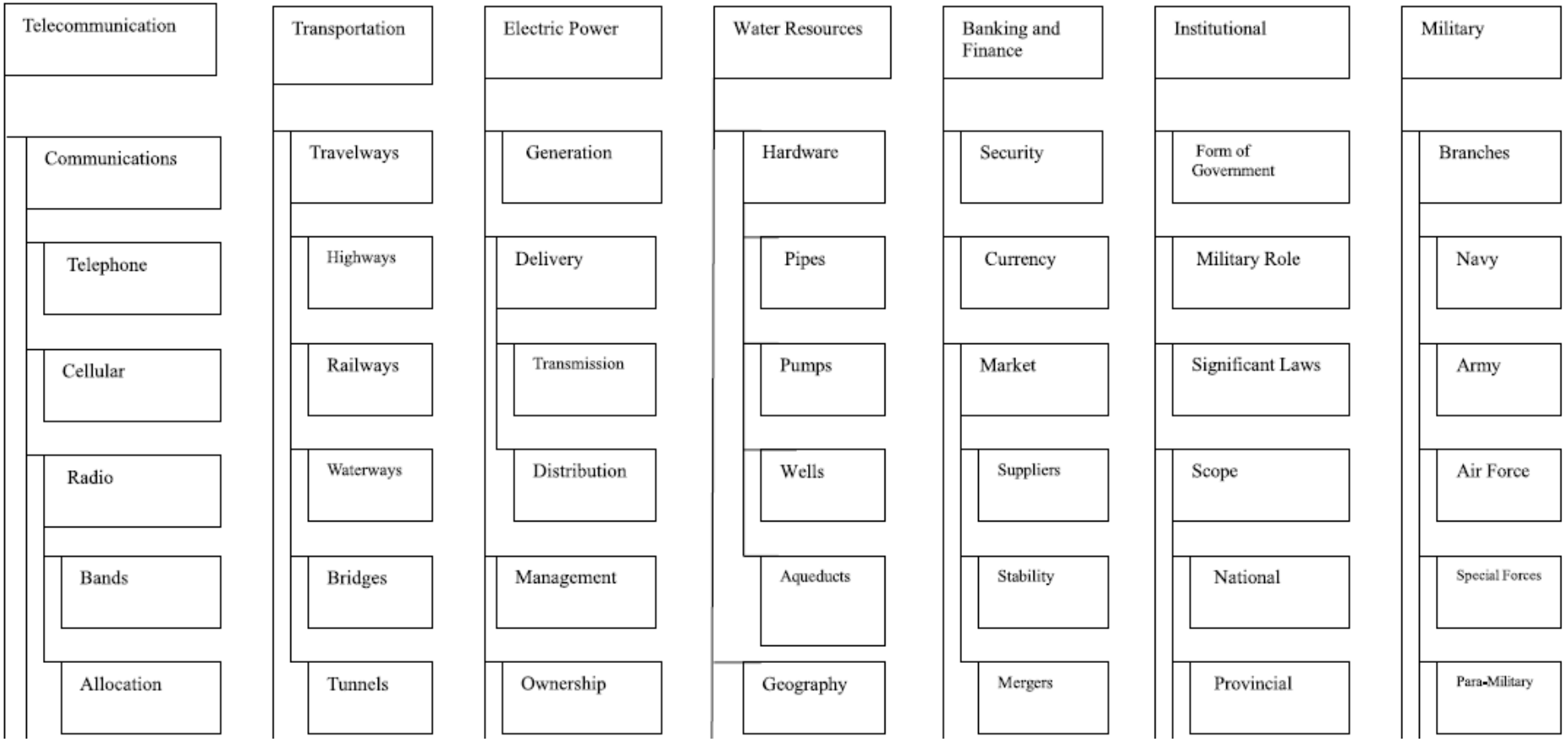
The HHM should be viewed as the success scenario

Every element in the HHM needs to perform properly for the system to function successfully

If we ask “what can go wrong” for each element, we can identify failure scenarios

The intent of phase 1 is to simply identify the failure scenarios, we do not assess or filter at this point

EXAMPLE HHM



Source: Haimes, Y.Y., S. Kaplan and J. H Lambert, 2002, Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397.

2. SCENARIO FILTERING

Phase 1 can easily result in hundreds of risk scenarios

The intent of phase 2 to is reduce that down to a manageable number by eliminating those that are clearly out of scope for the decision maker

This is accomplished by considering the scope, the level of decision making, and the temporal domain

- What is within the decision maker's scope of responsibility?
- What level is he or she operating at: strategic, planning, operational, etc.?
- What is the time line of interest: short-term, long-term, etc.?

Risk scenarios are filtered based on expert knowledge of the system

The intent is to reduce the set of scenarios down to about 50

3. BI-CRITERIA FILTERING AND RANKING

In this phase we introduce a qualitative assessment of likelihood and consequence

Each of the scenarios are evaluated against an ordinal risk matrix (next slide)

Based on the combination of likelihood and consequence, each risk is assigned a severity of extremely high, high, medium, or low

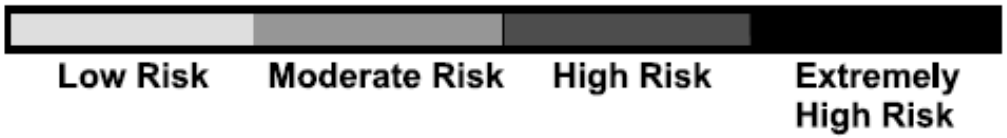
Those that receive a low rating are set aside for future consideration

One caution is that each risk scenario is likely made up of sub-scenarios

- Need to ensure that there is not a more severe sub-scenario hidden in an otherwise low-risk scenario

EXAMPLE: RISK MATRIX

Likelihood / Effect	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of Life/Asset (Catastrophic event)					
B. Loss of Mission					
C. Loss of capability with compromise of some mission					
D. Loss of some capability, with no effect on mission					
E. Minor or No Effect					



Source: Haimes, Y.Y., S. Kaplan and J. H Lambert, 2002, Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397.

4. MULTI-CRITERIA EVALUATION

In this phase, we consider the ability of each remaining scenario to withstand the defensive capabilities of the system in terms of resilience, robustness, and redundancy

- Resilience – the ability of a system to recover from an adverse event
- Robustness – the ability of the system to absorb an adverse event
- Redundancy – the ability of a system to use alternate paths or components

Haimes, et. al identified 11 criteria over which to evaluate the scenarios in terms of high, medium, and, low (next slide)

Those with low scores may be set aside at the analyst's discretion for future consideration

EXAMPLE: EVALUATION CRITERIA

Table II. Rating Risk Scenarios in Phase IV Against the 11 Criteria

Criterion	High	Medium	Low	Not Applicable
Undetectability	Unknown or undetectable	Late detection	Early detection	Not applicable
Uncontrollability	Unknown or uncontrollable	Imperfect control	Easily controlled	Not applicable
Multiple paths to failure	Unknown or many paths to failure	Few paths to failure	Single path to failure	Not applicable
Irreversibility	Unknown or no reversibility	Partial reversibility	Reversible	Not applicable
Duration of effects	Unknown or long duration	Medium duration	Short duration	Not applicable
Cascading effects	Unknown or many cascading effects	Few cascading effects	No cascading effects	Not applicable
Operating environment	Unknown sensitivity or very sensitive to operating environment	Sensitive to operating environment	Not sensitive to operating environment	Not applicable
Wear and tear	Unknown or much wear and tear	Some wear and tear	No wear and tear	Not applicable
Hardware/Software/ Human/Organizational	Unknown sensitivity or very sensitive to interfaces	Sensitive to interfaces	No sensitivity to interfaces	Not applicable
Complexity and emergent behaviors	Unknown or High degree of complexity	Medium complexity	Low complexity	Not applicable
Design immaturity	Unknown or highly immature design	Immature design	Mature design	Not applicable

Source: Haimes, Y.Y., S. Kaplan and J. H Lambert, 2002, Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397.

5. QUANTITATIVE RANKING

By phase 5, the set of risk scenarios should be reduced to the point that those remaining merit the effort of developing quantitative assessments of likelihood

Likelihoods should be computed using all available evidence and Bayesian approaches

Based on the quantitative assessment of likelihood, the risks are placed on the “cardinal” version of the risk matrix (next slide)

Scenarios can be filtered out based on the resulting risk severity rating

The intent is to reduce the number of scenarios from about 20 to 10

EXAMPLE RISK MATRIX

Effect \ Likelihood	0.001≤Pr<0.01	0.01≤ Pr<0.02	0.02≤ Pr<0.1	0.1≤ Pr<0.5	0.5≤ Pr≤1
A. Loss of Life/Asset (Catastrophic event)					
B. Loss of Mission					
C. Loss of capability with compromise of some mission					
D. Loss of some capability, with no effect on mission					
E. Minor or No Effect					

Low Risk Moderate Risk High Risk Extremely High Risk

Source: Haimes, Y.Y., S. Kaplan and J. H Lambert, 2002, Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397.

6. RISK MANAGEMENT

At this point, the risk scenarios should have been reduced to those that are the most important

Risk management options should be identified to avoid, mitigate, or transfer the risks

- For example, alter the system design to avoid the risk or add redundancy to mitigate the risk

Tradeoffs for each option should be assessed and the appropriate risk management policies should be selected

- For example, trading the cost of the mitigation for the level of risk reduction

7. SAFEGUARDING AGAINST MISSING CRITICAL ITEMS

With any filtering and ranking process, there is always a chance that a critical risk was inadvertently filtered out

Furthermore, there is also a chance that our selected risk management policies may actually make a previously low-risk of scenario into a high-risk scenario

- For example imagine a safety critical system that had a critical dependence on the continuity of the gas supply. To avoid this risk one could switch to electrical power, but that might just make loss of electrical power the critical risk.

This phase involves looking for any interdependencies between each of the selected risk policies and the discarded risk scenarios

If any of the discarded risk scenarios are now critical because of the policy, revisit both the discarded risk and the policy

8. OPERATIONAL FEEDBACK

Risk management is never done

It is impossible to foresee all possible outcomes

Establish a data collection and operational feedback processes

Use this feedback to update and refine the model

Revisit risks as necessary

Update risk management polices as necessary

SUMMARY

Risk is traditionally defined as a two dimensional metric: the probability and severity of an adverse event

Risk management is the process of identifying, assessing, prioritizing, and addressing risks

- The two dimensional nature of risk makes prioritization a fundamentally subjective task

The challenge is that for many risks that we care about, we lack sufficient data to identify and quantify them

As a result, many creative methods have been developed to help us identify and rank risk scenarios

While we have discussed some general purpose tools in this lecture, in subsequent lectures we will discuss some domain specific tools