



7

Probabilistic Risk Assessment for Climate-Safe Infrastructure

Probabilistic Risk Assessment Process and Case Application

James R. Deane, AIA, CDT, LEED AP, PMP
Design and Development Section Supervising Architect
California High-Speed Rail
July 2018

1. Summary

1.1. Purpose

The purpose of this document is to define processes that agencies can employ to objectively assess climate change risks across their portfolio. This can be used when they have a need to either integrate climate change risk management into their current risk management plans or develop tools where none currently exist.

1.2. Disclaimer

The work presented within this document summarizes some of the work products developed as part of California High-Speed Rail and generalizes those processes as related to climate change adaptation but is not intended to represent CHSRA opinion or position on any issues.

2. Definitions

- **Threat:** An indication of imminent harm, danger or pain, e.g., shocks
- **Hazard:** Anything that can cause harm e.g. stressors
- **Risk:** A chance, probability or likelihood that harm may occur
- **Vulnerability:** An exposure to a hazard¹
- **Event:** The hazard is realized

2.1. The Challenges

The challenge of developing climate-safe infrastructure begins with determining the type and intensity of future hazards and their likelihood of happening. This is achieved through five steps agencies can take:

1. Identify boundaries, assets and climate change-related hazards, e.g. flooding for their assets
2. Assess the risks by:
 - *Organizing* the risks into common categories for evaluation
 - *Quantifying* the risks for likelihood and severity
 - *Evaluating* the risks against their ability to manage them
3. Mitigate the risk to "As Low As Reasonably Practical" (ALARP)
4. Accept the residual risk
5. Monitor their decision-making against the evolving hazard

Climate change presents the design and engineering community with a unique challenge in that:

- The types of *hazards* are uncertain
- Their *severity* is uncertain
- Their *likelihood* is uncertain
- The *vulnerability* of the infrastructure is dependent on the uncertainty of the hazards

For governments, utility providers, planners and communities there are also additional challenges. These include: (1) that there is not enough funding for all the existing and new infrastructure projects; (2) there are not enough resources (e.g., land, steel or cement) to replace or build new, resilient infrastructure; (3) lack of action to address a hazard often creates or escalates environmental hazards; (4) unplanned reactions by the public or responses by government often have unintended social consequences; (5) lack of or poorly considered mitigation can negatively impact the local *economic* systems.

2.2. Where Does Risk Management Reside?

Most agencies will likely have some form of risk management processes already and can then focus on how to integrate climate risk into their existing processes. Risk management can occur at two levels of an agency:

- **Program Risk Management:** high level policy often bound by legal obligations of the Agency; and
- **Project Risk Management:** specific risks that occur because of taking an action, e.g., building a culvert.

¹ Vulnerability is variably defined as merely the exposure to a hazard as done here, or more as a combination of exposure, sensitivity and adaptive capacity.

Both influence, and are influenced by, the other in that the program provides for strategic decision making while the project provides tactical feedback as to the effectiveness of the strategy.

2.3. How Do You Analyze for Risk?

Risk can be *qualitatively* or *quantitatively* assessed. This document focuses on quantitative assessment. There are many tools to analyze for risk and an agency needs to evaluate their unique set of responsibilities and select a system that best provides a methodology for risk evaluation. Below are some of the methods:

- Fault Mode Effect Analysis;
- Fault Mode Effect and Criticality Analysis;
- Fault Hazard Analysis;
- Double Failure Matrix;
- Event Tree Analysis;
- Political, Economic, Social, Technological, Environmental and Legal Factors (PESTEL) Analysis; and
- Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis.

3. Risk Management

3.1. What Is Risk Management?

Risk management seeks to, in order of preference²:

- Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Taking or increasing the risk to pursue an opportunity;
- Remove the risk source;
- Change the likelihood;
- Change the consequences;
- Share the risk with another party or parties (including contracts and risk financing); and/or
- Retain the risk by informed decision.

Risk management relative to climate hazards has evolved around the following similar concepts: eliminate, avoid, mitigate, absorb, resist or accept the hazards to the system.

The goal of a managed risk approach is to quantify the hazard severity and frequency and compare it against the vulnerability of a component or system to enable an agency to make reasoned decisions as to where to focus efforts with limited resources. The risk management process typically consists of the following steps³ :

- Plan Risk Management
- Identify Risks,
- Perform Qualitative Risk Analysis,
- Perform Quantitative Risk Analysis,
- Plan Risk Responses, and
- Monitor and Control Risks.

The Planning and Investing for a Resilient California: A Guidebook developed by the Governor's Office for Planning and Research provides a similar structure for State agencies, but it is organized specifically around climate (Figure 1).

² ISO 31000:2009 – Risk management -- Principles and guidelines

³ The Project Management Institute Body of Knowledge (PMBOK)

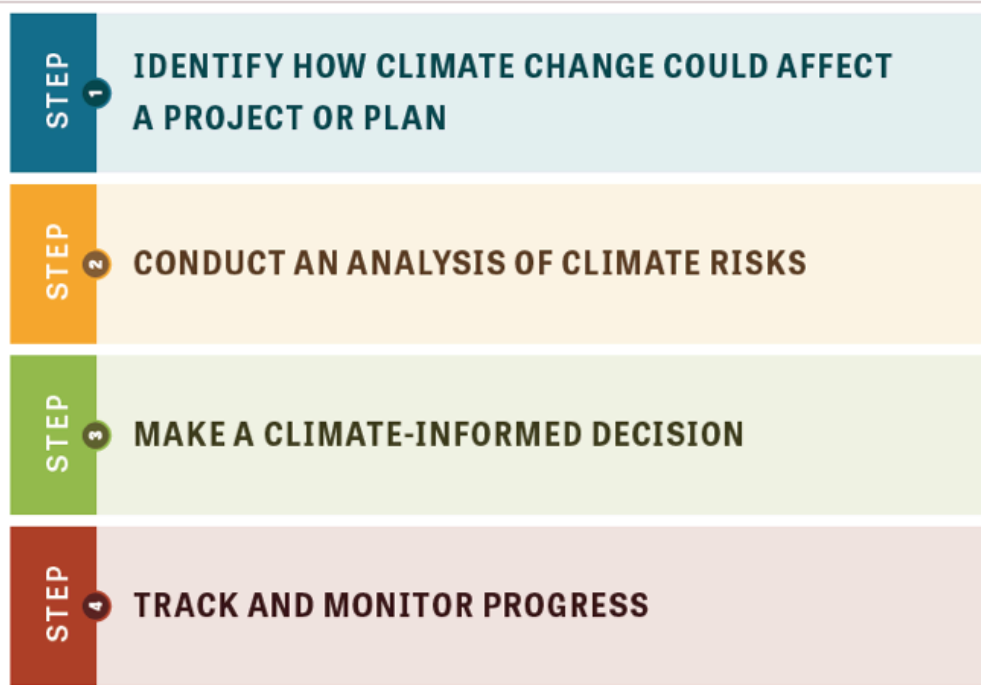


Figure 1: Climate Risk Management Steps. (Source: Planning and Investing for a Resilient California: A Guidebook for State Agencies, used with permission).

A more detailed breakdown of the risk assessment process is shown below in Figure 2.



Figure 2: Risk Management Process.

The Network Rail Risk Assessment Process below (Figure 3) from Network Rail shows a functional risk assessment process.

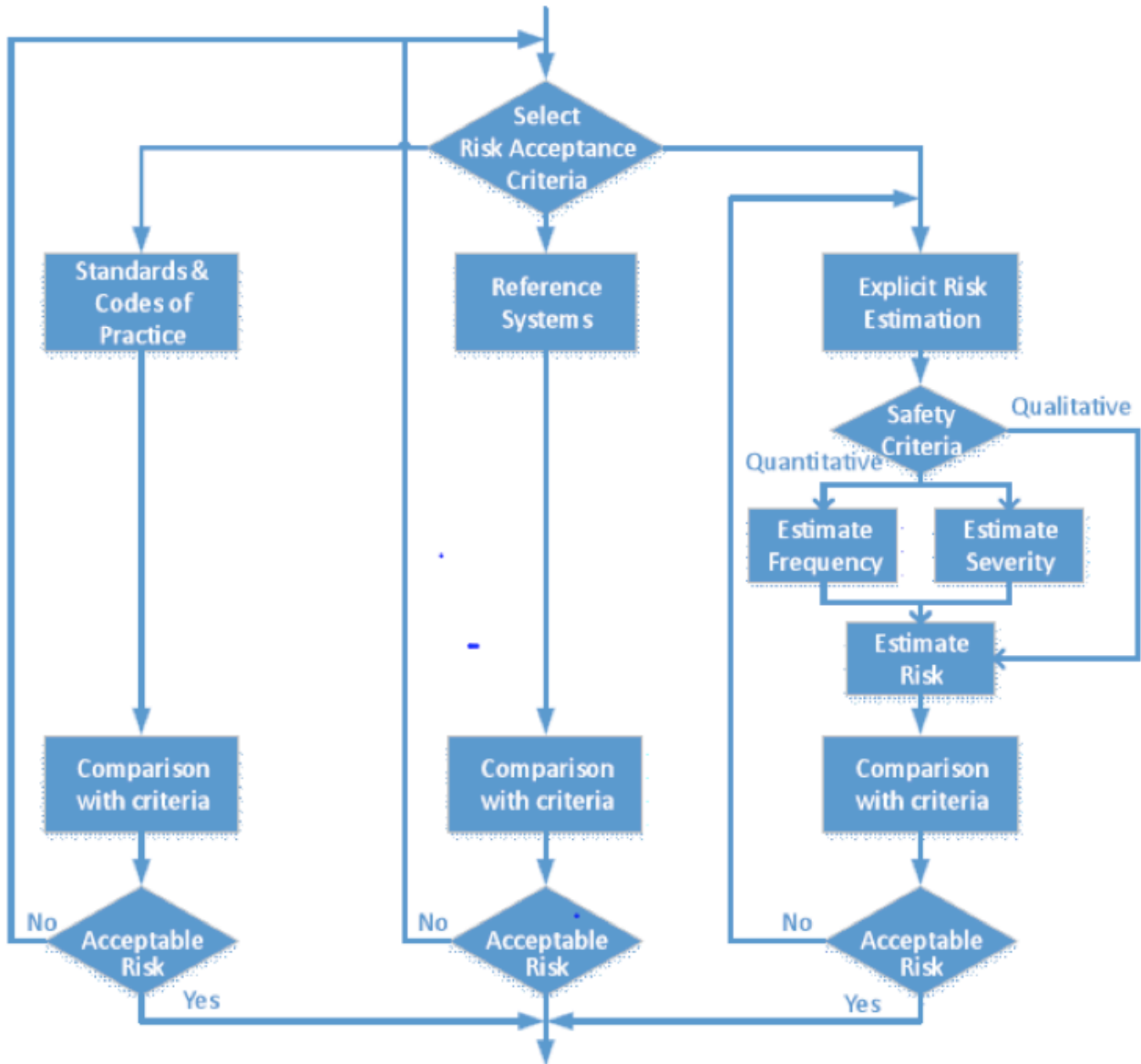


Figure 3: Network Rail Risk Assessment Process. (Source: Network Rail Risk Management Design, used with permission).

The Federal Highway Administration Adaptation Decision-Making Assessment Process (FHWA ADAP) below (Figure 4) provides detail on a more comprehensive process developed for the Federal Highway Administration and adopted by Caltrans.

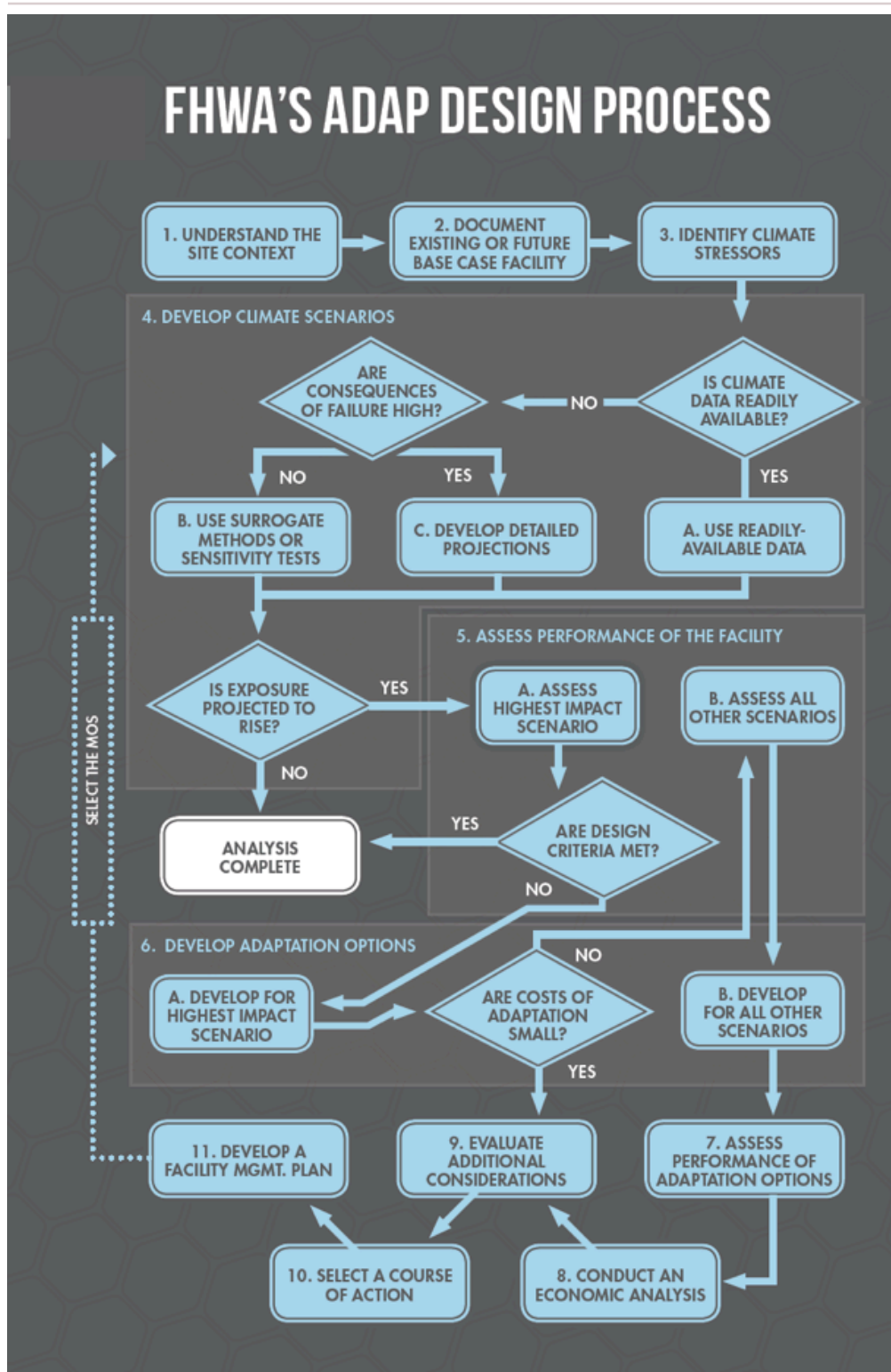


Figure 4: FHWA ADAP design process flow chart. (Source: D4 Caltrans Vulnerability Assessment v49, used with permission.)

3.2. Probabilistic Risk Assessment (PRA)

PRA is a process that allows for hazards to be identified, categorized, evaluated and mitigated based on their severity and frequency. PRA uses probability calculations to establish the likelihood of a hazard occurring and economic analysis to establish severity. PRA seeks to provide a quantifiable weighting to risk rather than subjective assessment. It uses a systems approach which encourages users to consider all aspects of their system and the interrelationships between pieces.

PRA is often expressed as a simple formula, several of which are listed below:

- Risk = Hazard Likelihood + Hazard Severity
- Risk = Hazard Likelihood x Hazard Severity
- Risk = Hazard Likelihood + Hazard Severity + Vulnerability
- Risk = Hazard Likelihood x Hazard Severity x Vulnerability
- Risk = Asset Value x Hazard Rating x Vulnerability Rating⁴

Likelihood or frequency establishes how often a hazard may occur. This is useful in climate adaptation as event frequency is often identified as a key indicator that change is occurring, e.g., a 1:100 precipitation event may become a 1:25 event, indicating that intense precipitation events of a certain magnitude are happening more frequently.

Severity can be identified quantitatively as:

- Cost of replacement for the component or system;
- Cost of damage to the system resulting from component failure; or
- Total cost of damage to life, environment, infrastructure damage, economic (loss of revenue), social fabric and reputation.

Vulnerability is useful for evaluating existing infrastructure as this allows one to focus on costs to upgrade a system.

4 Methodology

4.1. Plan

One of the first activities is to create a Risk Management Plan. This plan is used to:

- Document regulations, standards, and guidelines the agency will follow;
- Establish threshold for acceptance of risk and where action is required to mitigate a risk;
- Comprehensively document the types of hazards that may occur; and
- Identify response the agency will take should an event occur.

4.2. Identify

Many different methods can be used to identify requirements, assets, design criteria, threats, hazards and vulnerabilities:

- Historical records;
- Stakeholder interviews;
- Professional judgement;
- Brainstorming;
- Statistical modeling;
- Cause and effect analysis; and
- Strength Weakness Opportunity Threat (SWOT).

To complete a Risk Assessment there are three primary components that must be identified:

- Risk Acceptance Criteria: how much risk can we accept? (section 4.2.1)
- Asset identification: what do we own and what do we know about it? (section 4.2.2 and 4.2.3); and
- Hazard Identification: what can negatively impact our asset and how badly? (section 4.2.4).

⁴ FEMA 428, Primer for Design Safe Schools Projects in Case of Terrorist Attacks (2003)

4.2.1. Identify Risk Acceptance Criteria

The chicken and egg dilemma with climate adaptation is that we often can't know how much we can accept until we have completed an evaluation. For this document, we place identifying risk acceptance criteria as the first step. If at the end of our analysis, we need to modify our criteria it can be accomplished as part of our monitoring activity. Because there are many potential risks to consider, PESTEL is useful for comprehensively identifying and organizing the risk into related categories:

- Political or governmental: What are the agencies' capabilities and how can it respond?
- Economic: What is the cost of mitigating a hazard versus accepting the impacts of the event?
- Societal: Who are we protecting and how will impacts affect their ability to continue to function?
- Technological or Infrastructure: What are the physical and virtual structures we seek to assess?
- Environmental: How will our natural systems be impacted?
- Legal: What is our ability to mandate change and will consequences of hazards be addressed by the courts?

The Risk Acceptance Criteria flow chart below is a representation of how risk acceptance criteria can be organized (Figure 5).

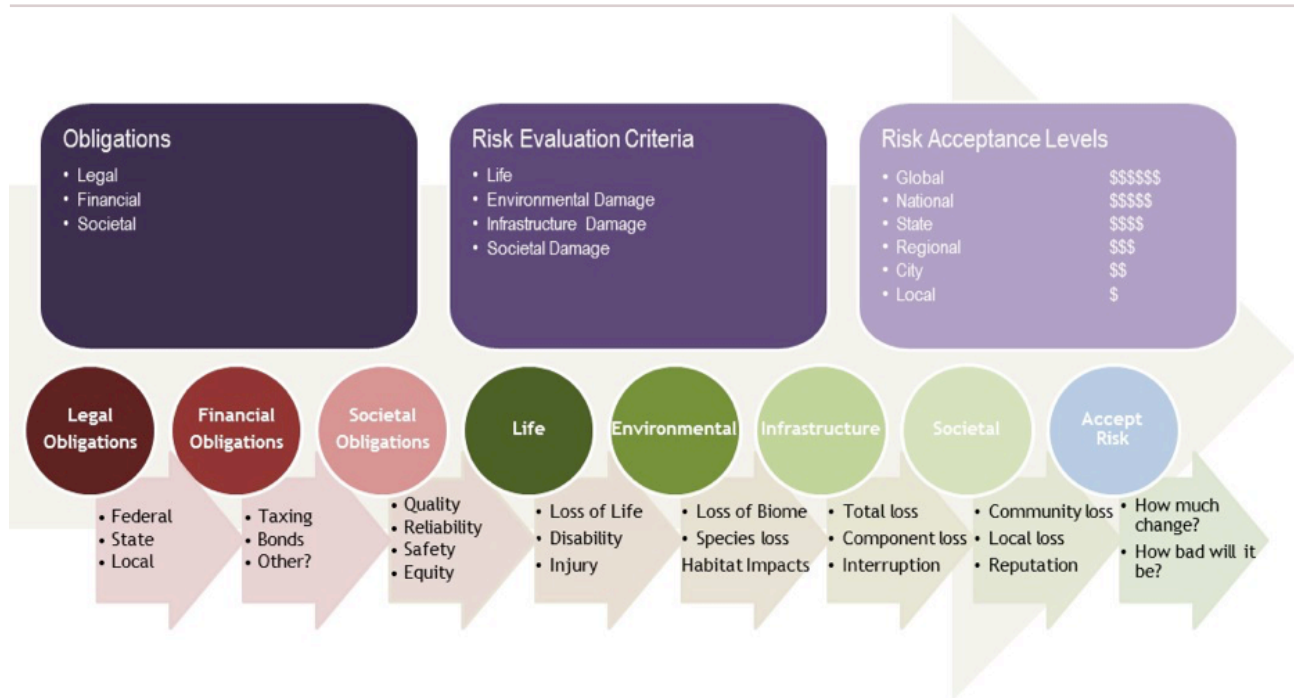


Figure 5: Risk Acceptance Criteria flow chart

4.2.2. Identify Design Criteria

Most agencies will be working with legacy regulatory structures that include design criteria that their assets must adhere to. Frequently, those design criteria do not address climate adaptation as a criteria or evaluation process. As part of the identification process it is important to understand how climate adaptation will be addressed. It is not uncommon to determine after a risk assessment that there are simple and effective mitigations that can be achieved by modifying the agencies design criteria. A new concept for agencies is that climate adaptation must be considered as part of the normal design process. Figure 6 provides a simple diagram to illustrate how to use a Design Criteria Assessment in decision-making around wildfire risk.

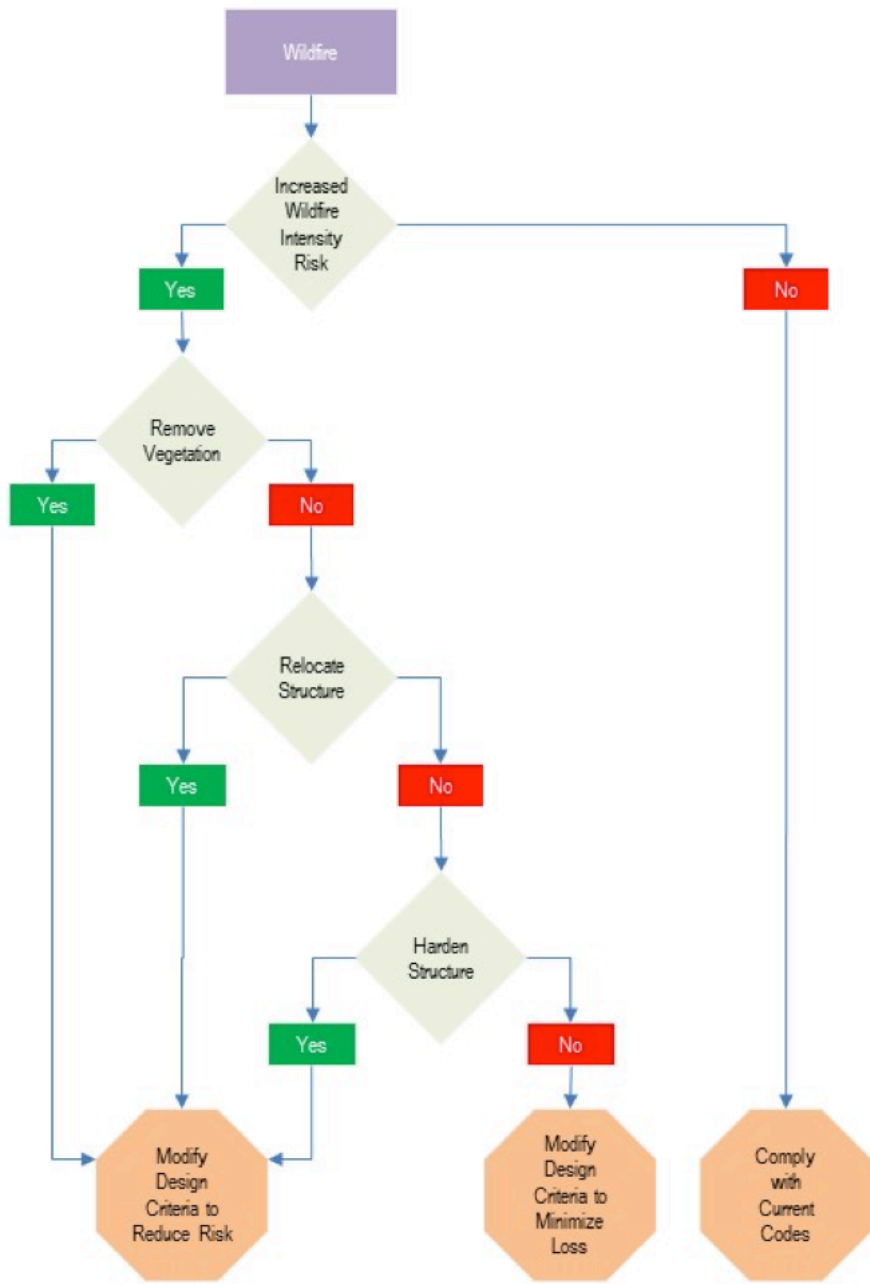


Figure 6: Design Criteria Assessment flow chart for a wildfire example

4.2.3. Identify Assets

Assets can exist in many forms:

- Physical infrastructure: buildings, roads, bridges, pipes, wires, dams, etc.
- Virtual Infrastructure: processes, software, etc.
- Human: staff, customers, communities, etc.
- Environmental: Inorganic (air, sea, land) and organic (plants, animals, habitats)

Who owns what is often a complex question due to the nature of funding, service agreements and regulatory authority. A key component of PRA is to establish a boundary for the analysis and this is also useful for cross-agency coordination so that all parties who influence a project also participate in the risk assessment. The example Risk Boundary Assessment below is one example of a simple boundary determination flow chart to illustrate how responsibility can be assigned (Figure 7).

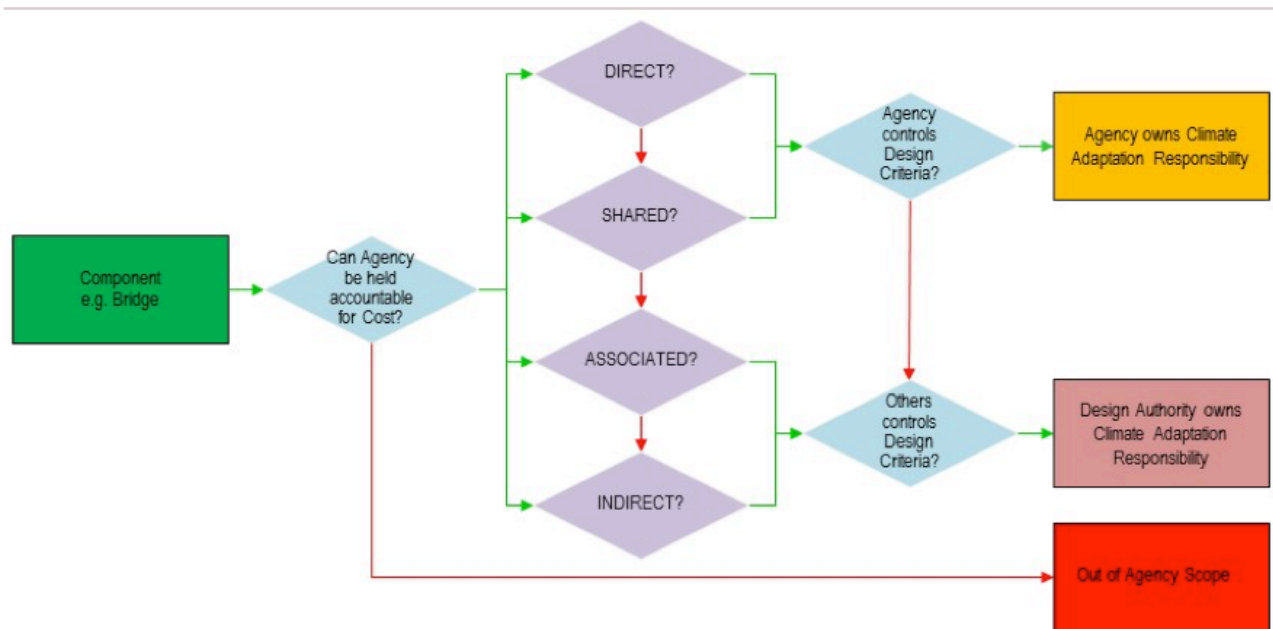


Figure 7: Risk Boundary Assessment flow chart

- Direct: Fully funded by Agency through purchase including design and construction activities directly related service; Agency owns the design criteria and directly benefits from construction
- Shared: Partial funding by Agency in support of others activities that benefit Agency; Agency Influences design criteria and directly benefits from construction
- Associated: Funded by Others and Agency directly benefits or manages; Agency does not influence design criteria but benefits from construction
- Indirect: Funded by others for their principal use but Agency indirectly benefits; The agency does not influence design criteria and does not directly benefit from construction

4.2.3.1. Physical Asset Identification

As this document is primarily focused on physical infrastructure, it is useful to discuss what kinds of data are important to be able to assess an asset. Relevant data include: asset name, function, location, age, service life, condition, design life, geographic conditions, climate zone, and biome. Note that much of this information is already captured by agencies (Table 1):

Table 1: Sample asset identification information

Temperature range						
Component	Design Life	Design standards	Impact	Severity	Justification	Mitigation
Foundations	80		No		Concrete piling is resilient to temperature change	N/A
Masts	60		No		Steel masts are resilient to temperature change	N/A
Small Part steel	40		Negligible	4I	increased operational temperature range may increase maintenance frequency (items loosening)	Monitoring and inspection as part of maintenance regime
Contact Wire	30		Marginal	3I	may reduce capacity and increase maintenance activities (stretch recovery)	Monitoring and inspection as part of maintenance regime
Messenger Wire	60		Marginal	3I	may reduce capacity and increase maintenance activities (stretch recovery)	Monitoring and inspection as part of maintenance regime
Auxiliary wires	60		Marginal	3I	may reduce capacity and increase maintenance activities (re-tensioning)	Monitoring and inspection as part of maintenance regime
Insulators	40		No		Ceramic	N/A
Section Insulators	15		No		Ceramic	N/A
Switches	30		Negligible	4I	may require additional maintenance setup due to thermal expansion	Monitoring and inspection as part of maintenance regime

4.2.4. Identify Climate Hazards

Climate change is sometimes reduced to a single type of impact, such as: sea-level rise, but the changes affect the entire planetary system, including: atmosphere, hydrological systems, geology, ecological systems, natural biomes, species, human-made systems, agriculture, cities, transportation, utilities, and human systems.

Each of these systems can be further divided. For example, atmospheric system impacts include: temperature, humidity, precipitation, rain, snow, extreme weather such as hurricane, lightning, wind, extreme wind such as tornados, dust storms, fog, elevation and air pressure, air quality, aerosols, particulates, and UV radiation.

4.3. Prioritize: Organizing Hazards

From the initial identification process a more systematic method should be used to categorize events (hazards) to show relationships between events, to assign likelihood criteria, and to identify key hazards

Below is an example from California High-Speed Rail that shows how a working group brainstormed various events and then classified them into the Initiating Event Categories and Initiating Events (Table 2).

Table 2: Categorization of Climatic Events into Types of Initiating Events

Initiating Event Category	Initiating Event
Fires	FQ- On a train - in an on-board equipment room
	FO- On a train - in an on-board occupied area
	FX- On a train exterior
	FE- Within the tunnel but not on a train
Tunnel structure failure	CC- Tunnel structure failure
Tunnel blockage	CF- Tunnel flooding
	CD- Debris flow at tunnel portal
Trainset failure	CT- Trainset structure failure
	TE- On-board electrical system
	TB- Brake system
	TP- Pantograph
	TA- Automatic train control (ATC)
	TT- Traction power
	TW- Bogie / wheelset
Track and systems	CE- Overhead electrification structure failure
	CS- Track system failure
	II- Icing on overhead line electrification
	ID- Lineside intrusion detection
	IS- System short circuit
	IE- Earthquake detection and Landslide Detection?
	IP- Incoming power feed failure
	IN- Non-catastrophic safety integrity level (SIL) 4 event
Operator induced	OM- Manual wayside stop signal
	OA- Emergency general alarm activation
	OH- OCC shuts off overhead line electrification
	OB- On-board staff activates emergency stop
	OC- Operational control center issues stop instruction
	OD- Driver stops train (independently)
Passenger induced	PT- Traincrew advised of incident
	PO- External train door opened by passenger
	PV- Vandalism on train
	PB- Broken window
	PH- Train hi-jacked in cab
	PC- Cyber-attack on train
	PE- On-board emergency alarm triggered
	PF- Activation of fire alarm system (no fire)

Because harms resulting from hazards are often interrelated, their significance needs to be evaluated by comparing them to each other. Many mechanisms exist to organize hazards and to understand their linkage. These include, but are not limited to:

- Cause and Effect Diagrams (section 4.3.1);
- Fault Tree Analysis (section 4.3.2); and
- Event Tree Analysis (section 4.3.3).

4.3.1. Cause and Effect Diagrams

Cause and effect diagrams are useful for understanding the relationship of impacts to the larger issue of climate change. These diagrams are also useful for informing an agency where other hazards may exist that are not apparent using other techniques such as historical records. The diagram (Figure 8) shows the cause and effect relationship from fossil fuel consumption to coastal flooding. Note that a single hazard can create multiple additional hazards and that multiple hazards can combine to create new hazards.

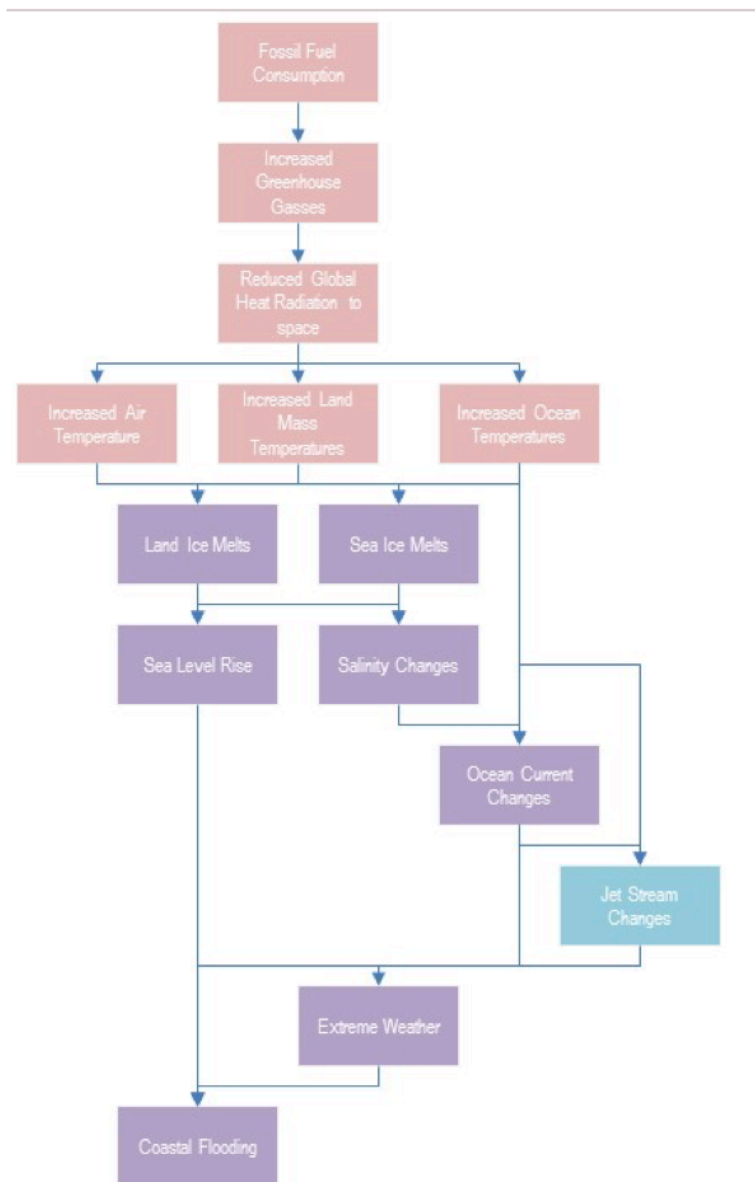


Figure 8: Cause and effect diagram on how fossil fuel consumption flooding can have ripple effects down the chain to coastal flooding

4.3.2. Hierarchical Risk Assessment: Root cause analysis

Probabilistic Risk Assessment processes use inductive and deductive processes to determine where hazards are and assigns a mathematical value to determine risk. There are two main methods for organizing and visualizing the hazards, Fault Tree Analysis (FTAn) and Event Tree Analysis (ETAn) (Figure 9).

Fault Tree Analysis is deductive modeling that looks backward for all events that can lead to a failure. This methodology can be useful for evaluating existing systems by working backward to predict how an element may fail and what are the resulting consequences for the system

Event Tree Analysis is inductive modeling that looks forward for consequences that may arise from events. They are useful for planning new systems especially where there are a range of possible responses. Root cause analysis Ishikawa, or fishbone diagrams, are often used to illustrate event trees. They all aim to roll back the layers of causality to better understand system function and get at the root causes of problematic events.

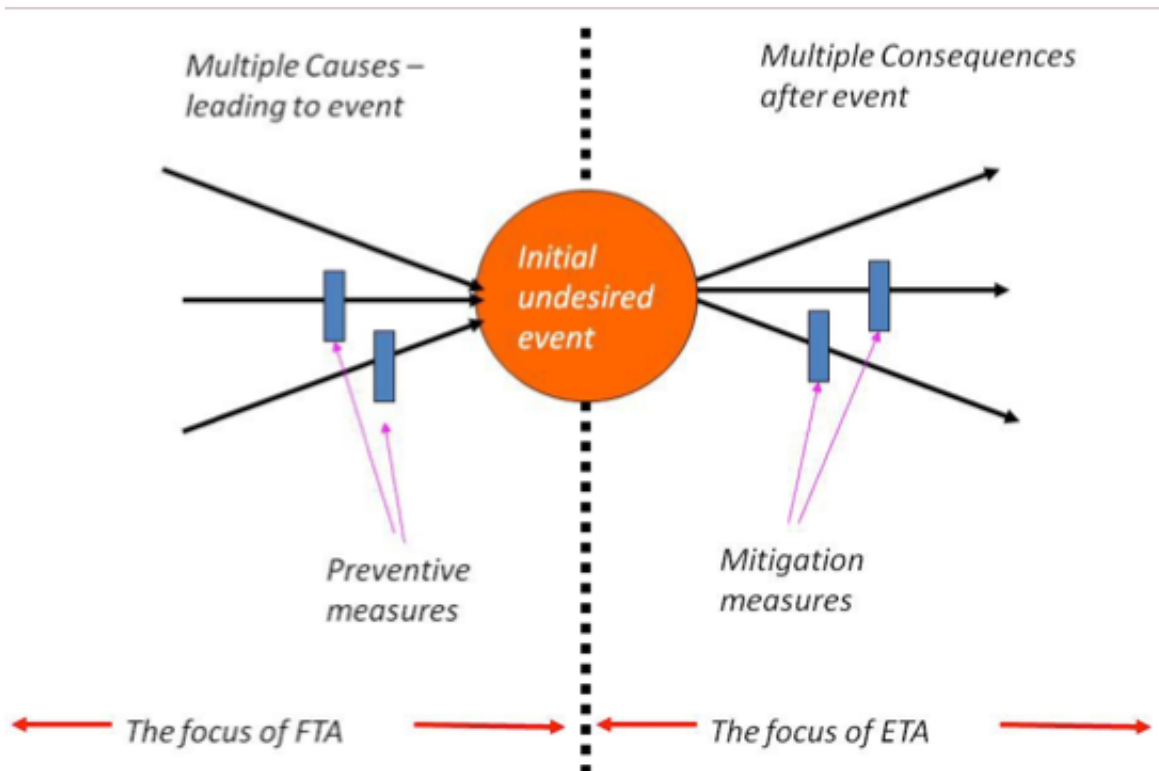


Figure 9: FTA versus ETA is useful in understanding the differences between the two processes. (Source: NEBOSH National Diploma - Unit A | Managing Health and Safety, used with permission)

4.3.3. Developing Event Trees

Event Tree Analysis allows us to start with climate change impacts and look forward to understand the hazards that it creates. Once each of the event scenarios are identified an event tree is developed to identify actions and responses and following each to a terminal action from which no further possible event branches occur. Steps to perform an event tree analysis (Clemens et al. 1998) include the following:

- Define the system: Define what needs to be involved or where to draw the boundaries.
- Identify the accident scenarios: Perform a system assessment to find hazards or accident scenarios within the system design.
- Identify the initiating events: Use a hazard analysis to define initiating events.
- Identify intermediate events: Identify countermeasures associated with the specific scenario.
- Build the event tree diagram.
- Obtain event failure probabilities: If the failure probability cannot be obtained, use fault tree analysis to calculate it.
- Identify the outcome risk: Calculate the overall probability of the event paths and determine the risk.
- Evaluate the outcome risk: Evaluate the risk of each path and determine its acceptability.
- Recommend corrective action: If the outcome risk of a path is not acceptable, develop design changes that change the risk.
- Document the event tree analysis: Document the entire process on the event tree diagrams and update for new information as needed.

Each event has a binary Yes or No action that leads to Resolution Event or another Intermediate Event. Three types of Resolution Events are considered:

- Non-Event: No risk occurs;
- Satisfactory Outcome: An identified action is taken to address the risk; or
- Unsatisfactory Outcome: Remaining risk that requires further action.

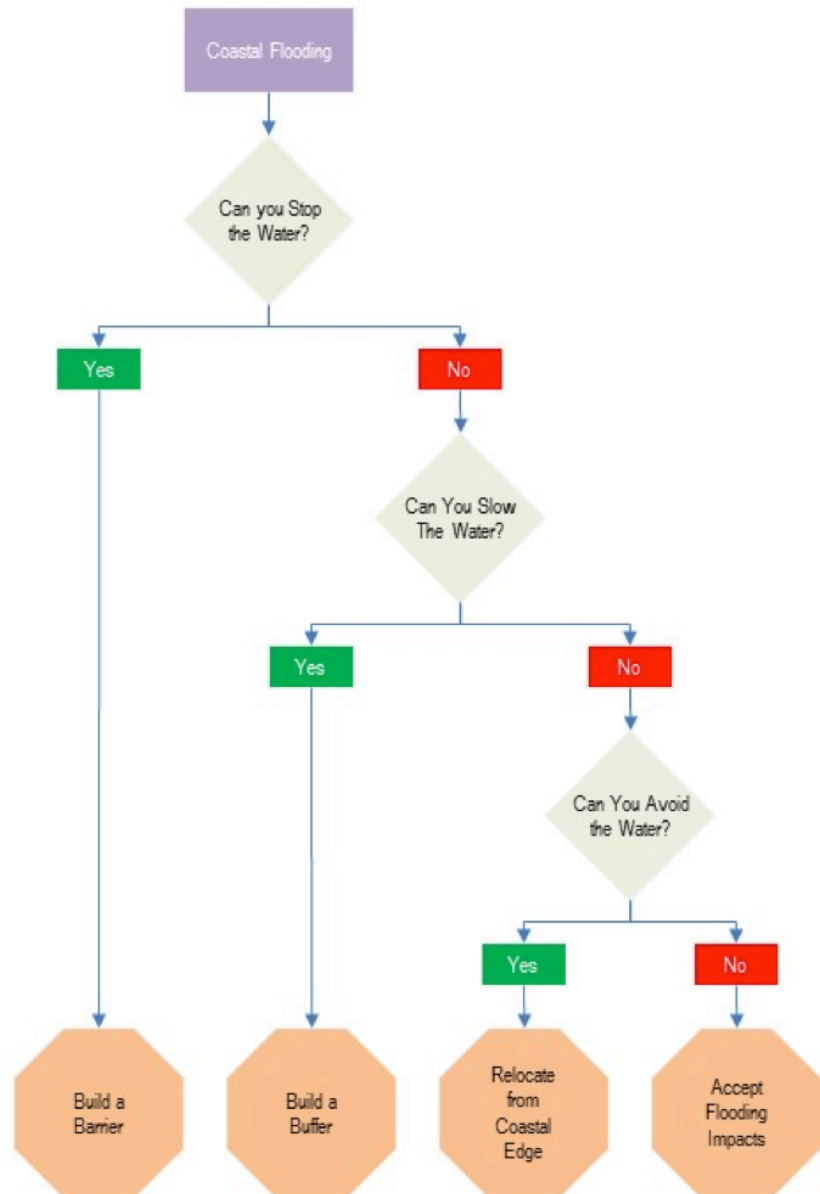


Figure 10: Example of an Event Tree Diagram

4.4. Risk Assessment

Using a methodology similar to the one shown in Figure 3 (Network Rail Risk Assessment Process), most risk assessment processes use some variation of a 4-step process:

- Establish Event Hazard Frequency: What is the likelihood an event will occur? (section 4.4.1);
- Assign Event Hazard Severity: How bad will the event be? (section 4.4.2);
- Calculate Event Risk Rating: What is the risk rating (frequency and severity)? (section 4.4.3); and
- Determine Risk Acceptance: Can we accept the risk? (section 4.4.4).

4.4.1. Establish Event Hazard Frequency

Once the event trees are completed, the team assigns frequency/likelihood of occurrence to the event based on historical data looking at past similar events against their systems relevant operational miles traveled. Hazard frequency is based on MIL-STD 882E and EN50126 Safety Integration Levels for probability of occurrence. Hazard Frequency is one example of how climate change may the risk calculations associated with each hazard type (Table 3).

4.4.2. Assign Event Hazard Severity

Hazard Severity categories are based on criteria defined in MIL-STD 882E (Table 4). California High Speed Rail has established criteria for determining the severity of an event or hazard for each of the following categories:

- Loss of life;
- Environmental Impact;
- Financial loss;
- Operational delays;
- Reputational harm;

For each, what are the consequences of risk being realized? Multiple factors often exist and interact, and each must be evaluated.

Table 3: Example hazard frequencies

Hazard Frequency Table													
Frequency	Qualitative Definition	Qualitative Description for the System	Probability of Occurrence	Flooding	Drought	Wild Fire	Temperature Events	Temperature rise F	Sea Level rise ft.	Air Quality Index	Extreme Weather	Earthquake	Landslide
E	Highly Unlikely	These are events beyond planning and other mitigations- only impact responses are available- Infrastructure elements may fail completely	$10^{-6} > p$	1:1000	>7	>7 major fires/year	>7	>7	>7	300	1:1000	1:1000	1:1000
D	Remote	Physical systems have capacity to resist impact but significant damage may occur	$10^{-3} > p > 10^{-6}$	1:500	7	7 major fires/year	7	7	7	200	1:500	1:500	1:500
C	Occasional	Physical systems have capacity to absorb impact- minor damage with minimal to no operation impacts	$10^{-2} > p > 10^{-3}$	1:100	5	5 major fires/year	5	5	5	150	1:100	1:100	1:100
B	Probable	Other systems are used to mitigate risks	$10^{-1} > p > 10^{-2}$	1:50	3	3 major fires/year	3	3	3	100	1:50	1:50	1:50
A	Frequent	Operational planning to cope with impact	$p > 10^{-1}$	1:25	1	1 major fires/year	1	1	1	50	1:25	1:25	1:25

*Values are for illustration purposes only as the State should establish these values as a common standard for State agencies to work from.

Table 4: Hazard Severity Categories

Hazard Severity Table												
Severity	Category	Life:	Natural Environment	Commentary	Economic:	Societal:	Commentary	Built Environment	Commentary	Geo significance	Recovery Time	Commentary
5	Catastrophic	Loss of Life: Many-overwhelms HC infrastructure Injury: Many-overwhelms HC infrastructure	Extinction of species	habitat and/or species completely lost	Infrastructure: >\$10B Resources: Businesses: Jobs:	Shutdown of services	All communities are affected	Infrastructure: Complete loss Critical infrastructure: Significant damage	Total loss of distribution Total loss of generation and reservoirs	State	>3 years	Arkstorm equivalent event
4	Critical	Loss of Life: Many- HC infrastructure accommodates Injury: Many- HC infrastructure accommodates	Loss of Biosphere	loss at location but biosphere exists elsewhere	Infrastructure: >\$1B Resources: Businesses: Jobs:	Significant disruption	Many Communities are affected	Infrastructure: Significant damage to Critical infrastructure: Moderate damage to	Significant loss of distribution Significant loss of generation and reservoirs	Region	1-3 years	Northridge equivalent event
3	Moderate	Loss of Life: Few- HC infrastructure accommodates Injury: Many- HC infrastructure accommodates	Loss of species	Loss of some species at location but other species and partially functioning habitat remain	Infrastructure: >\$100M Resources: Businesses: Jobs:	Limited disruption	Whole community is affected	Infrastructure: Moderate damage to Critical infrastructure: Limited damage to	Widespread loss of distribution Minimal loss of generation or reservoirs	County	6-12 months	
2	Marginal	Loss of Life: Few- HC infrastructure accommodates Injury: Many- HC infrastructure accommodates	Permanent change to habitat/species	permanent disruptions that species and habitat can adapt to e.g. change in migration patterns, change in flowering etc.	Infrastructure: >\$10M Resources: Businesses: Jobs:	Limited disruption	Isolated portions of community are disrupted	Infrastructure: Moderate damage to Critical infrastructure: Limited damage to	Local loss of distribution No loss of generation or reservoirs	City	4-6 months	
1	Negligible	Loss of Life: None Injury: Few- HC infrastructure accommodates	Temporary changes	Temporary disruptions that species and habitat can recover from	Infrastructure:>\$1M Resources: Businesses: Jobs:	No disruption	Community at large continues to function	Infrastructure: Limited damage to Critical infrastructure: No damage to	Isolated loss of distribution No loss of generation or reservoirs	Neighborhood	0-4 months	

*Values are for illustration purposes as the State should establish these values as a common standard for State agencies to work from.

4.4.3. Calculate Event Risk Rating

Risk is assessed for frequency and severity and assigned a Risk Assessment Code (Table 5). Each type of hazard is assessed separately, and frequency and severity provide a single score.

Table 5: Risk Assessment Matrix

Risk Assessment Matrix					
Frequency \ Severity	5 Catastrophic	4 Critical	3 Moderate	2 Marginal	1 Negligible
(E) Highly Unlikely	5E	4E	3E	2E	1E
(D) Remote	5D	4D	3D	2D	1D
(C) Occasional	5C	4C	3C	2C	1C
(B) Probable	5B	4B	3B	2B	1B
(A) Frequent	5A	4A	3A	2A	1A

Colors provide an indication of the risk level where:

- Red = High Risk
- Orange = Serious Risk
- Yellow = Medium Risk
- Green = Low Risk
- Blue = Eliminated Risk

*This table is for illustration purposes only; it is recommended the State establish these values as a common standard for State agencies to work from.

4.4.4. Determine Risk Acceptance

Once the Hazard Likelihood and Hazard Frequency are determined a score is generated for each evaluation criterion as shown in Table 6. The Risk Acceptance Criteria are developed at the beginning of the risk assessment process and they determine whether the agency can accept a risk. For instance, where the outcome has an "acceptable" risk rating, it may be accepted. If the outcome has a "tolerable" risk rating, the agency may consider other mitigation measures. If the outcome has an "undesirable" or "unacceptable" risk rating, the agency must develop additional mitigation measures until the subsequent branches have a tolerable or acceptable risk rating or the risk is eliminated.

Table 6: Risk Acceptance Matrix

Risk Acceptance Matrix			
Hazard Risk Index	Risk Rating	Action Required	Infrastructure Actions
5E	Catastrophic	Residual risks beyond those in critical category risks cannot be avoided	Accept Impacts
5D, 4E	Unacceptable	Risk must be reduced and managed	Resist Impacts
5B, 4C, 5C, 2D, 3D, 4D, 1E, 2E, 3E	Undesirable	Risk is acceptable only where further risk reduction is impracticable.	Absorb Impacts
4A, 5A, 2B, 3B, 4B	Tolerable	Apply mitigations where reasonably practicable. Risk can be tolerated and accepted with adequate controls.	Mitigate Impacts
1A, 2A, 3A, 1B	Acceptable	Current, normal management processes	Prepare for Impacts

4.4.5. Risk Mitigation

At a program level, it is appropriate to look at larger issues such as where to spend money or expend effort to mitigate risk if an agency is resource constrained. In the example below from the US EPA (Titus 2007), several criteria are identified that are useful for evaluating mitigation measures.

- Economic Efficiency: Will the initiative yield benefits substantially greater than if the resources were applied elsewhere?
- Flexibility: Is the strategy reasonable for the entire range of possible changes in temperatures, precipitation and sea level?
- Urgency: Would the strategy be successful if implementation were delayed ten or twenty years?
- Low Cost: Does the strategy require minimal resources?
- Equity: Does the strategy unfairly benefit some at the expense of other regions, generations or economic classes?
- Institutional feasibility: Is the strategy acceptable to the public? Can it be implemented with existing institutions under existing laws?
- Unique or Critical Resources: Would the strategy decrease the risk of losing unique environmental or cultural resources?
- Health and Safety: Would the proposed strategy increase or decrease the risk of disease or injury?
- Consistency: Does the policy support other national state, community or private goals?
- Private v. Public Sector: Does the strategy minimize governmental interference with decisions best made by the private sector?

4.4.6. Monitoring

Once a risk assessment is complete and all mitigation measures that can be taken have been identified, a risk baseline can be established. From this baseline, it is possible to evaluate climate change on an ongoing basis as new data becomes available, update assets as systems age and components are added or replaced, input actual frequencies and severities as events occur.

5. Reference Standards and Resources

Below, we identify reference standards that the California High-Speed Rail Authority uses for its planning and highlight additional resources that provide good examples of the components of PRA discussed above.

Standard EN50126 - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) EN50126 establishes design standards based on the use of the system under various conditions. It incorporates a comprehensive risk assessment/mitigation protocol to provide a system that achieves a safety level As Reasonably Low as Reasonably Practicable (ALARP). ALARP allows one to address uncertainty and acknowledge in a structured way where residual risk may still exist. Each system is assessed individually and is assessed as an overall interactive system. California High-Speed Rail Authority (CHSRA) uses EN50126 to define its RAMS criteria and is now developing climate adaptation and resilience criteria into the program using this methodology.

MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY (11-MAY-2012)

This Standard is approved for use by all Military Departments and Defense Agencies within the Department of Defense (DoD). It is referenced in FRA 49 CFR Part 238 Subpart G (3). This system safety standard practice is a key element of Systems Engineering (SE) that provides a standard, generic method for the identification, classification and mitigation of hazards. Systems Engineering is a process that focus on the idea that all components of a system are interrelated and that there are cause and effect relationships that must be evaluated. California High-Speed Rail Authority (CHSRA) uses MIL-STD-882E for risk identification, quantification, mitigation and acceptance measures.

NASA-STD-8739-8 NASA Systems Engineering Handbook SP-610S June 1995 This standard addresses risk management as part of its larger program management strategy. It also addresses probabilistic cost and effectiveness as it relates to uncertainty and modeling. NASA-STD-8739-8 deals with RAMS as part of the program management strategy and addresses measurement and verification which points to the need to be able to evaluate the completed work against the program and project goals to understand if what was done fundamentally works as it was intended. Finally this standard discusses the relationship of Event Tree Analysis to Probabilistic Risk Assessment.

Fault Tree Handbook NUREG-0492 United States Nuclear Regulatory Commission January 1981

The fault tree handbook provides a systems approach to decision making. It discusses Failure Mode Effect and Criticality Analysis as a method for identifying faults and their effects on the larger system and discusses Preliminary Hazard Analysis.

NASA Fault Tree Analysis (FTA): Concepts and Applications (Bill Vesely)

The document provides detailed examples of how an FTA is developed.

RRC Training NEBOSH Nation Diploma – Unit A: Managing Health and Safety element; A3-Identifying Hazards, Assessing and Evaluating Risks.

A Scalable Systems Approach for Critical Infrastructure Security Sandia National Laboratories Sand REPORT SAND2002-0877 April 2002

While focused primarily on security, the process is easily adaptable to climate assessment. It contains an extensive appendix of risk assessment tools for infrastructure.

How-To-Guide (FEMA386-5): Using Benefit-Cost Review in Mitigation Planning

This is a good example of using PESTEL (STAPLEE) in a qualitative risk assessment process.

ISO 31000:2009 – Risk management – Principles and guidelines

ISO provides the global standard for risk management, and show how to integrate risk management with other ISO standards.

The New York City Panel on Climate Change Climate Protection Levels report

This is a good example of assigning probability to climate change events.

SSMP: California High-Speed Rail Safety and Security Management Plan

The SSHP is a good example of a risk management plan.

6. References

Clemens, P.L.; and Rodney J. Simmons (1998). "System Safety and Risk Management". *NIOSH Instructional Module, A Guide for Engineering Educators*. Cincinnati, OH: National Institute for Occupational Safety and Health: IX-3 – IX-7.

Titus, J.G. (2007) Strategies for adapting to the greenhouse effect. *Journal of the American Planning Association*. 56:311-323. (Available at: <https://doi.org/10.1080/01944369008975775>)