Idaho Community-Engaged Resilience for Energy-Water Systems Dynamic Risk Assessment Overview & Primer

R. A. Borrelli

University of Idaho
Department of Nuclear Engineering
and Industrial Management

2024.04.19

I-CREWS

Goals for the session

Introducing the concepts of risk and risk assessment without lecturing

Integrating dynamic risk within the context of the project description

Stimulate discussion for May

Let’s first look at the **Strategic Plan**

Research Component 2 – Model Dynamic Existing and Alternative E-W Configurations

Leads –

Lan Li (BSU)

Tim Link (UI)

Lesley Kerby, Bruce Savage (ISU)

Team members –

Bob Borrelli, Erin Brooks, Brian Johnson, Terry Soule (UI)

Mojtaba Sadegh, Brian Wampler (BSU)

New hires!

Research Component 2 – Model Dynamic Existing and Alternative E-W Configurations

The modeling component has three objectives –

Objective 2.1 – Build datasets to develop the ML modeling platform.

Objective 2.2 – Build ML models suitable for use in the testbed regions.

Objective 2.3 – *Quantify dynamic risk.*

This component aims to increase capacity in computational modeling and machine learning, advancing our understanding of –

(i) scales of data needed to effectively model the risks and losses of multiple interacting stressors on E-W systems, and

(ii) stressor conditions, tradeoffs and feedback decisions leading to state-shifts.

Objective 2.3 – Quantify dynamic risk

Objective 2.3: Quantify dynamic risk.					
Determine risk to be assessed and relevant variables contributing to risk.					
	Year 1	Year 2	Year 3	Year 4	Year 5
2.3.A	Conduct literature review on similar risk problems. Coordinate with Characterize and Alternative Futures teams.	**SETS variables and stressors based on Characterization team results established.**	**‘Status quo’ futures (to compare) defined with Alternative Futures team.**	**Risk to be assessed determined.** **Food for thought**: Suggested discussion topic for May workshop.	**Risk definition reiterated.**

Objective 2.3 – Quantify dynamic risk

<table>
<tr><th colspan="6">Objective 2.3: Quantify dynamic risk.</th></tr>
<tr><th colspan="6">Derive or apply relevant models to characterize risk.</th></tr>
<tr><th></th><th>Year 1</th><th>Year 2</th><th>Year 3</th><th>Year 4</th><th>Year 5</th></tr>
<tr><td><b>2.3.B</b></td><td>Conduct literature review for any relevant dynamic risk modeling techniques and metrics that could be applied and/or modified.</td><td>Explore how SETS variables change with changes to stressors.</td><td>Explore how to integrate ML results.</td><td>Integrate ML results into SETS variables andstressors.
<b>Dynamic behavior of stressors defined.</b></td><td><b>Knowledge Holder Inputs coupled and aligned with Alternative Futures team.</b></td></tr>
</table>

Objective 2.3 – Quantify dynamic risk

Objective 2.3: Quantify dynamic risk.					
Assess risk.					
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**
2.3.C	Explore incorporating risk within the context of resilience or related construct with all teams.	I couldn’t think of anything new for Year 2.	**E-W Resilience Indicators applied.**	Conduct sensitivity analysis of risk/resilience to changes in SETS variables and stressors if needed.	**Risk assessed.**

Let’s jump into the topic

What is risk?

Risk has been around for a long time

> *. . . the appearance of disease in human populations is influenced by the quality of air, water, and food; the topography of the land; and general living habits.*

– Hippocrates; Air, Water and Places

(Make sure everyone knows who this guy is)

Risk is the possibility of loss *due to a hazard*

A hazard is –

. . . a dangerous factor

. . . a person or event that induces a dangerous factor

A hazard is an existing or potential condition that can cause injury, illness, or death; damage to, or loss of equipment, property, finances. . .

Risk is the probability of a hazard occurring multiplied by its consequences

$$Risk = f \times C \tag{1}$$

Frequency and probability are interchangeable

Consequence and severity are interchangeable

Probability = How often a hazard could occur. . . once per facility lifetime, three failures per month, etc.

Consequence = Expected result of a hazard. . . degree of injury, property/financial damage, latent cancers, etc.

Mitigation = Action taken to eliminate or reduce risk identified

Risk is the expected value of an undesirable event

$$E[X] \equiv \int xf(x)dx \tag{2}$$

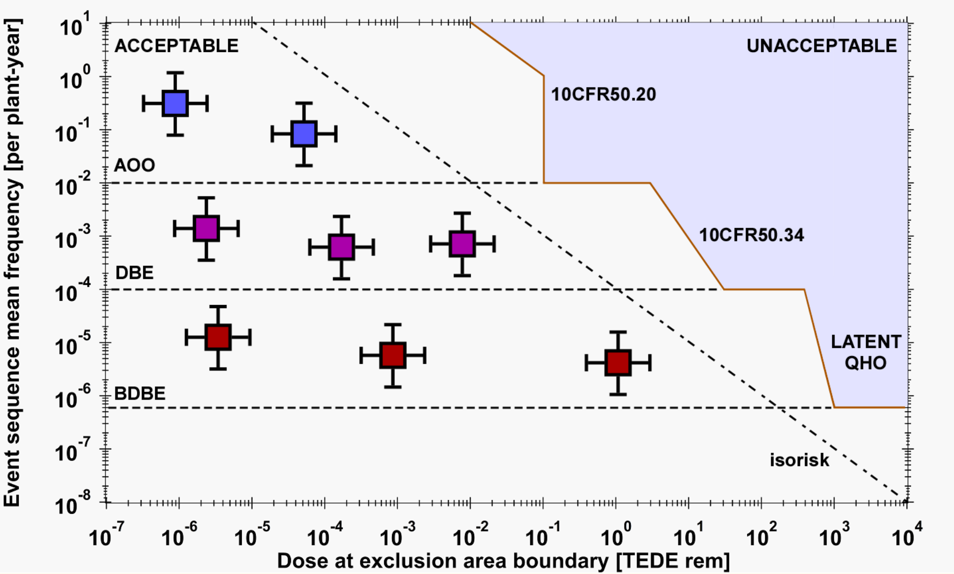
$$E[X] \equiv \sum_i x_i f(x_i) \tag{3}$$

$f(x) = \lambda e^{-\lambda x} \quad x > 0$

$E[X] = \int_0^\infty x\lambda e^{-\lambda x} = -\frac{1+\lambda x}{\lambda} e^{-\lambda x}\Big|_0^\infty = \frac{1}{\lambda}$

$E[DICE] \; = \; \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \frac{1}{6} \cdot 4 + \frac{1}{6} \cdot 5 + \frac{1}{6} \cdot 6 \; = \; 3.5$

We can visualize risk with the Farmer's chart [1]



[1] Farmer, F. R., 1967. Reactor Safety and Siting: A Proposed Risk Criterion. Nuclear Safety 8, 539

Risk assessment involves three essential questions [2]

What can go wrong?

How likely is it to happen?

What are the consequences?

[2] **Kaplan, S. et al., 1981. On the quantitative definition of risk. Risk Analysis 1, 11**
(Kaplan & Garrick is so important that the paper is hosted on the NRC website.)

Quick overview

Risk assessment is a retrospective process

Developed by the US Space Program in 50s and 60s

Reactor safety study WASH-1400

Only after about 75 NPPs designed, built, operating

First real use of Probabilistic Risk Assessment (PRA) analysis and techniques

Came to prominence after Three Mile Island in 1979

Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants

First Level III full scope PRA

Risk assessment involves substantial breadth and depth

Requires diverse expertise – Highly dependent on detailed system analysis

Start by identifying hazards

Then characterize all identified hazards combined to complete a task

Multiple hazards have varying risk

Risk assessment as one input into design and operational changes

Risk assessment is deterministic and reductionistic and highly data driven

Sophisticated modeling is usually required

Classifying risk

Risk matrix

A risk matrix is a high level assessment tool

Severity	Probability				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	E	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L
E – Extreme Risk			M – Moderate Risk		
H – High Risk			L – Low Risk		

Risk matrix for cyberattacks on a Nuclear Power Plant

Table. Preliminary Hazards Analysis results for selected NPP plant systems. The product of Accessibility and Impact nominally reflects the vulnerability of the system as to whether the reactor will be tripped or if the operator can take corrective or mitigating actions to recover operability [3].

Impact	Accessibility				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic					Reactor controls
Critical		Spent fuel pool Boron monitoring			
Moderate		Exciter	Steam generator Condenser		
Marginal		Cooling water systems			
Negligible					

[3] Root, S. J., et al., 2023. Cyber Hardening of Nuclear Power Plants. Progress in Nuclear Energy 162, 104742

Qualitative techniques

Qualitative analysis yields meaningful results if you know what you’re doing

Preliminary Hazards Analysis (PHA) early to identify hazards

Failure Modes & Effects Analysis (FMEA) to determine high level frequency and consequences; nominal risk measure

Fault trees are top down, deductive failure analysis tool to decompose hazards

Event trees identify accident sequence and consequences

Hazard & Operability Analysis (HAZOP) analyzes how hazards affect system operations

Cyberattacks throw a wrench into everything

Uncertainty

Uncertainties come in different flavors but are essential in risk [4]

There are things we know we know

Then there’s things we know that we do not know

But there’s still things that we don’t know we don’t know

[4] Der Kiureghian, A. et al., 2009. Aleatory or epistemic? Does it matter? Structural Safety 31, 105

Aleatory uncertainty is statistical

Random variations and chance outcomes in the physical world, natural randomness in a process

If a parameter sometimes has one value and sometimes has another values

Epistemic uncertainty is systematic

Lack of knowledge about the physical world, scientific uncertainty in the model of the process

If a parameter always has either one value or another, but we are not sure which

Ethics

There is an ethical theory basis for risk

Based on universal rules and principles by Descartes (1596–1650)

Rights ethics by John Locke (not the guy from the Island) (1632–1704)

Duties ethics by Immanuel Kant (1724–1804)

Utilitarianism by Jeremy Bentham and John Stuart Mill (1748–1832),(1806–1873)

‘Greatest good for greatest number of people’ (Red Wedding)

Drawbacks

What are some drawbacks of utilitarianism?

Only the greatest good, as a singular body and not distributed among people

Difficulty in quantifying the greatest good

Anthropocentric

Utilitarianism judges by consequences rather than actions

Low probability–high consequence events carry as much weight as high probability–low consequence events

Alternatives

What else can be used?

Justice ethics by Rawls (1971)

Each person is to have an equal right to equal basic liberties

Social and economic inequalities are to the greatest benefit of the least–advantaged

Treating everyone equally is a challenge

Environmental justice for consent-based siting

Other classic PRA cases

The Hyatt Horror [5]

The Pinto Case [6]

WASH1400 documents

Other contemporary cases in media

[5] Pfatteicher, S. K. A., 2000. The Hyatt Horror: Failure and Responsibility in American Engineering. Journal of Performance of Constructed Facilities 14, 62

[6] De George, R. T., 1981. Ethical Responsibilities of Engineers in Large Organizations: The Pinto Case. Business & Professional Ethics Journal 1, 1

Dynamic Risk Assessment (DRA)

Quite simply, DRA refers to time dependent frequencies

$$Risk(t) = f(t) \times C \tag{4}$$

Proposed initially as a way to model complex accident scenarios with higher fidelity [7]

[7] Siu, N., 1994. Risk assessment for dynamic system: An overview. Reliability Engineering & System Safety 43, 43

Typically, some phenomenon is modeled in time and integrated with stochastic models to evolve system risk dynamically [8]

Hazards are advanced in time using appropriate models

Continuous – Integral, differential equations

Discrete – Monte Carlo, Markov

Graphical – Petri nets

Machine Learning – Natural language processing, deep mapping

Bayesian analysis can also be applied to update posterior probabilities in time (ML)

Use of 'bow-tie' analysis to combine event trees and fault trees in time

Fuzzy set theory also can be applied [9]

$$\lambda(t) = \beta t^{\beta-1}\theta^{\beta} \tag{5}$$

[8] Aldemir, T., 2013. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy 52, 113

[9] Redfoot, E. K., et al., 2022. Applying analytic hierarchy process to industrial process design in a nuclear renewable hybrid energy system. Progress in Nuclear Energy 145, 104083

Hypothesis

The hazard (stressor) evolves system component response (SETS) over time

Focus on time dependence allows risk to be re-assessed as new data is obtained

Here, we can integrate with ML as we obtain new data from Characterization

Sounds like specifying system states in time (Alternative Futures?) and defining the transitions between states

Similar to Discrete Event Simulation (DES) [10]? – Each state evolves in time as needed, rather than the entire architecture, thereby allowing a more flexible definition of risk.

Or –

$$Risk(t) = f \times C(t) \; ? \tag{6}$$

Food for thought: Can C(t) reflect resilience?

[10] Lee, J. et al., 2019. Use of discrete event simulation for material throughput. Nuclear Engineering and Design 345, 183

Examples

Review paper

A comprehensive review on dynamic risk analysis methodologies [11]

Hazard identification is the first key part of a risk analysis

Dynamic Logical Analytical Methodology – Markov modelling time-dependent state transition matrix

Dynamic Event Tree Analysis – Models dynamic variation of state space

Food for thought: Possible mechanism for Alternative Futures

Bow Tie model – Qualitatively and quantitatively represents a complete scenario from initial hazard to final consequences

Artificial Neural Network – Updated real time frequencies through a back propagation

[11] Raveendran, A., et al., 2022. A comprehensive review on dynamic risk analysis methodologies. Journal of Loss Prevention in the Process Industries 76, 104734

Water/Gas

Dynamic Bayesian network-based operational risk assessment for industrial water pipeline leakage [12]

Applied dynamic Bayesian network to update frequencies for hydraulic failures

Uses fault trees for hazards where Bayesian updating is used to model frequency

Dry out scenario– Less flow, protection failure, valve failure

Fault tree is updated at discrete time intervals based on failure scenarios

Projecting failures in time can aid in managerial decision-making

[12] Abdelhafidh, M., et al., 2023. Dynamic Bayesian network-based operational risk assessment for industrial water pipeline leakage. Computers & Industrial Engineering 183, 109466

Fault tree for dry-out failure

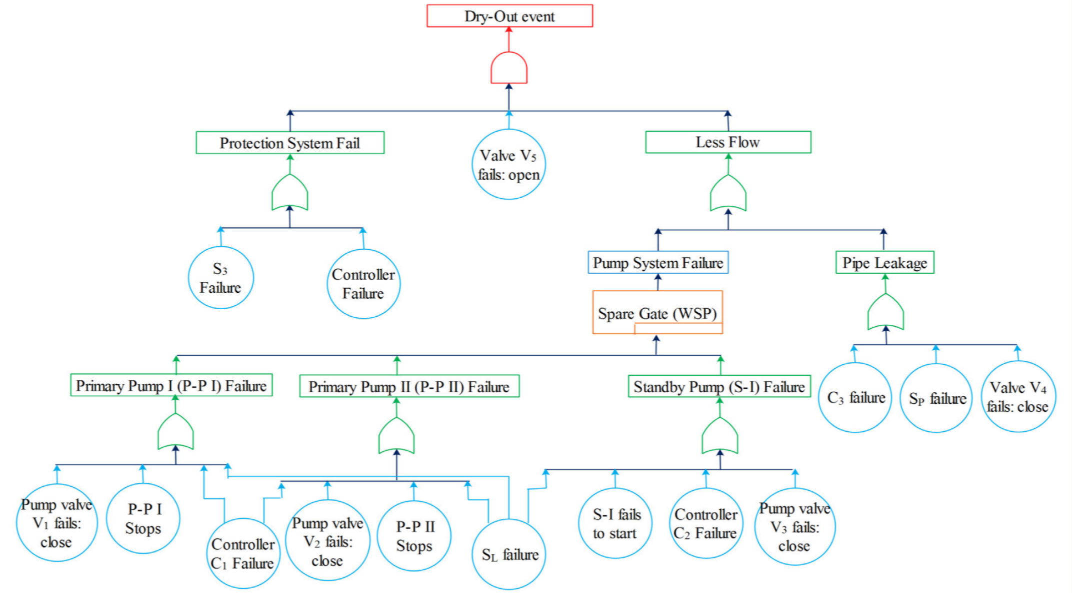


Figure. Fault trees should be precise, clear, and detailed. This could use improvements.

Dynamic risk of coastal flood and driving factors [13]

Combination of urban growth and sea level rise drive significant increases in coastal flood risk

Time dependent component to risk is sea level rise and urban growth

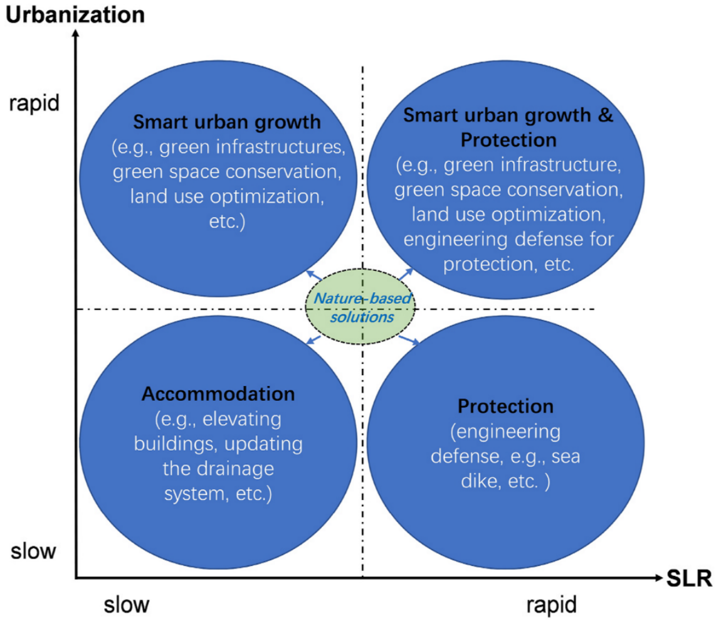
Markov model predicts future land use

Risk defined as physical damage, economic loss due to coastal flooding

Risk informs urban planning strategies

[13] Xu, L., et al., 2021. Dynamic risk of coastal flood and driving factors. Journal of Cleaner Production 321, 129039

Policy alternatives for adapting to coastal flood risk



Smart urban growth
(e.g., green infrastructures, green space conservation, land use optimization, etc.)

Smart urban growth & Protection
(e.g., green infrastructure, green space conservation, land use optimization, engineering defense for protection, etc.

Accommodation
(e.g., elevating buildings, updating the drainage system, etc.)

Protection
(engineering defense, e.g., sea dike, etc.)

Dynamic risk analysis of hydrogen gas leakage using Bow-tie technique and Bayesian Network [14]

Bow-tie and Bayesian Network used to assess risk of hydrogen gas leak from chlorination unit

Bow-tie was used to combine fault trees and event trees

Bayesian network updated posterior & conditional probabilities in the bow-tie in time

Bayes can carry out deductive reasoning on the bow tie to update probability

Food for thought: Possible application of ML.

Decrease in flow rate leading to fire or explosion highest risk

[14] Borgheipour, H., et al., 2021. Dynamic risk analysis of hydrogen gas leakage using Bow-tie technique and Bayesian network. International Journal of Environmental Science and Technology 18, 3613

Bow-tie diagram of hydrogen gas leakage from chlorination unit

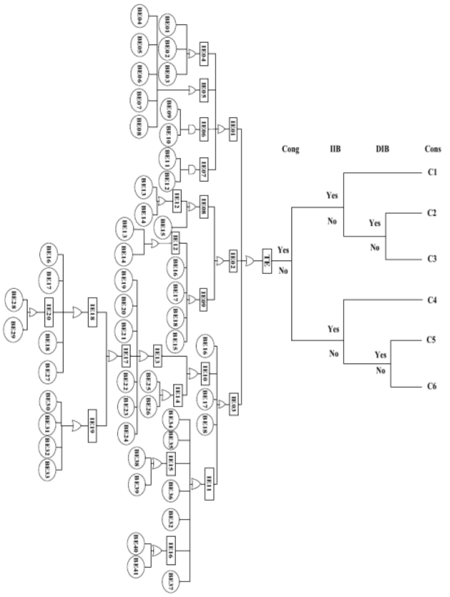


Figure. Bow tie combines fault & event trees by the top event (TE).

Takeaways

What can we learn from DRA relevant to I-CREWS?

DRA is widely applicable to many topics

Based on fundamental risk principles

Difficult to find example directly relevant to I-CREWS strategic goals

Upside – Demonstrates the novelty of I-CREWS

The ‘dynamic’ part of risk assessment is largely focused on frequency analysis

Risk and resiliency should be related but not clear on how yet

We should agree on what risks we will assess and an overall framework

Is a new definition of DRA needed?

References

1. Farmer, F. R., 1967. Reactor Safety and Siting: A Proposed Risk Criterion. Nuclear Safety 8, 539.
2. Kaplan, S. et al., 1981. On the quantitative definition of risk. Risk Analysis 1, 11.
3. Root, S. J., et al., 2023. Cyber Hardening of Nuclear Power Plants. Progress in Nuclear Energy 162, 104742.
4. Der Kiureghian, A. et al., 2009. Aleatory or epistemic? Does it matter? Structural Safety 31, 105.
5. Pfatteicher, S. K. A., 2000. The Hyatt Horror: Failure and Responsibility in American Engineering. Journal of Performance of Constructed Facilities 14, 62.
6. De George, R. T., 1981. Ethical Responsibilities of Engineers in Large Organizations: The Pinto Case. Business & Professional Ethics Journal 1, 1.
7. Siu, N., 1994. Risk assessment for dynamic system: An overview. Reliability Engineering & System Safety 43, 43.
8. Redfoot, E. K., et al., 2022. Applying analytic hierarchy process to industrial process design in a nuclear renewable hybrid energy system. Progress in Nuclear Energy 145, 104083.
9. Aldemir, T., 2013. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy 52, 113.
10. Lee, J. et al., 2019. Use of discrete event simulation for material throughput. Nuclear Engineering and Design 345, 183.
11. Raveendran, A., et al., 2022. A comprehensive review on dynamic risk analysis methodologies. Journal of Loss Prevention in the Process Industries 76, 104734.
12. Abdelhafidh, M., et al., 2023. Dynamic Bayesian network-based operational risk assessment for industrial water pipeline leakage. Computers & Industrial Engineering 183, 109466.
13. Xu, L., et al., 2021. Dynamic risk of coastal flood and driving factors. Journal of Cleaner Production 321, 129039.
14. Borgheipour, H., et al., 2021. Dynamic risk analysis of hydrogen gas leakage using Bow-tie technique and Bayesian network. International Journal of Environmental Science and Technology 18, 3613.

I-CREWS