

Site Assessment and Probabilistic Risk Analysis (PRA) of Grid Computing Facilities

Joe Higgins Staff Engineer Sun Labs
Robert Sewell Senior Staff Engineer
Sun Microsystems

Agenda

- Introduction
 - Business and societal risks of grid computing
- Risk management and decision analysis
- Environmental & operational variables
- PRA techniques and approaches
- Example

Business and Societal Risk

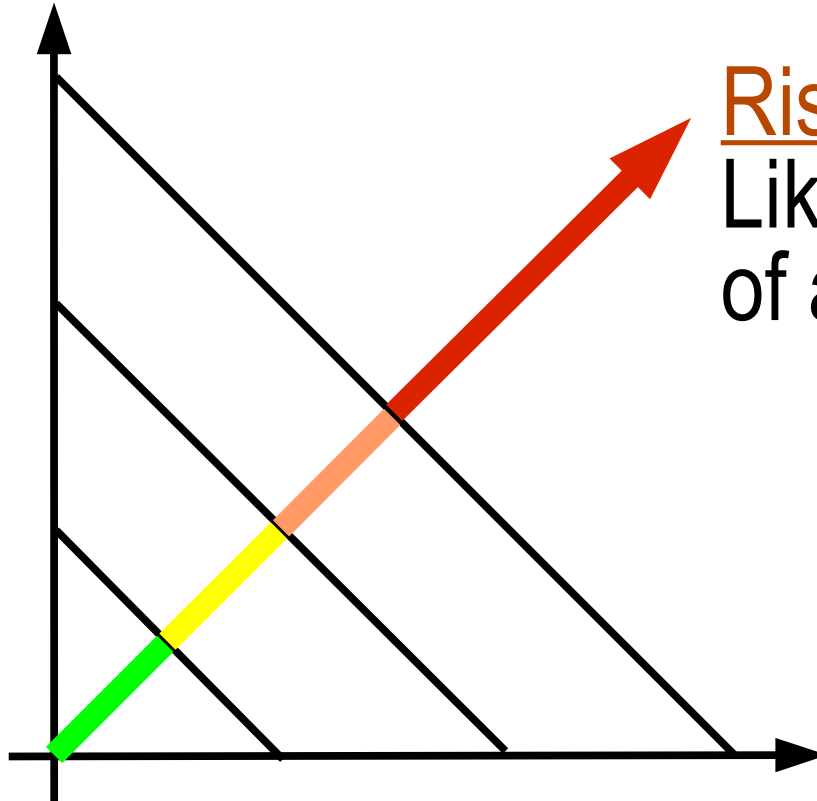
- Non-Mission Critical applications
 - Types of systems
 - Acceptable reliability
- Mission Critical applications
 - Types of systems
 - Acceptable reliability
- Regulations
- Conveying reliability/risk to a customer
 - Education
 - Standards

What is Risk?

- We associate the word “Risk” with something that has a chance of producing an adverse outcome
 - What can go wrong?
 - How likely is it?
- To understand Risk, we need to be able to:
 - Identify the various scenarios leading to adverse outcomes
 - Assess the scenario consequences/outcomes
 - Assess the scenario likelihoods

The Concept of Risk

Likelihood



Risk : Increases with
Likelihood and Severity
of an Outcome

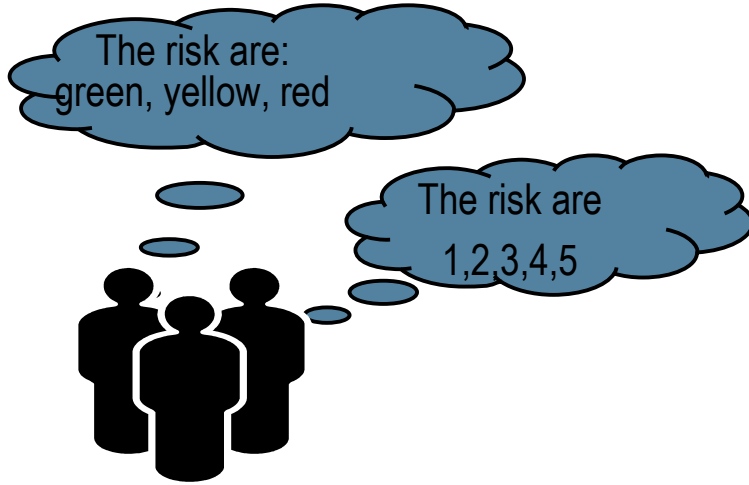
Undesirability (Severity)
of Consequences

Goal of Risk Management: Reward – Risk Target

- Rewards require risks
- Strive to
 - Hit 1
 - Avoid 4
 - Move 2, 3 toward 1
- How to best accomplish this?

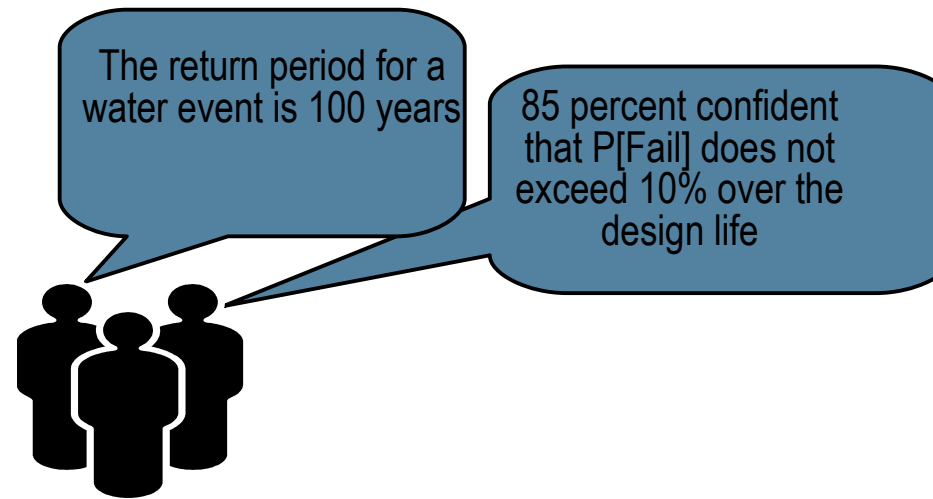


Communicating Risk



Qualitative

Truthiness
ad-hoc

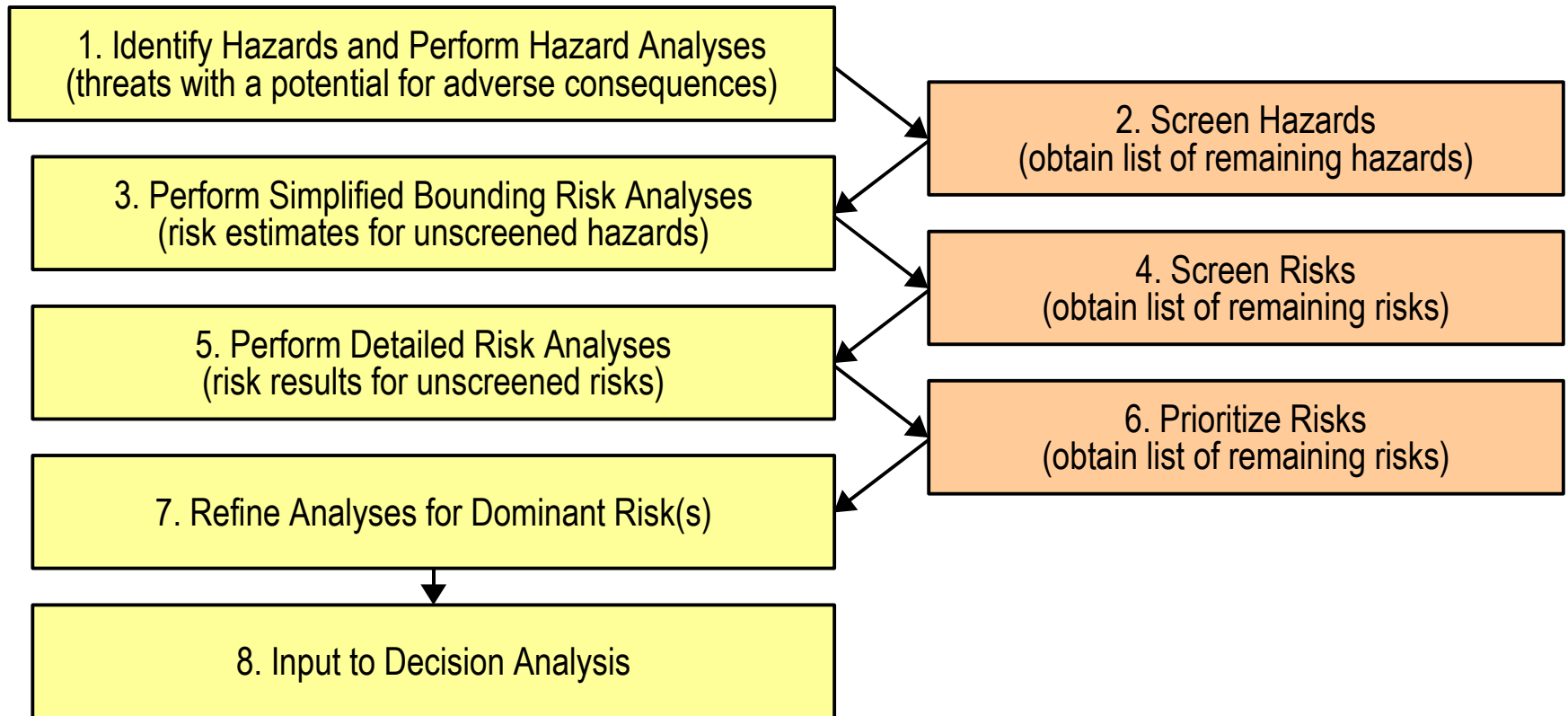


Quantitative

facts
reproducible

Probabilistic Risk Assessment Methods

General Risk Assessment



Generalized Approach to Risk Quantification

- For each unscreened hazard/risk:
 - Identify a complete set of possible adverse scenarios
 - Quantify consequences of each scenario
 - Quantify likelihoods of each scenario, using probabilistic analyses:
 - Hazard analysis results; and
 - Fragility / vulnerability analysis results

Risk Quantification

- Generalized mathematical formulation

$$\begin{aligned}
 \lambda[\text{Adverse Consequence}] &= \sum_{\text{All Scenarios, } k} (\text{Rate of Scenario})_k \times P[\text{Adverse Consequence}]_k \\
 &= \sum_{\text{Hazard Scenarios, } S} v_S P[\text{Threat Level, } T]_S \times \\
 &\quad \sum_{\text{Vulnerability Scenarios, } V|T} P[\text{Vulnerability Level} = V | T] \times P[\text{Adverse Consequence} | (V \text{ and } T)]
 \end{aligned}$$

λ denotes likelihood

v denotes rate of occurrence

Advantages of Generalized Procedure

- Risk and reliability problems that pertain to vastly different phenomena (e.g., unavailability of a computer system due to over-current failure in a circuit versus core damage of a nuclear power plant due to aircraft impact) can be evaluated in very similar ways

Data Needed for Risk Quantification

Expert Assessments (Experienced-Based Data)

Identify Scenarios
Describe Scenarios
Develop
Subjective Probabilities

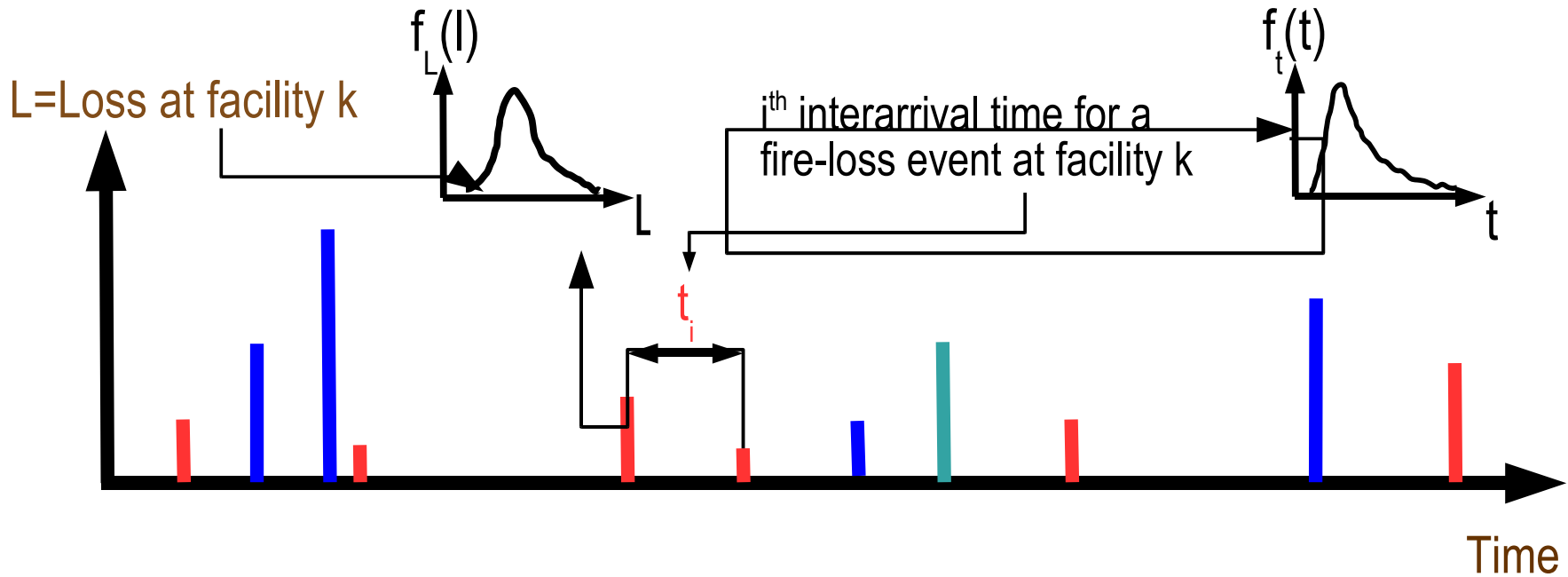
Numerical Data

Suggests Scenarios
Enables Direct Quantification
of Rates and Probabilities

Partial List of Environmental & Operational Hazards

<i>Hazard</i>	<i>Hazard</i>	<i>Hazard</i>
Loss of HVAC	Onsite impulse/vibratory event	Water leaks and moisture intrusion
Loss of air quality (particulate, humidity)	Earthquake ground shaking	Security breaches/violations
Loss of onsite cooling water (building services)	Tornado	Violations of operating procedures
Loss of onsite water treatment	Hurricane	Violations of maintenance procedures
Loss of offsite water treatment	Flooding	Violations of safety procedures
Loss of normal onsite power (building services)	Lightning storm	Errors in procedures
Loss of emergency onsite power (back-up power)	External/offsite fire	Cosmic radiation and related natural events
Loss of onsite battery back-up	Ground/foundation deformations	Man-caused electrical and electromagnetic fields
Loss of lighting (building services)	Structural failures	Electrostatic discharge
Loss of offsite power	Adverse component interactions; falling components	Mislabeled components, cabling, signage
Onsite fire	Nearby transportation accidents	Loss of network connectivity
Onsite explosion	Aircraft crashes	failure of telemetry sensors

Example: Catastrophe Risk



Source of Loss Event:

- Fire
- Earthquake
- Flood
- Tornado
- Aircraft Crash
-
- Other Events

Example: System Outages

L = Outage Duration at Site k

$f_L(l)$

i^{th} interarrival time for System 1 outage at site k

$f_t(t)$

t

Time

Source of Outage Event:



.....

System 1

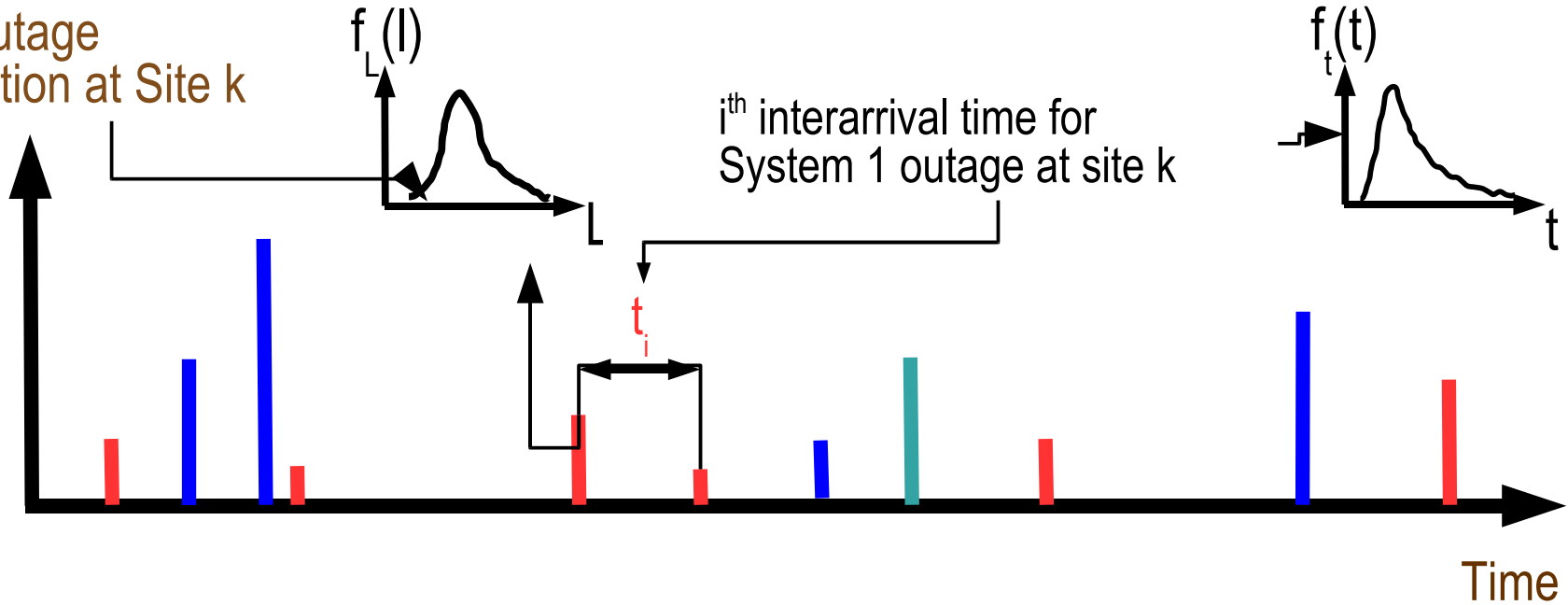
System 2

System 3

System 4

System 5

Other Systems



Example Decisions Using Risk Quantification

- Decide on a design that explicitly achieves a desired safety or reliability level
- Decide if risk is acceptably low, and if not, what is the most effective risk mitigation strategy

PRA Tools

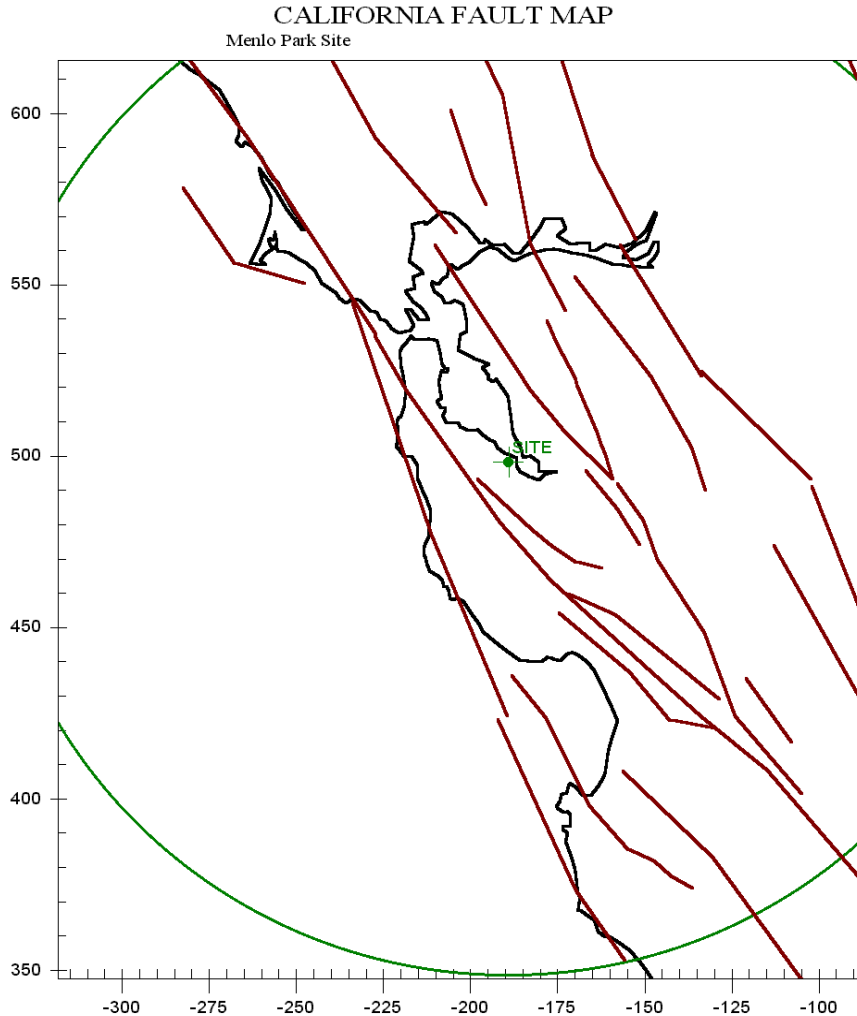
- Tools for Developing Scenarios:
 - Failure Modes and Effects Analysis (FMEA)
 - Physical inspection of components and systems
 - Logic models
 - Event trees, fault trees, logic/decision trees
- Tools for Quantifying Probabilities/Likelihoods
 - Failure analysis
 - Failure rate data and probability analysis
 - Expert opinion and subjective probability analysis
 - Bayesian probability updating
- HRA (human reliability analysis) understanding human error

Example, Simplified Hazard Results: Earthquake Hazard

- Representative Sites
- Typical Results
 - > Hazard curves
 - > Return period versus ground acceleration
 - > Probability of exceedance for given duration
 - > 475-year response spectrum
 - > Map of nearby fault locations
 - > Distance to nearest fault(s)
- Influence of soil/site conditions

- Sample of Applicable Tools for Geo-Hazards
 - > Hazard analysis software
 - > USHAZ
 - > Multi-risk software
 - > e.g., by EQE/ABS, RMS, AIR, REI
 - > GIS software
 - > ESRI, ARCInfo, MapInfo
 - > Existing reports, databases, and web tools (governmental agencies)
 - > USGS, CGS, USNRC/LLNL

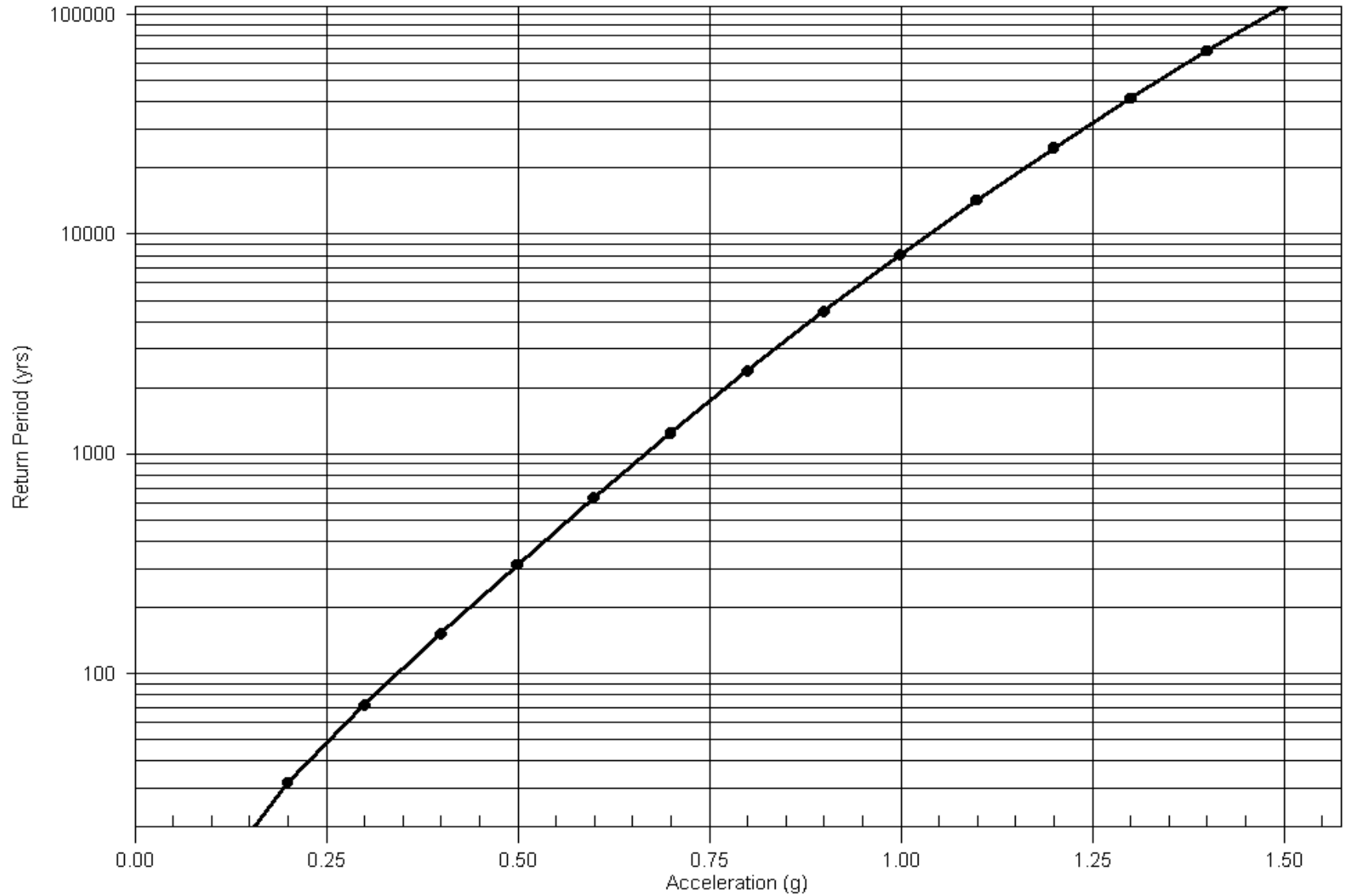
Menlo Park



- Nearest Faults:
 - > Monte Vista—Shannon
 - > 6.1 miles
 - > San Andreas
 - > 7.6 miles
- Site Coordinates
 - > Lat/Lon
 - > 37.4844 N
 - > 122.1484 W

RETURN PERIOD vs. ACCELERATION

Menlo Park, Rock



Conclusion:

- We can apply leverage work in other fields and apply it to understanding grid risk
- These environmental effects can have a serious impact the reliability of a grid.
- Bring in experts when needed.
- Contact us:
 - > joe.higgins@sun.com
 - > robert.sewell@sun.com

Site Assessment and Probabilistic Risk Analysis (PRA) of Grid Computing Facilities

Joe Higgins Staff Engineer Sun Labs
Robert Sewell Senior Staff Engineer
Sun Microsystems