



A Risk-centric Decision Process that Leads to Improved Defect Detection and Prevention



Martin S. Feather
Jet Propulsion Laboratory
California Institute of Technology

Martin.S.Feather@Jpl.Nasa.Gov

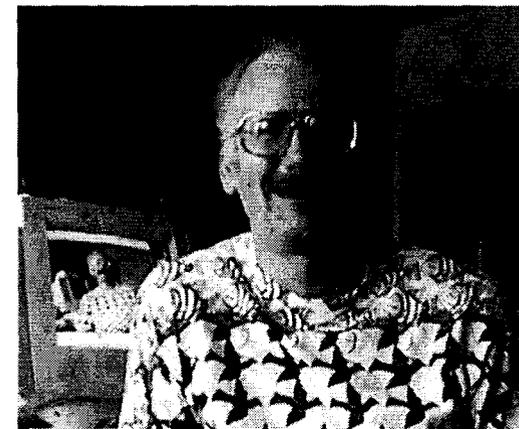
This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Funded by NASA's Code Q (FDDP program and IV&V ARRT task) and Code R (ECS program).

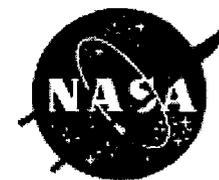
Reports on use of the DDP tool, the lead for which is JPLer Steve Cornford →

<http://ddptool.jpl.nasa.gov>

CL 02-446



NASA's mission challenges



– Groundbreaking

- New mission concepts, new technologies (autonomy, agents, ...), unknown environments

Past experience provides only a partial guide

– Multi-disciplinary

- Navigation, telecom, fault protection, commanding/sequencing, ...
- Cross-coupled interactions

No individual is an expert in all areas

No individual can juggle all the details at once

– Resource constrained

- Schedule and budget, testbeds,
- CPU, RAM, data storage, bandwidth,

Many risks that, if untamed, lead to cancellation, underachievement, or even loss of mission

– Need good decisions early

- Cost of correcting a bad decision escalates over time

Early on, lack information (e.g., detailed design) on which to base decisions

What do you want?

“Objectives”
“Requirements”
“Goals”

Mick Jagger
(Rolling Stones):

“You can’t always get what you want”

Descoping – strategic abandonment of objectives.

Reprioritize objectives; primary, secondary...

Determine attainment if given additional resources (\$, mass, ...)

What can get in the way?

“Risks”
“Failure Modes”
“Defects”

Dr. Michael Greenfield
(NASA HQ):

“Risk as a resource”

Trade risk for other resources.

Use risk as an intermediary between other resources.

What can you do about it?

“Mitigations”
“Solution Options”
“Preventions, Analyses, Controls, Tests – PACTs”

Matt Landano
(JPL):

“Do the right thing & do it right”

Can’t afford all possible mitigations, so must choose judiciously.

Know the purpose(s) of each mitigation.

Objectives

Risks

Mitigations

~~Return data Software bug ridden Become CMM level 3~~

Insufficient detail for decision making. Elaborate!

In flight s/w upgrades	Requirements risks	Requirements practices
Code/Data separable	Unstable	Documented
Real-time control loops	Incomplete	Formal CM
Sync to external clock	Unclear	Peer review
Tolerate memory errors	Invalid	Formal inspections
Run time memory =...	Infeasible	Formal reviews
Storage = ...	Unprecedented	Criticality analyses
CPU utilization = ...	Large size/complex	Verifiability check

...

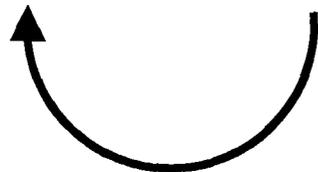
...

...

Risk

x Objective :

How much of objective will be lost if risk occurs? – “Impact”



Mitigation

x Risk:

How much will risk be reduced if mitigation applied? – “Effect”



Elaborate enough to be able to say by *how much*

Day 1 – day of the pessimists!

Objectives – *what you want*

Risks* – *what could occur to detract from attaining objectives*

Impact (Objective x Risk) – *proportion of the Objective lost if Risk occurs*

* *All risks, including those whose mitigation is planned:*

Makes available for scrutiny explicit assertions of risk reduction

Allows risk and its mitigation to be involved in trades

Reveals dependencies on mitigations (what if can't do it on time?)



Experts' estimates, past
experience if available,
models & simulations...

Day 2 – day of the optimists!

Mitigations – *what could be done to reduce risk*

Effect (Mitigation x Risk) – *proportion by which Mitigation reduces Risk*

Day 3 – day of the realists!

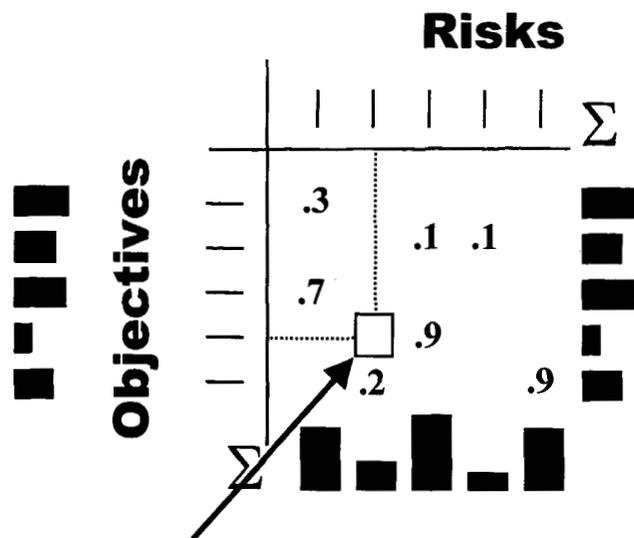
Select – Mitigations to perform
Objectives to discard
Resources to ask for

Decision-making guided by
accumulated information

Getting the right people is key!!!

Mission scientists, technologists, relevant disciplines' engineers,
assembly/integration, testing, QA, operation, programmatic

Day 1 – day of the pessimists!



Impact – proportion of objective lost if risk occurs

Sum the rows: how much each objective is “at risk”.

Sum the columns: how much each Risk causes loss of Objectives.

Objectives – *what you want*
have **weights** (their relative importance)

Risks – *what could occur to detract from attaining objectives*
have **a-priori likelihoods** (how likely they are to happen if not inhibited by Mitigations), usually left at the default of 1 (certain!)

Impact (Objective x Risk) - *proportion of the Objective lost if Risk occurs*
Combine *additively*: $I_1 \& I_2 = I_1 + I_2$
(therefore objectives can be more than 100% killed!)

Disagreement about an impact number usually (always?) resolved by refinement of Objective and/or Risk

Day 2 – day of the optimists!



Mitigations

- *what could be done to reduce risk*
- have **costs** (\$, schedule, high fidelity test beds, memory, CPU, ...)
- have **type** (prevention, detection, alleviation)
- have **status** applied / not applied: major purpose is to decide which to apply!

Effect (Mitigation x Risk) – *proportion by which Mitigation reduces Risk*

Combine as serial “filters”:

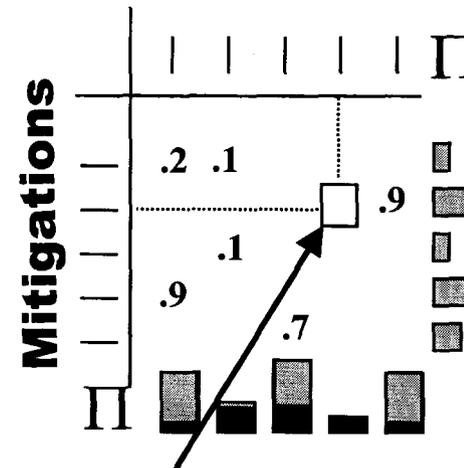
$$E1 \ \& \ E2 = (1 - (1-E1)*(1-E2))$$

- e.g., a 0.8 effectiveness Mitigation catches 80% of incoming Risk ,
- a 0.3 effectiveness Mitigation catches 30% of incoming Risk ;
- 100% -> 20% -> 14% so together have 86% effectiveness

$$(1 - (1 - 0.8)*(1 - 0.3)) = (1 - 0.2*0.7) = (1 - 0.14) = 0.86$$

Note: a law of diminishing returns as apply additional Mitigations

Risks



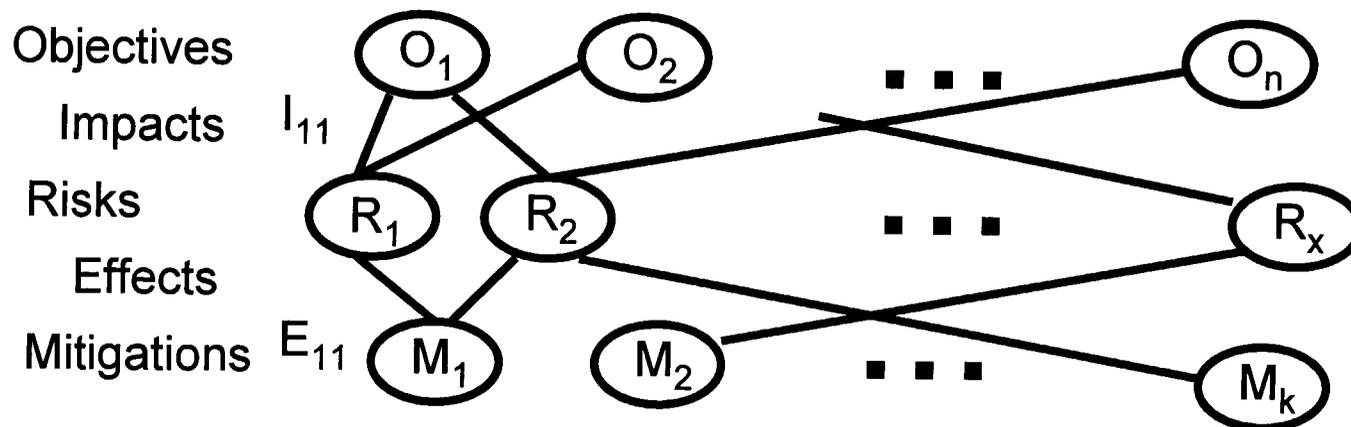
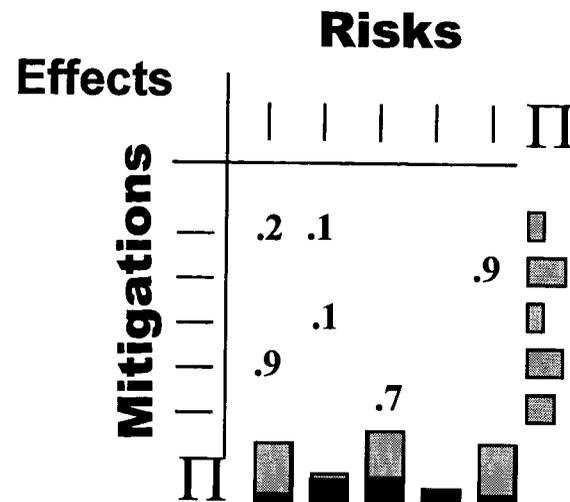
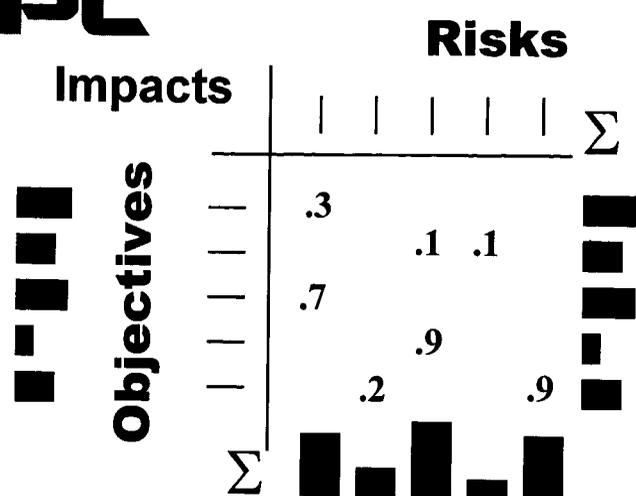
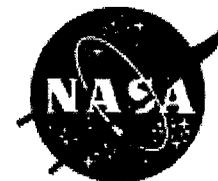
Effect – proportion by which risk reduced if mitigation applied

Sum the rows: how much each Mitigation reduces Risks; “solo” or “delta”.

Sum the columns: how much each Risk detracts from Objectives (1) when Mitigations off, (2) when Mitigations on.

Note: some mitigations can make risks worse (increase likelihood or impact)!

Day 3 - day of the realists!



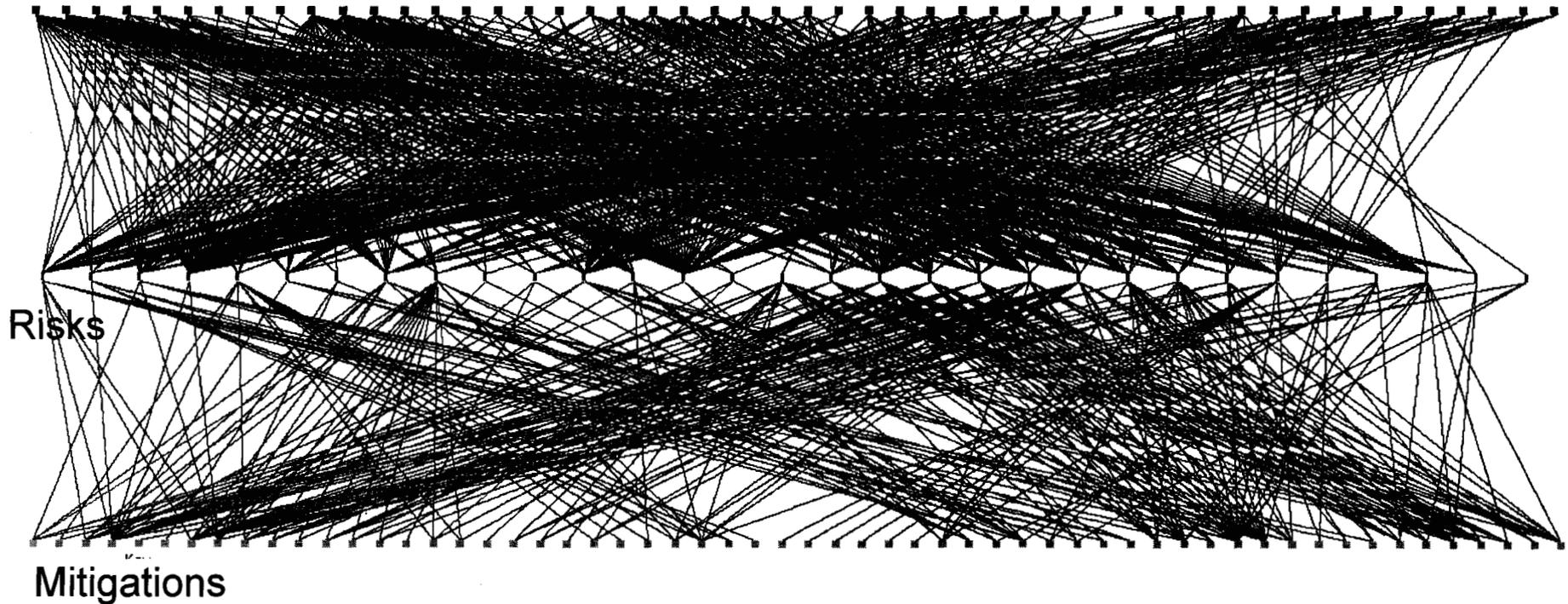
Goal: select mitigations so as to cost-effectively reduce risk

Typical DDP information set:



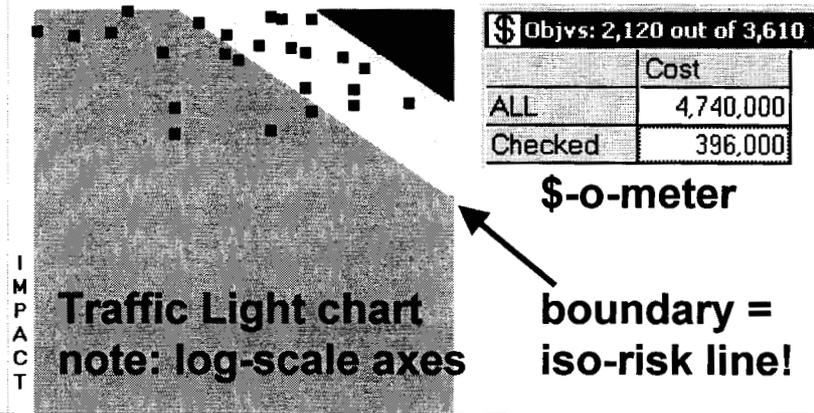
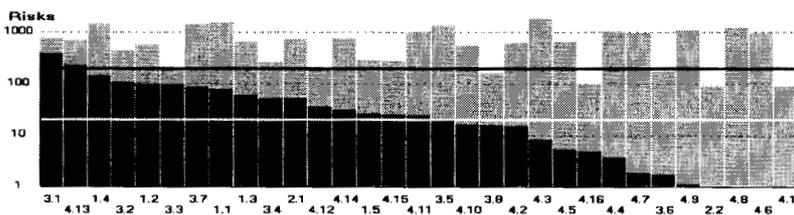
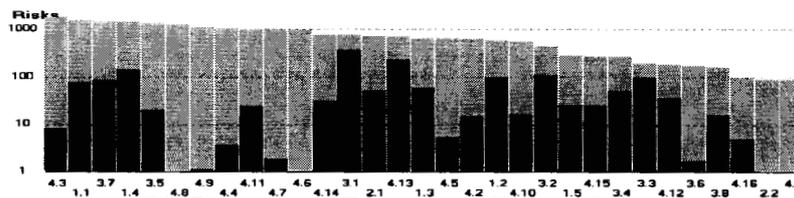
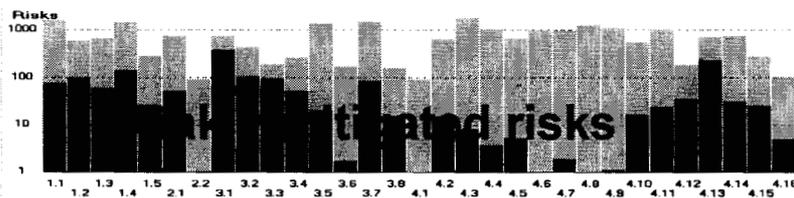
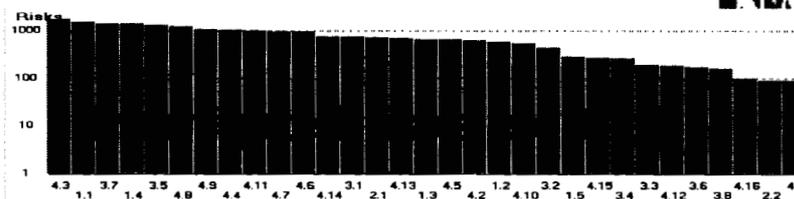
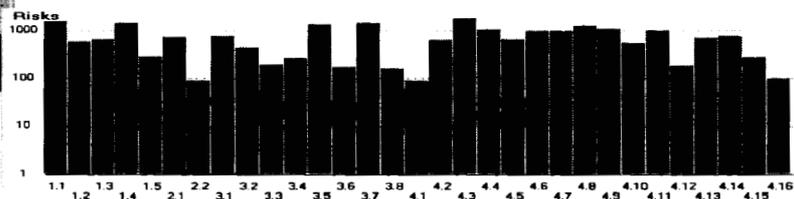
JPL 50 objectives, 31 risks, 58 mitigations

Objectives

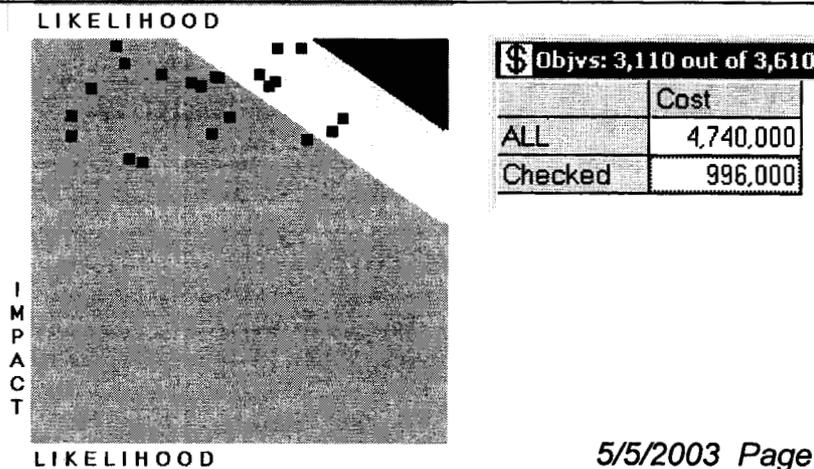
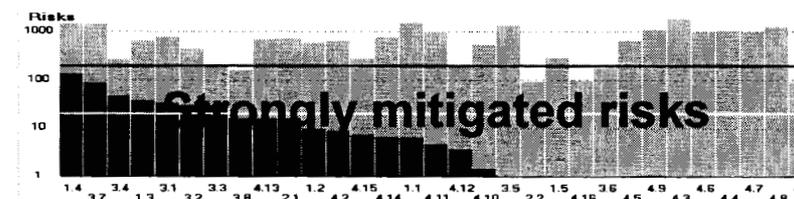


**DDP process and custom tool enables models
of this scale to be built and used effectively**

Visualizations of aggregate information



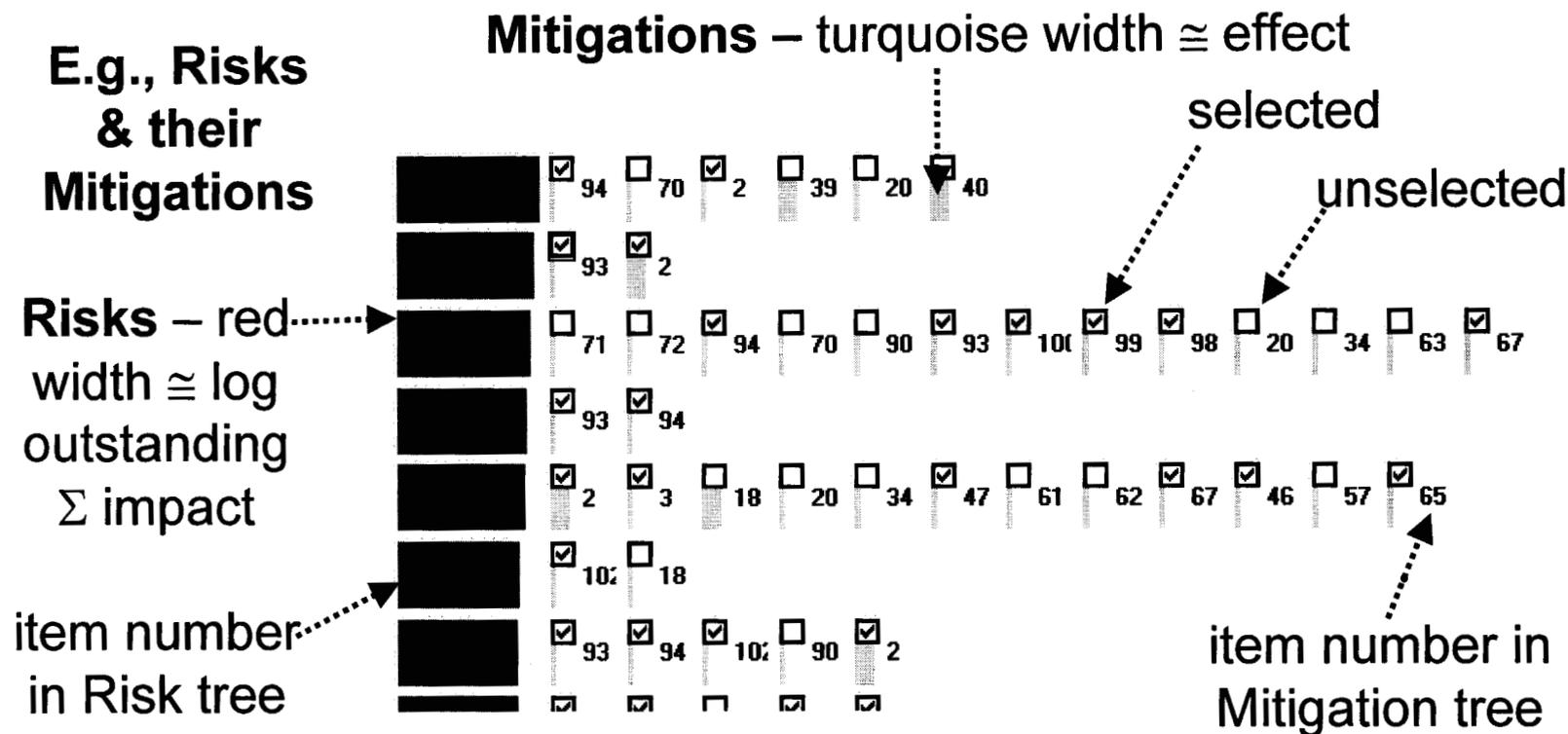
Red = remaining risk
Green = mitigated risk (but at a cost)



Goal: select mitigations so as to cost-effectively reduce risk

“Stem-and-leaf”(*) visualization of DDP

JPL parse matrices



(*) Tuftte attributes these to John W. Tukey, “Some Graphical and Semigraphic Displays” Their usage was introduced into RBP (DDP without numbers) by **Denise Howard & Chris Hartsough**, extended further by us in DDP.

Typical DDP screenshot



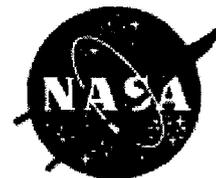
The screenshot displays a software interface for Design Definition Process (DDP) management. It is divided into three main sections:

- Objectives:** A tree view on the left showing various requirements such as "3.1.3: 200 cycles, e.g., for LED, GEC", "3.2: Survive launch", and "4:ilities". Each objective has a weight and a checkbox indicating its status.
- Risk, Mitigs:** A central panel showing a list of risks and their associated mitigations. A specific risk is highlighted with a box, and its mitigations are listed below it.
- Objective Drivers:** A bar chart at the bottom showing the impact of various objectives on different risk categories. The chart has a logarithmic y-axis (1, 10, 100, 1000) and an x-axis with numerical labels.

Annotations on the screenshot include:

- An arrow pointing from the "Objective Drivers" bar chart to the "Risk, Mitigs" list, with the text: "Click objective's bar to get list of risks impacting it".
- Text on the right side of the "Risk, Mitigs" panel: "Lists of mitigations applicable to each risk".

JPL Examples of DDP-assisted improvements

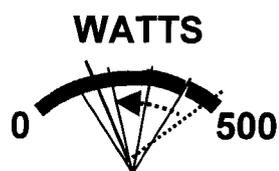


▪ Cost & Time Saved

\$\$\$

- At least two instances of savings > \$1M (per study cost: \$10K - \$30K)
 - E.g., Storage technology study revealed problematic overly-stringent requirement, whose removal permitted dramatic cost & time savings

▪ Designs Improved



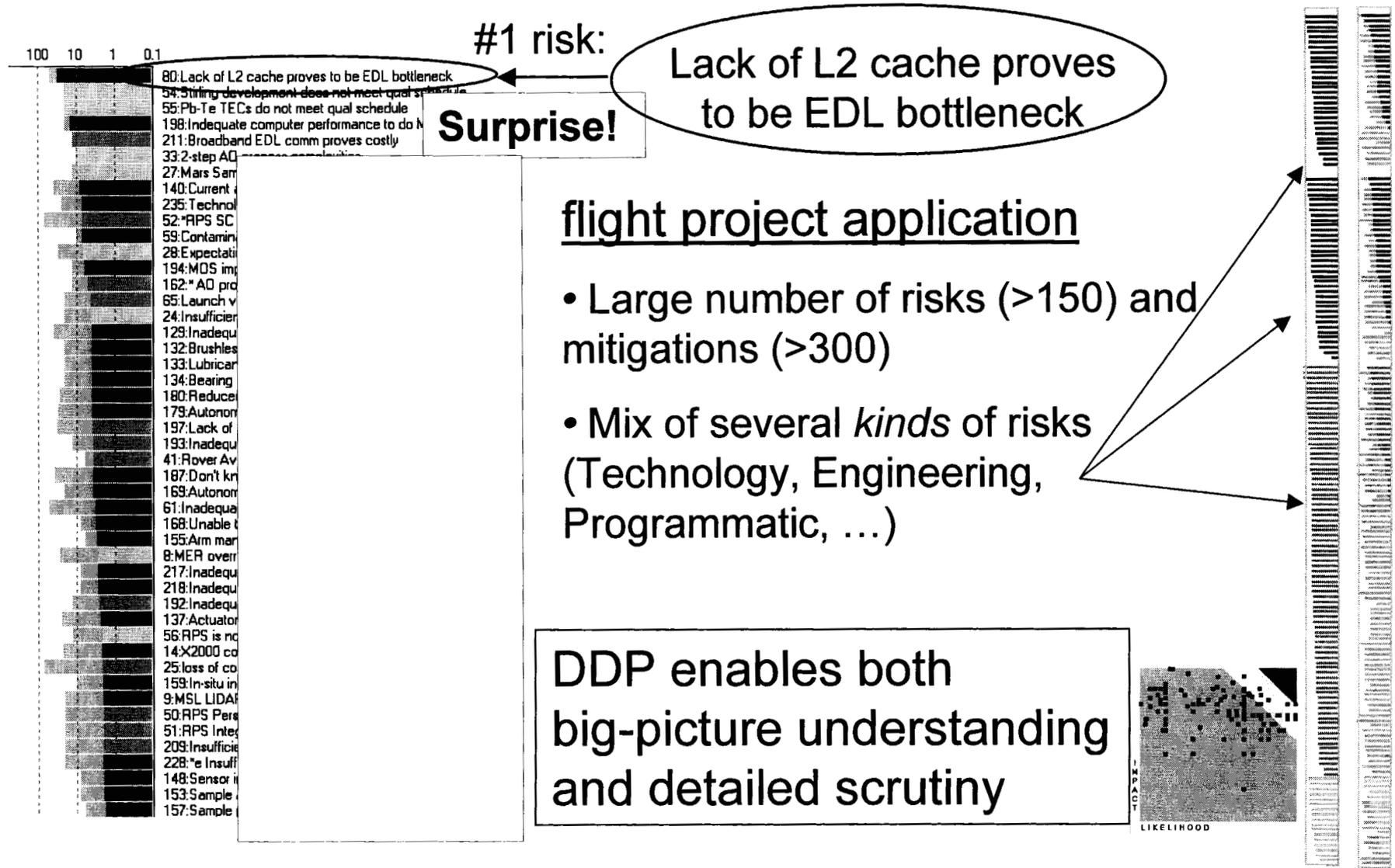
- Savings of critical resources (power, mass, ...) seen in comparison of designs before & after DDP sessions
 - E.g., LTMPF redesign: power needs decreased by 68%, mass decreased by 13%, cost decreased by 9%, major category of risk changed from architectural to well-understood design

▪ Reliability and Safety Increased



- Non-obvious significant risks identified and mitigated
 - E.g., Lander – Sufficient L2 cache size on computer identified as critical to successful EDL

Flight Project risk insights from DDP



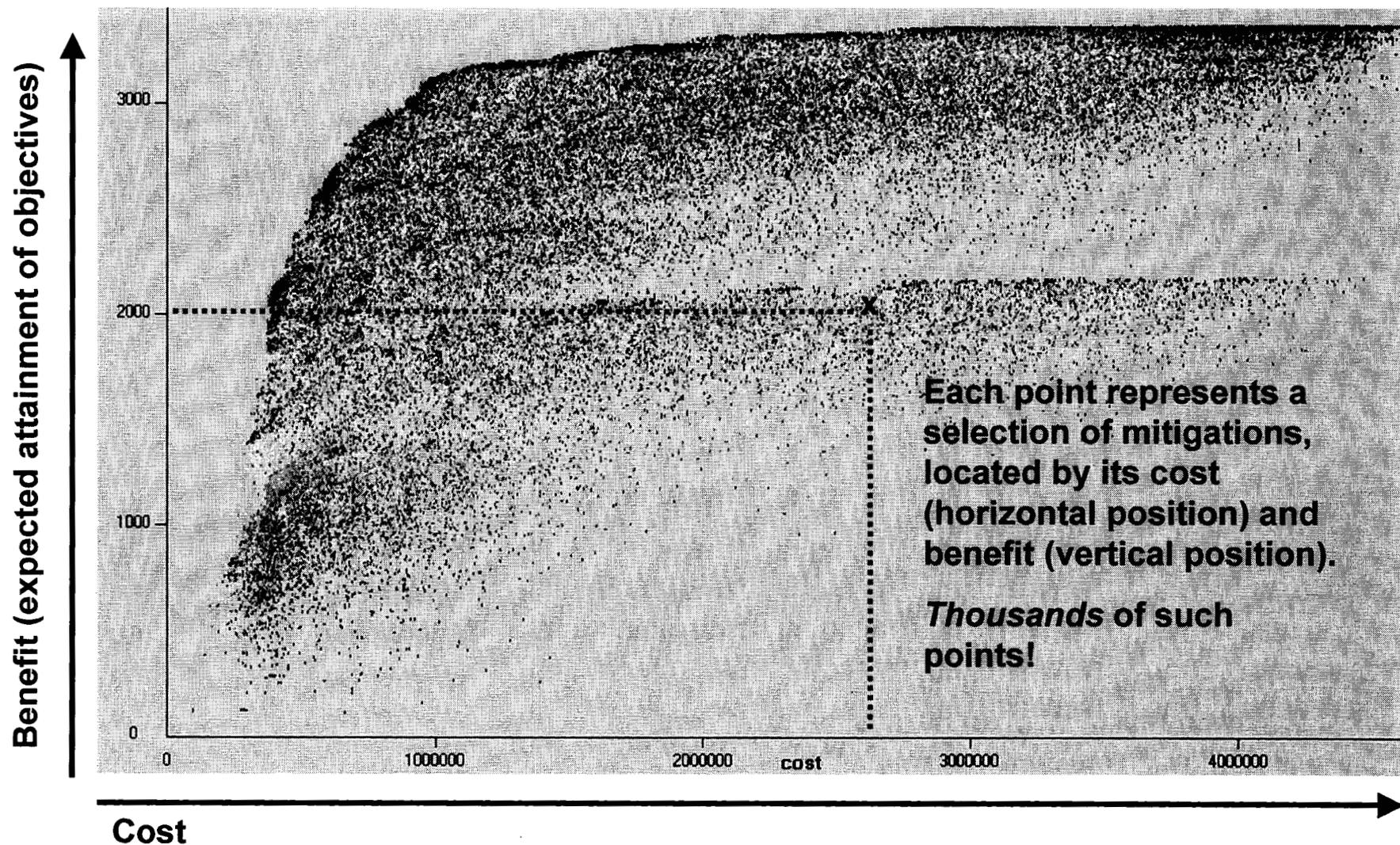
Cost-Benefit trade space



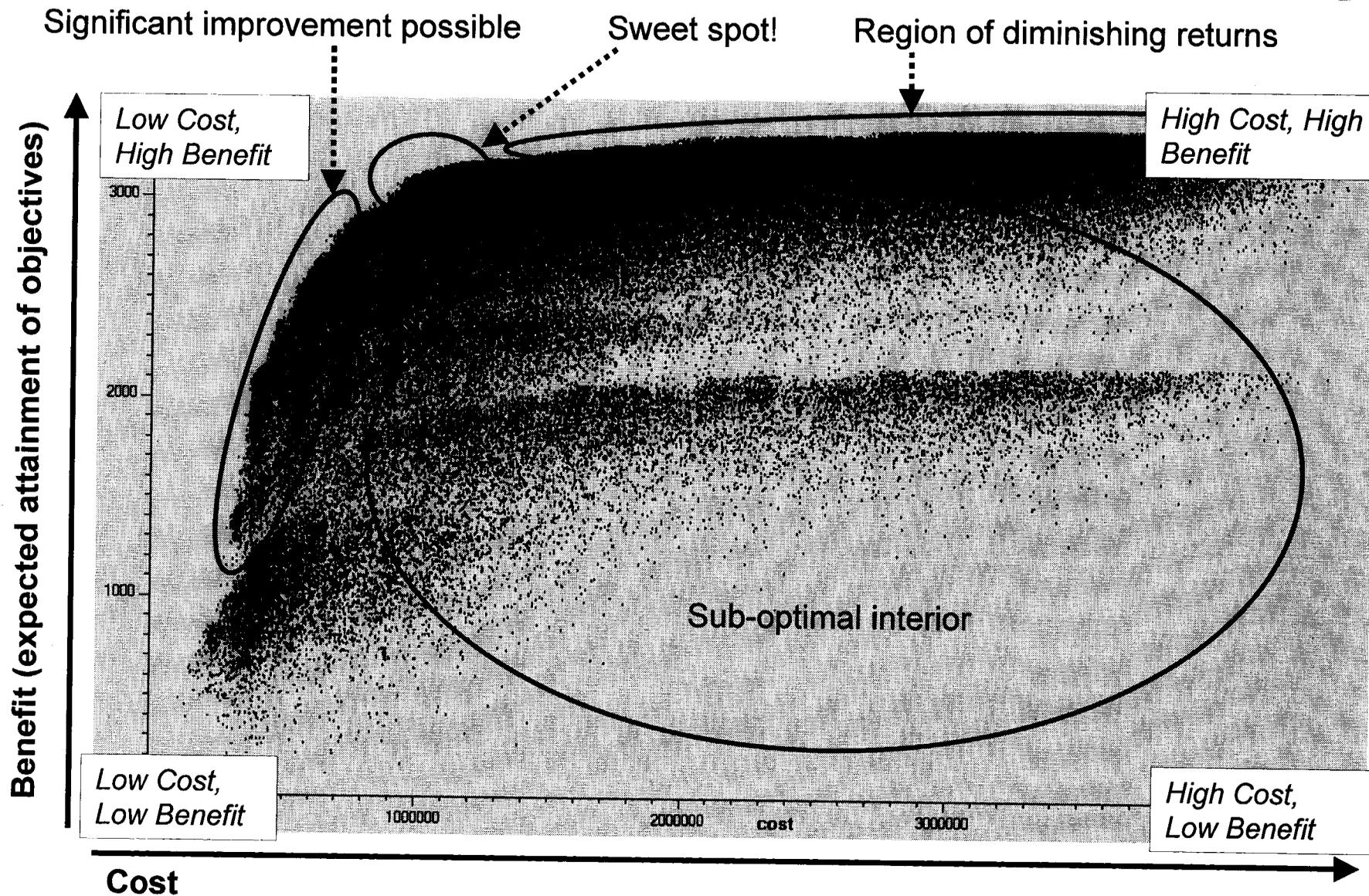
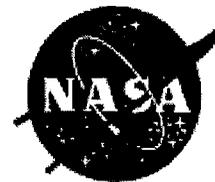
JPL

8 mitigations = 2^{58} (approx 10^{18}) ways of selecting.

Simulated Annealing used to search for near-optimal selections.

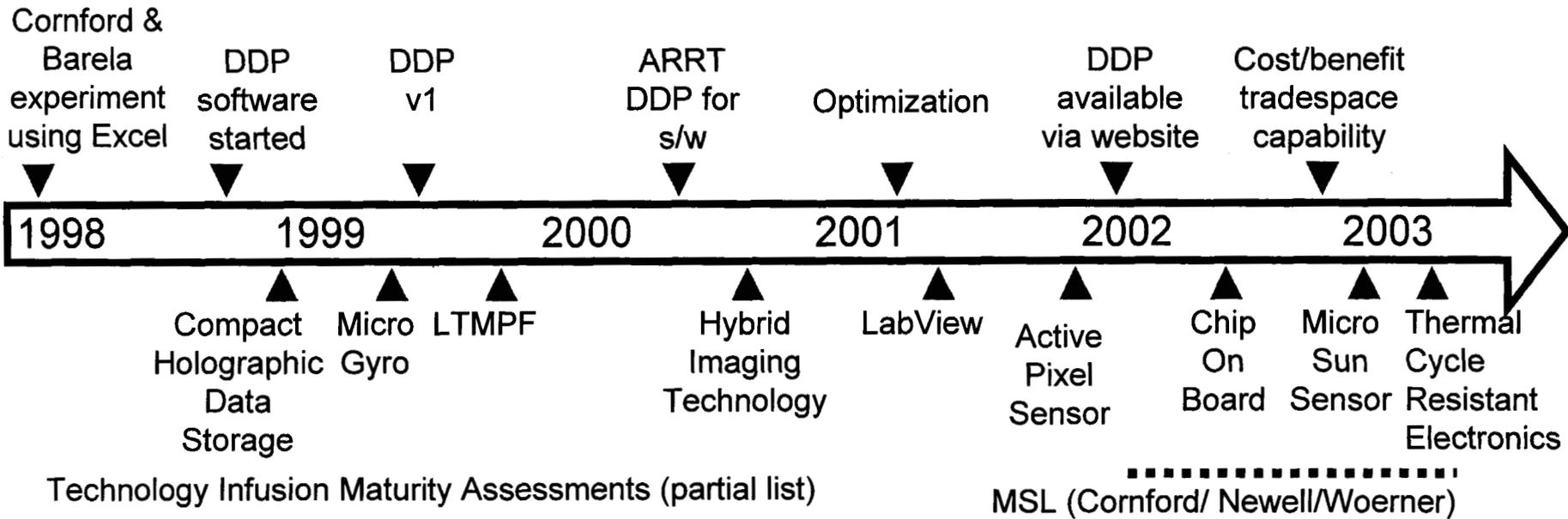
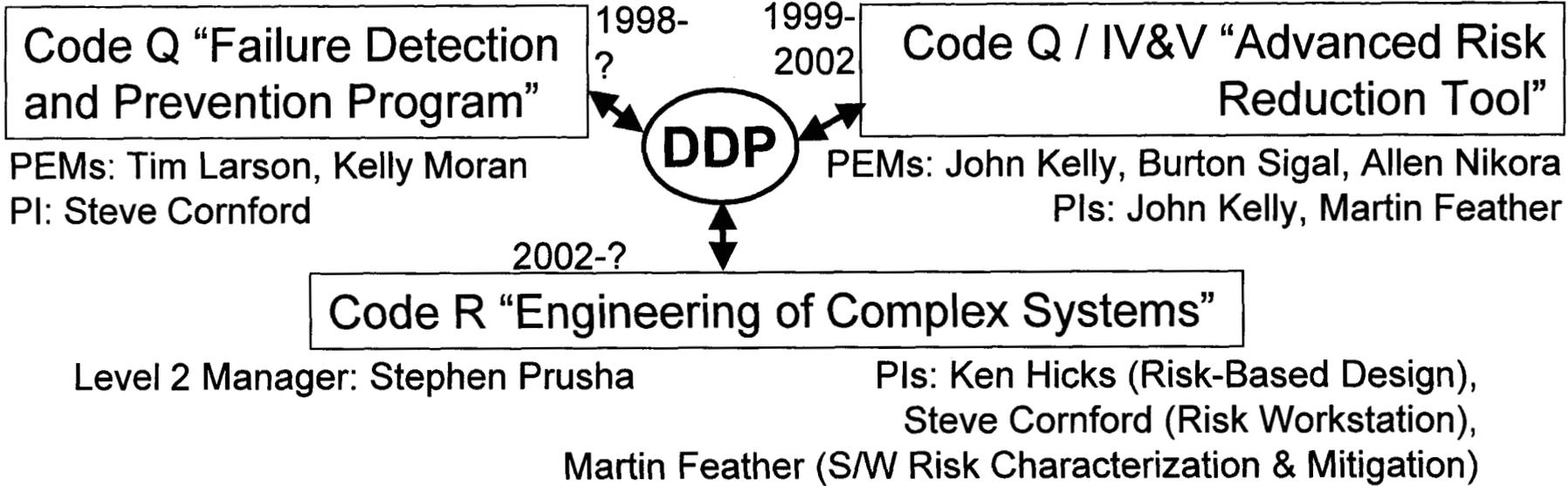


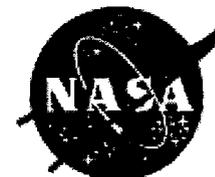
Cost-Benefit trade space insights





DDP Timeline





PRA

Benefits

Probabilistic Risk **Assessment** computes risk from knowledge of:

- o Individual components' reliabilities (e.g., MTBF)
- o System architecture (e.g., Fault Tree)
- o Calculate system risk / reliability
when system too expensive/complex/long lived/critical to directly measure
- o Gain insight into system vulnerabilities
(e.g., cut-sets indicate key contributors to failure)

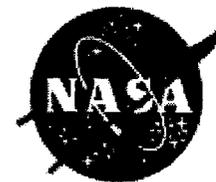
PRR

Benefits

Probabilistic Risk **Reduction** computes risk from knowledge of:

- o Individual risk mitigation activities (e.g., inspection, unit testing)
- o Potential risks - both product risks and process risks (e.g., late/over-cost)
- o Quantitative assessments of mitigations' effectiveness (at reducing risk) and risks' impacts (on system objectives)
- o Calculate system risk / reliability
when development process key system assessment (e.g., software)
- o Select mitigations to most cost-effectively reduce risk
- o Identify problematic objectives (those with expensive-to-reduce risks)
- o Gain insight into risks (reduction of, remaining) & mitigations (purpose)

CONCLUDING SUMMARY



- Information: make use of information available early in lifecycle
 - Combine knowledge from experts and past experience
 - Accommodate both evidence and estimates
- Process: gather the right information the right way
 - Objectives, including their relative importance
 - Risks, and by how much they impact objectives and requirements
 - Mitigations, and by how much their use would reduce risk
- Tool support: effectively handle voluminous amounts of information
 - Capture experts' knowledge on-the-fly during intensive sessions
 - Present information through cogent visualizations
 - Derive additional knowledge via calculation and search

<http://ddptool.jpl.nasa.gov>

Steven L. Cornford@Jpl.Nasa.Gov

Martin.S.Feather@Jpl.Nasa.Gov