Operationalization and Enhancement of the Advanced Risk Reduction Tool (ARRT)

JPL California Institute of Technology

Presentation to the 2nd Annual NASA Office of Safety and Mission Assurance (OSMA) Software Assurance Symposium (SAS)

Dr. Martin S. Feather
ARRT Center Initiative Lead*
Jet Propulsion Laboratory
California Institute of Technology

Martin.S.Feather@Jpl.Nasa.Gov
http://eis.jpl.nasa.gov/~mfeather

*Initiative began in 1999 with Dr. John Kelly as Lead

ARRT Acknowledgements

Heritage & Contributors ARRT is inspired by, and based on:
JPLer Steve Cornford's Defect Detection and Prevention (DDP)
and JPLer Tim Larson's Risk Balancing Profiles (RBP).

contributors (JPL)

John Kelly
Burt Sigal
James Eddingfield
Steve Cornford
Phil Daggett
Julia Dunphy
Denise Howard
Chris Hartsough

contributors (other)

Jim Kiper (U. Miami, Ohio)
William Evanco (Drexel)
Steve Fickas (U. Oregon)
Martha Wetherholt (NASA Glenn)
Richard Hutchinson (Wofford, SC)

primary collaborators

Tim Menzies (NASA IV&V)
Tim Kurtz (NASA Glenn)
Peter In (Texas A&M)

funding, management & guidance

Work sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program led by the NASA Software IV&V Facility (Siamak Yassini, Marcus Fisher, Ken McGill). This activity is managed locally at JPL through the Assurance and Technology Program Office (Chuck Barnes).

Motivational Insights

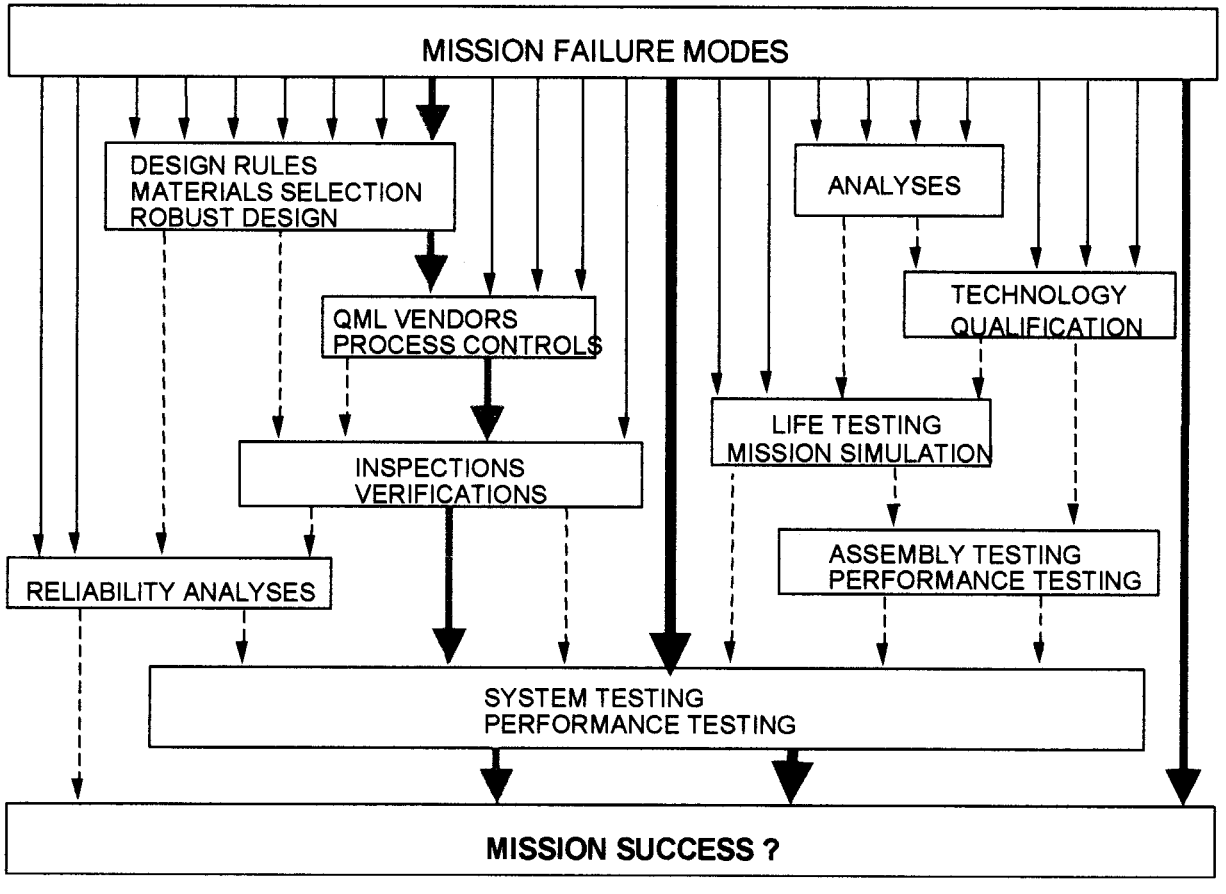
California Institute of Technology

***Assurance activities "filter out" risk* - Dr. Steve Cornford**

"Risk as a Resource" - Dr. Michael Greenfield

overfiltered risk

unfiltered risk



singly filtered risk

JPL
California Institute of Technology

Those insights led to the DDP and RBP risk reduction tools and knowledge.

ARRT focus has been the application of DDP to

Software Assurance Optimization

Software Estimation & Planning data: ARRT - Ask Pete collaboration

JPL
California Institute of Technology

Ask Pete runs to gather project characteristics, make first cut at suggested selection of risk mitigations.
Mitigation selection passed to ARRT

ARRT runs to allow user to assess risk, provide costs, **customize to project** (add/remove risks, refine effect values, etc.), tune selection accordingly.
Revised mitigation selection returned to Ask Pete

Ask Pete runs to generate final reports

Tim Kurtz Tim.Kurtz@grc.nasa.gov
SAIC/NASA Glenn Research Center

http//osat-ext.grc.nasa.gov/rmo/pete/index.html

Principal Investigator: Martha Wetherholt; Phuoc Thai

Semi-automatic optimization: ARRT - TAR2 collaboration

JPL
California Institute of Technology

- Optimization - automated search for (near) optimal mitigations suites
- Sensitivity analysis
  - On which data values do the results hinge?
- Retain human involvement
- Extends smoothly to more complex data

Dr. Tim Menzies tim@menzies.com
NASA/WVU IV&V Facility

http//tim.menzies.com

JPL
California Institute of Technology

Assurance Optimization Goals

The selection of assurance activities such that:

For a **given set of resources**
(time, budget, personnel, test beds, mass, power, ...)
benefits are maximized

or

For a given set of objectives
(science return goals; on-time and in-budget development; 99+% expectation of successful landing)
costs are minimized.

JPL
California Institute of Technology

What's Needed to do Assurance Optimization

1. A model to calculate assurance **costs** & **benefits**-
   we use Defect Detection and Prevention (DDP)

2. Data to populate the model –
   we populate with metrics from experience (when available) augmented with experts' best estimates

3. Optimization over the model –
   we use Menzies' TAR2 treatment learning system (confirmed using simulated annealing)

Assurance Costs & Benefits

JPL
California Institute of Technology

Assurance activities have costs:

- Requirements inspections take skilled peoples' **time**
- Test-what-you-fly takes **high-fidelity testbeds**
- Radiation shielding takes **mass** and **volume**

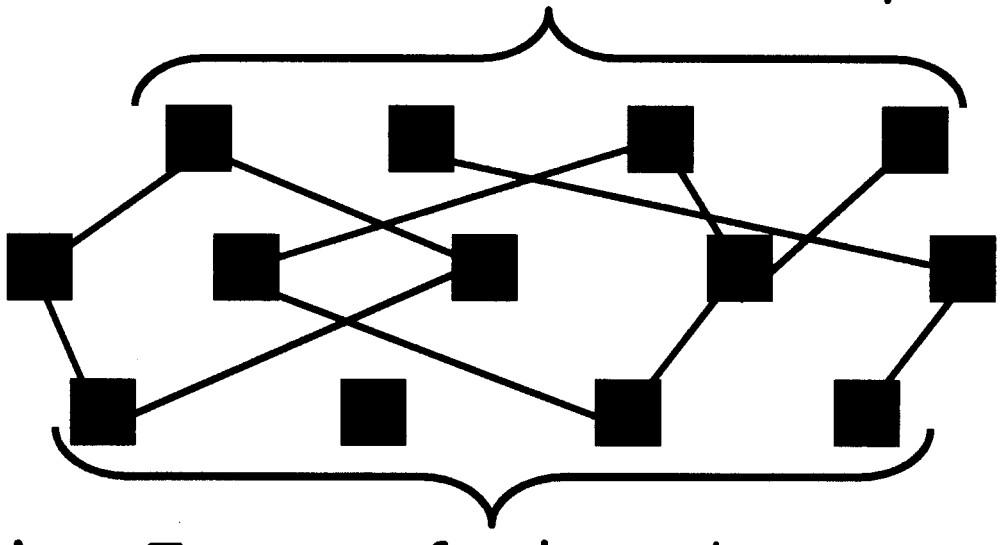
Assurance activities have **benefits**:

- Requirements inspections may **catch problems early**, when it is inexpensive to fix them
- Test-what-you-fly may **catches problems that would jeopardize the mission**
- Bounds checking may **decrease the frequency of switching into safe mode**

DDP Cost/Benefit Model

JPL California Institute of Technology

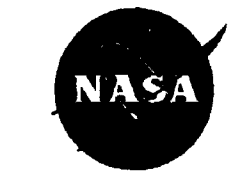
Benefits = Σ attainment of requirements



Costs = Σ costs of selected assurance activities

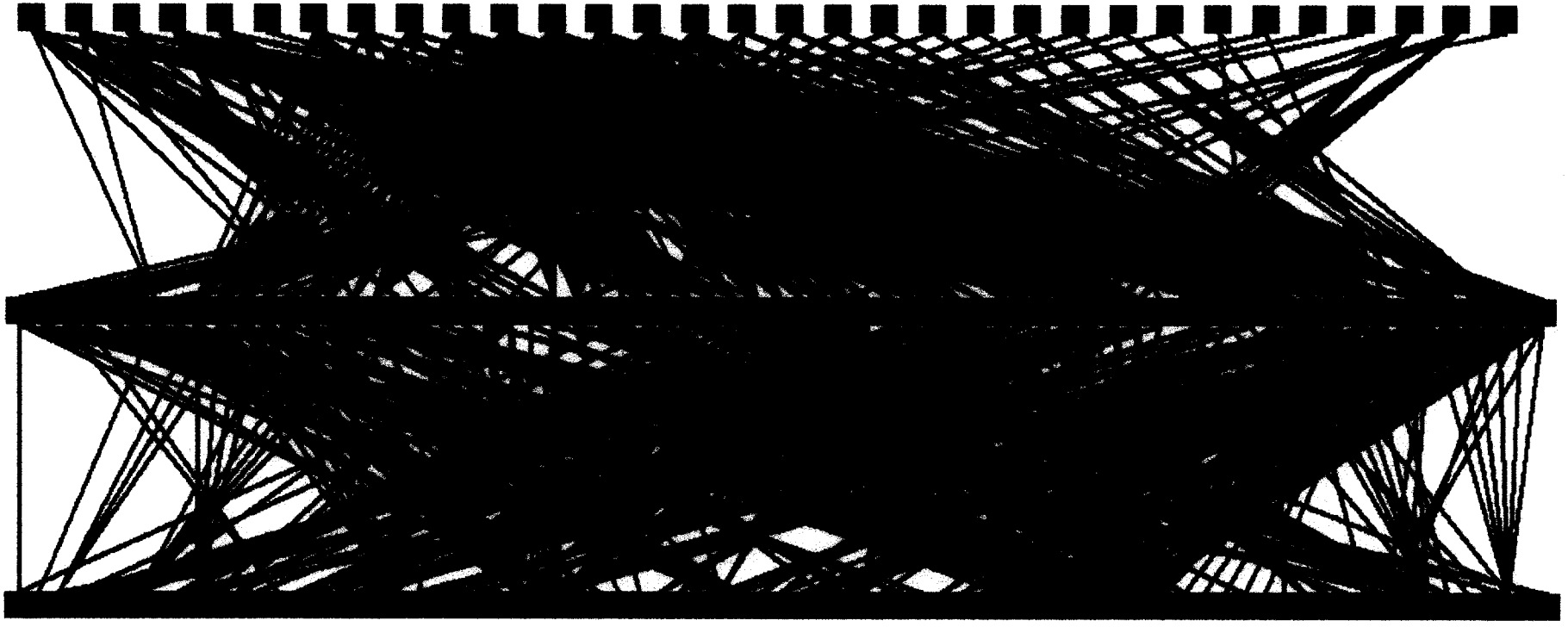
Model holds *quantitative* measures of:
How much each risk impacts each requirement, and
How much each assurance activity reduces each risk.

Risks are crucial intermediaries in the model –
requirements impacted by **risks** to differing extents
assurance activities mitigate **risks** to differing extents



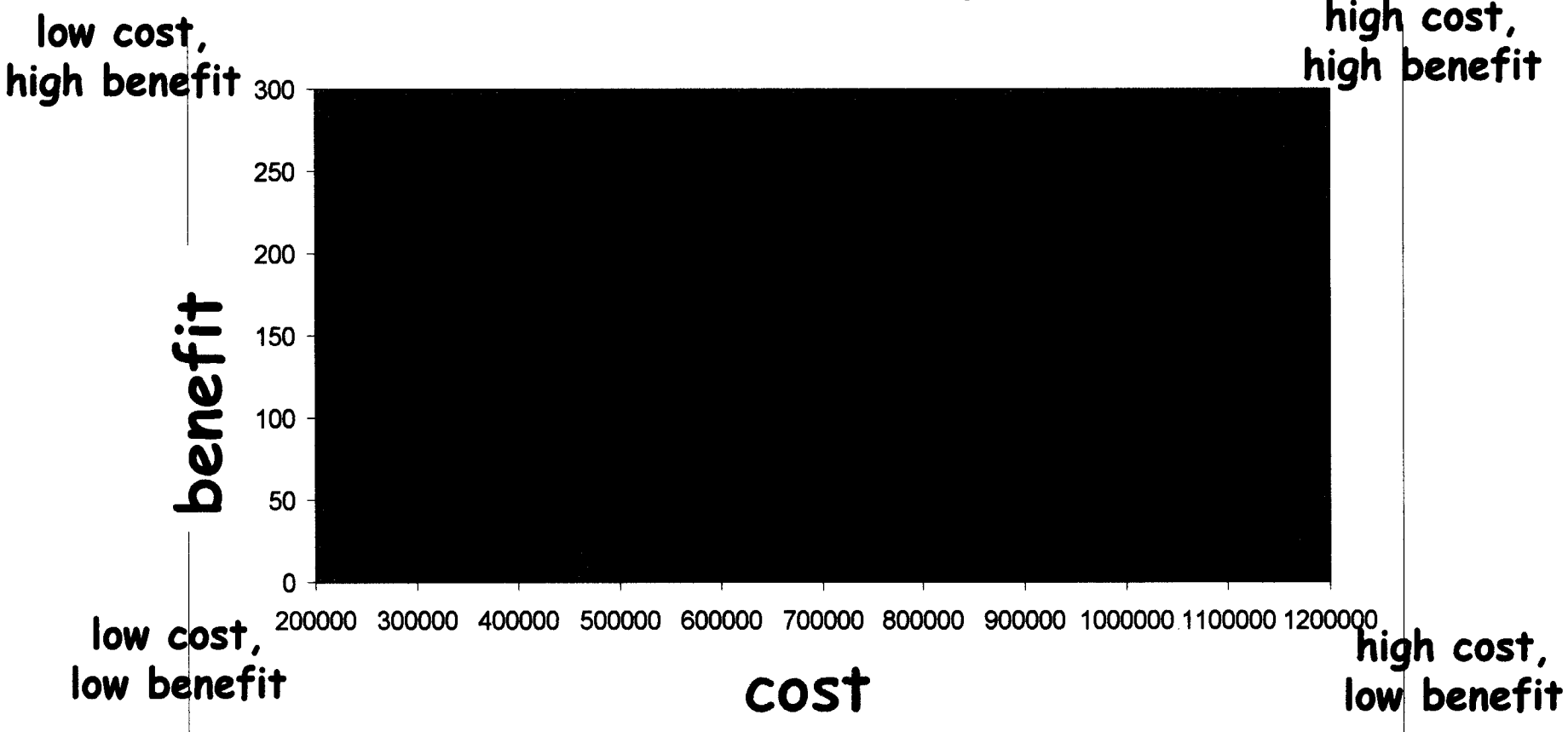
JPL
California Institute of Technology

A Populated DDP Dataset (Real Data from Experts)



32 requirements, 69 risks, 99 assurance activities
352 non-zero quantitative requirement-risk links
440 non-zero quantitative assurance-risk links

Dataset *before* Optimization

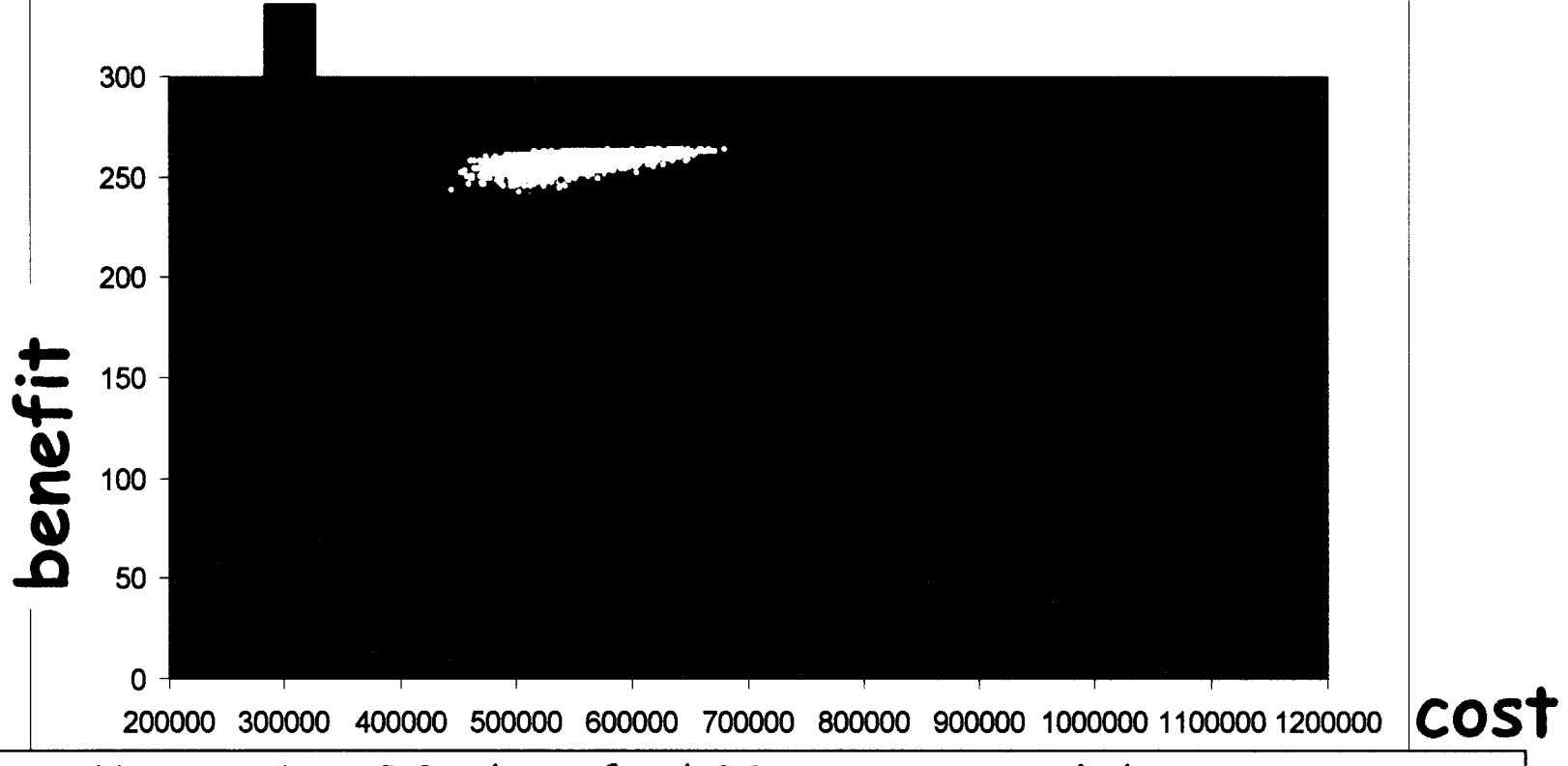


Each black point a randomly chosen selection of dataset's assurance activities. DDP used to calculate **cost** and **benefit** of each such selection.

Dataset *after* Optimization

California Institute of Technology

Each white point is an optimized selection of dataset's assurance activities (33 critical ones are as directed by TAR2, other 66 chosen at random).



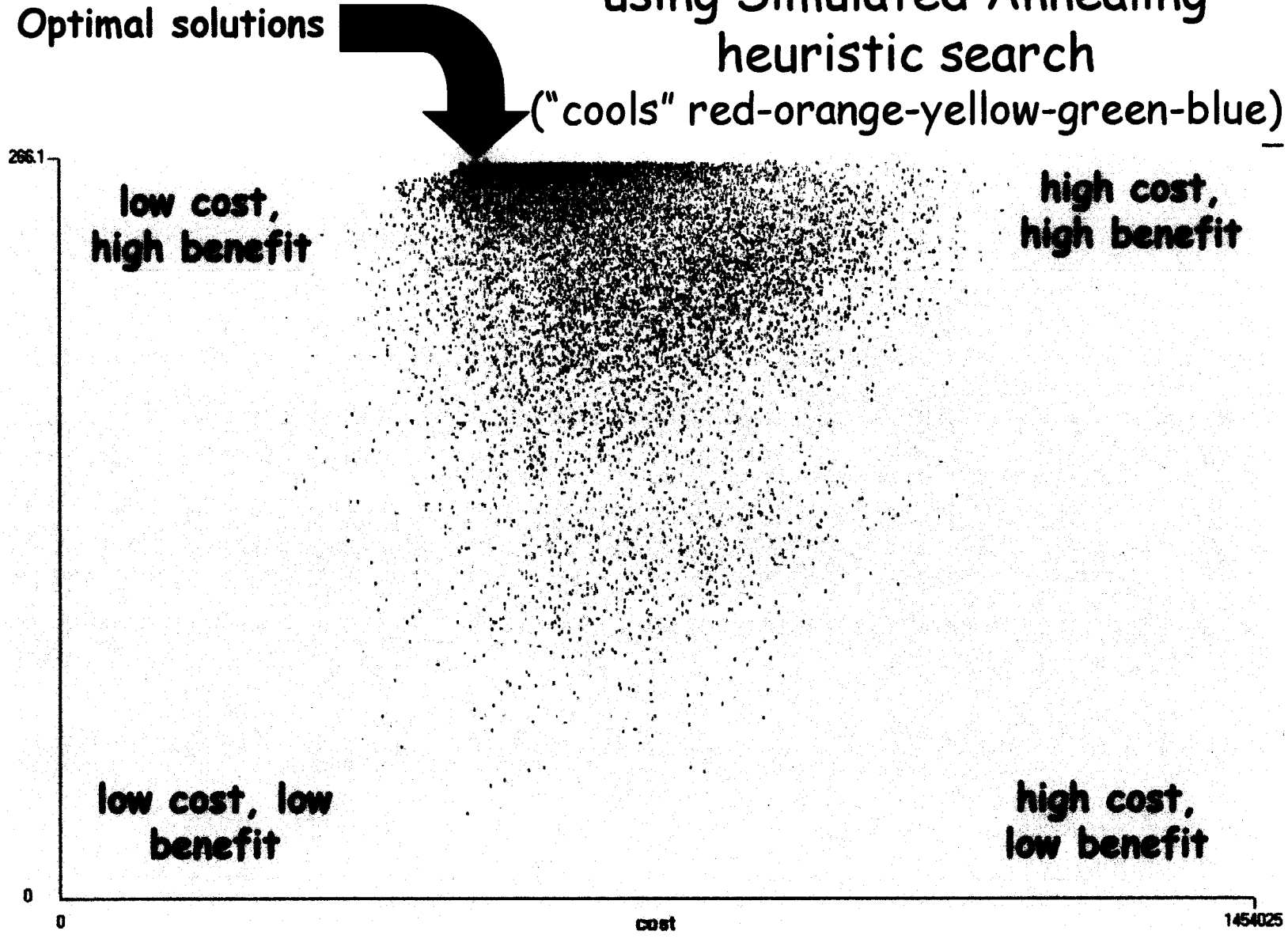
Menzies' TAR2 identified 33 most critical decisions:
21 of them assurance activities to perform
12 of them assurance activities to *not* perform.

Optimization confirmed

using Simulated Annealing heuristic search

("cools" red-orange-yellow-green-blue)

JPL California Institute of Technology



JPL
California Institute of Technology

Assurance Optimization

for more information:

Defect Detection and Prevention (DDP):

- http://ddptool.jpl.nasa.gov
- Steven.L.Cornford@Jpl.Nasa.Gov

ARRT customization for software assurance:

- Martin.S.Feather@Jpl.Nasa.Gov

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