Martin S. Feather
Jet Propulsion Laboratory
California Institute of Technology

Embedded systems *span discipline boundaries*

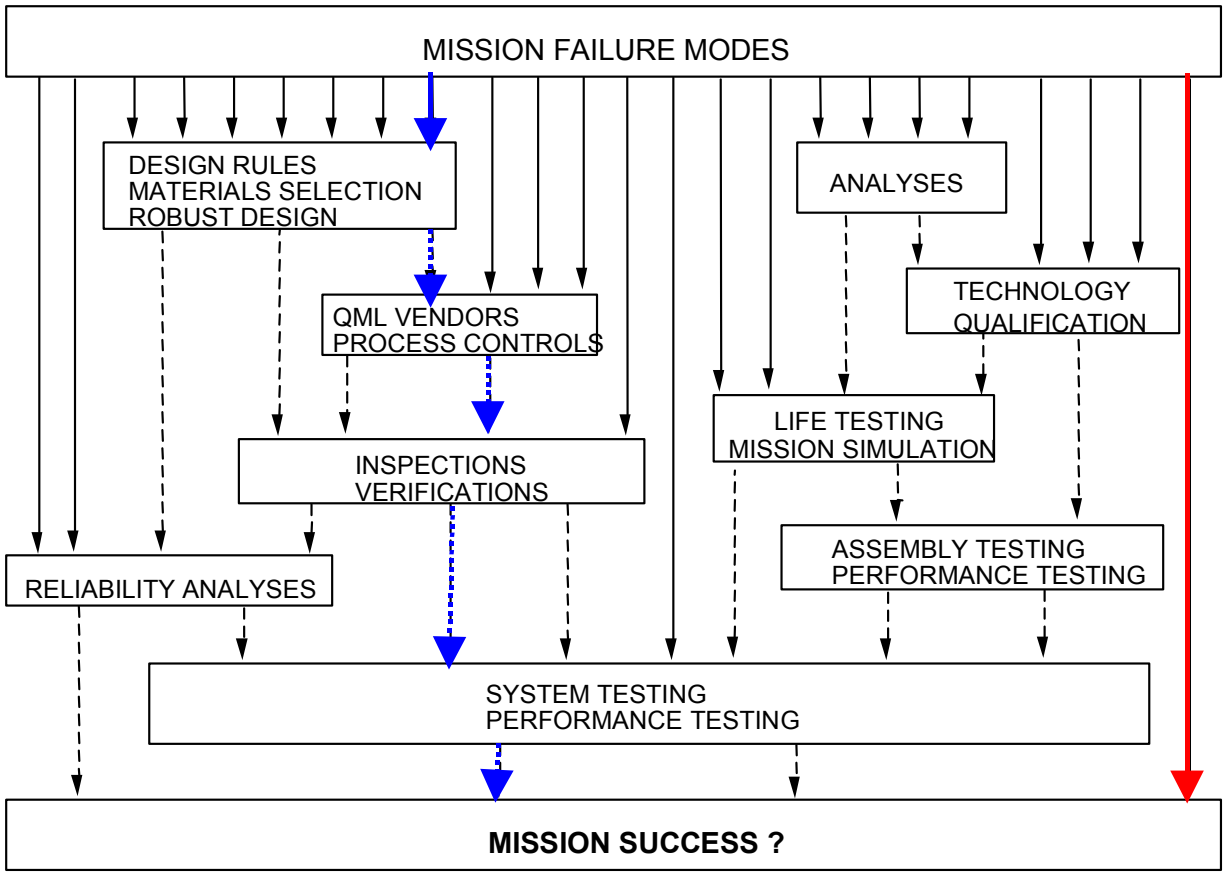
Hard to do trades/planning:

- performance/power/mass…
- time/budget/RISK

Symptoms:

- failures (e.g., Mars missions; “dumb” failures sw/hw)
- delays/overruns
- low rate of technology infusion (flight validation?)

Cornford's flow-down image: assurance activities filter out risk



Purposes of assurance planning

Cannot afford to do all the activities (too expensive, takes too long, too heavy, …)

- Choose the activities wisely (cost/benefit)
- Understand *why* activities are being done
- **for technology infusion**, allocate activities to science/engineering/both
- Push back on requirements!
- Treat **risk as another resource**, trade it ...

Concepts for qualitative & quantitative risk management

Requirements (what are we trying to achieve?)

- weight ("relative importance") (0+)

Failure Modes (what can get in the way?)

- a-priori likelihood (0 - 1)

Impact: if FM_i occurs, *how much* of R_j is lost (0 - 1)

Activities (what can we do about it?)
(**P**reventative measures, **A**nalyses, process **C**ontrols and **T**ests - **PACT**s)

- cost(s) ($, schedule, skills, mass, power, …)

Effect: *how much* of FM_i is filtered by $PACT_k$ (0 - 1)

JPL: Defect Detection and Prevention (DDP)
USC: WinWin

Plan Research the same way:

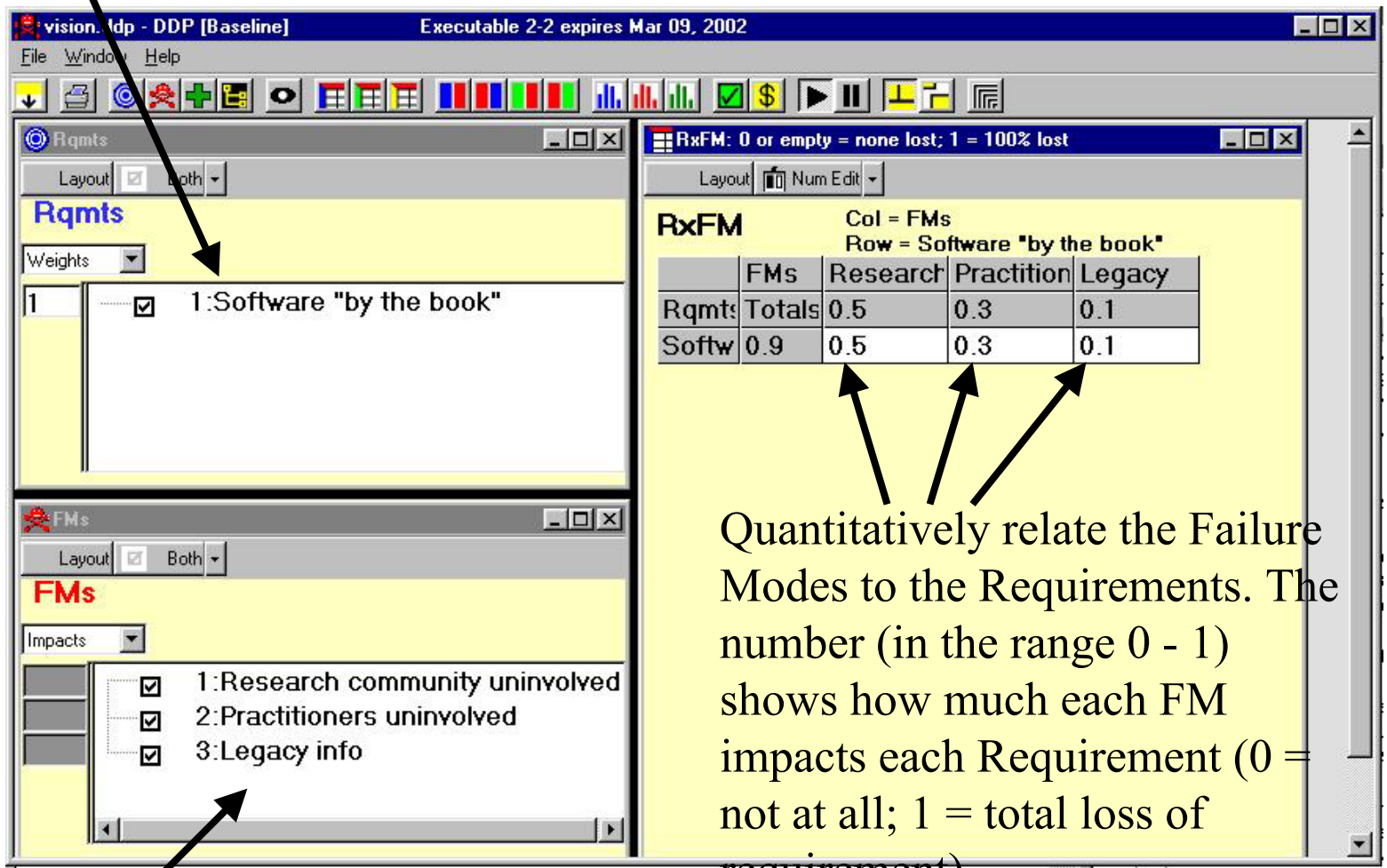
- Requirements - what are we trying to achieve?
- Failure Modes - what impedes our attaining these requirements?
- Investments - what research to do to overcome the FMs?
  - will some be done by industry anyway?
  - Federal government “research portfolio”!

Small demo of research planning

The four slides that follow show several annotated screenshots, taken from the tool demo in which the elements of research planning are demonstrated on a small example.

The example is based on material from Ralph Johnson's presentation, in particular his idea of software "by the book", in which he suggested using funding to support the development of detailed documentation ("books") of various software applications/domains. I alone am to blame for all errors and misrepresentations of Ralph Johnson's work.

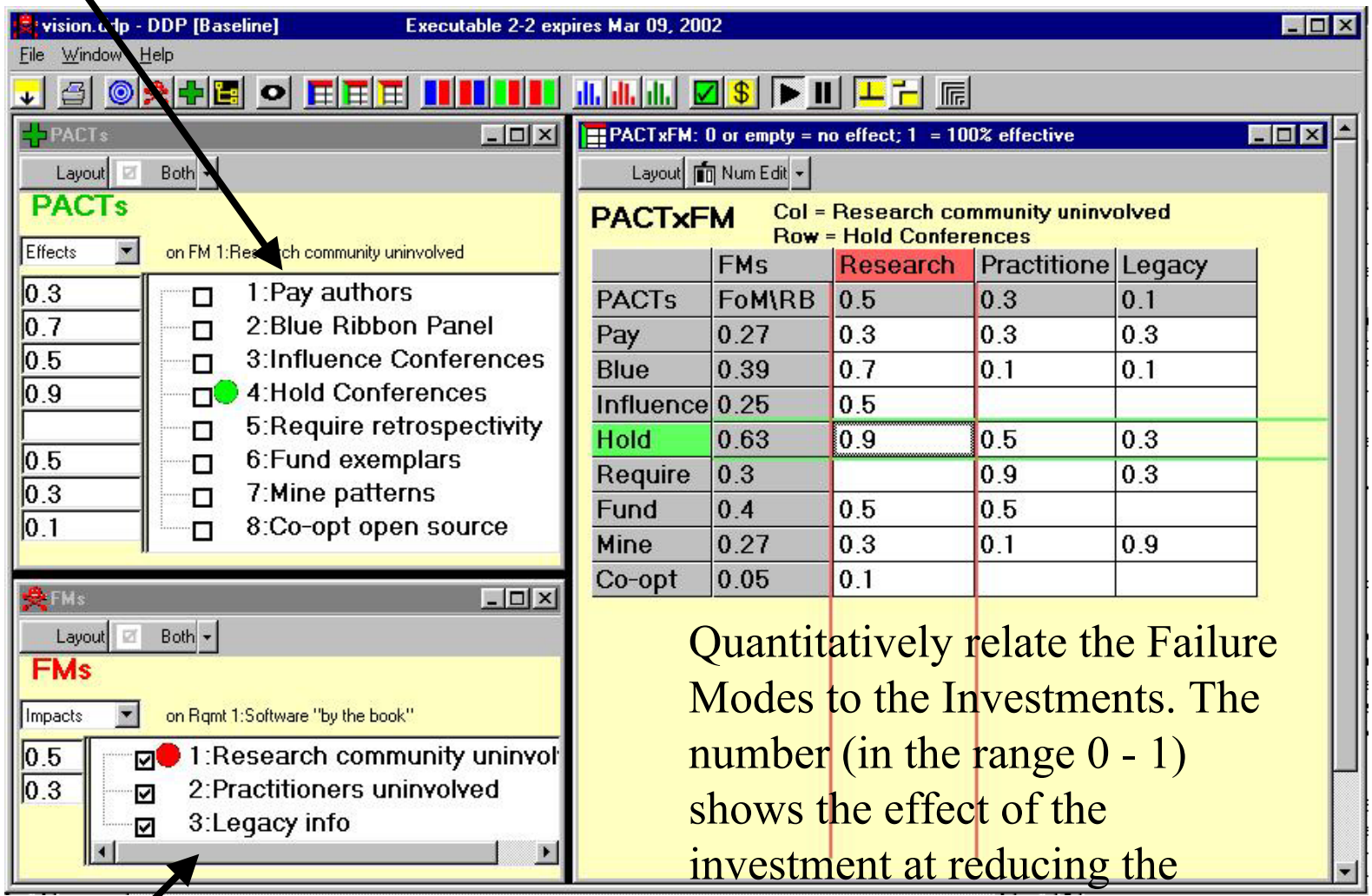
Requirements (in this tiny example, just the one)



Quantitatively relate the Failure Modes to the Requirements. The number (in the range 0 - 1) shows how much each FM impacts each Requirement (0 = not at all; 1 = total loss of requirement).

"Failure Modes" (impediments to meeting the requirement)

Investments (means to overcome Failure Modes)

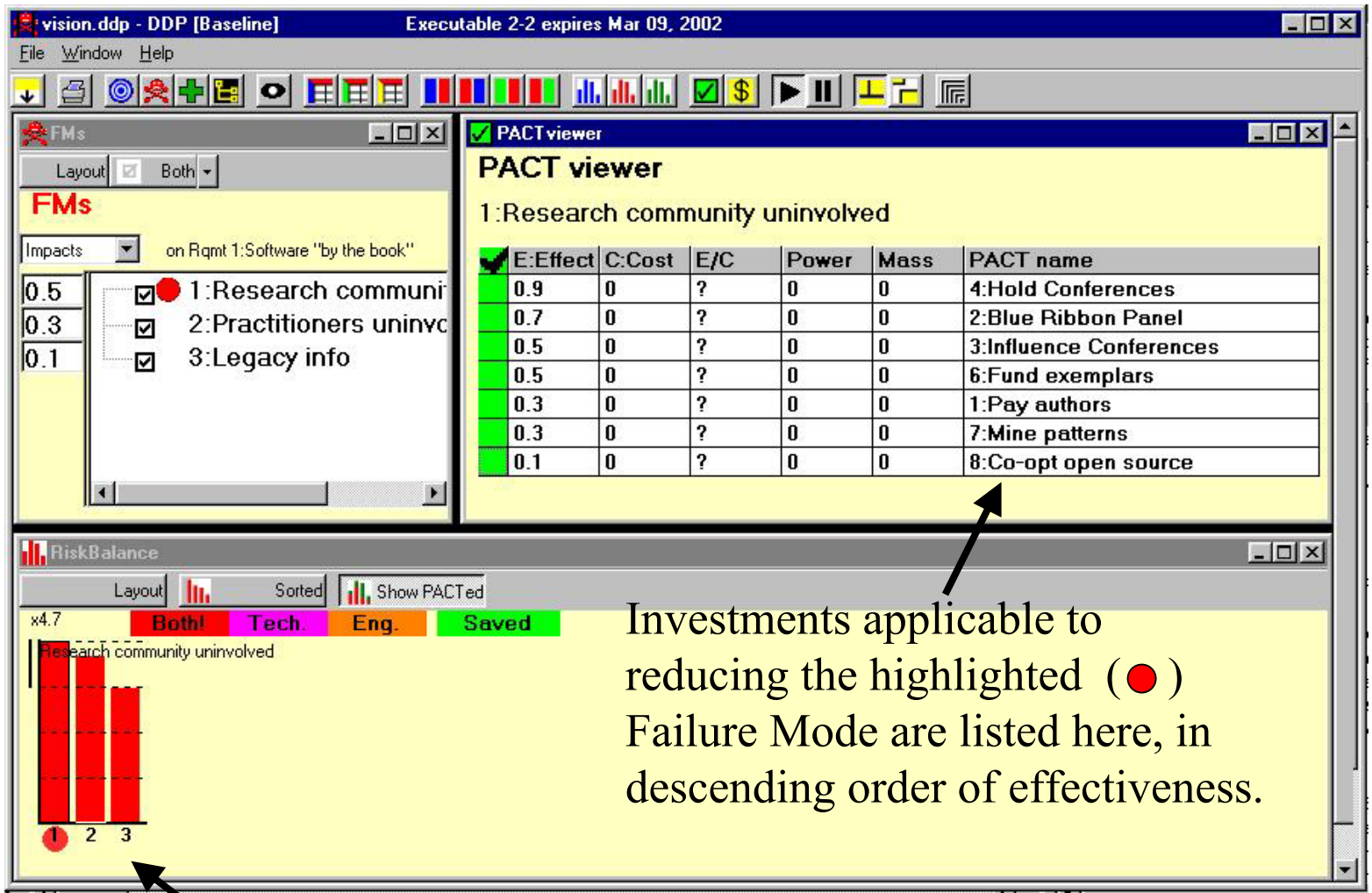


	FMs	Research	Practitione	Legacy
PACTs	FoM\RB	0.5	0.3	0.1
Pay	0.27	0.3	0.3	0.3
Blue	0.39	0.7	0.1	0.1
Influence	0.25	0.5		
Hold	0.63	0.9	0.5	0.3
Require	0.3		0.9	0.3
Fund	0.4	0.5	0.5	
Mine	0.27	0.3	0.1	0.9
Co-opt	0.05	0.1		

Quantitatively relate the Failure Modes to the Investments. The number (in the range 0 - 1) shows the effect of the investment at reducing the Failure Mode (0 = not at all; 1 = totally addresses Failure Mode).

"Failure Modes"

Selecting investments to form a “research portfolio”



Investments applicable to reducing the highlighted (●) Failure Mode are listed here, in descending order of effectiveness.

Each bar corresponds to a Failure Mode; higher = worse damage (more loss of requirements)

Further along in selecting investments to form a "research portfolio"