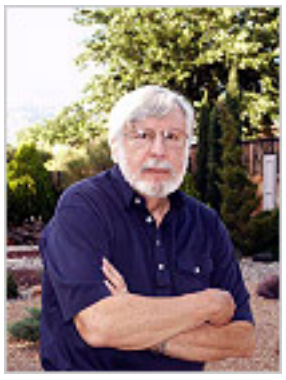
Volume 42, No. 3 • May-June 2006

Whose Risk Is It Anyway?

Evolution of Risk Acceptance Practices



by Ira J. Rimson and Ludwig Benner, Jr.

Page: **1** | 2 | 3 | 4

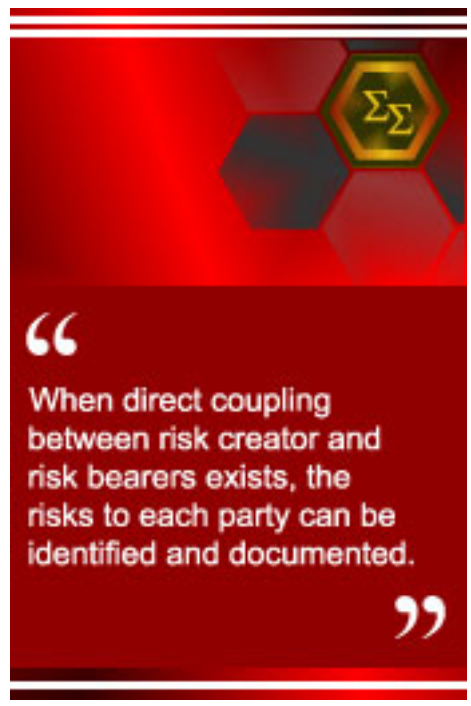
When thou buildest a new house, then thou shalt make a parapet for thy roof, that thou bringest not blood upon thy house, if any man fall from thence.[1]

If a builder build a house for a man and do not make its construction firm, and the house which he has built collapse and cause the death of the owner of the house, that builder shall be put to death.[2]

Accepting Risks = sticking the other guy's neck out.[3]

Risk, and risk taking, have ancient roots. Our ancestors who chose to risk gustatory chaos by bravely ingesting an oyster, lobster or other strange edible were risk-taking pioneers. They created and accepted risks to themselves. As members of societies became more specialized and inter-dependent, risk creators' actions began imposing risks on others. Dangerous events confirmed the need to define responsibilities of risk creators to the others they put at risk. Codes, such as those cited above, were instituted to standardize accepted practices. Insurance became an approach to sharing financial injuries that might result from the unintended consequences of ill-founded risk acceptance.

Inter-dependence among institutions became even more complex as technology introduced innovations to transportation and manufacturing activities that placed more numerous and diverse individuals and objects at risk. Risk-acceptance practices also became more complicated: decision-makers, who allowed risks to be accepted, became increasingly further removed from resultant risk bearers.



Uncoupling: The Gap in Risk-Acceptance Practices
In early days, the coupling between risk creator and risk bearer was direct. You build a house for someone; the house falls down on them; you pay a price. That is close coupling of accountability to results. In more recent times, societal changes, evolving laws and technological complexity have muddled — and frequently eclipsed — direct accountability between the risk creator and the risk bearers. This uncoupling has resulted in a substantial accountability gap in current risk-acceptance decision-making processes.

When direct coupling between risk creator and risk bearers exists, the risks to each party can be identified and documented. Risk-acceptance decisions can be negotiated directly among parties, based on those identified and documented risks. If direct coupling does not exist, risk identification and documentation are still feasible and desirable, even though risk-acceptance decisions become more complicated.

Example #1 of an Uncoupled Accountability Gap: The Ford Pinto Fuel Tank[4]
Ford decoupled its accountability as risk decision-maker from its actual risk takers — the buyers of the Pinto. Ford Chairman Lee Iacocca's specifications for the Pinto's design were uncompromising: it was not to weigh an ounce more than 2,000 pounds and not to cost a cent more than $2,000. During design and production, crash tests revealed a serious defect in the gas tank: In rear-

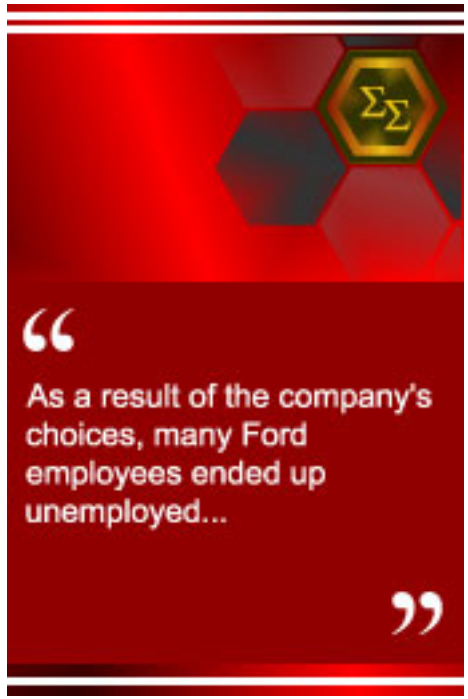
end crashes over 25 miles per hour, the gas tank always ruptured. Correcting it would have required changing and strengthening the design.

next page »

[1] Deuteronomy 22:8.
[2] Code of Hammurabi.
[3] C. O. “Chuck” Miller.
[4] http://www.engineering.com/content/ContentDisplay?contentId=41009014

During pre-production planning, Pinto engineers considered using the same tank used in the Capri, which rode atop the rear axle and differential housing, and was separated by a shielding baffle. In more than 50 crash tests, it withstood rear-end impacts of 60 miles per hour. So why wasn't the Capri tank used in the Pinto? Or why wasn't the Capri's tank baffle placed between the Pinto's tank and its axle? When it was discovered that the gas tank was unsafe, did anyone go to Iacocca and tell him?[5]

Accident reports of rear-end collisions involving Pintos confirmed that if you ran into one, its rear end would fold, the filler pipe would tear away from the fuel tank and gasoline would pour out. In worst cases, if the speed and collision angle were just right, it was likely that the Pinto's doors would jam, trapping passengers inside.



Ford used a "cost-benefit" study to support its design decision against altering the fuel tanks. It estimated that the unmodified tanks would cause 180 burn deaths, 180 serious burn injuries and 2,100 burned vehicles each year, costing the company a total of $49.5 million. In contrast, the cost of modifying the design was higher: alterations would cost $11 per car, totaling $137 million per year.

What are the consequences of ostensibly decoupling risk-acceptance outcomes from the risk-acceptance decision-maker? It's not about death to systems' participants or individual systems' destruction; it's about fall-out from major risk assumption decisions that lead to unintended consequences that really *do* affect decision-makers. As a result of the company's choices, many Ford employees ended up unemployed, with their reputations tarnished, after the Pinto succumbed to the unintended consequences of the company's assumed risks. The demise of the Pinto followed directly from those decision-makers' choices. We doubt that personal consequences were ever identified or even considered during the process of Ford's assuming risks on behalf of its customers.

Example #2 of an Uncoupled Accountability Gap: The Concorde's Fuel Tanks[6]

Hazards arising from the Concorde's fuel tank design resulted in a predictable, disastrous accident at Gonesse, France, in July of 2000, and initiated the supersonic transports' unintended retirement. The Concorde had dodged catastrophe after six earlier foreign-object penetrations into its poorly protected fuel tanks over more than 20 years.[7] *The Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile (BEA)*[8] reported that, incredibly, 57 cases of burst tires had occurred between June 1979 and October 1993, almost *four per year* in both the Air France and British Airways fleets.[9] In addition to tanks suffering structural damage, tire failures resulted in damage to critical aircraft components, such as wheels, brakes, hydraulic lines and control surfaces. Available BEA reports do not identify Air France's decision not to take action to mitigate the risks of foreign objects penetrating its planes' fuel tanks as contributory to the accident. We could find no evidence that Concorde program managers or risk-assessment decision-makers considered that their failure to take action to mitigate those obvious risks might lead to the demise of the entire Concorde program.[10]

[5] The phrase “safety doesn't sell” is commonly attributed to Iacocca.

[6] http://www.bea-fr.org/docspa/2000/f-sc000725ae2/pdf/f-sc000725ae2.pdf (Interim Report #2. BEA's Final Report [http://www.bea-fr.org/docspa/2000/f-sc000725a/pdf] is not available at its URL, ostensibly because "the file is damaged and could not be repaired").

[7] http://www.bea-fr.org/docspa/2000/f-sc000725a/pdf/appendix5p.pdf.

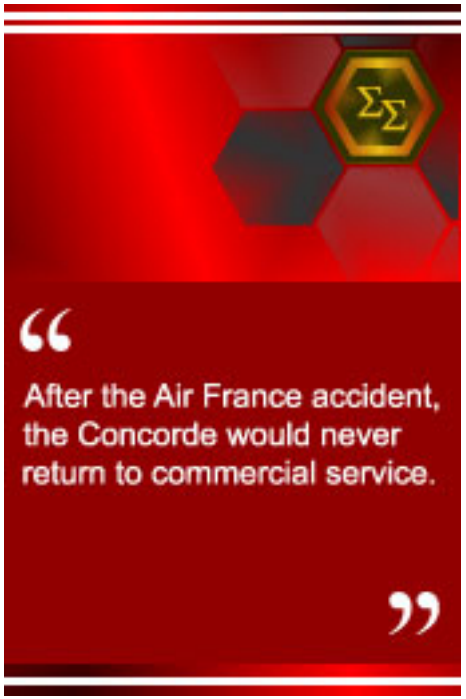
[8] France's Aviation Accident Investigation Agency.

[9] “Concorde fuel tanks burst 'six times'.” CNN.com, January 5, 2001.

[10] In fact, modifications that might have substantially minimized known risks already existed: Michelin had developed special heavy-duty radial ply tires for the Concorde. The accident plane's tires had bias-plies.

In contrast, after the Air France accident, British Airways developed Kevlar blankets for installation in its Concordes' fuel tanks to mitigate their vulnerability to tireburst shrapnel. The Kevlar blanket modification would have added about 400 kg (882 lbs.) - 0.2 percent - of the planes' maximum gross take-off weight of 185,066 kg (~408,000 lbs.).[11]

British Airways never got the chance to test its safer fuel tanks on the line. After the Air France accident, the Concorde would never return to commercial service.



Example #3 of an Uncoupled Accountability Gap that was Recoupled: NASA Space Shuttles *Discovery* and *Atlantis*

The decision by NASA administrators to accept the risks of launching the STS121 space shuttle *Discovery* with known potential insulating foam hazards is an example of how accountability can be uncoupled from decision-makers, despite concurrence by the sole risk-takers: the crew. The decision to launch was explained in terms of qualitative risk trade-offs by top managers over objections by NASA's risk-assessment staff. Risks of vehicle loss or personal harm to individuals operating or exposed to the system's operations were incorporated into the risk-acceptance calculus, but personal risk to the decision-maker — the risk creator — apparently was not.

In contrast, NASA's risk accepters recently made another decision that could have been critical to the success of the impending space shuttle *Atlantis* mission. As described in the Aero-News Network:

> *Engineers at NASA have discovered a potentially serious problem with the shuttle Atlantis…. At issue are a series of bolts holding the support box for… the KU-band antenna to the inside of the orbiter's payload bay. …Should the box break free during liftoff, it could cause catastrophic damage as it falls the length of the 60-foot-long cargo bay.*
>
> *…Incidentally, NASA has known of potential problems with the bolts for some time ... in fact, the bolts were replaced onboard sister shuttles Discovery and Endeavour after it was found the bolts may have been manufactured too short to safely accomplish their task. CBS News reports the bolts were not replaced in Atlantis….*[12]

NASA's risk decision-makers seem to have re-evaluated possible outcomes should another shuttle be lost, including the likelihood of termination of the program. As a result, they appear to have chosen to recouple the agency's accountability gap in favor of discretion:

> *It's something that's never been done before: repairing a component mounted inside the main payload bay of the space shuttle… on the launch pad…. NASA shuttle manager Wayne Hale gave Florida Today an extremely descriptive account of the potentially dangerous repair job …: "So imagine operating on a surfboard that's tied down at one end, sticking out over a six-story balcony.… I mean, this has got all kinds of implications."*[13]

Apparently, the "implications" of the risks to the technician who surfed out to change the bolts (which, in fact, *did* turn out to be too short, despite being engaged) could be interpreted as having been trumped by implications of the risks to NASA's space shuttle program had the antenna broken loose and damaged *Atlantis* irreparably.

« previous page next page »

---

[11] http://www.ainonline.com/issues/07_01/july_01_concordetheorypg12.html.
[12] From “Shuttle Comm Bolts Become A Worry - May Require Replacement.” www.aero-news.net, August 15, 2006.
[13] From “NASA Decides to Play it Safe.” www.aero-news.net, August 21, 2006.

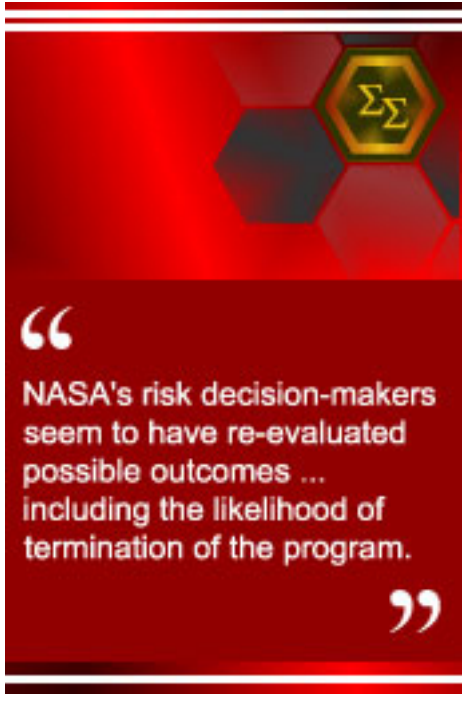
Is This a Problem and, If So, Is Anyone Working on It?

Coupling risk-acceptance decision-makers to risk bearers has received little, if any, attention in the system safety community. Do risk-acceptance analysts consider evaluating and documenting risks to decision-makers? We think not. Decision-makers are not part of the "operating" system and, thus far at least, that's the limit of our analyses. Clearly, unintended consequences may be weighed in decision-makers' minds, particularly where risks of serious harm may bring public rejection or disrepute, civil or criminal liability, and litigation. But for the most part, risks that might occur will be out of sight and mind, and neither weighed *nor documented* during the decision process.

Do system safety practitioners have professional or ethical obligations, either to their employers or to their products' users, to expand their horizons beyond the narrow limits of immediate system risks? Should they broaden the scope of risk detection methodologies and predictions to try to recognize unintended consequences? Should those potential consequences be brought to the attention of risk decision-makers? After all, in the end, it may be their jobs and reputations that are one of those consequences. No one seems to be considering the problem. If it really *is* a problem.

What do you think?

Copyright © 2006 by Ira J. Rimson and Ludwig Benner, Jr. All rights reserved.



« previous page

Copyright © 2006 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.