

Home

Subscriptions & Memberships

Contact

About eJSS

System Safety Society



Vol. 44, No. 3 • May-June 2008

Opinion

Numerology and System Safety

by Ira Rimson

*One winter night during one of the many German air raids on Moscow in World War II, a distinguished Soviet professor of statistics showed up in his local air-raid shelter. He had never appeared there before. "There are seven million people in Moscow," he used to say. "Why should I expect them to hit me?" His friends were astonished to see him and asked what had happened to change his mind. "Look," he explained, "there are seven million people in Moscow and one elephant. Last night they got the elephant."*¹

Numerology is a belief in the relationship between numbers and physical objects. It dates back to ancient cultures: Babylonian, Greek (Pythagoras and his followers — 6th century B.C.), Chinese and Egyptian, early Christian mysticism, occultism of the early Gnostics, Hebrew systems of Gematria in the Kabbalah, and Indian Vedas.² Numerology is often associated with divinatory arts, and it can be applied to those who are judged to place excessive faith in numerical patterns. Numerology can be applied appropriately to Probable Risk Assessments that are fabricated from unverified, unvalidated and irrelevant historical data, to meet specified criteria that would otherwise be impossible to achieve in the real world.

For example, FAA Advisory Circulars of the XX.1309-1(n) series specify "Allowable Quantitative Probabilities" for analyzed failure conditions for design certification.³ For commuter category airplanes, the acceptable quantitative probability for "Catastrophic" failure is "<10⁻⁹" per flight hour. In other words, an applicant for certification must demonstrate — or be able to calculate — that a catastrophic failure will not occur more frequently than once in 1,000,000,000 flight hours. There has never been a certificated airplane model that has come within 2.5 orders of magnitude of the billion flight hours specified by the FAA. Where do the data come from?

One source is defined in the section titled "Operational and Maintenance Considerations."⁴ Paragraph 10.a. specifies, first, that, "For the purpose of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and *found to be reasonable.*" [Emphasis added.] This is the equivalent of asserting that there is no such thing as human error. Under the circumstances, what would be the likelihood of an applicant finding "unreasonable" flight crew or maintenance tasks?

Second, it specifies that "...based on experienced engineering and operational judgment, the discovery of *obvious failures* during normal operational and maintenance of the airplane *may be considered....*" [Emphasis added.] Note that "obvious" is nowhere defined, and that consideration of operational and maintenance failures is permissive, not mandatory.

In case the foregoing absolusions are inadequate, paragraph 10.b.(1) lets the applicant completely off the hook with this exemption opportunity: "If the evaluation indicates that a potential Failure Condition can be alleviated or overcome in a timely manner without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, correct crew action may be assumed in both qualitative and quantitative assessments."

These "evaluations" are a condition for obtaining government certification. It is hardly likely that any new aeronautical system will have accomplished adequate operational experience from which to derive sufficiently robust data to validate a claimed 10⁻⁹ failure rate. Applicants thus may attest to the ability of system liveware to compensate for any failure mode short of total disintegration, absent supporting data from actual operational experience. Is it any wonder that "pilot error" is the most frequently cited cause factor in aviation mishaps?

Once certification or customer acceptance occurs, Probable Risk Assessment evaluation data have served their purpose. Predictive risk data are rarely, if ever, re-evaluated after a failure

President's Message

From the Editor's Desk

TBD

In the Spotlight:

Application of System Safety to Prevention of Falls from Height in Design of Facilities, Ships and Support Equipment for Weapons Systems

A Software Tool for Domino Effect Risk Assessment in Industrial Plants

Focus:

Large Hadron Collider: Cause for ConCERN or Tempest in a Teapot?

Chapter News

Mark Your Calendar

Opinion (Rimson)

Opinion (Benner)

ISSRC 2008

Announcements

About this Journal

Classifieds

Advertising in eJSS

Contact Us

Puzzle



The Next Generation
of System Safety
Professionals

August 25-29 2008

ideas
knowledge
experiences

The conference theme, "The Next Generation of System Safety Professionals", is an invitation for professionals at relatively early stages of their careers to benefit from the wealth of system safety knowledge and experience acquired by the membership of the System Safety Society[®].

More Information >

occurs. The regulators and the public continue to be gulled into believing the likelihood of an airplane failing is one in a million, or ten-million, or hundred-million, or a billion flight hours, when in reality, nobody really knows until the next shoe drops. When they "get the elephant," re-evaluating the risk to accommodate reality should be demanded.

I propose that system safety numerology be modified like this: When a system failure happens *for any reason*, that failure mode must be re-assigned the probability $\langle p=1 \rangle$, and all relevant system risk assessments must be re-calculated incorporating that unity. That is, of course, unless someone can assert to knowing precisely when the next similar system failure will occur. Until re-calculation has been accomplished, the following caveat should be required on all Probable Risk Assessments that lack sufficiently robust real-world operational data to support their "evaluations" with mathematical rigor:

WARNING!

THIS RISK ASSESSMENT MUST BE RE-CALCULATED AFTER EVERY UNDESIRED OPERATIONAL OUTCOME WITHIN THE SYSTEM TO WHICH IT APPLIES, PREDICTED OR NOT, APPLYING THE PROBABILITY $\langle p=1 \rangle$ TO EACH UNDESIRED OCCURRENCE.

Author's note: *I do not wish to pick unreasonably on the FAA; however, I am more familiar with its regulatory specifications than with those of other government or civil entities. I am certain that professionals in other fields can find similar examples within their expertise.* Σ

— IJR

¹ Peter L. Bernstein, *Against the Gods; The Remarkable Story of Risk*. New York, Wiley, 1998, p. 116.

² See <http://en.wikipedia.org/wiki/Numerology>.

³ FAA Advisory Circular 23.1309-1C, Fig. 2, p. 16.

⁴ *Ibid.*, p. 26.