This article is part of the IEEE Reliability Society 2007 Annual Technology Report.

Reliability, Law of Least Astonishment and the Interoperability imperative

Samuel Keene[1]
Email: s.keene@ieee.org

Of Pineapple Juice and Other Things….

William Claude Dukenfield, better known as W.C. Fields often had a flask filled with "Dutch Courage"[2] by his side. In spite of a common knowledge that Fields filled his flask with his favorite Gin, Fields, routinely and protestingly referred to his Gin as pineapple juice. While on a film set one day, to his amazement, Fields discovered that crew members had decided to substitute the Gin in his flask with real pineapple juice. More than a little infuriated, considering this act deplorable, Fields shouted out: "somebody put pineapple juice in my pineapple juice"![3] Unhappily, something other than that which was *reliably* expected by Fields was delivered. In that instance, between one's expectations and what was received, the *"law of least astonishment"* was violated. The *"law of least astonishment"* was amusingly made popular by the writings of James Geoffrey[4] in the 80's, but the concept and practice were part of a mainstream programming practice, more than a decade earlier;[5] during the adolescence of the computing age. What exactly is the *"law of least astonishment"?* From a reliability point of view, the *"law of least astonishment"* is a guidepost to designers and programmers of computer interfaces, propagating a 'mental checks and balances' archetype, affirmed by the ideal that interfaces should always perform in a manner originally intended, and not in a manner that will *astonish* (negatively) those 'interfaced.'

Elsewhere, centuries preceding the birth of the computing industry, professional practitioners In Medicine had to formally subscribe to a set of principles as they entered their practice. The principles embedded within the Hippocratic Oath emphasized that all practitioners of medicine, "do no harm." Today, from the design of human-machine interfaces in medical informatics,[6] to structuring knowledge distribution enterprises,[7] determining core values of professional management training,[8] deciding policy vectors to widely institutionalize operational stability of the Internet,[9] to the extent that scientists and scientific personnel within enterprises have been stimulated to engage the world[10] from their positions and professions of choice, have all stemmed from a communal, and a very human desire to be wedded to the *'law of least astonishment,'* or quite simply, to 'do no harm.'

Explanation of Relationships…

Quite naturally, the rule to 'do no harm' is not an alien concept to reliability engineers. Reliability engineers are beings that attempt to professionally thwart the rise of nasty surprises. However, as in other disciplines, reliability engineers are not exempt from challenge to operate in complex institutional settings, where professionals from multiple disciplines, must jointly emerge novel inter-disciplinary solutions to decidedly challenging problems. This requirement to *inter-operate* very often introduces the existence of a reliability 'fault-line' particularly in large-scale, highly complex and vastly distributed nature of operations.

Just recently, an intriguing thought-piece on reliability in terms of *interoperability* came across my desk, which attempted to analytically synopsize the results of efforts instituted over the past 40 years to improve the reliability of the United States electric power grid. IEEE-USA's Debra Schiff interviewed the authors, Dr. Luis Kun - Senior Research Professor of Homeland Security at the Information Resource Management College of National Defense University (NDU), and

Dr. Robert Mathews - Distinguished Senior Research Scholar on National Security Affairs and U.S. Industrial Preparedness at the University of Hawaii, in August of 2007, and discusses their findings in layman's terms in an IEEE' Today's Engineer article titled: "Taking a Wide-Angle View of the U.S. Electric Power Grid."[11] Within the article, Ms. Schiff makes a notation that it is the intention of Kun and Mathews' to be authoring a series of monographs [12] to highlight the non-trivial nature of disconnects in the *interoperability-reliability logic*, the nature of its persistence and perceived impermeability in significant national security related areas. Centered on reliability, and in their introductory writing, the authors offer a fresh perspective into why it is exceedingly difficult to employ remedies for misaligned components and pathways in a highly complex system to achieve the required level of reliability. They attempt to offer their perspective through the lens of *interoperability*, by representing the level of success of efforts that have been launched to improve reliability in the U.S. Electric Power Grid over the past 4 decades.

Rather than intimately dissecting their work here, the membership of the IEEE Reliability Society will perhaps be better served if I reported upon the relationships that have been surfaced by the authors, in their desire to further elevate the nature of reliability in nationally critical systems. Dr. Kun's professional interest in 'unreliability' within Homeland Security efforts and systems at the NDU, and Dr. Mathews' broad interest in the *uninteroperability* of ultra-complex systems intersected one fine day in June of 2006, in Cambridge, Massachusetts. There, Mathews, a national thought leader on the confounding subject of *uninteroperability* was the organizer and chair of a historic and seminal - IEEE sponsored 'Special Session' titled: "Interoperability and Integration of National Security Information Systems."[13] As never before in IEEE history, a bona fide procession of giants, a Who's-Who in the world computing, communications, engineering, genetics, economics, finance, management, innovations, government and policy-making, assembled in Cambridge. Through an array of riveting concepts and themes, the discussants elaborated upon the relationship between Interoperability, reliability and systems functionality. In the named article, Kun, who attended the Cambridge session, travels the extra mile to stress that the conference confirmed that the scientific community's *de facto* adoption of pre-existing understanding of *interoperability situations*, and definitions of *interoperability*, like the one inked by the United States Department of Defense (DoD) or the Department of Homeland Security (DHS) amount to a complete and utter violation of intellectual due-process; being plainly imprecise and misleading.

Therein, Mathews commits to present the nuances existing between interoperability and reliability – gently and more broadly, defining *interoperability* first, as 'that tightly coupled inter-disciplinary and multi-disciplinary capability where *all aspects of a system* are tailored to operate synchronously in order to continually achieve goals - in a safe, effective, efficient and reliable manner.'[14] He highlights that to institute and maintain systemic reliability, an intimate understanding of systems behavior must pre-exist, comprising such things as previously unknown component 'failure modes,' roles of unconventional systemic stressors, or the presence of malicious or non-malicious anomalies, which can cause severe reliability impediments. Said differently, he says, if we "consider the *"Law of Least Astonishment"* as a means to advance the state of reliability, it is **not the least bit reasonable** to inflict demands for higher and higher functionality, availability and reliability from complex infrastructures, resident services and service modes, while we lack the fundamental understanding of just how the layers of the onion are overlaid, and what the cohesion among the many layers means to the whole."

Additionally, Mathews says that in such things, we are often held back by a mental blindness where "our brain's desire to work in a reductionistic fashion, allows for a 'process violation' to be perpetrated upon ourselves; and analytical attention is diminished, drawn by conveniences, to a subset of all there is." The result he says, is an end-product that is "less logical, less scientific,

rational, efficient, effective, and least of all – reliable." He punctuates by saying that the intricacies and the highly delicate nature of working relationships among the multi-disciplinary and inter-disciplinary domains of sub-systems in a highly complex system 'is' everything."

And finally…

In my recent conversations with Luis Kun, he proceeded to underscore the importance of Mathews' insightful orientation, through an example. Kun states: "it is now known that the use of sub-standard gusset plates [15] were responsible for the failure of the I-35W Bridge over the Mississippi river in Minneapolis, Minnesota, which snuffed out the lives of 13 people, and injured 145."[16] Kun proceeded to ask a few 'now obvious,' nevertheless important questions: "do we now believe that the "law of least astonishment" was violated here? Can we represent the failure of the I-35W Bridge as a triumph for reliability engineering?

The central theme of Kun & Mathews paper is that "the very notion of *interoperability* presupposes a synchronous interworking of all components in a system to achieve [whatever] the desired goal. When all steps in the interoperability processes are not properly qualified, quantified, monitored, and improved, things are bound to go wrong."[17] Utilizing engineering principles, the likely *failure of any component,*[18] or a set of components in a system could be characterized and approximated, such that a corresponding *reliability function* for that system be determined. Being adequately prepared for eventualities such as a component failures, will then have satisfied, the *"law of least astonishment"* for that system. However, organizing one's enterprise and its competence to be ahead of the curve in this respect is never easy as it sounds; neither is it even remotely out of the possibility to institute. Both Kun and Mathews agree here that the implementation requires both, an uncommon organizational structure, and levels of competence.

I conclude, by borrowing from known eloquence of Dr. Noah Porter. The difficult task of improving reliability in highly complex systems can be summed by Porter's powerful sentiment. He states: *"few persons are so familiar with each of the several lines of argument in which lies its strength if it be true and its weakness if it is false, as to be able to judge of any considerable number. Fewer still are competent to pronounce upon the relation of each part to every other, and the cumulative force of all as they bear upon the grand conclusion"*.[19] This is the point at which reliability intersects with that little known, and even less understood field of *'interoperability.'*

References

[1] This paper was based on interviews and notes from interviews of Professors Luis Kun and Robert Mathews

[2]Origins and development of Gin, The Gin and Vodka Association, at http://www.ginvodka.org/history/origingin.html, accessed on January 14, 2008

[3]Fadiman, Clifton and Bernard, Andre' [Eds], "Bartlett's Book of Anecdotes," [revised edition], Little Brown and Company, September 2000

[4]James, Geoffrey, "The Tao of Programming," [Book 4 – Coding], InfoBooks, Santa Monica, California, 1987. Available on line, at: http://step.nasa.gov/tao.html

[5]Rubinoff, Morris [Ed.]; "Advances in Computers," Academic Press, New York, New York, 1972.

[6]Human-Machine Interface - Introduction to Medical Informatics (MDIF – G4001), Department of Biomedical Informatics, Columbia University, New York, NY., 1997 Online at: http://www.dbmi.columbia.edu/~hripcsa/textbook/

[7]McIlwaine, John; "First, Do No Harm: A Register of Standards, Codes of Practice, Guidelines Recommendations and Similar Works relating to Preservation and Conservation in Libraries and Archives," International Federation of Library Associations and Institutions (IFLA), Conservation Section, March 2005 **[**http://www.ifla.org/VII/s19/pubs/first-do-no-harm.pdf]

[8]"Managers consistently delude themselves about how much good they're [institutionally] doing. The oath for managers should be the same as physicians: First do no harm. "-- Robert Sutton is Professor of Organizational Behavior and Professor of Management Science and Engineering at the Stanford Engineering School. Additionally See: *"What I Worry About and Why"* – Harvard Business School Press [http://discussionleader.hbsp.com/sutton/2007/03/what_i_worry_about_and_why.html], and *"Exploring the Psychology of the Boss"* – NPR [http://www.npr.org/templates/story/story.php?storyId=9517852]

[9]"Staff Manager's Issue Report on the Need for a Predictable Procedure for Changes in the Operation of TLD Registries," Internet Corporation for Assigned Names and Numbers November, 2003 [Updated – December, 2003] http://www.icann.org/gnso/issue-reports/registry-svcs-report-19nov03.htm

[10]"Concern for man himself and his fate must always form the chief interest for all technical endeavors, concern for the great unsolved problems of the organization of labor and the distribution of goods--in order that the creations of our mind shall be a blessing and not a curse for mankind. Never forget this in the midst of your diagrams and equations." -- Rosenkranz, Ze'ev; "The Einstein Scrapbook," Johns Hopkins University Press, Baltimore, MD., 2002.

[11]Schiff, Debra; "Taking a Wide-Angle View of the U.S. Electric Power Grid," IEEE –Today's Engineer Online, Sept, 2007 [http://www.todaysengineer.org/2007/Sep/power_grid.asp]

[12]The first E-Book in this series, titled: "Interoperability: A Review of Activities To Ensure the Reliability of the U.S. Electric Power Grid," is now available from the IEEE-USA' E-Book store at: http://www.ieeeusa.org/communications/eBooks/default.asp

[13]"Special Session on Integration & Interoperability of National Security Information Systems," Institute of Electrical and Electronics Engineers (IEEE), U.S. Department of Transportation – John A. VOLPE Center, Cambridge, MA., June, 2006

[14]See ix [Schiff]

[15]large flat steel pieces that hold load-bearing columns in place

[16]"US finds bridge plates deficient in collapse probe," Reuters News Service, Jan 15, 2008 [http://www.reuters.com/article/latestCrisis/idUSN15535432]

[17]Kun, Luis; "Interoperability: the cure for what ails us," Government Affairs Editorial Column, IEEE-EMBS Magazine, Vol. 26, No. 1, January/February 2007.

[18]Mean Time To Failure (MTTF) / Mean Time Before Failure (MTBF)

[19]Porter, Noah, "Physiological Metaphysics; or, the Apotheosis of Science by Suicide", The Princeton Review [November], G. & C. Carvill, New York, NY, Volume 2, Jul-Dec 1878, and Porter, Noah, "Science and Sentiment With Other Papers Chiefly Philosophical" Charles Scribner's Sons, Franklin Press: New York, NY [Rand, Avery and Company, Boston], 1882