

IEEE Reliability Society Technical Operations Annual Technology Report for 2008

Abstract—The 2008 Annual Technology Report consists of contributed material from members of the IEEE Reliability Society Technical Activities Board, as well as outside contributors who practice reliability. This report consists of the following contributions.

- Introduction provided by Lon Chase
- Reliability Standards Status provided by Lou Gullo
- An Ethical Analysis of Automation, Risk, and the Financial Crises of 2008 provided by George F. Hurlburt, Keith W. Miller, and Jeffrey M. Voas
- Lean Now! provided by Gary Wickett
- Unreliability of Community Memories and Its Relativity to Blockading of U.S. Scientific Progress provided by Samuel Keene
- Summary of Selected Technology Advances provided by Dennis Hoffman
- The Challenges of System Health Management for Failure Diagnostics & Prognostics provided by Enrico Zio
- Delivering Reliability in the Healthcare System provided by Dev Raheja
- Some Faults Are Worse Than Others: And How That Is Useful for Low-Cost Hardening provided by Ilia Polian
- The Science and Pitfalls of Achieving Verifiable Data provided by Samuel Keene
- Trustworthy Medical Devices provided by John Harauz
- Degradation of the High-k Dielectric/Metal Gate Stacks Under Electrical Stress provided by Gennadi Bersuker
- Response to Counterfeit ICs in the Supply Chain provided by Gary F. Shade
- How Lead-Free Changes Can Impact Reliability provided by Joe Childs
- Risk Assessment and Mitigation of COTS Integration in High Reliability Systems provided by Kenneth P Rispoli
- Tin Whiskers: A Long Term RoHS Reliability Problem provided by Robert J. Landman
- Solutions to Sneak Circuit Analysis (SCA) of Very Large Equipment/System Designs provided by Scott Schulman
- Design Constraints That Make Software Trustworthy provided by Lawrence Bernstein, and C. M. Yuhas
- Malicious Code provided by W. Eric Wong, and Vidroha Debroy
- Preparing the Ground for Next Generation Software Engineering provided by Don O'Neill
- Software Security Engineering: A Key Discipline for Project Managers provided by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy R. Mead
- Some Progress in Software Testing Technology provided by Phillip A. Laplante, Robert Bucholz, and Albert Elcock
- Communications Network Reliability provided by John Healy

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TR.2009.2020845

I. INTRODUCTION

THIS annual technology report of the IEEE Reliability Society is based on material submitted by the technical activity segments of the Society, statements from experts in the field, industry reviews, and current special interest groups working in the field.

'Technical operations' is now called 'technical activities' to align with the naming used by the IEEE technical advisory board. 'Technical activities' is obviously the technical arm of the IEEE Reliability Society. Its charges are to:

- Help incubate new conferences
- Foster ways to get more technical information to our members through:
 - The Annual Technical Report that comes out each January
 - A content rich web site that will provide IEEE RS organizational data, technical reports and data, and tools (these capabilities are under development).
 - Publicizing the state of the art work in the IEEE Transactions, Spectrum magazine, our web site, and discussion groups.
 - Enhancement of the RS promotional flyer with technical activities content.
 - Building templates, guides, and resources to mentor new members of the society and profession
 - Interfacing with other technical societies, and collaborate on joint ventures to gain synergy
 - Delivering technical information through classes, tutorials, media, and online collaboration (meetings)

Society Technical Activities are structured into four pillars representing primary areas of technology operations that encompass the society's fields of interest:

Technical Pillar leads:

Joe Childs	System of Systems Development and Performance
Eric Wong	Software Development and Performance
Lou Gullo	System/Subsystem Development and Performance
Aaron Dermarderosian	System Foundation Development and Performance

The Technical Activities organization under Sam Keene, VP Technical Activities, includes the following:

Tech Ops Deputy	Dennis Hoffman
Tech Ops Japan	Shuichi Fukuda
Tech Ops Europe	Enrico Zio
Tech Ops Taiwan	Shiuhpyng Shieh
Tech Ops Communications	Lon Chase

II. TECHNICAL ACTIVITY REPORTS

A. Reliability Standards Status

Provided by Lou Gullo (louis.gullo@ieee.org)

Reliability Society Standards Committee: This year, the IEEE Standards Board approved 2 new standards developed by the IEEE Reliability Society Standards Committee (IEEE-RS-SC). These standards are IEEE 1633, and IEEE 1624. IEEE 1633 is the Recommended Practice for Software Reliability. IEEE 1633 was approved by the IEEE Standards Board in March 2008 and was published in August 2008. IEEE 1624 is the Standard for Organizational Reliability Capability. IEEE 1624 was approved by the IEEE Standards Board in September 2008. IEEE 1624 is going through final editorial review and should be published in early 2009.

Besides the development of these 2 new standards, the IEEE-RS-SC is revising 3 existing standards.

Standard	Title
IEEE 1332	Reliability Program For The Development And Production Of Electronic Systems And Equipment
IEEE 1413	Standard Methodology for Reliability Prediction and Assessment of Systems and Equipment
IEEE 1413.1	Guide for Selection and Using Reliability Predictions Based on IEEE

All 3 of these standards have active Project Authorization Requests (PAR) approved by the IEEE Standards Board.

Along with standards development, the IEEE-RS-SC has updated its Sponsor P&P (Policy and Procedures) to better formalize processes for operation of the committee, and its working groups. Lou Gullo, the IEEE-RS-SC Standards Chair has worked with the IEEE-RS ADCOM to gain approval to submit the P&P to the IEEE Standards Board for approval.

Dr. Diganta Das accepted an appointment to the IEEE-RS-SC as the Standards Committee Vice-Chair reporting to Lou Gullo. Dr. Das has been an active member of the IEEE-RS-SC working groups. He is knowledgeable about the preparation of PAR, and the completion of final drafts following the IEEE-SA processes for Standards Board approval.

Also this year, Lou Gullo, the IEEE-RS-SC Standards Chair, has accepted a position on the Executive Committee (EXCOM) for the IEEE Computer Society (IEEE-CS) Software and Systems Engineering Standards Committee (S2ESC). The advantage of joining the S2ESC is to enable co-development of standards between the IEEE Computer Society, and the IEEE Reliability Society.

The IEEE-RS-SC is contributing to the development of other standards outside of the IEEE, such as MIL-HDBK-217, which is sponsored by the Defense Standardization Program Office (DSPO), and Naval Surface Warfare Center (NSWC) Crane Division. The IEEE-RS-SC is providing IEEE with data sharing capability to the 217 working group (217WG) by using the IEEE On-Line Community to host data repository services. IEEE-RS-SC is also pushing to get the IEEE 1413 standard cited in the new version of MIL-HDBK-217, and increase the scope of reliability predictions in this handbook. We are pushing for these changes because it will help this handbook to become more holistic in its approach by including all causes of systems/products failures besides part/component, and interconnect failures.

Initiation of the MIL-HDBK-217 Revision Project: Defense Standardization Program Office (DSPO), OUSD (AT&L), under Mr. Greg Saunders created ASSIST Project # SESS-2008-001, to initiate the effort to revise MIL-HDBK-217. ASSIST is the Acquisition Streamlining and Standardization Information System which is a web-based online database. More than 100 government activities may prepare and submit documents to the ASSIST database using the electronic document submission tool.

DSPO is funding the Naval Surface Warfare Center (NSWC) Crane Division to release MIL-HDBK-217 Rev G by the end of 2009. DSPO is driving the revision of MIL-HDBK-217 based on the results of a survey conducted throughout government, and industry. This survey was initiated in 2004. It was conducted by NSWC Crane, and completed in 2007. The purpose of this survey was to determine what tools are being used by industry to generate MTBF data. NSWC Crane determined from the survey results that, although this handbook has not been updated in over a decade, it remains the most widely used reliability prediction method for electronic equipment. Under the leadership of NSWC Crane, a working group of individuals representing the government, DoD, and industry has been established to conduct this revision. The members of this working group, the MIL-HDBK-217 Revision Working Group (217WG), responded to the NSWC Crane call for volunteers, and were down-selected from the overwhelming list of respondents.

Other Related Activity: Besides this 217WG, DSPO has sponsored aerospace industry collaborative research through the Aerospace Vehicle Systems Institute (AVSI). AVSI is working to develop new reliability prediction models for new component technologies that are not covered in MIL-HDBK-217. AVSI is focused on commercializing Physics of Failure (PoF) models considering semiconductor wear out, and developing a new software tool for reliability predictions. Several members of the 217WG and AVSI are also members of VMEbus International Trade Association (VITA). VITA's mission includes not only promoting VMEbus, but promoting open technology as embodied in the many standards currently under development within the VITA Standards Organization (VSO). VSO is accredited as an American National Standards developer, and a submitter of Industry Trade Agreements to the IEC. VITA formed a Community of Practice for reliability engineering professionals called VITA51, which is focused on providing practitioners of MIL-HDBK-217F with an industry consensus-based approach to MTBF calculation. The efforts of AVSI, and VITA51 should have a benefit, and direct effect on MIL-HDBK-217 revisions in the future.

B. An Ethical Analysis of Automation, Risk, and the Financial Crises of 2008

Provided by George F. Hurlburt, Keith W. Miller, and Jeffrey M. Voas (JEFFREY.M.VOAS@saic.com)

The unprecedented financial market volatility of 2008 has profound implications. While there is plenty of 'blame' to be shared, some key elements of the instability are relatively straightforward to identify. We contend that a fundamental, underlying cause is the cavalier approach taken to applied risk management, an approach that was only possible because of the use (and some would say abuse) of automation.

We examine ethical issues associated with general behaviors leading to the market volatility of 2008. Then we isolate some related ethical factors that can be singularly attributed to automation. While the effects of market automation cannot be realistically blamed for the overall market situation, automation certainly contributed to, and still contributes to market uncertainty. Some of this uncertainty is due not merely to automation, but to decisions made as risk management was automated. These findings are reinforced by research work employing Latent Semantic Analysis (LSA). The LSA results inform our analysis of the impact of questionable ethical behavior in the 2008 financial crisis, and suggest that closer attention to the ethics of financial automation will help achieve eventual market stability and prosperity.

The Current Situation: History demonstrates that hysteria is only optional in a bear market, as the market always recovers given enough time. With peoples' life savings at stake, however, the influence of panic cannot be brushed aside. The 2008 market conditions are unique in that they are far more volatile, and seem to inspire the greatest fear-factor in the history of the modern market [1]. Moreover, because of extensive global networking and border-transcending fiscal interdependence, initial fluctuations in a single market resonate almost simultaneously world wide [2]. The degree to which automation plays a role in this phenomenon appears significant, although the extent of automation's role is likely impossible to quantify beyond the most general of assertions. While it is possible to build a working taxonomy of market related software offerings [3], it is virtually impossible to assess the installed base, much less the scope of networked interactivity among the finance programs operating across the globe. However, there is clearly an ethical imperative implicit in the growing influence of automation in market behavior. The ethical dimension of market automation is therefore worthy of serious study. It is first reasonable to separate some of the key ethical factors that do not relate to automation from the abundance of available information. In so doing, the ethical consequences of financial automation come more sharply into focus.

Ethics Take a Holiday: The 2008 volatility appears to have deep roots. The Government Sponsored Enterprises (GSE) Fanny Mae and Freddy Mac seem to have actively encouraged irrational lending practices as they celebrated a seemingly unending boom in the housing market. Buoyed by the lofty notion that everyone deserved to share in the American dream, and reinforced by explicit Federal decisions to relax or ignore market regulation, the mortgage industry embarked on a high risk journey. Fueled by a rare combination of optimistic exuberance and greed, easy loans became irresistible, even to those who clearly could not afford to pay the premiums. Those granting the loans did the most cursory checks as to the credit-worthiness of their recipients, thereby assuming astronomical risk based on ever increasing home equity values. When the bubble burst, many hapless homeowners were stuck with mortgage terms that once looked attractive, but became intractable as home equity values plummeted, often below market value. As interest rates escalated, Adjustable Rate Mortgages (ARM), and other risk-laden instruments worsened the effect.

The mortgage bubble is not as large as many imagined. As of the second quarter of 2008, only 9.14% of mortgages showed

signs of failure, leaving over 90% of Americans meeting their housing financial obligation relatively on time [4]. Moreover, 1/3 of the population had no mortgage burden at all. Were it not for the fact that the bad debt was repackaged, fractionalized, and sold many times over across international markets, the problem would have been burdensome, but far more manageable. The bad debt was not only sold and resold, but it was also insured by Credit Default Swaps (CDS). Because of the CDS "backing," the packages of mortgage debt that contained the poisoned pill of bad debts were traded as AAA rated financial instruments, a rating that masked the inherent risks. This led to a family of instruments of questionable value, which were virtually impossible to reverse engineer. These instruments were further guaranteed by intangible CDS derivatives that held no real intrinsic value of their own. The estimated face-value of the burgeoning CDS market is \$55 Trillion [5], which equates to more than the world's Gross Domestic Product [6].

In 2003, Warren Buffet called derivatives "financial Weapons of Mass Destruction" [7]. While some derivatives serve a useful purpose in moderation (some people think the Bible endorses a form of agricultural derivatives [8]), they appear to have become a massive, powerful hidden market force. The "Commodity Futures Modernization Act of 2000" [9] re-authorized derivatives in the modern market after they were banned subsequent to the Great Depression. Composed largely of intangible value, the sheer volume of derivatives, including hedge funds, looms over the tangible value of real assets, including stocks and bonds. The entire range of all types of derivatives are estimated to top \$350 Trillion in face value in 2006, and some say have reached a staggering face-value exceeding \$500 Trillion by 2008 [10]. There are no centralized derivative clearing houses, no regulation of derivatives, and consequently no required reporting mechanism for these instruments that often take the shape of nothing more than speculative bets. This has led some to equate the emergent derivatives market to a huge casino [11], but with a faceless house that may not always win. Thus, when housing prices began to decline, the derivative backed mortgage instruments posed sufficient uncertainty to eventually cause worldwide governmental bailouts, and globally frozen credit, devastating businesses, employees, consumers, and investors. It is relevant to this paper that the creation, marketing, and selling of these derivatives in their present ubiquitous form would not have been practical without automation.

Market Automation: The story of the 2008 meltdown harbors all manner of ethical transgressions, which while egregious in their own right, have no direct bearing on automated market mechanisms. Thus, it is difficult to "blame" the resultant problems solely on automation. In fact, The International Swaps and Derivatives Association (ISDA), the professional organization created to promote derivatives, calls for further automation in the world of Over the Counter (OTC) derivatives as a proactive means of reducing attendant OTC risk [12].

According to at least one newspaper report, however, the use of automation is highly suspect [13]. Senior managers at investment houses commissioned so called "quants," or mathematical gurus, to build mathematical models of staggering proportion to characterize financial risk in instruments the houses were developing. Given that these were models, however, they could only approximate real-world behavior, fraught with unquantifiable

influences. As most managers failed to understand the elegant mathematics underlying these models, they innocently or intentionally drove their own assumptions into the models, further skewing the potential outcomes in directions that were useful for selling the instruments, but ultimately ruinous for the economy as a whole. Thus, when it was time to alert buyers to the dangers that emerged as conditions changed, the risk management programs failed to raise the alarm. Their thresholds were skewed towards the underlying false, overly bullish assumptions. An additional problem is that many of the models incorporated standard distributions, distributions that have been widely criticized as inappropriate because they do not conform to the complexities of the market [14]. When a model depends on such distributions, deviations at the positive, and negative edges of the standard bell curve are liable to take gigantic, unanticipated excursions when perturbed by unpredictable patterns [15].

Most trading programs are mathematically biased to logically provide value to shareholders. When a quant, who creates and implements a model, focuses exclusively on short-term shareholder value, the social and economic consequences of the trades themselves may be completely ignored. This, in turn, can lead to actions that are, in retrospect, highly suspect ethically [16]. Because of the weak models implemented into automated risk management programs, alarms warning of impending danger failed to go off, presumed flat tails went asymptotic, and trades derived monetary value at the expense of unwitting world citizens. Moreover, this happens around the globe on a daily basis as networked markets feed upon one another in near real-time. Such automated market behaviors cannot help but fuel growing uncertainty and doubt, among people; and the automated, and human reactions feed upon each other in a vicious cycle.

Ethical Considerations: We note here two interrelated, but distinct phenomena: first, quants created models that did not accurately reflect the true risk of financial instruments; second, a vast network of sellers and buyers of financial instruments distributed these instruments in a way that was swift, and virtually impossible to track. The action of the quants is best viewed as “micro-ethics,” which analyzes the actions of individuals, and small groups. The financial institutions that all too eagerly bought and sold the products badly labeled by the quants is best viewed using “macro-ethics,” which aims for a large picture that encompasses companies, governments, and cultures. In both cases, the actors and their allies realized substantial personal gains; in both cases, there are all too obvious societal costs.

The micro-ethics of the quants and their immediate supervisors turns on the professional requirement to not deceive. Note that professionals are not always required to be transparent to the public; there are many professions (lawyers and doctors are notable examples) that require confidentiality. But confidentiality is not deception. If the quants and their supervisors knowingly skewed the risk assessments towards marketing, and away from reality, then they were not acting ethically as professionals. We could reason to this conclusion in different ways: professionals have duties to the public, and the quants and their supervisors didn't fulfill those duties; and the consequences of their acts were catastrophic for the public.

A slightly more involved ethical analysis is required if the quants and their supervisors did not realize that their predictive

models were inappropriate. If their mistakes were honest, then the analysis would have to explore if the mistake was unavoidable, or a result of negligence or willful ignorance. Many ethicists (though not all) would excuse the quants and their supervisors from ethical blame if it was due to circumstances or events that a professional using due diligence could not have reasonably predicted. At the time of this writing, there is insufficient detail available to the public for us to make a final judgment about this issue of “did they realize what they were doing?” However, events during the meltdown show that the models were completely unrealistic [17], and there were critics who warned of impending problems [18]. Furthermore, the people who developed and sold these financial instruments profited handsomely from these actions. These known facts suggest that the unrealistic models resulted at least in part from bad faith.

Although a micro-ethics analysis may find fault with the quants and their supervisors, a macro-ethics analysis would look at the broader picture. A macro-ethics issue is the power that was given to the quants and their employers by the commercial and governmental structures in place at the time they made their models. If the quants and their supervisors (and the companies that hired them) were in a position to both determine the risks, and sell the instruments, then the system placed them in a position with inherent conflicts of interest. If no regulations or disinterested third parties had effective oversight in the risk assessment and selling of these instruments, then the system (and the corporations and governments that established that system) also bear some ethical responsibility for the consequences. Were these problems foreseeable by regulators and legislators? At least some commentators think they were foreseeable, even obvious, if someone had been paying attention [19].

The micro- and macro-ethical analyses are distinct, but interrelated. The system may have put the quants and their supervisors into a difficult position, but that does not remove the quants' or the supervisors' professional responsibilities. The quants and their supervisors might have acted more responsibly, and thereby avoided the financial disaster; but that does not absolve those who created a system that placed people in a difficult (and tempting) conflict of interest situation.

Amid the aura of deregulation fostered by Dr. Greenspan and other powerful figures in the 1980s and 1990s [20], the Commodity Futures Modernization Act of 2000 kindled the real firestorm. This legislation went so far as preempting states from enacting anti-gaming legislation against derivatives [21]. Given these factors, one could argue that the macro-ethical atmosphere was super-charged with “go” cues that obliterated observable ethical boundaries at the micro-ethical level. This is not to say that Government was blameless, and that the risks were unforeseeable with appropriately deep analysis. *Rather, it suggests that the larger macro-ethical culture set the stage for a multitude of micro-ethical faults to appear as acceptable behavior.* If so, one could argue that the recent systemic market volatility, fueled by unraveling derivatives, was borne of a systemic breakdown of enlightened ethical leadership at all levels. Even Greenspan has recently acknowledged that he made a mistake in assuming that banks' self interest would be sufficient to avoid the disaster that eventually occurred after deregulation [22].

Much as Intellectual Property (IP) rights and copyright issues must be re-examined as a result of pervasive automation [23], the automation of markets should also receive new scrutiny. It may well be the case that the ascent of global market automation fueled unprecedented speculation while masking a very real requirement to deal with the outdated laws and regulations to accommodate the emergent near real-time global interdependent financial networks. In this sense, there remains a critical need for ethical leaders to step forward in the financial industry.

Perhaps the recent literature can be viewed as prescriptive to this end. The next section of this paper presents a nearly subliminal mandate as drawn from applied lexical analysis against a number of relevant documents.

Latent Semantic Analysis Findings: For confirmatory evidence of the importance of automation in the current financial meltdown, a Latent Semantic Analysis (LSA) [24] was performed against eighty-eight fairly substantial documents reflecting diverse points of view regarding the current economic situation. These documents were selected for balance, ranging from highly regarded conservative financial authors to the rants of Year 2000 self-styled survivalists and economic conspiracy theorists, with most viewpoints falling between these two extremes. In our opinion, lax regulation, mortgage speculation, and the flood of derivative products all contributed directly to the subsequent meltdown. We contend that automation played a significant, but yet to be quantified, role in the unwinding of the markets. To guide the semantic analysis, therefore, the collection of eighty-eight documents was subdivided into three topically relevant domains, embracing documents with central themes involving ethics, derivatives, or automation. A fourth domain for all eighty-eight documents taken together was also generated. This domain served as an aggregate cross-check against unions of the three topical domains.

The LSA process breaks documents in a topically bounded domain into tokens after excluding commonly occurring connecting words such as conjunctions, articles, prepositions, and other words whose presence adds no value to the real association between tokens. These tokens are stemmed to eliminate plurals, gerund forms, tenses, and other extensions. This stemming process yields the essence of the "word," normalized without any added letters. (For example, "automation," "automating," and "automate" will all be mapped to the same semantic core idea represented by "automat." The resulting stemmed tokens are then evaluated on a document by document basis, and across all documents for significant associations. Appropriate mathematical weighting is applied across the resulting matrices to accommodate for variations in relative document size, and other factors that could unduly skew the distribution [25].

Once subjected to initial LSA tokenization and weighted affinity organization, each domain was influenced by the same set of selected context phrases. These phrases were "ethics," "computer," "quant," "finance," "wall street," "derivative," and a mega phrase containing all the proceeding words. These context phrases served to build seven smaller sub-domains, or "small-worlds" within each of the four major domains. The resultant contextual hubs and selected topical modifiers were then cross referenced across both the four major domains, and the twenty-eight contextually generated sub-domains.

In most all cases, the tokens "deriv," "market," "risk," "manag," and "global" came up among, if not the most, highly significant hubs in the majority of the domains, sub domains, and combinations thereof. This means that these stemmed tokens represented exceedingly strong affinities to all other tokens in the four major domains. In essence, they may be considered major hub tokens.

The tokens "deriv," "market," and "risk" occupied the top three slots ranked by the number of direct associations to other tokens in the automation, and derivative domains. The same tokens still fell among the top 15 attractors in the ethics domain, which contained some documents aimed at computer ethics exclusive of market influences. Most significantly, these hub tokens also appeared with equally high frequencies in all the context influenced sub-domains. This also correlated well with the results of the all inclusive domain, whose aggregate associations, as expected, were far richer in their affinity counts, but nonetheless still similarly associated. In fact, the tokens "derive," "market," and "risk" also occupied the top affinity slots in the all inclusive domain. The same terms also appeared as highly significant when the three domains were normalized for percentage of the total, and cross referenced. These results represented repeatable numerically weighted associations without regard to the "meaning" humans are prone to assign to the underlying words. Interestingly, the phrase "risk-manag" appeared frequently among the n-grams or "phrases" generated for each domain. These findings strongly suggest that the consensus of eighty-eight diversely oriented authors is that "derivative market risk" "management" on a "global" scale is a central concern.

As ethics was an important area of concern for this research effort, a number of lesser context tokens were drawn from the ethics associations for purposes of correlation across the other domains. These context tokens were grouped by three eight-to-twelve word clusters. One cluster, closely related to ethically related concepts, used tokens found to exist under the ethics domain such as "polici," "rights," and "law". The second cluster associated with computer science tokens within the ethics domain, using tokens such as "research," "environment," and "privaci." The third cluster associated with the market, and used ethics-derived tokens such as "quant," "hedg," and "stock". The ethics cluster concepts showed up selectively in all domains, but tended to show an exceedingly low correlation with concepts dealing exclusively with automation and derivatives. Interestingly, the ethics-based clusters dealing with computer science and market factors either ranked highly, or had no presence in the automation and derivative domains. These results suggest that, while ethics derived concepts ranked highly in the overall and ethics domains, they were not as significant influences in either the automation or derivative domains when viewed as standalone domains. While it is dangerous to conclude that these two domains are devoid of legitimate ethical concerns, it is a reasonable conclusion that such concepts were not significant factors among the selected documents. This is likely to be the case with larger but untested sample sizes, which could potentially confirm the suspected thesis that ethics are not a strong consideration in either financial market automation, or the derivative market. However, the lexical analysis could also accurately reflect an attitude among people discussing automation that there

work is “technical,” and therefore ethics is not relevant. Such an attitude is not unheard of among computing professionals. For example, a recent article by Stieib claims that “competent creation,” not any responsibility for the public good, should be at the core of any professional ethics for computing professionals [26]. Others argue that the public good is at the heart of any professional ethic [27].

Conclusion: While it is an overstatement to claim that automation was the sole culprit, it is not an overstatement to acknowledge that automation was a key enabling technology in the financial crises of 2008. Without automation, it is unlikely that this sequence of events would have occurred [28].

When we consider “automation,” we are referring to the large amount of Information Technology (IT) required to turn the wheels of the financial markets. The IT intelligence (or lack thereof) is embodied in the software algorithms, and those algorithms can be adaptive, modifying trading decisions without hands-on human decision making. These algorithms can be deployed for many different motives, from purely malicious to completely ethical.

The results of our latent semantic analysis work suggest that there were many people who were involved as decision-makers in the financial crises of 2008. The genesis of this crisis was not the mischief of a few players. But even though there were many winners leading up to the meltdown, now it is clear that the losers greatly outnumber the winners.

That leads to a difficult question: if IT was an integral part of this problem, how many other problems can it foster of even greater concern? IT is supposed to be a great enabler of positive social, and economic good; but does it also hold the potential to be the great disabler? We are continually fed information about cyber-terrorism, and the insecurity of networks; could a cyber-pandemic lead to an even large disaster than the financial meltdown of 2008? We can't be sure, but it certainly gives us pause.

C. Lean Now!

Provided by Gary Wickett (wickegl@netzero.com)

BSIE, MBA, CLM, CSCA is a vice president with Transformance Advisors, a Lean training and consulting company.

Is Lean the approach for your organization in these difficult economic times? Lean can best be described as “the systematic elimination of waste.” The seven wastes as defined by the Toyota Production System are: over production, poor processing, excess inventory, unnecessary motions, waiting, unnecessary movements, and defects. The trained Lean practitioner will relentlessly go after these wastes, and put plans in place to eliminate them.

Lean and Six Sigma are now becoming the predominant improvement programs today.

For a history of Lean, see [29]–[31]. A 2007 Opinion Survey by the Lean Enterprise Institute [32] asked 2,500 business people what are the biggest trends in your industry now. The top 5 responses were: value stream mapping (a lean tool) within facility (44.4%), 6 sigma and lean (36.4%), implementing in non-production environments (32.1%), pull (30.1%), and continuous flow cells (25.9%). Lean initiatives including tools such

as *kaizen* (continuous improvement) have shown to dramatically improve process operations. The book “Gemba Kaizen” by Masaaki Imai [33] lists the following improvements among U. S. companies using Lean and *kaizen*: setup time (−66.4%), lead time (−55.7%), cycle time (−17.9%), downtime (−52.1%), operators required (−32.0%), work-in-process (−59.3%), finished goods inventory (−43.5%), distance traveled/part (−54.1%), floor space (−29.4%), parts required/unit (−57.0%), cost quality rejects (−95%), rework (−71.7%), scrap (−45.9%), and equipment required (34.0%). These trends still hold true today.

Not all companies have been successful with implementing Lean. The biggest roadblock, as with many failed programs, is the inability to change the corporate culture. A successful Lean transformation requires the organization to find a change agent, use trained Lean masters, identify the crisis or lever, map the value streams, and begin continuous improvement. The survey cited above also asked these same 2,500 business people what are the biggest obstacles to Lean implementation at their facility. The top three obstacles to Lean implementation were middle management resistance (36.1%), lack of implementation know-how (31%), and employee resistance (27.7%).

What lies ahead for Lean? With the downturn in the economy, this author believes Lean is going to play a major role for organizations in order to compete and survive. Supply chain management will be a core competency across the Lean enterprise, and involves supplier relationship management, and customer relationship management. Finally, the Lean master or sensei will be critical to manage resources, waste and reuse in the GREEN environment.

D. Unreliability of Community Memories and Its Relativity to Blockading of U.S. Scientific Progress

Provided by Samuel Keene, Ph.D., FIEEE

This body of work exists as a direct result of my professional exchanges with Prof. Robert Mathews (mathews@hawaii.edu). He is a Principal Scientist, and the Director of the Office of Scientific Inquiry and Applications, at the Center for Strategic Advancement of Telematics & Informatics. This article is drawn from Dr. Mathews' experiences, his research, and analyses in U.S. national security subjects; and wholly, this writing is an excerpt from his works. It would be effortless to class the message contained within, and its meaning as doctrinaire; however, such an action would be a grave mistake. Owing to the length of this article, the following note is offered. This message is presented from a mutual belief (his, and mine) that we in the scientific community are, from time to time, in need of the proper retrospective, if only to have a message such as this function as quality victual for the mind, to enhance and advance quests toward scientific excellence. Most of all, these thoughts are placed before you as homage to the giants in engineering/science, upon whose shoulders we continue to stand. Dr. Mathews wishes to keenly acknowledge the kind assistance of Dr. Gary Fishman, Director—National Material Advisory Board (NMAB) of the National Academy of Sciences (NAS); Dr. Rebecca Alvania of the NAS; Ms. Teri Thorowgood, Research & Administrative Coordinator at the NMAB of the NAS; Mr. Daniel Barbiero, Manager of NAS Archive & Records; and Ms. Kemberly A.M.

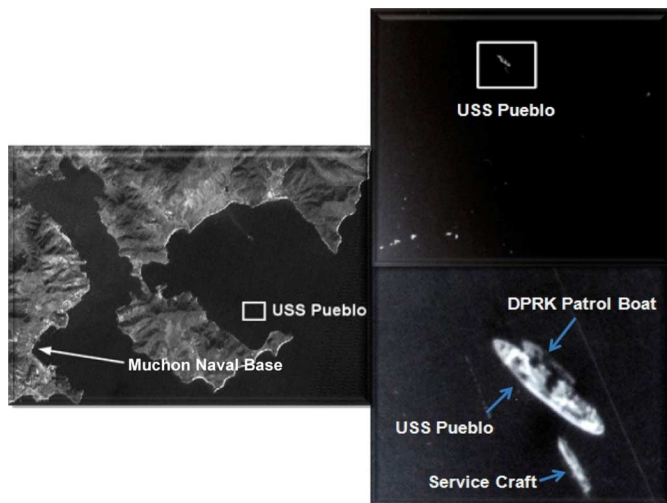


Fig. 1. Relief of North Korean operational area. Photo & information, courtesy: NARA & Global Security.



Fig. 2. A-12 about to be refueled. Courtesy: Lockheed Photo Archives.

Lang and her staff at the Battelle Memorial Institute, for their immense support in the collecting of archived information.

On Distorted Memories¹ and Other Things. . .: **Dateline 26 January 1968, 10 Am GMT (Local)**, Frank Murray is at the controls of an object that can only be described modestly as a *stratospheric bullet*, heading toward the center of the western coast of North Korea (Fig. 1). Piloting this craft, designated only as the 'A-12' (Fig. 2), and flying at an altitude greater than 80,000 feet, at an approach speed 3 times the speed of sound (Mach 3.1/2359.1 Mph), Murray's orders are to surveil the North Korean peninsula, easterly to Muchon Naval Base. In the vicinity, and only three days earlier, the U.S.S Pueblo [AGER-2],² while on a signals intelligence mission in international waters, was boarded, seized, and its crew imprisoned by North Korea. Code-named *Black Shield 6847* (BX6847), Murray is flying a mission with memories still fresh of Francis Gary Powers, in his U-2 reconnaissance aircraft, shot-down

¹Reference to memories herein generally infer to the ability of the scientific community to recall accurate impressions of circumstances, and outcomes (temporal, and spatial in character) as they relate to historical scientific events.

²Auxiliary General Environmental Research Ship.

over the USSR.³ Somewhere below him are 82 American souls being held prisoner, and presumably being tortured.

Director of Central Intelligence' Richard Helms's mission orders, at the behest of the United States Intelligence Board, are to locate the U.S.S Pueblo, and to determine North Korean military posture in the vicinity. Murray is confident, for he is hurling through space, cocooned in a creation fashioned out of high imagination and innovative American engineering; a product shaped from the fires of many unsurprisingly self-possessed spirits, by and large defiant against any prospect of capitulation in the face of scientific adversity. He is flying the perfect machine for a mission such as this. Capable of assuring *surprise, stealth, speed, and reach* beyond known threats, the A-12 is a high-flying reconnaissance platform, equipped with a Perkin-Elmer Type 1 camera, capable of capturing an incredible amount of detail in a seventy-two mile wide swath of terrain, with each pass.

At approximately 10:10 AM local time (GMT), traveling at 2,143.90 mph, Murray points the A-12's Type 1 camera towards the coastline, and snaps a photograph, which would later confirm the presence of the Pueblo, in North Korean waters. During BX6847, Murray will have photographed 12 out of the 14 North Korean Surface-To-Air Missile (SAM) sites, in detail. In all, the imagery collected by BX6847 spanned two-thirds of North Korea, and Frank Murray will have spent just under 17 minutes over denied areas in total!

Except, that is not exactly as events had come to pass. *Black Shield 6847* (BX6847) was in reality piloted by the Late Jack Weeks. Long publicized is the information that the planned over-flight of North Korea by Weeks was aborted because of engine problems. In fact, a recent CIA declassification notes that Jack Weeks completed his assignment on 26 January 1968, not only locating the U.S.S Pueblo, but also acquiring an opulence of intelligence information. The *Weeks* mission lacked sufficient coverage of Intel targets over North Korea. Therefore, the National Reconnaissance Office [34], per recommendations of Commander-In-Chief, Pacific (CINCPAC), and the Defense Intelligence Agency (DIA), petitioned for a second round of North Korean fly-overs to satisfy the Intel gap. Frank Murray flew that *Black Shield 6853* mission (BX6853) on February 19, 1968. It is not clear *why* many authors [35]–[41], who managed to research this event intimately, proceeded to *collate and publish incorrect memories* of that important event. In the immensely popular "*Body of Secrets*," author James Bamford takes literary license the extra mile, wrongly noting that Frank Murray was "ordered to make the *first* A-12 over-flight of North Korea," [39] adding that Murray originally attempted to launch on the 25th, however, a "malfunction on the aircraft had forced him to abort shortly after takeoff," [39] and he consequently launched on the 26th. At least two sets of authors, Remak & Ventolo, and Crickmore [42], correct previous errors in later revised versions of their respective works.

However, they offer no explanation regarding the changes they present in later versions. One author, a retired U.S. Air Force officer (Irwin/2000) [43] offers an incogitable proposition⁴ that 14 hours after the U.S.S *Pueblo* was hijacked, reconnaissance photos were presented before the President of the

³Francis Gary Powers was shot down near Sverdlovsk, on 1 May 1960.

⁴By facts available, and known today.



Fig. 3. First A-12 delivery to Groom Lake. Courtesy: Lockheed Photo Archive.

United States for decisioning. This could not have been possible, for the Pueblo was boarded by North Koreans on 23 January, at 1432 Hrs local time, or 0032 Hrs on 23 January, Washington time; and according to official records, the first over-flight over the region did not occur until 26 January. Finally, it needs to be said that the one person who was perhaps most intimate with the lifecycle of this aircraft, team leader Clarence L. Johnson of Lockheed Aircraft has declared in his report “History of The OXCART Program,” [44] that “a successful mission over North Korea, after the seizure of the Pueblo” was flown on 14 February 1968. Nonetheless, official records do not indicate any A-12 over-flight of North Korea on 14 February 1968.

There is opportunity for error to be introduced at any stage in a process, and by anyone involved. At the core, this paper endeavors to lay bare how error/propagating distorted memories ably produce a retarding of, and distortion in scientific progress, and also in formulating national science policies.

Funded by the CIA, and built by the Lockheed company, history continues to celebrate the genesis of the élan A-12 (later known as the SR-71 Blackbird) as an enduring symbol of American ingenuity, daring, technical brilliance, and institutional farsightedness (Fig. 3). For all the praises that are sung in its name, this engineering marvel almost failed to materialize. To use a common metaphor, the A-12 was born out of wedlock, and of high dysfunctionality, which is often the case when new paradigms are proposed against the longstanding traditions, where institutions predictably cling to moribund ideals. Washington Turf wars, bureaucratic dysfunctionality, institutional power grabs, and significantly more than the usual share of technical challenges bloomed to a full; all this during the A-12’s gestation, and much before it could exit the womb. Among the many struggles, orchestrating the availability of sustained research and development funding in a highly politicized world of intelligence program funds allocation, was, among other things, a principal necessity.

From an engineering point of view, however, one of the leading technical challenges associated with the A-12’s manufacture involved the use of Titanium as the chief metal with which the airframe was to be constructed. Even though Titanium was being used in small quantities, and in localized areas of commercial aircraft manufacturing starting in the early 1950s, the A-12 design was the first to require Titanium for the construction of the whole aircraft. However, reliable processes for Titanium alloy sheet manufacturing that ensured “increased

uniformity, reliability, strength, weldability, and fabricability characteristics” [45] to the scale required, did not exist.

Not only was there a significant Titanium shortage at the time when the A-12 was needing to be built, but to immensely complicate matters, the United States lacked the vital scientific knowledge to fabricate this aircraft.

In essence then, a *strategic national defense component was being planned* in the absence of 1) Titanium in sufficient quantities, and 2) the scientific knowledge needed to turn a characteristically brittle metal [44] into the desired usable state. In retrospect, materially, the genesis of A-12 was only possible due to the work of key parties at the Battelle Memorial Institute, National Academy of Sciences (in particular the Materials Advisory Board), and Anderson Aircraft, among others. Lockheed’s aerospace designer and engineer Clarence ‘Kelly’ Johnson is credited most, and often, for the creation of the A-12. However, from a scientific point of view, Johnson had no known role in the evolution of Titanium as a nationally strategic metal. To tidy-up misperceptions merely, Johnson rightly deserves many praises. The names of those significant contributors to the evolution of Titanium as a nationally strategic metal, and hence to the development of the A-12, have remained largely muted by the amplitude, and tune of praises for Kelly Johnson. Today, many important parts of the A-12’s evolution receive little attention, if any; and the footprints of great contributors to the effort have been significantly obscured. Consequently, at present, while the evolutionary detail of the A-12 is ably preserved within certain key institutions, personal and community memories regarding key contributors and events remain less durable.

If one were not careful in reviewing the history of A-12’s evolution, one is likely to unwittingly be left with an impression that the A-12 emerged from an ‘instant universe.’⁵ Such an impression spares the inquisitive mind from the details of the hefty institutional and intellectual acrimonies that surrounded the parturition of the A12. If it were not for the brilliant minds of scientists like Dr. William J. Harris, Jr.,⁶ Nathan E. Promisel, Dr. Robert I. Jaffee, and others, and their intimate involvements in evolving Titanium’s usability for national strategic purposes, the A-12 would have merely remained a sketch on the drawing boards at Lockheed’s *Skunk-Works* in Burbank, California. It has been quietly recognized that, if the demand to fabricate Titanium in a certain manner to build the A-12 had not existed, the Titanium industry as a whole would not have come into being at all, as it did, because military applications represented the most promising areas of continued use initially [46]. It is essential to note that the collaborative work between the pre-eminent

⁵Prof. Mathews attributes the term “instant universe” to the legendary R. Buckminster Fuller. Fuller has used the specific term to demonstrate to his audiences around the world that before the 20th Century, the ‘speed of light’ had never been a matter of scientific consideration, that in fact those involved in the pursuit of science had always considered the presence of heavenly stars in earthly skies to have been constant.

⁶Dr. William J. Harris, Jr., the ‘quiet giant,’ as Dr. Mathews has often referred to him, served as the Chairman of Materials Advisory Board—Main Panel of the DoD Titanium Alloy Sheet Rolling Program from 1955 to 1962. He also served as the Executive Director of the Materials Advisory Board between 1957 and 1960, and as Chairman (from 1969–1971) of the renamed National Materials Advisory Board (NMAB). Dr. Harris was a prime member of the Material Advisory Board Sub-Panel to Formulate a General Program on Titanium Fabrication of the DoD Titanium Alloy Sheet Rolling Program from 1957 to 1959, and the Material Advisory Board’s Sub-Panel on Alloy Selection of the DoD Titanium Alloy Sheet Rolling Program from 1957 to 1960.

naval and civilian materials scientist Dr. William J. Harris, Jr.,⁷ and the Titanium Metallurgical Laboratory (TML) at Battelle Memorial Institute, were crucial to the formation of the DoD' Titanium-Sheet-Rolling program.⁸ That work also substantially shortened the time, which would have been consumed otherwise to ready Titanium as a *reliable material* for construction, in both a qualitative, and a quantitative sense [47]. Fact remains that, outside of efforts to grow the technical knowledge to use Titanium as a strategic metal, and the *Manhattan Project* where the development of enriched Uranium also required a constitution of resources involving high concentration of scientific and technical talent plus financial support, there has never been another assemblage of resources in a similar manner to advance the use of a single metal for national strategic purposes [46].

The much-abridged description of the A-12 development, as surveyed here, is meant to demonstrate that there just may be quite significant aspects of a certain subject, such as the development of the A-12, of which we know little, none at all, or worse—are in possession of distorted knowledge, which somehow becomes the driving force for forward thought. With respect to the A-12's evolution, the advancements related to Titanium, or the design and construction of the aircraft can never be considered uniquely, or compartmentally from each other; for one could not have materialized without the other. As will be discussed, knowledge always represents an amalgamation of information. Therefore, dealing with the interpreted product of illusionary signals as in the case of Titanium development, result in a type of *cognitive parallax*,⁹ which must be corrected to enable progress, and to make our contributions to science effective and meaningful.

The principle to be carried forward from this chronicle, in relationship to facilitating the progress of science, is simple. To be

⁷Following the Battle of Britain, between 1941 and 1945, Dr. William J. Harris, Jr., was recruited to be the lead scientist at the (then) Navy Department, and charged with the responsibility to armoring US Naval Aircraft, which as a result, saved countless American lives. Dr. Harris and his team at the Naval Research Laboratory were the key parties responsible for defining the problem associated with the "Liberty Ship Steel" failures. In fact, he is the author of the definitive report on Liberty Ship failures. Knowledge gained in both areas, consequently went on to improve commercial ship and aircraft manufacturing, and improving both quality and safety of operations. In addition, from an engineering history point of view, his cutting-edge technical investigations at American Association of Railroads (which he had more than a hand in founding), and elsewhere, enabled the rise of world's railways and remains an impressive testament to one man's influential contribution to science.

⁸Titanium Steering Group of the Office of Assistant Secretary of Defense for Research and Development, directed TML (August 1955) to assist and guide the Navy Bureau of Aeronautics (on behalf of the Department of Defense) to develop a recommended course of action for Titanium development. Upon approval, the Navy was to then assume responsibility for coordinating the implementation of the Titanium-Sheet-Rolling program, and implementation of the various phases to be accomplished through various Department of Defense Agencies that were to be involved.

⁹Merriam-Webster defines a 'parallax' as "the apparent displacement or the difference in apparent direction of an object as seen from two different points not on a straight line with the object." Extending the physical principles behind 'Parallax Error,' to processes relating to cognition, Prof. Mathews chooses to use the term 'cognitive parallax' to describe the incongruity between informational and cognitive constructs that presents gaps in the logicity composite, having the potential to then go on to create/form the basis for incorrect historical memories and informational matrix unless corrected. For a holistic elaboration on the properties of a 'Parallax,' we refer you to "The Parallax View" [Slavoj Žižek], MIT Press, Cambridge, MA, 2006. Supplemental reading: Bradshaw, Mark F., *et al.*, "Surface orientation, modulation frequency and the detection and perception of depth defined by binocular disparity and motion parallax," Vision Research, Vol. 46, Issue 17, September 2006.

blunt, if parties in the scientific enterprise, or decision-makers that support the scientific enterprise, suffer from niggling effects of aforementioned *cognitive parallax*,¹⁰ the prospect to properly instrument strategic and/or tactical decisions in the national interest will likely be very slim. The complexities associated with attempts to replicate such efforts now in the national interests are exceedingly complicated all by themselves, and must not be obscured further by such errors. In such a context, the United States' scientific community is likely to face three major inhibitory factors when wanting to stimulate, or accelerate the progress of science and scientific policy in the national interest, in the 21st Century. They are: 1) lack of comprehensive scientific knowledge vital to national leadership roles, 2) ever increasing complexities associated with the uninhibited growth of information in the digital universe, and 3) the absence of rightly optimized operational enterprises, which can adequately leverage informational synergy and advantage. The lack of comprehensive scientific knowledge at the leadership level will only continue to result in a national inability to strategically plan, and/or support critical strategic, and tactical scientific activities. The uninhibited growth of information in the digital universe will undoubtedly present a significantly augmented, engorged proverbial '*needle in a haystack*' problem. Whereas, the absence of accountable, properly optimized, engineered, forward-thinking enterprises will permanently impede the materialization of goal oriented actions to bring about material and policy effectiveness and efficiency. America must urgently seek to instate a national science policy leadership that possesses deep humility, and the capability to recognize the amount of variance in the scientific environment, which now exists in large part directly due to errant, factious, contumacious, and perverse policy measures and mechanisms that were thought up, and have been put into place over the years. Decision makers must be open to contrarian ideas, and hear them out in full, as it is now an indispensable ingredient to reversing our national scientific plight. The three major factors stated above are expanded here briefly, to acquaint the reader ever so lightly to the great nub behind these significant issues.

With respect to 1) directly above, Dr. Edward Wenk, Jr. [48]¹¹ once observed that a national capability necessary to enable the proper decisioning for scientific progress is impinged when the role of government as either the means for change, and/or as the 'steering system' to achieve change, is essentially disabled by 'incompetence, error, exhaustion, self-delusion, bias, venality, or hubris.' Additionally, Wenk acknowledges that decisional error, for example, has the potential to be 'lethal to society.' With respect to 2), special interest groups, by adding more noise through sensationalism, and the introduction of bias in their reportage, now constantly vie for public attention. To the lay person, including policy makers and their staff, such actions by special interests groups often cause issue particulars to become blurred, which then introduces further complexity into the processes that otherwise ensure traceability and accountability for basis in policy decisions. Lastly, with respect to 3), the

¹⁰Thinking that one adequately comprehends a subject matter, when in fact, one does not.

¹¹Dr. Edward Wenk, Jr. served as the very first advisor to U.S. Congress. Afterward, he served in a scientific advisory capacity to Presidents Kennedy, Johnson, and Nixon.

consistent and almost predictable employment of reductionistic logic by leaders in enterprises, exempting full picture thinking, jeopardizing *interoperability*,¹² [49]–[54], and promoting *unintended consequences*, will produce in all likelihood, lethal societal effects.

Whether the three factors aforementioned stand-alone, or will combine, means little in terms of total outcome, as each is capable on its own to severely obstruct us from timely engaging nationally significant opportunities in science. Further, in terms of assuring U.S. competitiveness on a global scale, and possessing a sizeable national security edge in view of rising threats, the costs associated with the loss related to any nationally strategic scientific opportunity are presently immeasurable. Therefore, in this paper, three banded ideas that are substantively important to the orchestration of meaningful solutions are brought together. A) We¹³ identify that memories relating to scientific achievements need to be holistic, and complete such that any scientist can comprehend the nature of the road that was traveled to attain progress.¹⁴ B) Skewing in memories relating to past scientific achievements can substantially alter our perspectives regarding the type, and scale of effort among other things that had to be mounted to achieve progress. C) Lastly, we present a brief discussion on critical missing pieces that need to be included into a solution orientation as part of any reformative process. Remember that this discourse is not intended to be a segment-by-segment analysis of the many aspects or parties involved in U.S. science policy failures. However, we hope that this writing will stimulate further thought and conversation regarding much needed leadership, and rightly piloted direction in U.S. science policy development and research activities.

Of False Knowledge¹⁵ and Other Things. . .

The introduction of *false knowledge* into the scientific community is continually corrupting the way we need to advance scientific knowledge, institutions, capacities, and capabilities. However, the scope of this writing cannot address the breadth of this subject as necessary. Nevertheless, we shall attempt to demonstrate, in a small way, the error of our ways with regard to the advancement of science, and more specifically, how ill-thinking U.S. science policy instruments are now laying to waste many opportunities to seed innovation, and opportuni-

¹²Dr. Robert Mathews has defined interoperability as the capability by which all operating elements of interdependent and interconnected systems are able to operate synchronously to achieve mission success, or pre-determined goals and objectives continually. Synchronous operations here infers to an operational requirement for all components/sub-systems of interdependent and interconnected systems to be properly oriented, skillfully aligned, and readied across geographic and organizational boundaries, and professional disciplines to achieve mission objectives.

¹³When not referenced otherwise, use of the tense “we” in this article reflects the joint opinions of Dr. Robert Mathews of CSATI and this author, as it is sufficiently detailed within the Prologue to this article.

¹⁴See reference to the discovery of DNA structure in the section “On Acquiring Knowledge and Employing Wisdom. . .”.

¹⁵For the purposes of this writing, the significant distinctions between data, information, knowledge, and wisdom are not detailed herein; as such, an exploration is largely out of the narrow scope of this writing. Nevertheless, being familiar with the distinctions between them is expected of the reader. To refresh, reference to memories herein generally infer to the ability of the scientific community (or more the ‘inability’ in this case) to recall accurate impressions of circumstances, and outcomes (temporal and spatial in character) as they relate to historical scientific events.

ties to materialize a spirited scientifically competitive economic edge for America’s future.

On the impact of *false knowledge*, the administrator of the US Space agency was the invited speaker before the American Astronautical Society in October of 2008. In his presentation titled “NASA and Engineering Integrity,” Griffin attempted to disqualify incompetence at the agency, saying “[w]e at NASA cannot possibly make everyone happy with our decisions. Most decisions will produce an unhappy outcome for someone. However, that unhappiness is not by itself a symptom of incompetence, bad intentions, or a lack of integrity on our part,” and that “the taxpaying public and its elected representatives, our overseers, can and do expect from NASA be summarized in two words: *objective expertise*” [55].

Perhaps, Griffin is unaware that his agency was indicted for carrying on, keeping alive, a “*cycle of smugness substituting for knowledge*,” [56] and for maintaining a kind of ““arrogance” within NASA that led leaders and managers to be dismissive of the views of others, both within the organization, and especially from outside the Agency.” [56] Maybe he is indeed *arrogant and ignorant* [57], as one of the space agency’s foremost scientists has described Griffin. One thing is perfectly clear, given all that is publicly known, Griffin appears to have been “making a runtish proposition that the level of engineering insight and management vigor that **could have**, and **should have** been demonstrated by NASA, before Challenger and Columbia space shuttle missions, were indeed optimal!” [58] Logic would have it then that ‘taxpayers’ did not expect NASA’s “*objective expertise*,” which Administrator Griffin was peddling that day, to have been responsible for the destruction of two spacecrafts, the loss of 14 American lives, and very nearly shut-down the entire American space program. By Griffin’s own admission, the Challenger and Columbia disasters caused “extensive redirection, massive delays, and huge cost overruns” [55] at NASA. These redirections, delays, and cost overruns were also not endured with the consent of the American taxpayer. However, NASA administration evidently believes that *false knowledge*, and the organizational apparatus that used *false knowledge* to render the wretched decisions that almost tore-down America’s space agency, is in fact the “*objective expertise*” that the agency materially needs to tackle future scientific challenges! Fact remains that the opportunity costs and programmatic setbacks suffered by NASA, because of the Challenger and Columbia accidents, have yet to be tabulated accurately.

How does *false knowledge* hold back the progress of science? Francis Bacon in his treatise on ‘Advancement of Learning’ wrote, “. . .as navigation was imperfect before the use of the compass, so will many secrets of nature and art remain undiscovered, without a more perfect knowledge of the understanding, its uses and ways of working.” [59] Scientific progress depends primarily on our ability to navigate properly through the subject/field that is under observation. While mankind’s accumulated knowledge has provided a jumping-off point for arbitration, negotiation, and/or intercession, in the pursuit of new knowledge, the scientist must constantly be on alert for new clues that yield new information regarding our place in the universe [60]. In the here and now, when information is distributed at the speed of light across the world, how do we

organize ourselves to shed internal *false knowledge*, to collect, analyze, and use information comprehensively, to positively affect the state of scientific progress?

On Acquiring Knowledge, and Employing Wisdom...: Through the millennia, inscriptions that have conveyed the collective memories of humanity and knowledge were held in venerated places, such as the Royal Library of Alexandria, and The Pergamum library of antiquity. Only sands of time now exist as unchangeable testimonies to their greatness, and their once grand archives on human progress. Is destruction of the type that consumed the Royal Library of Alexandria possible in our time, and likely to annihilate consequentially, in near totality, all prior memories, knowledge, and detail of human progress? Given our state of existence, and our connections to, and employment of, processes and technologies, to distribute and share knowledge presently, we can combat a catastrophic loss such as that. Today however, in its place, the one very likely threat that is of an equal or greater magnitude to the inexpressible loss of the Royal Library of Alexandria is the approaching high hazard of expediting a widespread permeation of *false knowledge*. We must keep in mind that distorted memories, are in essence, *false knowledge*. Any permeation of *false knowledge*, to borrow from *Erasmus*, can compactly be stated only as “plagues of the mind [that] spare neither rank nor sex nor age, and are restrained by no boundaries, but sweep the earth with unimaginable speed.” [61]

What follows is an example of how one entity has managed to distinguish *between useful and useless information*, and to utilize the ‘useful’, to fuel operations and performance globally. Wal-Mart, the world’s largest retailer, is said to be storing and managing over 460 Terabytes of business information [62] to improve business practices. Wal-Mart routinely utilizes commodity, customer, business transactions, and business environment information to generate actionable wisdom, enterprise-wide, from the breadth of data it possesses and processes, which in turn allows them to have ‘the edge’ over their competition. By all measures, they seem to accomplish this goal exceptionally well. These days, organizations and businesses are not the only ones routinely straddled with the responsibility to distinguish *between useful and useless information*. At an individual level, our thirst for information and knowledge is equally great; we seem to be ever industrious, creating familial, personal, professional, and social libraries. Curious and full of brio, Americans appear to be in constant need to ferret-out some form of information from some part of the *Digiverse*.¹⁶ In October of 2008, Americans performed 12.6 billion searches at the core search engines [63]. Of this, Google alone handled 8 billion searches. 12.6 billion searches roughly translate to 4791 searches/sec. According to the ‘Diverse and Exploding Digital Universe’ report [64], this *Digiverse*, was roughly 281 ExaBytes, or 281 billion GigaBytes in 2007, 10% bigger than what was originally expected to be. Individuals create 70% of all information in the *Digiverse* [64]. The important question before us is, are people finding that for which they are searching?

Not all information is either knowledge, or wisdom. How are we to separate the wheat from the chaff? During Medieval times, kingly courts had food tasters who were present to ensure that a *bon vivant* monarch did not succumb to any venom of wicked-

ness. While not suggesting that we employ food or information tasters to daunt what wickedness comes, is there a modern day equivalent of this practice to be emplaced in each of our lives? Surely, considering the volume of information that is now available, when confronting it, mere mortal sensibilities could quite easily suffer vast strain! How are we able to ensure that which we read and take to heart is valid, and is indeed knowledge? Science is not immune from the challenge imposed by the aforementioned question.

Dr. Mathews reminds that science cannot progress at the expense of wisdom-in-debit; that true wisdom empowers us with the ability to observe ‘a matter,’ to be reasoned to it, and from it, in all manner, to be prudent, discerning, relational, expressionally lucid, and analytically incisive of the whole, and not just any single part, or a collection of select parts. He points out that, while James Watson, Francis Crick, and Maurice Wilkins have been credited with the discovery of the molecular structure of DNA, he emphasizes that DNA advancement would not have been possible if it were not for the simple fact that other scientists had unraveled key aspects of the puzzle before Watson, Crick, and Wilkins. The work of Erwin Chargaff, Linus Pauling, and indeed Friedrich Miescher are representative of *foundational work that preceded* Watson, Crick, and Wilkins’s endeavor. More in keeping with struggles we face today, F. W. Bain has expressed adds to this sentiment quite well in his elaborations of *Plato’s* teachings, urging that a reformed understanding of the *organic* whole, as Bain says, “. . . can do for modern science, something of which it stands in sore need [65].¹⁷” In terms of *false knowledge*, according to Nicholas Maxwell,¹⁸ responsibly for progressing science in our time, however, requires being attentive, for instance, to Bain’s proposition of the *organic whole*. According to Maxwell, this would require a communal correction in the manner we formulate and express our scientific/academic inquiries, one where the basic aim of all academic processes must be reorganized, “to promote wisdom, and not just acquire knowledge” [66].

Maxwell explicates that “[e]very branch and aspect of academic inquiry needs to change if we are to have the kind of inquiry, both more rational and of greater human value, [which] we really need.” He emphasizes that overall aims and methods of academic activity have the “responsibility to make clear what is wrong, and what needs to be done to put things right. . . shout out, loud and clear, that we urgently need to bring about an intellectual and institutional revolution in the aims and methods, the whole structure and character, of academic inquiry, so that it takes up its proper task of helping humanity learn how to create a wiser world” [66]. In instructing us to *Plato*, Bain poses an intellectually complimentary message, which connects *Plato* and Science, signifying that *Plato* cannot be discretely analyzed, or understood, without a comprehension of his works in terms of the style, the vehicle, the atmosphere, and the by-play involved [65]. So too in science, progress is tightly coupled to our intimate understanding of certain key fundamentals, such as the ways and means, which has facilitated humanity’s scientific progress through time. In this, and other vital concerns, we continually and detrimentally fail to recognize that our perspectives

¹⁷Speaks specifically to the need for highly integrated critical thinking.

¹⁸Nicholas Maxwell is Emeritus Reader in Philosophy, at University College London.

¹⁶The Digital Universe.

are not often whole. It is not the intent of this writing to provide a most comprehensive gap analysis on shortfalls in necessary actions. Inquisitive parties involved in the pursuit of science are well positioned to acquire that information on their own; to signify and correct errors in our perceptions. Some of our largest challenges achieve little resolve today, as we remain unable to realize and pinpoint the boundaries of our personal knowledge, which if we did, could permit us to cogitate problems more effectively, collaborate more efficiently, and to conceive solutions more expediently. Yet, in this realm, we lack many things. To break the deadlock, we must understand how *false knowledge* inhibits us from achieving the necessary breakthroughs.

On Permeation of False Knowledge. . .: Maxwell's proposition toward "helping humanity learn, how to create a wiser world" [66] presents a beguiling challenge indeed. Genuinely, the 'helping humanity learn' part intrinsically commands that mankind shed its *false knowledge*, and be prepared to progress forward with a clarified mind [65]. However, that is easier said than done. George Bernard Shaw has characterized the difficult situation, where humanity appears to consistently desire to be nourished with *poison from the fountain of false knowledge*. Shaw presses, "[e]very fool believes what his teachers tell him, and calls his credulity science or morality, as confidently as his father called it divine revelation" [68]. Clearly, he is pondering a most contemptuous likely state of the human-mind, where more than a freshman philosophy student may be let impoverished by *false knowledge*. Shaw strongly demonstrates that dedicating oneself to very hard work to correct one's accumulated mis-perceptions is the only path to ushering in progress. However, for a lack of toil, we have been free to tender *false knowledge* as a substitute. The impact of permeated *false knowledge*, in the sphere of scientific advancement, is immense. From scientists, who purport themselves to be subject matter experts, to policy makers and their staff, government department and agency heads and their scientific staff, and all parties in between are potentially subject to influence from the permeation of *false knowledge*.

In the 'helping humanity learn' with a clarified mind department [67], perhaps *Socrates* provides us with the best practical details from the ancient world—on how to root out error. To that purpose, *Socrates* chose to cross-examine his counterparts to root out 'pretenders of wisdom,' [69] or purveyors of *false knowledge*. Classical philosophy textually details an instance when *Euthyphro* is sardonically complemented by *Socrates* (a tactic/exploit now often referred to as *Socratic Irony*) upon the discovery that *Euthyphro* intended to prosecute his own father, for murder, by that which *Socrates* considered *false knowledge* [70]. It has been said that "[t]he irony of *Socrates* was the art by which he drew a pert and shallow sophist or pretender to wisdom out of his state of half-knowledge. It showed how men rested on words and passed mere tallies or counters about as if they were current coin," and "[u]nder an air of levity the *Socratic irony* was in reality, a call to seriousness a protest against those idols of the market place, the commonplaces and saws which passed for wisdom" [71].

Regarding the progress of science, *false knowledge* is the subject to which we must attend in our current time, to supervise and to clarify for ourselves as men and women of reason, of science, that the knowledge we foundationally hold dear as a basis

for our beliefs, our understanding, and our reality is sound. Beyond any personal struggle, there are organizational struggles as well. Bain is eloquent in articulating the nature of organizational struggles, to be precise, how educational systems indoctrinate persons into the realm of *false knowledge*. Bain says "when sophistry has become a classic; when it is taught in colleges and bound in vellum; when its commentators have become a fraternity, its elucidation, a trade; when critical reputations have been staked on its truth, and professorial expositions of its principles stand or fall with it; *it dies hard*. To convict it of error is, as it were, to take down great 'critical' philosophers from their pinnacles. . ." [65] "like little statues on great pedestals, only seem the smaller by their very elevation" [72].¹⁹ The world dislikes nothing so much as to see its idols broken, and have to confess that its gods were after all not porcelain, but common clay. Rather than admit this, it will obstinately refuse to see" [65]. In the case of *Socrates*, his cross-examining of pretenders of wisdom, his challenge against false information, and the spread of it so infuriated Athenians, they handed him a death sentence [73].

Democritus, Socrates, Plato, Aristotle, and others sought to understand the nature and constitution of knowledge at a personal level. Through the times, from *Kepler* to *Galileo*, and from *Newton* to *Einstein*, the amassing of cosmological knowledge has not been painless. We now know that Newtonian Physics fails, against Quantum Mechanics, General Relativity, and Special Relativity, while continuing to serve purpose in Classical Mechanics, which then points to the need for knowing the place, the purpose, and usage for each. Extending this thought to the prospect of advancing science in the national interest, at the very least implies then that those involved in policy processes *must have* an unmatched insight into human evolution in terms of the growth of knowledge, and its relativity to present circumstances, in order to be effective, efficient, and foresightful. In *Perspectives on Science*, Henry Bauer contends that guided evolution of science, or accelerating that evolution through sound "science policy," has the prospect to transpire only if we have the sufficient understanding of *how science works*, and how, and why, it has progressed in the past [74].

On Sowing Tainted Policies: William D. Carey²⁰ has held the following thought on making scientific progress. He said, "the nature of progress through science is a meandering and uncertain struggle toward discovery and verification, a search carried out in an environment of intellectual joy and disappointment. Such a perception, however, says nothing of the presence of competitiveness, of reward and punishment systems, of queuing phenomena, of sharp practices, of ethical and moral dilemmas, or of the arrogation of science or much of it into instrumental service to the State, and to the Corporation." [75] Carey has, gently and artfully exposed us to one of the many poisons swirling in the *fountain of false information*. He notes that,

¹⁹Attributed to Plutarch, by Sir. Francis Bacon "men of weak abilities set in great place, that they were like little statues set on great bases, made to appear the less by their advancement."

²⁰Formerly, director of American Association for the Advancement of Science (AAAS), and served under five presidents in the Bureau of the Budget, last as Asst. Dir. of the Executive Office of the President-Bureau of the Budget. He was formerly Chairman of the United States side of the bilateral working group with the USSR on science policy; and Chairman of the Visiting Committee of the National Bureau of Standards (NIST, today).

beyond the many ideational, paradigmatic, institutional, financial, and personal struggles, which those that pursue science are often forced to endure, there are even greater external forces, or aspects, that attempt to exert a corrupting influence over the direction of science. As an example, reflect on the fact that Young *et al.* have presented on one such aspect, and have presaged that commoditization of scientific knowledge is likely to distort Science itself [76].

At the risk of assuming that readers will be in possession of requisite knowledge, we intrinsically present that scientific research supporting institutions at the governmental level, their tenets and mechanisms to evaluate and to fund, are in fact broken. How are they to be righted? A very brief view of the state-of-affairs is put forward for considerations here, with due reference to the presence and permeation of *false knowledge* in establishments and persons.

In post WW-II America, McGeorge Bundy candidly expressed that government should not impede scientific progress, with paper-pushing bureaucracies, and organizational restrictions, saying "...there is a wide, deep, and important coincidence between the temper and purpose of American national policy and the temper and purpose of American science. Our science and our society are deeply alike in the pragmatic, optimistic, energetic, and essentially cooperative view of the way in which useful things get done" [77]. Of course, this cooperative view of science's place in society was presented by Bundy at a time when the political ideology, as explained by Proctor [78], celebrated scientific research as neutral, and requiring protection from barbed forces for the benefit of the nation. Proctor made clear a discernment of roles, which related to basic research as a whole on one side; and on the other, the application of research outcomes toward any specific purpose.

It was also before ramshackled ideals began to infiltrate Capitol Hill, and members of U.S. Congress began to view science and scientists, in Don Price's words, as "just another selfish pressure group, not as the wizards of perpetual progress" [79]. To make clear Price's expression, Congress has for whatever ham-fisted and capricious reason, begun to think of 'science' simply as another government program needing funding. Because Congress is not mindful of the need to finance basic science as the primary strategic constituent to nourishing the fountain of innovation and knowledge, strengthening and enhancing our national security capabilities, our quality of life, and domestic and global economic vitality, the road to improvement is that much harder. Then again, Congress has probably never heard of Jürgen Habermas, or of the Habermasian extensions of Aristotelian principles, which suggest that our pursuit of knowledge is largely motivated by our need to enhance human life, along a technical, practical, and emancipatory line [80]. In the absence of one's awareness of the building-block, Habermasian principles in the policy realm is likely to leave one informationally handicapped, and less capable to act in the best interest of all Citizens. An extremely compact examination of the extensions of Aristotelian principles by Habermas is therefore a reasonable exercise here.

Shirly Grundy interprets Habermas's particularization of 'technical knowledge' as 'a' domain interest in the 'control and technical exploitability of knowledge,' where civilization is innately "governed by a fundamental human interest in

explaining, explanations providing the basis for prediction and predictions providing the basis for the control of the environment" [81]. Grundy establishes a line from humankind's thirst for knowledge, to the need to free him/her from bondage of ignorance. At least an affirmation related to Grundy's proposition is discernible in the U.S. Government's interest in 'regenerative medicine.' Expectations are that 'regenerative medicine,' which include advancements in Genetic therapies, will be revealing ways by which previously unthinkable medical treatment approaches can now be employed. A U.S. Dept. of Health and Human Services report projects that the cost of American healthcare is expected to rise from 13% to 25% of US GDP by the year 2040. The same report states that integrated treatment approaches such as regenerative medicine will provide the technology edge to bring about not only cost containment, but previously unforeseen means to improve the quality of healthcare and healthcare practices as well [82]. The report, however, admits that the U.S. is behind the curve in terms of investment and support for such programs in comparison with other countries. As U.S. healthcare costs continue to soar, necessary are innovative approaches to dispense a superior level of patient care that makes it possible to contain costs without sacrificing quality. Policymakers must be well equipped to meet and exceed such national challenges. Congressional functioning under auspices of *false knowledge* is, among other things, a prime obstruction to the formation, and the sustenance of health policy regimes, among other policy areas, which are able to benefit the scientific community, and equally and complementarily in the service of the nation.²¹ Consider the genesis of NSF as the premier governmental research support vehicle for U.S. colleges and universities. President Franklin D. Roosevelt's science advisor Vannevar Bush is often credited with launching and shepherding the key ideas and efforts, responsible for the founding of the National Science Foundation. In familiar tales, U.S. Senator Harley Kilgore is often characterized as Bush's nemesis, holding up NSF related legislation in the Senate. While it is true that Bush and Kilgore were not on the same page with respect to the proposals to create the NSF, Kilgore had some very legitimate concerns regarding the creation of the NSF, as Bush had proposed it, and vice-a-versa. It must be noted that Kilgore, independent of Bush, had been thinking about the need for a government mechanism, similar to an NSF, that would not only advantage the nation from WW-II production efforts, but would see to it that technological innovations that resulted from production efforts could be quickly brought to the benefit of the nation [83]. Principally, Bush agreed with Kilgore on matters regarding national needs, acknowledging, "Without scientific progress no amount of achievement in other directions can insure our health, prosperity, and security as a nation in the modern world." In addition, Bush professed that it was incumbent upon "a stream of new scientific knowledge to turn the wheels of private and public enterprise" for the United States [84].

The point of interest here is that various details regarding the founding of the NSF may be mired in *false information*. The very reasons behind NSF's founding, and the form of its

²¹This article is not intended to be an expose' of Congressional disconnects with national priorities. A literature search will undoubtedly reveal numerous examples of the history of serious policy disconnects in multiple areas.

present-day existence, cannot be suitably understood if one is not habituated to the thoughts and actions of both Kilgore and Bush, among others. It would also be quite inappropriate to consider Vannevar Bush as the sole originator of vital ideas, in terms of the NSF's inception.

On Drinking From Poisoned Chalice. . . : "It is from investment in basic science . . . that the most valuable long-run dividends are realized. The government has a critical role to play in this regard," [85] so stated the Hart-Rudman Commission. Yet, fundamentally, there is little understanding among involved parties at U.S. government institutions supporting the furtherance of science, on the definition and the nature of *basic science* research; and that is severely impeding the future prospects for U.S. Science innovation and leadership. The relationship between *basic research*, national strategic investment as a whole, and aspects which are impeding United States progress in science, the capability to innovate, and to broaden the sphere of human knowledge, is **very highly nuanced; so much so that nearly all today have missed it.**

The Hart-Rudman Commission has also acknowledged, "Americans are living off the economic and security benefits of the last three generations' investment in science and education, but we are now consuming capital. Our systems of basic scientific research and education are in serious crisis" [85]. However, contradictorily, a report prepared for the Office of the Secretary of Defense [86] by RAND suggests that the challenge that America is facing is perhaps not as grave as many believe. The RAND report further poses that the U.S. is not under-investing in 'basic research.' The most disconcerting element in the RAND report, as it relates to their assessment of U.S. *basic research* investment, is that it remains unclear to the reader just how RAND defined *basic research*, and how 'that' definition relates to their overall assessment of U.S. *basic research* investment value, and ultimate determinations [87].²² We believe that the RAND report is not on target, especially with regard to the view, and representation of basic research. We present, and emphasize that the meaning of *basic research* today is vastly misunderstood. Institutional and individual memories of what *basic research* actually means is the key issue here, where the lack of an aggregated understanding of its meaning within the science community, and an integration of that meaning into a nationally strategic planning framework, is unquestionably crucial. With respect to the evolution of an organization such as NSF, and its present day existence, none can prospectively distinguish how well such governmental instruments, once created to further the scientific capacities and

²²It will be of interest to note the following comment by the late Dr. Merle Tuve regarding this also. He said, "[r]egardless of the doubling and redoubling year by year of the announced annual expenditures by government and industry for basic research in science, we all feel a bit helpless and disappointed because these large sums seem to contribute so little to the really basic core of scholarly accomplishment which is central to all the varied degrees and qualities of activity we now seem to include under the term basic research." In addition, Tuve said the following of the scope of apparent 'busyness,' which is often displayed. Tuve said, "[h]uge new synchrotrons and cosmotrons and electronic computers, and polar expeditions and balloon and rocket flights and great government laboratories costing more each year than the total academic costs of many of our greatest universities—all these conspicuous aspects of our new national devotion to science are subsidiary and peripheral. They do not serve appreciably to produce or develop creative thinkers and productive investigators. At best they serve them, often in a brief or a rather incidental way, and at worst they devour them."

capabilities of a nation, are now functioning and serving as it was meant to be, unless certain background on their emergence were available. United States' capability to materialize innovation, and to enable scientific and technological progress, is now fast diminishing [88]. In terms of crafting helpful strategic science policies, and deciding upon where to make appropriate investment for America's future, we must never just assess if we are investing enough. Instead, we must also ask if we are investing properly. **At the very foundation of whether we are investing properly lies the question: do we understand what basic research support is to be?**

During the summer of 1959, the National Academy of Sciences, the American Association for the Advancement of Science, and the Alfred P. Sloan Foundation sponsored a meeting titled, 'Symposium on Basic Research' in New York to detail the nature, and the various aspects of '*basic research.*' [89] The men who attended the symposium were the Roman equivalent of the *Decemviri*,²³ although they numbered more than 10, and were not given any powers to enact laws. While these men were not aristocrats themselves, they were patricians, and represented the *cream-of-crop* in American science, scientific philanthropy, and astute métiers of national scientific policy. At that meeting, many valuable and indelible points became known, which were to have served as guideposts to formulating U.S. national strategic policy directions, and scientific investments for the future. Yet, even after those worthy debates and their documentation, since 1959 the need to understand and to fervently support 'basic research' for the long-term success of U.S. scientific foundations is vastly mis-understood by organizations such as the NSF, DARPA, DHS, IARPA, and others. Some of this deficiency is evident in the manner U.S. research and development directions are considered, structured, funded, manned, and operated [90].

Undeniably, the first order of business here is to distinct *basic research* from *applied research*. In his work, Dr. Mathews has described 'basic science research' fundamentally as the funding and the initiation of scientific inquiries to "Understand and lay elaborate, the many aspects of man's existence and the environment, his surroundings and the things within it; how things come to be, why they are in the manner they are, and what function they serve" [91].

To aid the reader's understanding of basic research, some of the key points raised at the 1959 'Symposium on Basic Research' are presented here, in the hopes that it will remind, and cajole the scientific enterprise and those within it to right itself. After all, as Carey was so mindful to be interrogative once, "[i]n an age of directed, mission-oriented research, an age of high stakes and space stations. . . who speaks now for. . . the nature of scientific progress?" [75]

On the subject of *basic research*, and on making scientific progress, Dr. Warren Weaver²⁴ opened the symposium, asking among other questions, the following. 1) "Are not universities so deeply invaded by the demands for solving immediate prob-

²³*Decemviri consulari imperio legibus scribundis* was a Roman board of sorts, composed of former Consuls (wise men), generally seated by election after a prolonged expression of societal disenchantment with existing rules/laws in order to deliberate, reconcile, represent foundational changes in aspect of law, and to thereafter codify and publish the revisions, or newer laws entirely.

²⁴Then Vice President of the Alfred P. Sloan Foundation.

lems, and by the temptation of income for so doing, that there are all too few cases of competent scholars pondering about problems simply because it interests them to do so? Is there not a real danger that the scholars in our universities will lose—and indeed have already partly lost—the “maneuvering room for their continuing reanalysis of the universe?” 2) “Has it been effectively accepted in our country that the spirit of basic research is an essential ingredient of the educational process—and that this fact should affect educational procedures at all levels?” And, 3) “Has either industry or government learned how to protect basic research from the insistent demands of applied research and development?” [89] Weaver’s prescient questions have held like a yoke around the American Scientific enterprise’s (public and private) neck for half a century, painfully ‘dragging out’ the struggle by committed members of the scientific community to enlist national leadership’s interest in pursuing, and advancing the envelope of scientific knowledge in the strategic interest of the United States.

Also at the symposium, Dr. J. Robert Oppenheimer urged all to recognize that “great intellectual developments [by way of *basis research*], whether they will in time lead to practical application or not, are continuous with, and contiguous to, parts of science which have played an enormous part in practice” [89]. Perhaps more than anyone else at that symposium, Dr. Merle Tuve of the Carnegie Institution summed up the fundamentals of how we ought to view, and approach, *basic research*, which is to be supported by public investment. He identified *basic research support* as the financing of the ideas of the one “individual man, who has ideas.” Crediting Andrew Carnegie, Tuve emphasized that “buying a man’s time and giving it back to him, as a support for his ideas and his thinking. . . the support of thinking, in the search of new knowledge. . . which can enlarge our understanding, knowledge, which is not isolated facts but related to guiding hypotheses or principles” [93] *was not any national option, but an absolute necessity.*

Also in his talk, Tuve became indictive of the quagmire that politicians, scientists, and scientific establishments were complicit in creating, twisting the original intent and meaning behind the public support principle for *basic research*. Tuve agitatedly said further, “‘I wish it could be possible to make really honest men out of us in these discussions, so honest that we would all quit stretching the meaning of the words “basic research” to cover huge areas of essentially technological activity for which huge amounts of taxpayers’ money can be obtained.’ . . . So I’d like to point out, at least for today, that we have all contributed to a more or less purposeful confusion in our uses of the words “basic research.” A great deal of the money listed as spent for basic research is spent for highly peripheral activities and operations, and too small a fraction actually goes for the subsidy of thinking, to give selected competent individuals both the freedom and the time to think. . . the subsidy of ideas, not the operations aspect of technological performances, however spectacular. . .” [75].

On Antidotes. . .: Equally of weight is how policy-makers themselves purvey false information. The public wrecking of Dr. John Marburger, III, is a fine example of how, a reputed scientist’s spirit can be re-worked by the political instruments of the day in Washington, to spew *false information*, and to use the *kind of science that gives one the policy they want* [94],

in lieu of exercising one’s *free will* to halt the White House’s science policy madness. Marburger, the past president of State University of New York at Stony Brook, was appointed as science advisor to the 43rd President of the United States. To this, the American science community applauded. Nevertheless, that applause quickly transitioned to a pin-drop silence, followed by the sprouting of vehemence, and its escalation to vitriol. At the time of Marburger’s appointment, the White House had in advance diminished the position to which he was being appointed. Among other things, the President’s point man on science was instructed to not report to the President as his predecessors, but instead, to the White House Chief-of-Staff. Marburger has often energetically denied this diminution, in despite of its authenticity [95]. At the very least, the circumstances relating to Marburger’s appointment as science advisor should have been seen as an urgent telegram from the White House to the science community, saying that the welcome-mat was being pulled in, and that science policy would be crafted without the participation of, or input from science. Public civility was sacrificed as never before, when the voice of Dr. Howard Gardner of Harvard, if for a moment, seemed to express the sentiments of an exceedingly disgusted scientific community, when it reverberated through the nation airwaves via the syndicated Diane Rehm radio program. There, Gardner exclaimed, “I actually feel very sorry for Marburger, because I think he probably is enough of a scientist to realize that he basically has become a prostitute.” [96] In the mind of much of science, Marburger had become an able-bodied tool for crack-pot political plotters. In retrospect, the Union of Concerned Scientists (UCS), whose public statement sums up the situation, best offers a glimpse of the political climate overflying the potential to organize highly beneficial science policy in Washington, D.C. UCS has said, “[p]olitical interference in federal government science is weakening our nation’s ability to respond to the complex challenges we face” and that “[t]he scope and scale of the manipulation, suppression and misrepresentation of science by the Bush administration [has been] unprecedented” [98]. For nearly a decade, highly corrosive U.S. national policy mechanisms had a cornucopia full of opportunities at their disposal to retard thoughtful propagation of reason, and to surcease national progress, in favor of advancing a few national administration themes. Such is the type of poison for which the scientific community must now quickly deploy an antidote.

Possessing unobstructed issue perspectives, and the inimitable understanding of our achievements, are clearly important pre-requisites in national science policy, and resource planning. Len Peters, former Director of Pacific Northwest National Laboratory, and Senior-Vice President of Battelle, have been quoted saying “If we want to steer the Titanic of American competitiveness out of danger, we also need to address the deeper, less-obvious issues underneath, and we all have a part to play” [99]. Dr. Peters’ statement on U.S. competitiveness is relevant here for two reasons, 1) in so far as U.S. science and technology is foundationally the enabling competition engine, *basic research* represents the essential seed to fruits, and 2) because Dr. Peter’s quote is problematic, and it is illustrative of the type of problem disconnects showcased throughout this article. With many apologies to Dr. Peters in advance, we note that, while it might not have been Dr. Peter’s intention to equate

American competitiveness to the Titanic, establish any direct connection, or even any distant relationship between the two matters, we believe the proximal placement of the two—more than murk issues. One fact is amply clear: the Titanic is forever lost; prospect for U.S. competitiveness however, is not lost, which may very well have been the point Dr. Peters was intending to make. However, that which we know today tells us that the fate of the Titanic was perhaps etched in stone. From the loss of sensibilities in leadership at the helm, and in rank duty, to the usage of sub-standard materials and engineering of the vessel, cumulatively lead to more than a human tragedy during the early morning hours of 15 April 1912 [100]. To make a point explicit regarding Dr. Peters' suggestion that the Titanic could have possibly been steered away from harm, and similarly, U.S. competitiveness too can possibly be steered away from irreversible decline, is a meaningless and untenable statement, according to Dr. Mathews. To clarify, Mathews recalls David Brown's recently unearthed evidence, which strongly suggests Titanic ran aground on a submerged iceberg; one which none apparently even saw [100]. Likewise, Mathews says, "the way in which science can be made to contribute evocatively to long-term U.S. economic security may not be steerable at all, chiefly because those who formulate funding policy in support of vital science programs are by and large, not properly clued-up. However, this is a correctable situation, and for the good of the nation, it must be rectified." He adds, "Now, we say we are funding 'basic research,' when in fact we are not, and much worse, many have miscomprehended the meaning of 'basic research' more deeply."

With the beginning of a new national administration, who not unlike others, have promised our deliverance from intellectual inequity and mediocrity in nationally relevant leadership areas, the President, and his cabinet must ensure progress of science by improving the fidelity in the objectivity and validation data, to limit proliferation of false information, and refine our current knowledge base. To that extent, the following intelligence, a series of ineffaceable observations from Carey, will be worthwhile remembering. He has said, "[m]y view is that the public business today is in a state of exceptional fluidity, and because of this the public manager's first responsibility is to have an *open mind*, and his second is to *want passionately to understand the meanings—not the forms*—of his changing world. The hard and terrible truth is that we age and cling to axioms and Bible texts while the ground under us shakes and trembles." [101] With respect to the role of science in the assurance of our national security, Carey says, "if national security and strong national economy presume a first-class technology base, and if the conduct of foreign policy presumes that the United States will be a reliable partner in cooperative undertakings, the management of the science component of the policy system takes on a centrality that oncoming Presidencies cannot ignore." He forewarns though, "[i]n science policy, as elsewhere, homework counts" [102] signifying essentially that what we know, how we know it, and when we know it, are all important questions to answer while doing the necessary homework. Finally, Carey most importantly reminds, "we need to take our courage into our hands and make choices about major scientific or technological investments on the basis of their social contribution." [103]

We would be wise to take this advice to heart, and urgently act upon it.

E. Summary of Selected Technology Advances

Provided by Dennis Hoffman; IEEE Sr. Member, RS Sr. Past President, RS (Reliability Society) and AESS (Aerospace and Electronic Systems Society) Member, (d.hoffman@ieee.org)

1) *National Renewable Energy Laboratory (NREL)*: The National Renewable Energy Laboratory is an interesting place if you have an interest in renewable energy. The lab is located on the west side of Denver, Colorado, and if you are in the area it definitely is a place to visit. If you can't visit directly, then visit their web site at <http://www.nrel.gov/overview/>. The following is an overview from their web site.

"The National Renewable Energy Laboratory (NREL) is the nation's primary laboratory for renewable energy and energy efficiency research and development (R&D).

NREL's mission and strategy are focused on advancing the U.S. Department of Energy's and our nation's energy goals. The laboratory's scientists and researchers support critical market objectives to accelerate research from scientific innovations to market-viable alternative energy solutions. At the core of this strategic direction are NREL's research and technology development areas. These areas span from understanding renewable resources for energy, to the conversion of these resources to renewable electricity and fuels, and ultimately to the use of renewable electricity and fuels in homes, commercial buildings, and vehicles. The laboratory thereby directly contributes to our nation's goal for finding new renewable ways to power our homes, businesses, and cars.

R&D expertise: NREL's focused R&D capabilities are positioned to advance national energy goals by developing innovations to change the way we power our homes and businesses, and fuel our cars. Our R&D capabilities allow us to develop and advance renewable energy and energy efficiency technologies more effectively through the full R&D life-cycle—from basic scientific research through applied research and engineering; to testing, scale-up, and demonstration. NREL's R&D areas of expertise are:

- Renewable electricity
- Renewable fuels
- Integrated energy system engineering and testing
- Strategic energy analysis

Technology transfer: A critical part of the Lab's mission is the transfer of NREL-developed technologies to renewable energy markets. NREL's Technology Transfer Office supports laboratory scientists and engineers in the successful and practical application of their expertise and the technologies they develop. NREL's world-class R&D staff and facilities are recognized and valued by industry, as demonstrated through hundreds of collaborative research projects and licensed technologies with public and private partners. NREL's innovative technologies have also been recognized with 42 R&D 100 awards. The engineering and science behind these technology transfer successes and awards demonstrates NREL's commitment to developing and applying innovative renewable energy solutions for the nation's secure and sustainable energy future."

2) *Compressed Air Driven Cars*: Compressed air vehicles are being developed around the world. Below are a few articles to provide some insight on these vehicle developments.

What's up with compressed air-powered vehicles?: <http://www.theautochannel.com/news/2008/11/24/260043.html>

"Recently, we were asked 'What companies make Air Powered Cars?' Given all the noise that surfaced about 10 months ago concerning the state of this amazing technology we thought an update was needed.

There are at least three companies working on producing compressed air-powered vehicles. The most well-known is MDI, based in France. MDI is headed up by Guy Negre (www.mdi.lu). It is MDI's company that has, or had, an agreement with Tata Motors (India) to bring an air car to market. MDI (with an American affiliate) exhibited a working prototype of the car at last Spring's NY Auto Show, where it won an award for innovation. When Guy Negre originally made his deal with Tata Motors it was said that the vehicle would be ready for distribution in some global markets by 4th quarter of this year (2008). So far there's no sign of it, and the status of his relationship with Tata is unknown.

For several years, Guy Negre had an associate in Spain, Miguel Celades Rex, but a business dispute ended their relationship. Miquel now runs Air Car Factories in Barcelona. (www.aircarfactories.com).

At the beginning of 2008 Air Car Factories also announced that they would have a compressed air vehicle ready for the public at the end of the year. We had planned to visit the company two months ago, in September, to test drive the vehicle, but we were informed that the vehicle was still just in design and that there were no working test cars.

Angelo Di Pietro in Melbourne, Australia (www.engineair.com.au) has developed an air-powered rotary engine that he has put to work on small utility vehicles.

Di Pietro had been a Wankel rotary engine mechanic in Stuttgart, prior to emigrating to Australia in 1971; hence his familiarity with rotary engines.

While none of these innovators are really ready for prime-time, the concept and the technology appears to be more than just vapor-ware. Unfortunately, there's a lot more to bringing a new engine to market than just proving it works, you also have to have a manufacturing and distribution relationship with carmakers that are really interested in making it happen, and who aren't concerned that the new technology will make your other technology too obsolete or irrelevant."

Rotary engine: Engineair's Ultra-Efficient Rotary Compressed-Air Motor, "Elegant minimalist design eliminates most of the working parts traditionally associated with internal combustion engine; offers nearly 100% energy efficiency for a variety of transport and stationary applications by Mary-Sue Haliburton, Pure Energy Systems News, Copyright 2006"

"Imagine a vehicle with nothing under the hood (or bonnet), no gearbox, no transmission, no carburetor or other fuel feeds. Yet it converts virtually all the energy fed to its motors into actual motion. With the elegance of absolute simplicity, this concept makes traditional internal-combustion cars look like the Rube-Goldberg contraptions they are: using way too many parts and stages to do what is really a simple task.

All we have to do is to get wheels to turn, preferably with as little wasted motion and energy as possible.

By comparison, the traditional car's engine uses up to about 65% of the energy potentially available from the fuel, just to move all its parts such as pistons and cams, plus what is wasted generating excess heat. Then the transmission uses 6%, the accessory load 2% and idling losses come to about 11%, leaving about 16% of the energy actually engaged in making the wheels turn. Because of the weight of all these structures, the engine block, crankshaft, gears, transmission, etc., that 16% of the energy is having to move a vehicle weighing perhaps a ton and a half—which may have only one person sitting in it, weighing only 150 lb.

There is a lot wrong with that 100-year-old picture. It should be laughed off the road as unsuitable for the 21st century.

In Melbourne, Australia, an Italian-born mechanical engineer named Angelo Di Pietro has been experimenting for many years to find a more efficient design than the traditional reciprocating combustion engine. Inspired by his earlier work on Wankel rotary engines at Mercedes Benz in Germany, he pursued the notion of a rotary engine with fewer parts. Since his 1999 breakthrough, Di Pietro has been testing and perfecting his unique design which also eliminates traditional pistons and their housings. Though it weighs only 13 kilograms (28.6 lb), this rotary air motor is capable of powering a car without creating any pollution."

The following article, **Zero Pollution compressed Air Car set for U.S. launch in 2010**, is from gizmag Automotive, February 29, 2008:

"The Zero-Pollution MDI Air Car, invented in France and licensed by Tata Motors in India, is coming to American shores. Zero Pollution Motors have announced they will begin taking reservations for the first U.S. deliveries in the next couple of months, but it will be 2010 before Americans get their first taste of the ingenious compressed-air motor, which runs to 35 mph entirely on air, or uses a trickle of petrol to heat and compress more air to reach higher speeds up to 90 mph. It'll cost next to nothing to run (how do 30,000 km service intervals sound?), have a range of up to 1000 miles, and retail for well under US\$20,000."

This article provides some overview information and pictures associated with the Indian air car: AIR CAR-FROM INDIA (http://www.housejeanie.com/air_car.htm).

"This is the same company who, a few months back, came out with a car that costs only \$2,500.00 new (but it's not available in the US, why does that not surprise me?).

A non polluting vehicle that eliminates the reason to buy gasoline from off shore companies. How bad is that?

Amazing Air Car!: The Compressed Air Car developed by Motor Development International (MDI) Founder Guy Negre might be the best thing to have happened to the motor engine in years.

The \$12,700 CityCAT, one of the planned Air Car models, can hit 68 mph and has a range of 125 miles. It will take only a few minutes for the CityCAT to refuel at gas stations equipped with custom air compressor units. MDI says it should cost only around \$2 to fill the car up with 340 liters of air!

The Air Car will be starting production relatively soon, thanks to India's TATA Motors. Forget corn! There's fuel, there's re-



Fig. 4.

newable fuel, and then there's user-renewable fuel! What can be better than air?

Check it out yourself and see—What A Cool Car! Enjoy! “

3) *Hybrid Electric Vehicle*: Hybrid electric cars are also making headway, and China's BYD (Build Your Dream) corporation is trying to bring their hybrid technology vehicles to the West. The following is an article, supplemented by a couple of BYD charts, that provides some information about their vehicle. Their hybrid vehicle greatly reduces the CO₂ emissions as compared to petroleum fueled vehicles.

China's BYD Unveils Second Plug-in Hybrid Model at Geneva Motor Show; Plans to Begin Sales in Europe in 2–3 Years, <http://www.greencarcongress.com/2008/03/chinas-byd-unve.html>.

5 March 2008: “China's BYD Co Ltd., which introduced its plug-in hybrid electric vehicle technology at the North American International Auto Show in January (earlier post) in the form of the F6DM (Dual Mode, for EV and HEV), has introduced another, smaller model using its hybrid powertrain at the Geneva Motor Show: the F3DM (Fig. 4).

The F6DM shown in Detroit, a variant of the front-wheel drive F6 sedan that BYD introduced into the China market earlier this year, offers three modes of operation: full battery-powered EV mode driving its 75 kW, 400 Nm motor; series-hybrid mode, in which a 50 kW, 1.0-liter engine drives a generator as a range-extender; and parallel hybrid mode, in which the engine and motor both provide propulsive power.


Wang Chaufu, BYD's Chairman, said that the company planned to introduce a dual-mode sedan in Europe as early as in 2010.

“*Battery technology is our core competency, and we think we are well-placed against GM and Toyota,*” he said, adding that BYD's dual-mode car could be driven 110 km on electricity before recharging (Fig. 5).

The F6DM shown in Detroit uses a 20 kWh lithium iron phosphate battery pack, based on BYD's own production cells (which the company calls its Fe cells). The pack, which runs down the center console, has a lifetime of 2,000 cycles. A 100% recharge with household 220 VAC takes approximately 9 hours. BYD says that the pack can achieve a 50% recharge in 10 minutes.

The company has said it will apply the DM technology across its product line (Fig. 6).

BYD recently celebrated the opening of its engine plant and a new R&D center in Shenzhen. The design and testing of the



BYD Dual Mode: F3DM

- ↪ **Range:**
 - EV: 60 miles or 100 Km per charge (90% efficiency)
 - HEV: 200 miles (@ ~40 mpg)
- ↪ **Battery Life:** 2000 cycles, 10 years
- ↪ **Electricity consumption:**
 - 16 kWh per 100km
- ↪ **Power:** 48Kw **0-60:** 10.5s
- Top Speed:** 100 mph
- ↪ **Quick charge:** 50% in 10 min
- ↪ **Overnight charge:** 110/220V outlet




Fig. 5.

core components of BYD's electric vehicle technology will be done in the new R&D center.”

4) *Buckypaper*: This new material is bringing international attention to its developers at Florida State University. The material looks like ordinary carbon paper, but it could revolutionize the way things are made.

The following article will provide some insight is to this remarkable material: **Stronger Than Steel, Harder Than Diamonds: Researcher Developing Numerous Uses For Extraordinary 'Buckypaper'**, <http://www.buckypaper.com/>

“Working with a material 10 times lighter than steel—but 250 times stronger—would be a dream come true for any engineer. If this material also had amazing properties that made it highly conductive of heat and electricity, it would start to sound like something out of a science fiction novel. Yet one Florida State University research group, the Florida Advanced Center for Composite Technologies (FAC2T), is working to develop real-world applications for just such a material.

Ben Wang, a professor of industrial engineering at the Florida A&M University-FSU College of Engineering in Tallahassee, Fla., serves as director of FAC2T (www.fac2t.eng.fsu.edu), which works to develop new, high-performance composite materials, as well as technologies for producing them.

Wang is widely acknowledged as a pioneer in the growing field of nano-materials science. His main area of research, involving an extraordinary material known as “buckypaper,” has shown promise in a variety of applications, including the development of aerospace structures, the production of more-effective body armor and armored vehicles, and the construction of next-generation computer displays. The U.S. military has shown a keen interest in the military applications of Wang's research; in fact, the Army Research Lab recently awarded FAC2T a \$2.5-million grant, while the Air Force Office of Scientific Research awarded \$1.2 million.

‘At FAC2T, our objective is to push the envelope to find out just how strong of a composite material we can make using buckypaper,’ Wang said. ‘In addition, we're focused on developing processes that will allow it to be mass-produced cheaply.’

Buckypaper is made from carbon nanotubes—amazingly strong fibers about 1/50,000th the diameter of a human hair that

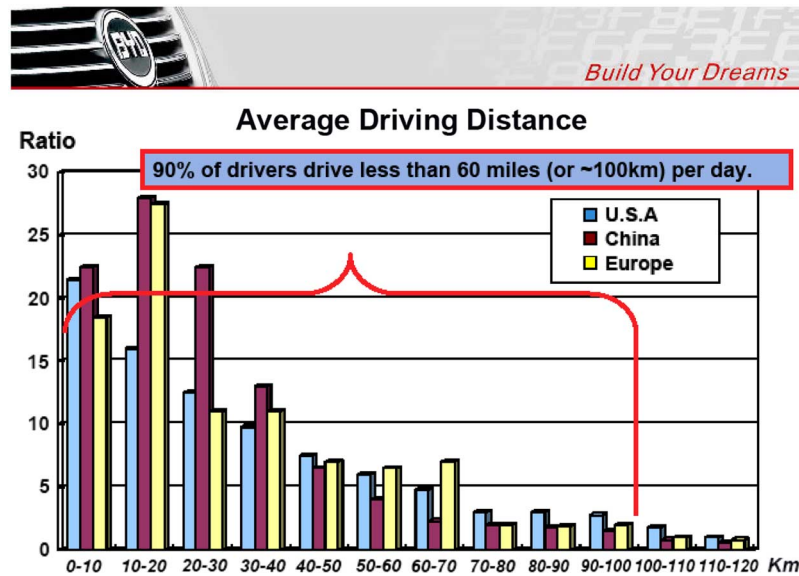


Fig. 6.

were first developed in the early 1990s. Buckypaper owes its name to Buckminsterfullerene, or Carbon 60—a type of carbon molecule whose powerful atomic bonds make it twice as hard as a diamond. Sir Harold Kroto, now a professor and scientist with FSU's department of chemistry and biochemistry, and two other scientists shared the 1996 Nobel Prize in Chemistry for their discovery of Buckminsterfullerene, nicknamed 'buckyballs' for the molecules' spherical shape. Their discovery has led to a revolution in the fields of chemistry and materials science—and directly contributed to the development of buckypaper.

Among the possible uses for buckypaper that are being researched at FAC2T:

- If exposed to an electric charge, buckypaper could be used to illuminate computer and television screens. It would be more energy-efficient, lighter, and would allow for a more uniform level of brightness than current cathode ray tube (CRT) and liquid crystal display (LCD) technology.
- As one of the most thermally conductive materials known, buckypaper lends itself to the development of heat sinks that would allow computers and other electronic equipment to disperse heat more efficiently than is currently possible. This, in turn, could lead to even greater advances in electronic miniaturization.
- Because it has an unusually high current-carrying capacity, a film made from buckypaper could be applied to the exteriors of airplanes. Lightning strikes then would flow around the plane and dissipate without causing damage.
- Films also could protect electronic circuits and devices within airplanes from electromagnetic interference, which can damage equipment and alter settings. Similarly, such films could allow military aircraft to shield their electromagnetic 'signatures,' which can be detected via radar.

FAC2T 'is at the very forefront of a technological revolution that will dramatically change the way items all around us are produced,' said Kirby Kemper, FSU's vice president for Research. 'The group of faculty, staff, students and post-docs in this center have been visionary in their ability to recognize the

tremendous potential of nanotechnology. The potential applications are mind-boggling.'

FSU has four U.S. patents pending that are related to its buckypaper research.

In addition to his academic and scientific responsibilities, Wang recently was named FSU's assistant vice president for Research. In this role, he will help to advance research activities at the College of Engineering and throughout the university.

'I look forward to bringing researchers together to pursue rewarding research opportunities,' Wang said. 'We have very knowledgeable and talented faculty and students, and I will be working with them to help meet their full potential for advancement in their fields.'"

5) *Getting to Root Cause—Why the 5 Why's?:* Added for a little change in pace, but very usable.

Source: http://www.mindtools.com/pages/article/newTMC_5W.htm

"The 5 Whys is a simple problem-solving technique that helps users to get to the root of the problem quickly. Because it is so elementary in nature, it can be adapted quickly and applied to most any problem. The strategy involves asking: 'Why?' and 'What caused this problem?' multiple times (can be more or less than five) until reaching the true root cause.

Here is an example of the **5 Whys in action:**

The Jefferson Monument was disintegrating.

Why? Use of harsh chemicals

Why? To clean bird mess

Why so many birds? The birds eat the spiders around the monument

Why so many spiders? The spiders eat the gnats around the monument

Why so many gnats? They are attracted to the light at dusk

Solution Turn on the lights at a later time

As you can see, many times the solution to a problem doesn't require a great deal of resources. Try out the 5 Whys the next time you need to solve a problem!"

F. The Challenges of System Health Management for Failure Diagnostics & Prognostics

Provided by Enrico Zio (enrico.zio@polimi.it)

In Medicine, a clinical picture for diagnosis & prognosis purposes can be made based on the values of some measured parameters related to the health condition of a human being. Similarly, in equipment operation & maintenance, it is possible to have an idea about the functional condition of equipment from the observation of the evolution of indicative parameters.

Under a program of system health management, the condition of equipment is monitored to identify the level of degradation. A decision is then taken of replacement or maintenance, based upon an analysis of the monitored data. In this view, maintenance is carried out when a measurable equipment condition shows the need for repair or replacement. This strategy allows identifying problems in equipment at the early stage so that necessary downtime can be scheduled for the most convenient and inexpensive time. The approach let a machine run as long as it is healthy (equipment is only repaired or replaced when needed), as opposed to routine disassembly triggered on a schedule. Maximum availability can thus be achieved by minimizing unscheduled shutdowns of production and scheduling maintenance actions as economically as possible.

Usually, the equipment condition is monitored at a regular interval. Once the reading of the monitored signal exceeds a threshold, a warning is triggered and maintenance or replacement actions are scheduled. Obviously, the monitoring interval influences the operating cost, and overall performance of the plant. A shorter interval may increase the cost of monitoring, whereas a longer one increases the risk of failure.

On the other hand, condition monitoring should be reliable to avoid false alarms. A decision must be made every time an alarm is indicated. To ignore an alarm may give rise to serious consequences. A first option is to make further investigation of the cause of alarm, without stopping the equipment; a second option is to stop the equipment for an overhaul of the suspected part. In the first option, a false alarm would result in extra cost due to the time and manpower necessary to make the diagnosis. The second option could result in greater losses, where lost production and manpower costs occur simultaneously. The greatest losses will occur when ignoring the alarm.

Condition-based maintenance implies that maintenance activities be scheduled in a dynamic way, because the execution times of certain activities will be continually updated as condition information becomes available. Such scheduling is significantly more difficult than scheduling the static policies implied by routine preventive maintenance. Indeed, the dynamic scheduling of condition-based maintenance represents a challenging task which requires the integrated simulation of the equipment state transitions, and the prediction of the monitored physical variables which represent the equipment evolving condition. Hence, it is important to develop reliable models of equipment degradation, for its estimation and prediction. Given the complexity of the processes underlying mechanical and structural degradation, and the ambiguous, uncertain character of the experimental data available, one may have to resort to empirical models based on collected evidence, some of which may very well be of a qualitative, linguistic nature. In this

direction, soft computing techniques (e.g. neural networks, and fuzzy logic systems) represent powerful tools because of their capability of representing highly non-linear relations, learning from data, and handling qualitative information [104]. Embedding these models within the simulation of the stochastic processes governing the equipment life could represent a significant step forward for the evaluation of the safety & reliability of equipment under condition-based maintenance regime.

From the practical point of view, it is important to note that condition monitoring will be efficient only if the information retrieved from the monitored equipment is relevant, and it is filed, processed, and used in a timely manner, so that the decisions can have effectiveness, and result in an increase of productivity [105]. The capability of acquisition and handling of system and process information in real time is therefore a necessary condition for performing on condition maintenance.

Within a condition monitoring strategy, failure prognosis is becoming attractive in Reliability, Availability, Maintainability, and Safety applications. The primary purpose of a prognostic system is to indicate whether the equipment of interest can perform its function throughout its lifetime with reasonable assurance; and in case it cannot, to estimate its Time To Failure (TTF), i.e. the lifetime remaining before it can no longer perform its function. The prediction is more effective if informed by measurements of parameters representative of the state of the equipment during its life.

The attractiveness of prognostics comes from the fact that, by predicting the evolution of the equipment dynamic state, it is possible to provide advanced warning for preparing the necessary corrective actions to maintain the equipment in safe, productive operation.

However, in reality, often the dynamic states cannot be directly observed; on the other hand, measurements of parameters or variables related to the equipment states are available, albeit usually affected by noise and disturbances. Then, the problem becomes that of inferring the equipment state from the measured parameters. Two general approaches exist: i) the model-based techniques, which make use of a quantitative analytical model of the equipment behavior θ ; and ii) the knowledge-based or model-free methods, which rely on empirical models built on available data of the equipment behavior θ , θ .

The soundest model-based approaches to the estimation of the state of a dynamic equipment build a posterior distribution of the unknown states by combining the distribution assigned a priori with the likelihood of the observations of the measurements actually collected θ , θ . In this Bayesian setting, the estimation method most frequently used in practice is the Kalman filter, which is optimal for linear state space models, and independent, additive Gaussian noises. In this case, the posterior distributions are also Gaussian, and can be computed exactly, without approximations.

Yet, in practice, the dynamic evolution of real equipment is non-linear, and the associated noises are non-Gaussian. Moreover, the state estimation task becomes quite challenging for equipment with a hybrid dynamic behavior characterized by continuous states, and discrete modes evolving simultaneously. Sudden transitions of the discrete modes, often autonomously triggered by the continuous dynamics, affect the equipment evolution, and may lead to non-linear behaviors difficult to

predict. The problem of state estimation becomes quite complex for such hybrid equipment, due to the large computational efforts needed to keep track of the multiple models of the equipment discrete modes of evolution, and the autonomous transitions between them. In these cases, approximate methods, e.g. analytical approximations of extended Kalman (EKF) and Gaussian-sum filters, and numerical approximations of the grid-based filters [111], can be used, usually at large computational expenses. Alternatively, one may resort to Monte Carlo sampling methods, also known as particle filtering methods, which are capable of approximating the continuous and discrete distributions of interest by a discrete set of weighed ‘particles’ representing random trajectories of equipment evolution in the state space, and whose weights are estimates of the probabilities of the trajectories. As the number of samples becomes large, the Monte Carlo approximation yields a posterior pdf representation which is equivalent to its functional description, and the particle filter approaches the optimal Bayesian TTF prediction.

The predictive task underpinning equipment failure prognosis must give due account to the uncertainty associated to the future behavior of the equipment under analysis, for the prognostic results to have operational significance, e.g. in terms of maintenance and replacement decisions. Sources of uncertainty derive from: i) randomness due to inherent variability in the equipment degradation behavior (aleatory uncertainty), and ii) imprecision due to incomplete knowledge and information on the parameters used to model the degradation and failure processes (epistemic uncertainty). While it is commonly accepted that the aleatory uncertainty is appropriately represented by probability distributions, current scientific discussions dispute the potential limitations associated with a probabilistic representation of epistemic uncertainty under limited information. In this respect, a number of alternative representation frameworks have emerged, e.g. fuzzy set theory, evidence theory, possibility theory, interval analysis, and imprecise probability.

In conclusion, system health management for failure diagnostics & prognostics have arisen to being an engineering discipline focused on detection, prediction, and management of the health and status of complex engineered equipment. The practical and research interest is quite significant in diverse application areas such as aerospace, transportation, automotive, energy, and industrial automation, as witnessed by the success of PHM08 (Denver, 6–9, 2008), the first international forum dedicated to this emerging discipline.

G. Delivering Reliability in the Healthcare System

Provided by Dev Raheja (Draheja@aol.com), (raheja@PatientSystemSafety.com), Chair, IEEE Design for Reliability Committee

Introduction: The alarming truth for patients in US hospitals is that their likelihood of dying highly correlates with their choice of hospital. This fact is cause for hospitals to continuously evaluate best practices to eliminate preventable deaths. Hospital mortality rates can be systematically reduced through reliable implementation of proven interventions. This is a statement [112] from the Institute for Health Improvement (IHI), a not-for-profit organization, widely recognized in healthcare. This organization has taken the initiative to apply industry methods of system reliability to healthcare systems.

IHI defines Reliability as failure-free performance over time [113]. The aim is to have no failures over extended periods of time in spite of variability in patient environment. This aim is in line with the technical definition of reliability as the probability of successful performance of intended functions for a specified length of time under a specified user (patient) environment. In a system where the severity of consequence is high, such as in hospitals, the goal is to achieve reliability as close to 100% as possible. This is called failure-free performance. Some hospitals have achieved this goal for specific medical procedures for several quarters. Can they extend this performance over years instead of quarters? That depends on many factors such as management culture, changes in the process, and teamwork.

The failures of the U.S. healthcare system are enormously important considering their severity. As much as 100,000 patients die each year from hospital mistakes. In addition, about 2.1 million patients are harmed from infections during hospital stay. The cost is in the billions of dollars (USD). My personal discussions with doctors show that there is reluctance to apply reliability principles to healthcare systems because the variability in healthcare is enormous compared to aviation, and other industrial fields. Each customer (patient) is different, and each illness is unique in its own way. Then there are interconnecting systems, such as cardiology, gynecology, gastroenterology, emergency medicine, oncology, and patient data from various doctors, pagers, computers, vendor software, and intensive care, which operate independently most of the time.

In healthcare, each critical process can have its own reliability goal. For example, if a protocol requires that a patient coming to the ED (emergency department) must get attention within ten minutes of arrival, then the performance can be defined as ‘patient must be registered with the triage nurse within 10 minutes.’ A failure can be defined as ‘patient waiting longer than 10 minutes.’ A woman in a New York hospital died while waiting for an hour in the emergency department. Her blood clot in the leg traveled all the way to her brain. In another New York hospital, a woman waited about 24 hours before collapsing on the floor.²⁵

The time dimension for reliability can be defined in terms of calendar time every three months (quarterly), or every 1000 patients. Then the reliability can be measured as a percentage of patients receiving service within 10 minutes during the quarter, or per 1000 patients. IHI is taking a similar approach for patients needing anti-biotic within an hour after surgical incision. In this case, reliability is measured as the ratio of the number of patients receiving the antibiotic within an hour, and the number of patients requiring this treatment.

This paper identifies reliability principles we can apply to healthcare based on my experience of over 25 years as a consultant to the aviation and medical device industry. More comprehensive knowledge can be found in [112]–[115].

System Reliability Theory: Before we define system reliability, we need to define a medical system. It is a composite, at any level of complexity, of medical equipment, caregivers, medical procedures, lab work, environment, communications, and patients with a specified system mission. Medical equipment may include CRT, MRI, ventilators, artificial heart, and dialysis machines. People include physicians, residents, interns,

²⁵All 24 hours were recorded on the hospital video.

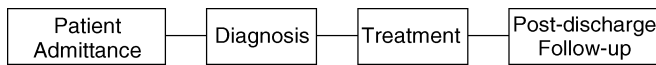


Fig. 7. The chain shows that if any subsystem fails, then the mission fails.

attendants, nursing staff, medical technicians, support associates, administrative personnel, patients, and visitors. Medical procedures include diagnosis, surgery, intensive care, intermediate care, lab procedures, intubations, intra-venous fluid infusions, patient visits, admittance, discharge, emergency patient processing, and trauma support. Communications include patient handoffs, verbal communications, and communication among pharmacists, doctors, nurses, residents, patients, pagers, telephones, and computer screens.

The mission obviously is to have a safe, positive, successful experience for patients. Therefore, system reliability is the function of the integrated performance of all these. This model is illustrated in Fig. 7, and is called a series system. If any block in the system fails, then the whole mission fails.

We can write the reliability model as follows, where System Reliability is denoted as R_s , R_a is the reliability of Patient Admittance, R_d is the reliability of Diagnosis, R_t is the reliability of Treatment, and R_p is the reliability of Post-discharge follow-up. Numerically, the system reliability is the product of subsystem reliabilities of R_a , R_d , R_t , and R_p :

$$R_s = R_a \times R_d \times R_t \times R_p$$

A hospital may modify the model if this model is not comprehensive. This model assumes that each of these four processes is statistically independent of each other, and each task must be performed correctly. If not, the laws of conditional probability apply. Reference [114] explains how to calculate conditional probability.

To my knowledge, no hospital is measuring reliability at a system level. Most of them are applying the concepts to a component of a system, at most. The IHI is applying reliability measurements to components such as diagnoses, community acquired pneumonia, heart failure, acute myocardial infarction, hip/knee replacements, and bypass graft surgery. The reliability for each is simply the ratio of patients receiving the right care to the number of patients requiring the care. It may be noted that the system reliability model can be applied at a component level also, as long as the components are functions of equipment, people, procedures, environments, and communications. The mission is still the same, a safe, positive, and successful patient experience.

How to Design the System for Reliability?: Reliability begins with the design. The design is constantly improved through verifications, and validations. At a minimum, the following design process is followed.

- 1) Assess the current reliability using the above model, and past data.
- 2) Identify weak links, and allocate higher reliability goals to them.
- 3) Perform Healthcare FMEA (Failure Mode and Effects Analysis) on weak links to predict potential failures of healthcare, and determine strategies to achieve the desired reliability goals. Use Fault Tree Analysis when the causes of failure in the FMEA are too complex.

- 4) Redesign the healthcare system using reliability improvement techniques.
- 5) Verify that the work done on the FMEA, and the design improvements, was done using divergent brainstorming, and convergent solutions.
- 6) Understand the “bath tub” shape of the failure rate behavior over time, and take proactive actions to minimize failures.
- 7) Validate that the new design is achieving the reliability goals.

A brief description of each is in order. Hospitals should adopt what fits into their culture, and should use innovation as much as possible. Continuous improvement is often insufficient because teams tend to make marginal improvements that yield very low return on investment.

Assessing the Current System Reliability: Whether one is dealing at system level or component level, the expected reliability (percent patients receiving the treatment as intended) needs to be established from the current data.

Because reliability is a measure of the proportion of successes, we must define what a failure is. If a physician fails to sanitize hands before touching a patient, is it a failure? Also, no one generally documents such failures. In aviation, there are four categories of failures measured by the amount of harm which is documented: category I for deaths; category II for major harm such as amputation of the wrong body organ; category III for minor harm such as a patient falling out of bed, but recovering from pain within a day; and category IV for negligible harm such as a diabetic patient given a glass of grape juice with the breakfast, and then given high dose of insulin to lower his blood sugar. Hospitals should decide which categories constitute a failure before assessing reliability.

If the data are not documented, an estimate can be made by a cross-functional team, to be verified as data accumulates. This process of estimating reliability is called reliability prediction. The purpose of this step is to see if the expected performance is acceptable. If not, then there is a need to redesign the process for higher reliability.

Identifying Weak Links: In healthcare, reliability depends on a sequential chain of tasks done correctly. If any link in the chain fails, the whole performance fails. The weak link theory says that the chain is only as strong as the weakest link. Each critical task must be performed as intended. Any of these tasks done incorrectly can result in a patient mishap. Knowing the weakest link sets priority for reliability planning. We have to strengthen the weak links first. In the system level chain at the beginning of this paper, there are four links in the chain: the patient admittance process, the diagnosis process, the treatment process, and the post-discharge care. If the treatment process has the lowest reliability number, we need to fix this process first. The reliability of the entire chain cannot be higher than this number, no matter how much improvement we make on other links. A fraction multiplied by another fraction cannot be higher than the lowest fraction. This does not say that we must work on weakest link only, but the priority should be fixing the weakest, then fixing the next weakest, and all the way to other links, until the reliability goals are achieved.

Performing Healthcare FMEA: The purpose of FMEA is to identify all the possible things can go wrong by having a divergent brainstorming. The composition of the team is very impor-

tant. At a minimum, there should be a doctor associated with the procedure, nurses, a person from the patient safety office, and a quality assurance representative.

The team constructs a process flow chart of work, and documents the following in a standard FMEA table.

- What is the description of each step in the process?
- What can go wrong in each step (failure mode)?
- Why would it go wrong (cause)?
- What are the consequences (effects)?
- How frequently is this event likely (occurrence)?
- If anything is going wrong, how early is it going to be detected (detection)?
- How severe can the harm be (severity)?
- How would you mitigate harm (action)?

Reference [113] shows the portion of the FMEA conducted at the East Alabama Medical Center.

There will be hundreds of potential things going wrong. It is a time consuming process. It can take one to three days, but the return on investment is very high. Most hospitals do this in blocks of a few hours at a time. If we prevent 50 or so mishaps such as infections, wrong medications, or medication at the wrong time, the savings can be in millions. As an example, Dr. Peter Pronovost introduced a simple checklist to decrease catheter-related bloodstream infections in the surgical intensive care unit at Johns Hopkins Hospital. That process brought down the infection rate to zero most of the time. When 103 ICU in Michigan started to use this mitigation strategy, the infection rate went down from 7.7 per 1000 catheter-days to 1.4 over a 16 to 18 month follow-up period. This is a very significant improvement in reliability, resulting in millions in savings. The cost of implementing the checklist is practically nothing.

In the aviation system, only occurrence (frequency), and severity are estimated to assess the risk. In industrial systems such as the one used by East Alabama Medical Center, the occurrence, detection, and severity are estimated on a scale of 1 to 10. They are multiplied to calculate the relative risks. This multiplication is called the risk priority number (RPN). Reference [114] has such guidelines. As an example, the following is one of the many items in the East Alabama Medical Center FMEA.

Step in the process: Order medication

Failure Mode: Miscommunication about the dose

Causes: Illegible writing, calculation mistake or pharmacist has mental lapse

Effects: Potential for death

Occurrence: 2 (on a scale of 10)

Detection: 5 (scale of 1 to 10)

Severity: 10 (scale of 1 to 10)

RPN: 100

Mitigation Action: The report did not contain a list of actions

As mentioned earlier, fault trees are to be used when the causes are unknown, or not understood. Fault tree analysis was developed by Boeing on the Minuteman Missile Program to

avoid any mishap. It has been a standard practice for over 40 years in aviation, nuclear power, and many industries [114]. It systematically forces the team to think of all the possibilities of hidden hazards, errors, and unusual events. The users use the aviation guide for mitigation, in the following precedence order (I have tailored this list to application in the healthcare field).

- Change the design to avoid or eliminate hazards.
- Design for failsafe exit (if the procedure fails, then there should be no harm to the patient).
- Provide early warning (if the physician does not sanitize their hands before touching a patient, it is a warning of more things to go wrong).
- Provide special training with frequent validation.

Redesign the System Using Reliability Improvement Techniques: Here we present some useful reliability improvement techniques.

- **Fault Tolerance:** Mitigate the effect of error by providing redundancy such as the nurse checking the doctor's actions. You can add one more redundancy, which could be the head of the unit periodically confirming that the doctors welcome the reminder by the nurses, and provide rewards for good work.

Here are three reasonable choices:

- 1) only the physician is controlling the infection;
- 2) the physician is controlling, and the nurse is cross-checking (dual redundancy); and
- 3) the physician is controlling, the nurse is cross checking, and the medical director is validating periodically (triple redundancy).

If the reliability of each of the three persons performing right is 0.90, then the reliability is 0.90 for scenario 1, 0.99 for scenario 2, and 0.999 for scenario 3 [114].

- **Derating:** Put fewer loads than the capability. Allow some spare time for doctors and nurses, minimize interruptions, not assign to too many patients.
- **Minimize the number of components** (for example, minimize the number of steps in the checklists because fewer steps are sometimes easier to remember).
- **Perform root cause analysis** to eliminate as many root causes as possible.

Understand the Bath Tub Shape of the Failure Rate Behavior: This understanding is especially critical on any new procedure, or using a new medical device. The failure rate is very high in the beginning because of learning curve problems, and until training gets validated. During this time period, the failure rate decreases over time because the care providers are learning from mistakes, and latent hazards are being addressed.

The second behavior of constant failure rates over time is called the random failure region. You know that unexpected failures can occur, such as someone inadvertently disconnecting the power, or someone cannot find the replacement battery.

The third region is called the wear out region. Medical devices such as artificial heart valves, pacemakers, and defibrillators wear over time, and eventually they fail. People can wear out too in their attention to details when they use the same procedure for years, especially when no one is cross-checking. This period is called the region of increasing failure rate over time.

These regions occur sequentially, and the three together may look like a bathtub. Knowing this nature of failures, we need to have a mitigation strategy for each region.

Validating the Design for Reliability: After defining what constitutes a failure, the data collection effort needs to be planned to measure reliability (percent successes over time). One must review trends of failure rates. They tell that our mitigation actions are providing high value or not. If the progress is too slow or negative, we need to review if the FMEA was done correctly. Go back to the drawing board and redesign the process and procedures. We need not wait until there is a mishap!

H. Some Faults Are Worse Than Others: And How That Is Useful for Low-Cost Hardening

Provided by Ilia Polian, Albert-Ludwigs-University, Freiburg, Germany (polian@informatik.uni-freiburg.de).

Traditionally, a fault handling strategy is considered effective if it covers large classes of faults, e.g., all single faults. This conventional wisdom has recently been challenged by identifying sub-sets of faults which are acceptable at a system level. One example is a fault in an imaging microchip which does not result in a deterioration of the calculated image to the extent that a human viewer would notice the difference. In the context of micro- and nanoelectronic circuits, dropping the restrictive requirement that all faults be covered, enables cost-effective selective hardening solutions, where only parts of the circuit are equipped with fault protection mechanisms. In this way, eliminated is the need for traditional massive redundancy schemes such as triple-modular redundancy, which are associated with massive area and energy consumption overheads. Handling most critical faults could be associated with overheads as low as 10%, which is practical even for cost-sensitive embedded systems with a limited energy budget.

There are two enabling technologies for selective hardening based on fault criticality. First, it must be possible to harden parts of the circuit while not spending chip area or energy budget for the parts which require no protection. Techniques recently developed are able to perform selective hardening with ultra-fine granularity; it is possible to specify individual logic gates to be hardened [116]–[119], while other gates remain unchanged, and do not cause hardening costs. Second, proper methods must determine which faults may result in critical system behavior, as opposed to non-critical faults, which require no protection. We now address these methods in more detail.

Fault criticality was first studied in the context of permanent chip manufacturing defects. A circuit with a defect known not to cause critical effects on a system level could be sold at a lower price rather than thrown away, thus increasing the effective yield. A number of generic metrics were proposed in the last few years, such as error significance, and error rate [120], as well as specific approaches for multimedia circuits [121], [122].

More recently, the research focus turned to transient or soft errors caused by such mechanisms as electrical noise or cosmic radiation. In contrast to manufacturing defects, their impact to the system operation is limited by a very short period of time, typically one clock cycle. However, the error effect may be propagated to the memory elements, and thus corrupt the system state. Consequently, one definition of non-critical errors requires that their effects be eliminated from the system state within a small number of clock cycles. In other words, errors from which the system recovers itself within a short period of time do not need

to be handled. It was proven by Polian [123] that over 70% of possible error spots in an MPEG subsystem had the property that an error on one of these spots was non-critical with respect to the definition above, irrespective of the system input or system state. This concept has been enriched by probabilistic aspects by Hayes [124]. It was shown that the rate of critical errors can be reduced by several orders of magnitude by hardening 10% of the circuit or less.

A couple of application-specific criticality definitions were also studied. A communication chip with a set of formal properties describing its specification was considered by Seshia [125]. A model checker was used to formally show that errors in approximately two-thirds of the chip's flip-flops did not lead to a system behavior which violated the properties. Hence, only the remaining one third of the flip-flops required hardening. A large-scale fault injection study by May [126] demonstrated the resilience of a rather complex communication device to randomly injected soft errors up to a certain error rate. Further application-specific metrics were studied by Li [127]. In [128], the concept of cognitive resilience was defined to denote the ability of a human user to compensate the effects of certain soft errors by her cognitive apparatus. Less than half of the flip-flops in a JPEG compressor need to be hardened, according to that definition.

The future of computing is expected to be centered on a class of applications commonly known as recognition, mining, and synthesis (RMS). These methods will tackle difficult problems such as natural language translation by identifying patterns in large sets of data, and correspondences to data-sets already resolved (recognition); automatically learning new patterns, and correspondences (mining); and derive problem solutions from principles learned (synthesis). It is obvious that these approaches must have mechanisms to deal with incorrect decisions. Hence, they can also be expected to be intrinsically tolerant against hardware faults, rendering only a small portion of errors critical. On the other hand, the continuing transition to nanoelectronics will result in error rates further increasing. Hence, there appears to be an increasing need for criticality-based hardening for applications of tomorrow.

I. The Science and Pitfalls of Achieving Verifiable Data

Provided by Dr Samuel Keene (S.keene@ieee.org)

Background: A Life Long Search: This author has long been a student of reliability successes, and more often, of reliability failures [129]. This article seeks to identify some of the underlying causality in experimental errors, and report the “lessons learned,” as well as best practices found for assuring data validity. Some of the “lessons learned” came about in testing and qualifying parts for military, space, and commercial programs. These part-qualification efforts are data collection intensive with lots of opportunities for error. These data errors have come from:

- *Drifting in the measurement apparatus, corrupting the reported data.* One case had a resistor heating up in the measurement system that skewed the measured data. Plotting the Measured data from 50 identical devices showed a definite data pattern vs. the random pattern that should have been observed. This data pattern was not observed or acted

upon by the technician collecting the data. It was only observed in hindsight.

- *Measurement equipment out of calibration.* The lab technician was measuring the gate to cathode voltage in the range of hundreds of volts across a triac motor driver. The differential scope probe was subsequently found to read the same level of spikes when the probes were on the same triac terminal. The hundreds of volts were due to a timing offset in the probes.
- *Measured data was not representative.* Devices tested during development testing were not representative of the production product. The design point determined during the initial development was based on early samples, and did establish a robust solution using production samples.
- *Data can be confounded where a trend of one variable's effect is mistakenly attributed to another co-varying variable.* For example, the cocky rooster crowing every morning believes he brings up the sun each day.
- *There can be variable interaction effects that are not properly isolated or recognized.* When Firestone tires (condition 1) were underinflated (condition 2) to increase vehicle stability on Ford Explorers (condition 3), rollovers increased. It took all three conditions to create the problem. This is an interaction.
- *Lack of control samples to contrast experimental effects, demonstrate measurement repeatability, or maintain traceability of test results.*
- *Human bias can corrupt experimental results.* We want to minimize the effect of the experimenter on the experiment outcome. This measurement effect can be mitigated by using the double blind experimental practice, often used in medical studies to determine the efficacy of a new drug, for instance. Then the subjects undergoing the testing don't know if they are getting the new drug or the placebo. Also the doctors running the test do not know who is getting the real drug vs. the placebo. This takes out the effect of the doctor's or the patient's expectation on the experiment result.
- *There are also data transcription and recording errors.* This even happens today with all the automated data logging capability that we have. An example of this is the "hottest October on record," which actually turned out to be September data inadvertently repeated. This will be discussed below.
- One can also see errors in the routine polling processes to assess customer preferences. To be done correctly, the polling must be scientifically designed, including drawing a statistically significant, representative sample from the relevant population that we are trying to assess. The polling sample needs to be randomly drawn to preclude potential bias in the polling results. This quality is sometimes difficult to achieve, so needs a plan, and the plan execution must be monitored. Poling questions often force decisions into too few selections, and don't allow for the cases of don't know, don't care, or feel equal between the choices.

"life is the art of drawing sufficient conclusions from insufficient premises" Samuel Butler 1835–1902

Some Recent Data Problems: Michael Mann, along with his co-workers, published an estimation of global temperatures from 1000 to 1980 [130]. They arrived at this estimate by combining the results of 112 previous proxy studies. By "proxy studies" I mean tree-ring, isotope, and ice core studies that are intended to provide an indirect measurement of temperature in the time before thermometers existed. Mann's results appeared to show a spike in recent temperatures that was unprecedented in the last one thousand years.

Mann's assessment of the data was criticized on several fronts. The first was historical fact: his chart didn't appear to show the well-known medieval warm period, or the so-called little ice age that began around the year 1400.

Two Canadian researchers, McIntyre, and McKittrick, obtained Mann's data, and repeated his study. They found numerous grave and astonishing errors in Mann's work, which they detailed in 2003 [131]. For example, two statistical series in Mann's study shared the same data. The data had apparently been inadvertently copied from one series to another. In addition, nineteen other series had data gaps, which Mann's team had then filled in, but did not disclose. In addition, all 28 tree ring studies had calculation errors, and so on and so forth. In the end, the Canadians' corrected graph looked quite different. The corrected graph suggests that the global temperature today is very far from the warmest it has been in the last thousand years.

Mann has countered these claims, so the debate continues [132].

Another facet of this global warming data controversy was the Goddard Space Information Systems reported (incorrectly) that October 2008 was the hottest October on record [133]. An excerpt from that report: "A GISS spokesman lamely explained that the reason for the error in the Russian figures (that they had used) . . . were obtained from another body, and that GISS did not have resources to exercise proper quality control over the data it was supplied with."

"The great danger here is that public policy and law can be launched from a faulty premise.

If language be not in accordance with the truth of things, affairs cannot be carried on to success." Confucius

Is Snopes the Final Answer?:

"Whoever undertakes to set himself up as judge in the field of truth and knowledge is shipwrecked by the laughter of the gods."

Albert Einstein

"Who dares to say that he alone has found the truth?"

Henry Wadsworth Longfellow

For the past few years, www.snopes.com [134] has positioned itself, or others have labeled it, as the 'tell all final word' on any comment, claim, and email. Wikipedia reports snopes is run by a husband and wife team [135]. No big office of investigators and researchers, no team of lawyers. It's just a mom-and-pop operation that began as a hobby.

David and Barbara Mikkelsen in the San Fernando Valley of California started the website about 13 years ago, yet they have no formal background or experience in investigative research. It is doubtful that Snopes is run without bias, and they have been proven wrong [136]. So Snopes is a good starting place, but it should not be totally relied upon, or considered the final arbitrator. Use it only to lead you to their references where you can link to, and read the sources for yourself. Plus, you can always Google a subject, and do the research yourself.

“If you add to the truth, you subtract from it.”

The Talmud

Data Discipline: As scientists, engineers, and decision makers we need to routinely question:

- 1) measurement requirements,
- 2) experiment design,
- 3) measurement process,
- 4) measurement calibration,
- 5) gage r&r (see below),
- 6) data collected, and
- 7) data legacy depository capability for traceability.

Six Sigma uses a programmed Gage Repeatability and Reproducibility (GR&R) process to validate the measurement capability [137]. Data measurements are replicated in randomized order by the first measurer, and then repeated a second time by an independent measurer in a different randomized measurement order. There are Six Sigma guidelines on what constitutes an adequate data measurement capability. “What gets measured (data gage), gets improved”.

We possibly need Six Sigma GR&R experimental verification, design of experiments, best practices, independent and open data, and analysis reviews of critical government funded research. A lot of policy (\$) rides on the premises formed by this experimentation. It might make sense to triplicate critical environmental research experiments, across diverse teams, with cross reviews. The operating cost is millions of dollars. But the potential policy cost savings is billions of dollars more.

“The truth may be puzzling. It may take some work to grapple with. It may be counterintuitive. It may contradict deeply held prejudices. It may not be consonant with what we desperately want to be true. But our preferences do not determine what’s true.” Carl Sagan, ‘Cosmos’

J. Trustworthy Medical Devices

Provided by John Harauz, (j.harauz@computer.org)

Advances in health information systems and healthcare technology present opportunities to improve the quality of healthcare, while reducing healthcare costs. The Healthcare Market in The US is roughly \$2 trillion/year in 2006, and is projected to reach \$4 trillion (or 25% GDP) by 2015. Because the current trends are unsustainable, US and worldwide governments are “changing the game” by building National Healthcare Information Networks (NHIN), essentially bringing eCommerce, and automated manufacturing tools and techniques to healthcare.

There is a proliferation of diagnostic and therapeutic devices due to advances in computing, networking, sensing, and medical device technology. They have revolutionized patient monitoring, allowing small teams of nurses to monitor larger numbers of patients. They now extend to more active intervention, including programmable infusion systems, and surgical robots.

What Is a Medical Device?: According to the Food and Drug Administration (FDA), a medical device is “any product (or portion of a product) that affects a patient’s diagnosis or therapy of” [138]. In a recent 2008 FDA proposed ruling, *data communication or storage devices or networks that merely transmit or store patient data will become “medical devices”* [138]. There is a strong movement now occurring inside and outside government to include a new class of “consumer health/medical devices,” and associated communication, storage, and computing accessories such as heart monitors used with treadmills as non-regulated, but still *partially valid*, sources of medical data. Low cost products suit Medicare plans to reduce costs [138].

Medical Device Incidents: Adverse medical incidents due to innovative technologies are estimated at 45,000–100,000 fatalities per year in the US, and at 850,000 adverse events in the UK [139]. IOM/National Academies of Engineering report in 2005 for the healthcare market stated that errors are running at 2–3 Sigma levels, and that medical errors are killing 70,000–100,000 patients each year [140].

The number of devices recently recalled due to hardware and software problems is increasing at an alarming rate. FDA Analysis of 3140 medical device recalls between the years 1992 and 1998 showed 242 (~8%) attributable to software (79% of those caused by software defects were introduced when changes were made to the software after initial production and distribution) [141]. Of 23 recalls in 2007 that the FDA classified as life-threatening, three involved faulty software [142].

Research on medical errors suggests that the frequency and consequences of medical device use errors may far exceed those arising from device failures. Recent FDA reports show that more than 1/3 of medical device incident reports involve use error, and more than 1/2 of the recalls due to design problems can be traced to design of the user interface [143].

State of Practice: The medical industry as a whole does reasonably well in developing and approving stand-alone devices with moderate complexity, based on mature technology. However, designing bug free code is difficult, especially in complex devices that might be used in unanticipated contexts. Large scale complex devices require extensive validation, and certification. The development of high confidence medical devices has not kept pace with software assurance techniques practiced in other safety critical domains, due to time-to-deliver pressures, and a shortage of properly trained software engineers. The number of medical devices to be networked and integrated is increasing significantly, and there are no standards or regulations yet for their integration or interoperation. Medical devices are embedded not only in information networks, but also in human patients. The design of medical devices must also include the device’s interaction with the patient and the environment, and the context in which they coexist. The development and certification processes effectively need to undergo a paradigm shift to not stifle innovation in medical devices.

What Standards Govern Medical Devices in the US?: Unlike Europe, the FDA has no standards for medical devices. FDA chooses to regulate quality and safety by pre-market screening, and post-market surveillance. The furthest the FDA goes is to provide a few “guidance documents” for manufacturers:

- FDA 21 CFR 820 (Title 21, Code of Federal Regulations (CFR), Part 820) Medical Devices Quality System Regulation (QSR).
- FDA Final Guidance, General Principles of Software Validation: 2002.
- FDA Guidance for Off-the-Shelf Software Use in Medical Devices: 1999.
- FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices: 2005.
- FDA Guidance, Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management: 2000.

The Association for Advancement of Medical Instrumentation (AAMI), an industry association, develops consensus clinical, technical, and safety standards for specific medical devices like IV Pumps. AAMI is now “importing” European standards from IEC, and other sources. IEC 60601, and some ISO standards cover European medical devices. Key medical device standards include:

- ISO 13485:2003, Medical devices—Quality management systems—System requirements for regulatory purposes.
- ISO/TR 14969:2004, Medical devices—Quality management systems—Guidance on the application of ISO13485:2003.
- ISO 14971:2007, Medical devices—Application of risk management to medical devices.
- AAMI TIR32:2004, Medical device software risk management.
- IEC 60601-1-4, Medical Electrical Equipment—Part 1 General Requirements for Safety, 4 Safety Requirements for Programmable Electronic Medical Systems.
- IEC 62304:2006, Medical device software—Software life cycle processes.

Standards have been established for best practices in human interface design, and training techniques:

- ANSI/AAMI HE74: 2001 Human factors design process for medical devices.
- ANSI/AAMI HE48:1993 Human factors engineering guidelines and preferred—practices for the design of medical devices.
- ANSI/AAMI HE-75: 2008 *Human Factors Engineering—Design of Medical Devices* (released for public review).
- ISO/IEC 62366:2007 Ed 1, Medical devices—Application of usability engineering to medical devices.
- IEC 60601-1-6:2004 Medical electrical equipment—Part 1–6 General requirements for safety: Collateral Standard: Usability.

Professional Responsibility Needs: People developing any safety critical software systems should be adequately trained in basic software development, and they should understand their limitations. Software developers have responsibility for minimizing the risk of failure, and ensuring public safety and security. Certification of software safety engineers is becoming

an increasingly important consideration in the development of safety-critical systems. Just as in other fields where the consequences of failure are very high, there is a need to ensure that practitioners are properly monitored by their colleagues, independent auditors, and government regulators.

K. Degradation of the High-k Dielectric/Metal Gate Stacks Under Electrical Stress

Provided by Gennadi Bersuker (gennadi.bersuker@se-matech.org), SEMATECH, Montopolis Dr. Austin TX 78741

To sustain the historical rate of transistor scaling, the conventional SiO₂ gate dielectric layer must be replaced with a material that offers a higher dielectric constant k (HK). While significant milestones were reached with respect to the performance of high- k devices, their reliability is still a critical issue to be addressed.

Recent HK reliability studies reflect increasingly complex, diverse gate stack structures fabricated to meet device scaling requirements. Essential progress towards achieving low values of the threshold voltage was made through the introduction of the metal oxide capping layers in gate stacks that, in turn, instigated a number of reliability studies of these systems. Employing fast measurement techniques has provided new insights into the characteristics of the defects in the gate stacks. Interfaces between the high- k dielectrics, and high mobility substrates (III-V, and Ge), which are being considered for use in transistors in the future technology nodes, have started to attract significant interest from a reliability standpoint. In the present study, we focus on the breakdown mechanism of the scaled high- k /metal transistor gate stacks targeting high performance logic applications.

The essential factor, which differentiates HK stacks from the conventional SiO₂ gate dielectric, is that the former is presented by a multi-layer structure, which includes both HK film, and thin (usually around 1 nm) SiO₂ layer near the gate stack interface with the substrate, as in Fig. 8. Such multi-layer structure complicates forecasting reliability behavior in the highly scaled stacks. Indeed, with scaling of the gate stack dimensions, the ratio of the high- k to SiO₂ portions in the total stack thickness changes, while each layer is known to exhibit a distinct response to the applied electric field. Therefore, lifetime evaluation performed under the accelerated stress conditions on a given gate stack may not be directly applicable for a scaled down stack. One needs to understand which layer contributes the most to the reliability margins in order to focus process improvement efforts on a “weak link” in the gate stack.

The quality of the interfacial SiO₂ layer in the HK gate stack (hereafter we limit our consideration to the HfO₂, and Hf-silicate HK dielectrics, which are currently used in manufacturing) is known to be strongly affected by processing conditions, which determines to what degree the stoichiometry of this layer is affected by its interaction to the overlaying HK/metal films. Indeed, as has been demonstrated by the electrical, physical (STEM/EELS, ESR, XPS [146]–[150]), and modeling studies, Hf-based high- k films modify the stoichiometry of the underlying SiO₂ layer by rendering it oxygen-deficient. This leads to an increase in its dielectric constant, and a higher density of fixed charges in this layer, thereby degrading the mobility of the channel carriers. Precursor defects associated with the oxygen

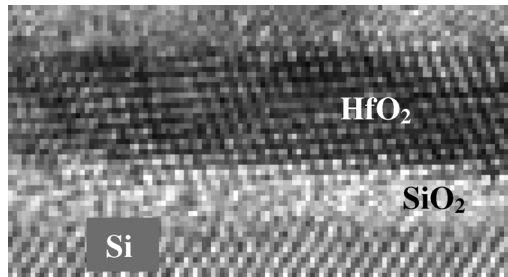


Fig. 8. HR-TEM image of the typical gate stack with HfO₂ high-k dielectric, and SiO₂ interfacial layers, after the standard transistor fabrication processing including the 1000C/10sec source/drain dopant activation anneal.

vacancies can be converted to electron traps during device operation under bias, giving rise to stress-induced leakage current (SILC), and contributing to subsequent electrical breakdown.

Previous studies have shown that the evolution of SILC during stress closely correlates to the various stages of the dielectric degradation: soft BD, progressive BD, and finally hard BD [151]. This allows employing SILC as a gate stack degradation monitor. Thus, an understanding of the nature and origin of the defects controlling SILC would lead to uncovering of the major contributors to the dielectric BD.

By applying periodically the variable frequency charge pumping measurements (which was shown to probe the electron/hole traps through the thickness of the interfacial SiO₂ film) during the constant voltage stresses at different voltages, we have established at the room temperature a 1:1 correlation between the trap generation, and SILC within the wide ranges of the stress times, and voltages [152]. This demonstrates that SILC, and hence the stress-induced gate stack degradation, is controlled by the defects in the interfacial SiO₂ layer. On the contrary, stress performed on the MIM high-k capacitors (with no interfacial layer) does not show either any trap generation, or an appreciable SILC. To confirm the above findings, we performed simulations of the gate leakage current and SILC during stress using the model, which considers a multi-phonon trap-assisted tunneling conduction mechanism, including random defect generation, and barrier deformation induced by the charged traps [153]. An excellent match to the experimental data for both NMOS, and PMOS transistors in inversion was obtained (Fig. 9) by using the spatial distribution of stress-generated traps within the interfacial layer, as extracted by the above mentioned CP measurements. In Fig. 9, the following fitting parameters were used: energies $E_T = 2.4 - 2.8$ eV and $E_T = 1.1 - 1.6$ eV and capture cross-sections $\sigma = 2 \times 10^{-14}$ cm² and $\sigma = 4 \times 10^{-15}$ cm² for the stress generated traps in SiO₂ and pre-existing traps in the HK film, respectively. In this simulations, we used the following earlier extracted gate stack characteristics: equivalent oxide thickness $EOT = 1.25$ nm, metal gate workfunction $W_{gate} = 4.4$ eV, and HK band offset $\Psi = 1.6$ eV. Electron spin resonance (ESR) measurements performed on the SiO₂/HfO₂ stack of the identical composition and thickness revealed that the generated defects in the SiO₂ layer are indeed the oxygen vacancies with the characteristic g-factor value of 2.0025. Comparison of the temperature-dependent time-to-dielectric-breakdown (TDDDB) distributions collected

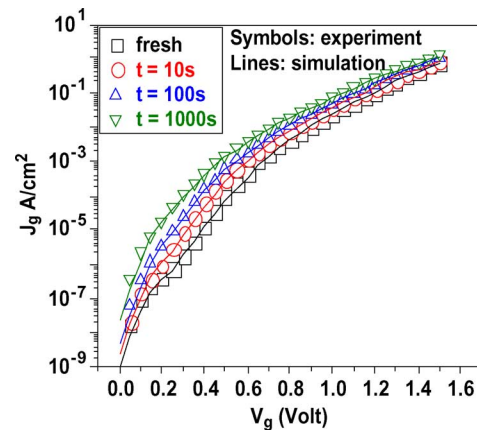


Fig. 9. Measured (symbols), and simulated (lines) I_g-V_g curves during 1.1 nm SiO₂/3 nm HfO₂/TiN NMOS stress at $V_g = 3$ V.

on the MIM, and MIS structures confirms distinctly different BD origins in the HK dielectric, and SiO₂/HK stack [152].

Our study demonstrates that the stress-induced defects leading to the gate stack breakdown are generated in the interfacial SiO₂ layer in the HK gate stacks. Control over the SiO₂ layer composition and stoichiometry is critical for meeting reliability requirements for future technology nodes.

L. Response to Counterfeit ICs in the Supply Chain

Provided by Gary F. Shade (gshade@ial-fa.com), Sr. Staff FA Engineer at Insight Analytical Labs (IAL) and a charter member of the Electronic Device Failure Analysis Society (EDFAS).

Introduction: Webster [154] defines a counterfeit item as “made in imitation of something else with intent to deceive”. In the case of electronic components, this is done with increasing regularity to meet market demand with products at inflated prices, often substituting complete frauds that do not match the form, fit, or function of the intended component. The counterfeiters attempt to deceive the consumer into thinking they are purchasing a legitimate item, or convince another supplier that they could deceive others with the imitation. An example of a remarked IC is shown in Fig. 10. The IC was remarked to match a more desirable memory, thus increasing its present value.

Counterfeiting of electronic components is occurring in increasing numbers requiring resources to maintain or improve quality levels. The presence of counterfeit components in the supply chain (and in use) has an impact to all who supply, and use these components, and their assemblies. Procurement methods coupled with failure analysis, utilizing industry experience, and a disciplined approach, can provide great improvements in reducing this impact. This article addresses this topic to promote awareness of the problem, as well as to offer some solutions. Each example will raise many questions, and only some will be answered here. It is sufficient that those who use or analyze electronic components learn to be aware of counterfeiting, and to take appropriate action.

Examples From the Supply Chain: The traditional opportunities for counterfeiters increased as semiconductor technology spread across multiple continents, making basic IC processing more accessible. Now the opportunity is expanding even further as mature products are discontinued in favor of more profitable ones, and supply chains reach across the globe, and across

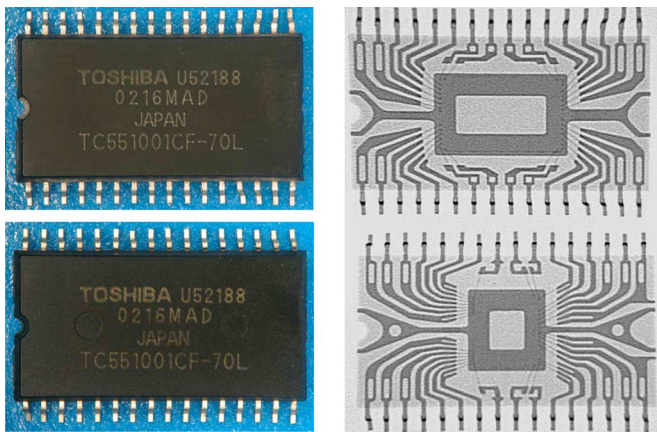


Fig. 10. (a) Optical photographs of two packages with same date code show very similar markings, but mold marks are missing on one device. (b) X-ray inspection of packages in (a) indicates two products that are clearly different. One has been re-marked and mixed in with authentic components to prevent detection.

many different languages, cultures, and legal systems to meet demands. Thus, the ability to analyze and detect counterfeit components can be critical in insuring high quality.

In the past, it was assumed that most counterfeit parts were copies (or clones) of high value components to be sold as the original for the full price. These clones were made by (often intensive) reverse engineering, and reproduction of an IC. They were meant to operate like the original, but each was produced without the experience and quality of the original manufacturer. This limited the choices for components likely to be counterfeit. With the maturing of the Electronic component industry, and its expanding range of low-cost commodity products, the opportunities for counterfeiters have increased. In addition, there are increasing numbers of components that are obsolete, or have dwindling supplies driving their value higher. Due to shortages, any electronic device can potentially increase in value, and be a target for counterfeiting. To compound this, the worldwide shift towards lead-free solders has provided additional opportunities for fraud, as manufacturers struggle in some cases to provide both leaded, and lead-free products. This situation is leading to increased use of traditional counterfeit methods, such as re-marking the product type, or the speed of high-end components. At the same time, new methods are appearing, such as modified RoHS markings, and other fraud of low cost components. As a result, the quantity and variety of counterfeit IC entering the supply channels is increasing.

The next example shown is an IC marked as Lattice, in Fig. 11. Two parts are shown side-by-side from the same lot packaging. Notice that both parts have alpha-numeric markings indicating the same device type, and assembly lot. Oddly, only one has a pin-1 indicator, and the mold marks are only partially visible on the second unit. This is very unlikely to occur within the same assembly lot. Internal inspection after decapsulation [155] added more concern, as the die on the right was produced by AMD, a foundry known to be used by Lattice for this MACH production, but not until the late 1990s. (See Figs. 12 and 13). The date on the die is 1991, indicating the die is not likely to be authentic. The conclusion is the package has been sanded to remove old markings. Next it is remarked to look like the

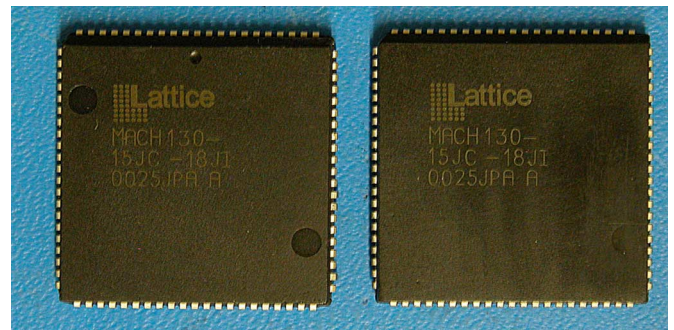


Fig. 11. Sample with no Pin-1 marker. Lighting has been adjusted to enhance the markings.

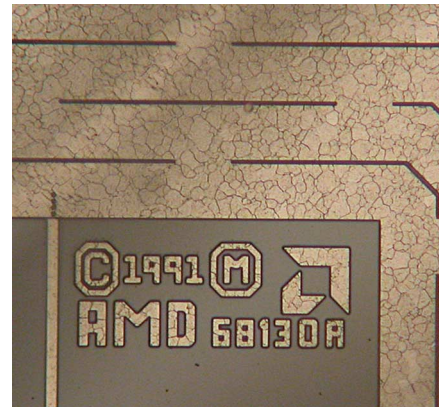


Fig. 12. After decapsulating the part in Fig. 11, the die markings are visible showing the AMD logo, mask set number, and copyright date.

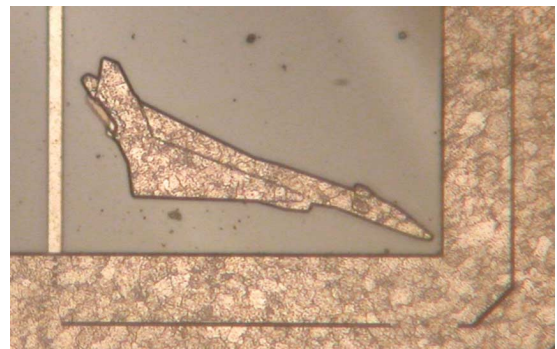


Fig. 13. Also visible after decapsulation is a second AMD logo of an aircraft representing the "Mach" name.

more recent (and valuable) one beside it. In addition to these observations, the product undergoes several tests to determine its authenticity. Each test result is then used to determine the overall confidence. Some products require many tests before authenticity can be determined.

Current Observations: Today's leading edge process technology is becoming more difficult to copy with 7–10 layers of copper metallizations, 45 nm geometries, and sophisticated packaging. These same products often use sophisticated anti-counterfeit measures that are a challenge to overcome for all but a few counterfeiters. These difficulty factors appear to be expanding the market for forgeries of mature, less complex components. Such components are still in very high demand, and can be easy to introduce into the supply chain.

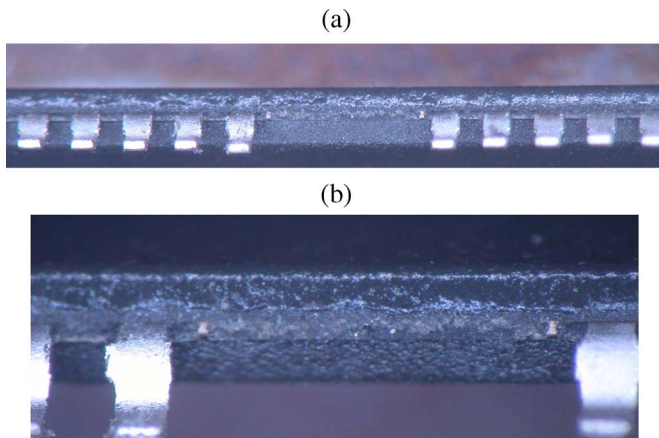


Fig. 14. (a) Example of paint at package edge from remarking. (b) Example of package remarking: close-up view of (a).

To date, over 150 product types have been inspected for authenticity by the author's company. From these, forgeries have been observed that range from complete frauds (do not match the form, fit, or function of the original) to subtle changes of the date code. The former are not likely to elude detection for long, but may pass through one or more distributors before being detected. More typical are parts that have the correct package type, but are remarked to indicate a match to a desirable part. Visual inspection alone will not detect these, and they are often mixed in with authentic parts to further reduce detection. Remarketed components recently detected have been from different date codes that are re-marked at the package level to appear from the same date code, and revision level. Fig. 14 shows an example of detecting remarketing. The top surface has been polished or ground away to remove the original marking, and then a textured, black paint was sprayed on to refresh the surface. Careful inspection is required to observe the black paint, as seen in this figure. Next, the package is re-labeled to match the original. The ink on counterfeit components may or may not meet mark permanency tests required by the industry.

Impact, and Summary: The size, and impact of the counterfeit problem is difficult to measure. This past year (2007), the U.S., and European Union worked jointly to seize 360,000 counterfeit IC, and computer network components bearing over 40 different trademarks. These products were selected for the joint operation because they presented either a safety, or security risk (along with infringing intellectual property rights) [156]. Globally, all forms of counterfeiting are on the rise. Experts estimate the total as 5–7% of total world trade [157].

The range of impact, however, is quite wide. Suppliers must now take extensive measures to secure supply channels to protect their image. Board, and system manufacturers in turn need to qualify suppliers, with inclusion of methods for detecting counterfeit products. Component suppliers (brokers, distributors, etc.) need additional inspections to screen potential counterfeit products from reaching their customers. Finally, failure analysts need to apply additional measures to determine if failures are caused by the wrong component, potentially one that appears and operates similarly to an authentic device. Such counterfeit failures have been seen at IAL in the course of analysis.

M. How Lead-Free Changes Can Impact Reliability

Provided by Joe Childs, P.E. (joechilds@ieee.org)

Abstract: The European Union and other countries have imposed a ban on the use of substances in manufactured products. Eliminating or severely limiting the use of lead has begun to have serious impact on the electronics industry, especially in the area of reliability. Lead has been used for the past 40+ years in solder to preclude a phenomenon called “whiskers” that can cause shorting over time. The removal of lead in solder has also caused the industry to investigate new solders and finishes that can result in changes to the electronics reliability. Many companies and organizations are investigating potential manufacturing materials and processes, along with corresponding new issues and causes. These entities are testing new materials and techniques to assure the reliability of electronic products meet user needs. Examples of such investigations, their associated tests, and conclusions are provided to afford the reader insight into the progress being made.

The Initial Problem: Anyone who has been paying attention knows that governments are turning ‘green,’ meaning they are banning ‘hazardous’ substances. The European Union (EU) took the lead in this endeavor with a directive, ‘restriction on the use of certain hazardous substances in electrical and electronic equipment,’ or simply ‘RoHS.’ This directive (with some exceptions) bans or limits the use of six substances from manufacturing products: cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBB), polybrominated diphenyl ethers (PDPE), and lead.

The prohibition or limitations on the use of lead in particular has turned the electronics manufacturing industry on its ear. China, Japan, and other countries are developing their own bans or limitations on the use of lead, and other substances, as well.

Since the 1960s, we have known of a phenomenon called ‘tin whiskers.’ This artifact appears when tin is in pure enough form to result in conductive outgrowths, or ‘whiskers.’ These whiskers are conductive, so over time they can result in short circuits in otherwise reliable circuits. This is a particularly critical problem in the electronics industry now, because for decades the industry has depended on tin-lead solder to attach ever-shrinking components onto very dense printed circuit cards. However, without the lead in the solder to metallurgically bond with the tin in the solder, the tin will grow whiskers. This goes for finishes, too. Care must be taken to assure a high-percentage tin is not on the lead finishes. If tin is there, whiskers can form there, as well.

The ‘Solutions’ . . . and Why They’re Not Really Solutions: One of the unintended consequences of trying to solve this issue is that the industry has had to turn to new materials and methods for attaching parts to boards. This comes at a time when the semiconductor industry is devising new ways to package their integrated circuits (IC) to crowd continuously smaller geometries into them, and at the same time introduce smaller logic voltages, and tinier lead spacing to accommodate the high speeds, and increased computing power the market is demanding. So now this ‘growth problem’ is complicated by using new attachment technologies, trying to avoid the known tin-whisker problem. Three techniques used today are:

- New metal combinations for solder with different melting.

- Refinishing the package leads (for industries in which tin is allowed).
- Coating the devices to help mitigate the whisker risks. This technique has its own set of problems: little or no test data that verify the coatings will work, and configurations like ball grid arrays (BGA) that make coating in the inner connections difficult, if not impossible.

These changes in themselves result in new issues affecting quality and reliability. For instance, many of the new solder combinations require higher temperature solder profiles to assure they melt and properly bond. Many of the electronic components are impacted by these higher temperatures. This is a particularly trying issue when rework or repair is required on printed circuit cards.

Another issue associated with this tin-whisker phenomenon is not fully understood. For that matter, neither are the potential 'improvement' techniques. Part of that concern is tied to the fact that tin whiskers can take years to develop. This is compounded by the fact that the *cause(s)* of the whisker phenomenon is not well-understood. Because there is incomplete knowledge about the underlying physics that result in the formation of whiskers, there is not a good way right now to perform accelerated testing.

The impact of this issue varies from segment to segment in the industry. For instance, the mobile telephone segment may not need to worry as much for phones that won't last many years; but for the automotive, defense, space, and other segments that have products that are expected to last many years, whiskers is a problem. True, in some cases the military designs have some exemptions (or did have them). However, with the industry being driven to lead-free, the tin-lead products and solders are becoming scarce. And those telecom guys? They're not off the hook, either. Because new attachment and packaging techniques are being devised, their equipment must be able to withstand the higher reflow temperatures that are tied to lead-free solders, and they still can't assume the new materials are adequate. They still must survive the use and abuse by their customers.

So, What Do We Do? Where Is That Masked Man?: All is not 'gloom and doom.' Although there is no 'Lone Ranger' who will single-handedly save us from this problem, there are many companies and organizations working to develop not only new techniques, but test them to understand their strengths and weaknesses, to verify they are effective and don't introduce new issues.

Below is a sampling of the types of efforts that are under way that address the reliability of lead-free packaging. The sources of the referenced cases provide a partial listing of organizations that are quite active in such investigations:

- IEEE RS—Institute of Electrical and Electronics Engineers Reliability Society
- iNEMI—International Electronics Manufacturing Initiative
- CALCE—Center for Advanced Life Cycle Engineering, University of Maryland, College Park, MD
- Electronic Packaging Laboratory, Center for Advanced Microsystems Packaging, Hong Kong University of Science & Technology, Clear Water Bay, Kowloon, Hong Kong
- SMTAi—Surface Mount Technology Association International

The study of tin whisker bridging on compressive contact connectors [167]: A scanning electron microscope was used to measure tin whisker length, direction, origin location, and count. These data were used to develop a Weibull probability model, plotting probability vs. whisker length. The researchers found that 74% of the observed whiskers would fail National Electronics Manufacturing Initiative (NEMI) criteria for length in about a year, but based on probability modeling, only about 0.0074% of those whiskers would actually cause bridging in that year.

This is an interesting observation, because the fact that whiskers are present does not mean that a cause will result. As mentioned above, the impact of the whiskers depends on the condition, composition, and configuration of the solder, and time. If the product isn't intended for use over decades, then viewing its main life over a one or five-year period is useful.

Another observation was that the count of whiskers tended to fit a Poisson probability distribution. This observation, combined with data about the location and direction of the whiskers, then allowed the model of the failure probability to be created.

The Assessment of the reliability and quality of reballed plastic BGA packages [168]: In responding to the lead-free directives, manufacturers with exemptions (such as the defense industry) are experiencing a shortage of BGA parts with tin-lead materials. Reballing, which is the replacement of existing solder balls with balls of another material, may be an option. The idea would be to replace the lead-free balls with tin-lead ones to eliminate production and reliability risk, if the reliability and quality of the end-product is not compromised.

The two steps of solder ball removal and solder ball re-attachment must both be evaluated in terms of the end result. The reliability and quality of the resultant package's BGA must be at least equivalent to the original configuration for this approach to be a valid alternative. To evaluate the reballed BGA robustness, attach strength was measured. Two methods to evaluate this strength are solder ball attach strength (shearing each ball from the body to measure the shear force required), and cold ball pull (CBP) test (pulling the ball at low temperature to measure the tensile force required). In this evaluation, both of these methods were used with two ball removal, and two ball replacement processes for comparison.

The two removal processes were performed, as described here.

- *Solder Wick*—In the solder wick process, a soldering iron heats a copper braid, which is manually wiped over the solder ball. The braid wire melts the solder balls, and adheres to the molten solder.
- *Low Temperature Wave Solder*—In this process, the component is suspended in a solder wave for a sufficient time to remove the solder balls. The solder in the wave is eutectic tin-lead.

The BGA packages without reballing, and the reballed BGA packages, were compared with, and without aging exposure. Statistical box and whisker plots indicated that the non-reballed BGA packages exhibited higher shear strength than the reballed BGA. This finding was consistent in two types of packages, and was *s*-independent of the reballing technique used.

Failure analysis of the balls that underwent the destructive ball shear test indicated that all displayed ductile failure (the

fracture was within the bulk solder). The failure sites showed that, as would be expected, the tin lead solder was softer than the lead free (tin-silver-copper, SnAgCu, or "SAC," solder).

The cold bump pull (CBP) test was also performed on a sample of virgin, and reballed BGA. Similarly, virgin, and reballed were compared with, and without exposure to aging environments. These tests also showed a higher strength for the non-reballed over the reballed BGA. This was true for a high pull rate (5000 $\mu\text{m/s}$), and a low rate (500 $\mu\text{m/s}$).

In this testing, the reballed failures occurred within the solder ball, itself. The non-reballed failures were a mix of failures associated with the ball (as with the reballed sample), as well as the bond, the pad, and the ball extrusion.

The conclusions drawn were:

- there was no correlation with the process used in reballing;
- aging does not greatly influence the interconnect strength of the tin-lead solder after reballing; and
- non-reballed lead-free solder balls were found to have greater strength, and a wider statistical distribution than the reballed tin-lead samples.

A Study of the effects of mechanical shock on the reliability of solder joint adhesion [169]: This study focused on two areas: the effectiveness of different board level adhesive technologies, and the identification of key attributes to optimize adhesive geometry. Although mechanical shock resistance was a key parameter, the cost effectiveness of the adhesive method was also considered. There were three categories of board-level adhesive methodologies evaluated:

- full under-fill (FF)—under-fill applied to all parts of the board;
- partial under-fill at package corner (CF)—under-fill applied to the board corner areas, covering a portion of the board at each location; and
- corner glue (CG)—under-fill applied at the card edge at the four corners.

Assembled packages were tested to failure with increasing shock levels to serve as a performance indicator.

The handheld sector has driven the use of under-fill, and partial under-fill to mitigate drop risks in the field. The evolution of this technique includes full under-fill, under-fill at corners, board-level adhesive, and mixtures of full under-fill with corner glue. Interestingly, the use of under-fill is used for flip chip, as well as BGA technologies. However, the under-fill serves two different purposes for these package types. Flip chip under-fill helps to mitigate issues associated with coefficient of thermal expansion (CTE) difference, which are especially problematic when exposed to thermal cycling. However, board-level under-fill helps to provide mechanical shock protection.

Results—Adhesive Type

- The full under-fill (FF), corner under-fill (CF), and corner glue (CG) underwent shock testing.
- For the FF, and CG adhesive types, no open was detected after shock exposure. In failure analysis, minor cracks were observed in CG, but none were detected with the FF.
- However, because the CG still provides sufficient margin, and provides ease of rework, as well as uses less material, further studies were focused on the CG adhesive type.

Results—Fillet Geometry

- Because the corner-glue (CG) method is frequently manually dispensed, the study focused on variations in the manufacturing environment.
- Fillet height, width, and coverage were included in a finite-element analysis (FEM) to predict mechanical shock protection of the CG method. In particular, fillet height was modeled with respect to CG stresses, where the lower the force shown, the better the protection for the package. Fig. 8 in [169] shows the FEM results, that CG stress for a given shock is inversely proportional to the fillet height (at least between 10–70% of the side wall of the package).
- Also, fillet width (the distance from the external to the internal glue footprint) was important. The FEM indicated the wider the fillet width, the smaller the glue stress. Also, there is better protection if the fillet covers the first three rows of a BGA package, but the advantage tapers off beyond those first three.
- The FEM models were verified with empirical data collection. Five configurations with different fillet geometries were tested, showing that indeed the fillet height, and width were the most significant factors.

The study concluded that using CG seems to be the most cost effective attach method. The key attributes is the fillet should be a continuous application that is more than 1 mm wide, more than 50% height up the wall of the component, and greater than 3 ball rows deep.

What Else?: Tests and studies like those described above are under way in many companies, organizations, universities, and other laboratories throughout the world. The findings from such efforts are the necessary steps towards having known processes, materials, and standards to guide the manufacture of lead-free products. With this emphasis reliability test, it would not be surprising if the industry ended up with materials-compliant, high reliability attachment methods for the new high density designs and applications in the electronics industry. There will still be a mystery involved in the testing to verify tin-whisker fixes for quite awhile. Without a more complete knowledge of what drives these whiskers, "accelerated testing" could be confounded. Even the Lone Ranger doesn't have a silver bullet for this one.

N. Risk Assessment and Mitigation of COTS Integration in High Reliability Systems

Provided by Kenneth P Rispoli, Senior Principal Engineer, (Kenneth_P_Rispoli@raytheon.com)

Aaron DerMarderosian Jr., Senior Electrical Engineer II, (Aaron_Dermarderosian_Jr@raytheon.com)

Application of Commercial Off The Shelf (COTS) products in DOD applications became possible with Secretary Perry's initiative of the 1990s, and further driven by the diminishing acquisition demands of the defense industrial sector. In parallel, the commercial sector had an explosion of advance technology driven by the Internet, auto electronics, telecommunication, home entertainment, and computing to name a few. This explosion provided the developers of high reliability systems the opportunity to tap advanced COTS technology for integration

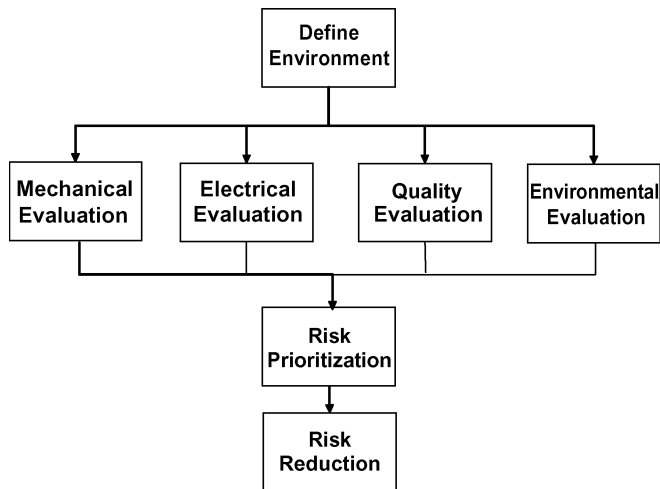


Fig. 15. Risk assessment flow diagram.

into their designs without incurring the cost of design and development. However, application of COTS is not without potential problems, and risk to system reliability and maintainability [171]. Commercial products are designed to less stringent application needs, and rapid introduction of new technology leads to shorter product life cycles. These aspects have to be addressed, weighted, and if gaps exist, mitigated to insure system life and reliability are not compromised. There are many definitions of COTS from components to single boards to modules to system level boxes. However, this paper will define COTS as any electronic, electrical, or mechanical item including firmware and software developed by a supplier for an open market place using industry ‘best practices.’

Risk can be defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on a project’s objectives; in other words, risk is simply the deviation from the expected. A risk assessment flow diagram as shown in Fig. 15 outlines a top down process to identify and prioritize key risks, and then reduce or if possible eliminate system risk altogether [172].

The first step to identify COTS integration risk is to perform a full requirements review to determine critical, non-critical, and requirements that can be mitigated or modified. From here, a full review of the COTS supplier documentation needs to be performed to determine any gaps between product capabilities, and application requirements. Due to the often short life cycle of commercial products, obsolescence needs to be assessed. This review could include the possible insertion of future technology that would provide system enhancements.

Either following or in parallel with the specification to requirements review, a review of past application of similar products, and any experience with the potential supplies, should be conducted. This should include but not be limited to the following.

- Comparison to similar designs to access what worked, and hopefully avoid past failures.
- Lessons learned & team experiences to bring together cross discipline experiences [173].
- Knowledge base to expand beyond the immediate application.

- Trade studies to determine capabilities of the technology available.
- Supplier review & assessment to choose the “best in class”.

At this point in the process, obvious gaps between the proposed product and the design requirement may be detected. The impact of these gaps on critical system performance will need to be assessed with one or more of the following tools.

- COTS integration program plan to control selection, evaluation, acceptance, and life cycle support of COTS.
- COTS supplier assessment scorecard to provide qualitative performance across all disciplines, and functions.
- COTS Assessment Flow Diagram as shown above to provide a top down risk identification process.
- Failure Mode & Effects Analysis (FMEA) provides a systematic approach to identify potential failure, and prioritize failures according to risk. Fig. 16 shows an example FMEA conducted on an RF amplifier for a critical gain requirement.
- Risk Trade Off (RTO) to balance program risk against potential performance gains
- Un-desirable effects (UDE) analysis provides risk ranking based on occurrence.
- Non- Destructive teardown analysis provides cursory product review for possible design risks based on lessons learned, and physics of failure.
- Destructive Physical Analysis (DPA) based on Physics of Failure (PoF) provides additional product design information from subject matter expert review. DPA review can provide insight into product performance, and reliability. As shown in the example DPA results in Fig. 17, workmanship issues associated with die attach material dendrite growth and die corner crack were found with potential long term reliability impact.

Gaps between system requirements and product capabilities can be closed or mitigated by either establishing compliance of the COTS item to the requirement or modification of the COTS item or system environments. If gaps between critical system requirements and product capabilities can not be closed, the product should not be considered for the application. In some cases this might lead to a critical decision point in the process in that there does not exist any commercial product that meets the desired critical requirement. This would require possible system requirement relaxation, or possible design change that would mitigate or isolate the commercial item to a level that is within the products’ capabilities.

To fully analyze the risk associated with the application of COTS items requires the involvement of all the stakeholders. This requires collaboration across electrical, mechanical, reliability, software, test, manufacturing, safety, compliance, and systems engineering. These stakeholders need to work together with the supply chain, program office, and contracts to insure the customer’s objectives are met. The key to the successful design with COTS requires the flow of information, experience, and lessons learned across all these groups. One approach is through Technical Interest Groups (TIG) that can act as a medium for focused technology interchange, and connectivity across business units to gather and disseminate technical knowledge. Because risk may not be limited to a single discipline, Communities of Practice (CoP) can provide a boundary-less vehicle for

Design Function	Potential Failure Mode	Potential Effects of Failure Mode	C	S	Potential Cause of Failure	O	Current Controls	D	RPN	Recommended Action
12.5 db RF Gain	Maximum specified temperature of 50C will be exceeded at maximum system requirement of 70C	Mechanical mounting failure	Yes	3	Differences in package to board TCE	3	ESS	6	54	None
		Loss of mechanical integrity of internal components	Yes	5	Assembly workmanship	5	None	7	175	Perform DPA inspection
		Reduced Mean Time To Failure	Yes	5	Excessive junction temperature	5	Life Prediction Calculated	2	50	None
		Reduced gain	Yes	7	Excessive junction temperature	5	Undetectable	5	175	Perform Thermal Test Analysis

C = Is the component or operation considered critical, key or significant?
 S = Severity of effects of the failure
 O = Probability of failure occurring
 D = Likelihood failure is detected
 RPN = Risk Priority Number

1 = low, 10 = high
 1 = low, 10 = high
 1 = high, 10 = low
 S x O x D

Fig. 16. Example of component level design. FMEA.

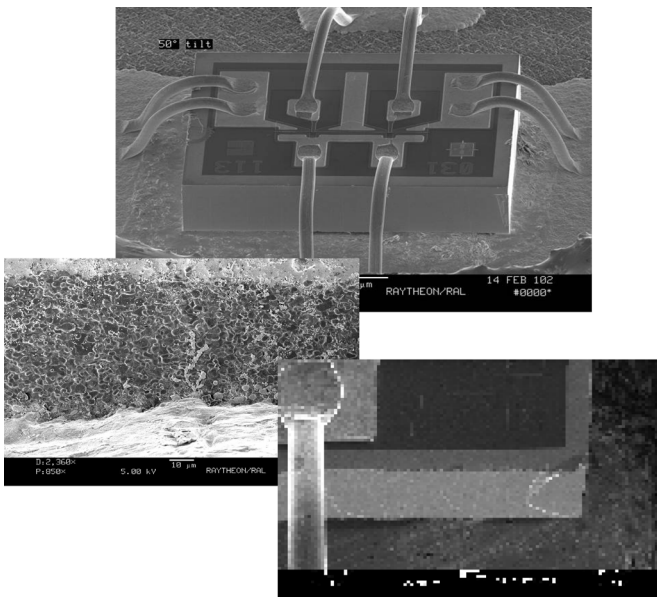


Fig. 17. Example DPA results.

peer-to-peer collaboration, and knowledge sharing. A CoP is similar to a TIG, but aligned by product or core technologies.

In summary, the COTS design integration approach should utilize existing processes with new tools to drive a successful implementation strategy through the application of a COTS management plan together with a robust risk defining tool set.

O. Tin Whiskers: A Long Term RoHS Reliability Problem

Provided by Robert J. Landman, President, H&L Instruments, LLC, North Hampton, NH Senior Member IEEE, (rlandman@hlinstruments.com)

“It ain’t what you don’t know that gets you into trouble. It’s what you know for sure that just ain’t so.”—Mark Twain.

History of the Problem: The first recognition of electrical problems caused by metal whiskering appears to have happened in 1942–43 in aircraft radios made by the Aircraft Radio Corporation in Boonton, New Jersey [174]. Air-spaced variable capacitors were cadmium plated to retard corrosion; then the cadmium plating whiskered, and these whiskers dropped the Q of the tuned circuits to unusably low values. This company’s radios included those used to land under conditions of zero visibility. How many died as a result of these whiskers? As this was during the war, perhaps there were reports, classified at the time, and now perhaps declassified since more than 50 years have passed; does anyone know where to find such?

That the growth of whiskers is not a new phenomenon may be concluded from the examination of undisturbed old equipment. For example, a number of zinc plated details installed in a telephone central office in 1912 were removed for study. Surfaces which had been protected from cleaning operations and from excessive air circulation had numerous whiskers present. Bell Labs learned during the early part of 1948 that “channel filters”, used in carrier telephone systems, were failing, and that Bell eventually traced the problem to whiskers growing from zinc plated steel. (Note: tin plating was not the cause in this case [175].)

NASA Goddard Space Flight Center (GFSC) scientist Dr. Henning Leidecker reports that studies showed that as little as 0.5% lead was effective in lessening tin whisker growth. These studies have been repeated with the same findings. Because many plating shops do not hit the target of lead concentration with high precision, specifications often call for 2% or even 3%,

in order to increase confidence that one will get at least 0.5% [176].

Tin whiskers grow in the absence of lead in solder, and pose a serious reliability risk to electronic assemblies. Tin whiskers have caused system failures in earth and space-based applications, as well as in missile systems. At least three tin whisker-induced short circuits resulted in complete failure of in-orbit commercial satellites. The cause of the side-B failure in Galaxy 4 is highly certain. The cause of the other *side failures* (it takes the failure of both side A and B to kill the satellite) is less certain [177].

Ignorance of the scope of the tin whiskering problem is the simple, sad answer as to why it took NASA GFSC until the 1990s to act on what Bell Labs had clearly published in the 1950s and 1960s.

During a conversation with GFSC scientist Dr. Henning Leidecker, he said, "We were taught the seriousness of this problem by a contractor in 1998, and have continued learning about it since then, and have been sharing what we have collected."

Here is a list of publicly known catastrophic failures resulting from tin whiskers [177].

- 1974—20 Years of Observation—Trans. Inst. Of Metal Finishing
- 1986—Pacemaker FDA Class 1 Recall—Total Failure Crystal Oscillator Short
- 1989—Phoenix Air-to-Air Missile Failures
- 1991—Raytheon Patriot Missile Intermittent Misfire Problems
- 1998—Galaxy IV & VII (PanAmSat)
- 2002—Northrop Grumman Relay Failures—Military Aircraft—approximately 10 years old—failed. Rated at 25 amps/115 Vac/3 phase
- 2005—Millstone Unit 3 Nuclear Reactor Shutdown: Dominion Learns Big Lesson
- 2006—Galaxy IIIIR (PanAmSat)

The space shuttle Challenger exploded in 1986, tragically killing its crew. Congress supplied NASA with the funding for a replacement shuttle: OV-105, Endeavor. NASA started building Endeavor in 1986, almost a decade after the first batch. At least one waiver was granted at the request of a manufacturer. During that decade, OSHA made it more expensive to dispose of tin plating baths that had some lead in them. The contractor, that had won the bidding to make the electronics for NASA was, again, Honeywell (Clearwater, FL). They proposed to *go green* by providing pure tin-plated card guides. NASA's procurement department effectively approved their proposal with their understanding that pure tin coating might grow tin whiskers, but that these whiskers were only theoretical.

During 2006, NASA found some 100 to 300 million tin whiskers growing on Endeavor's card guides, with lengths between 0.2 mm, and 25 mm. There were also whiskers having lengths approaching zero; it is not the case there were NO whiskers with lengths shorter than 0.2 mm. Rather NASA only counted whiskers with a range of lengths between 0.2 mm and 25 mm. The wildly ironic thing is that the card guides are beryllium copper, and never needed any tin plating to protect them from corrosion! They found a guide that was uncoated, and it was perfectly free of any corrosion at all, because the

Be-Cu metal does not corrode, and does not to present a risk of problems by peeling (i.e., shedding conductive chunks of tin onto the electronics). The tin coatings grew whiskers, and they did present a threat of causing short circuits. Clearly, the tin coating failed to satisfy the requirement: no production of conductive debris.

NASA Goddard tin whiskers scientists believe that there was a shorting event induced by a tin whisker while undergoing ground testing in an electronics box made for use in OV-105, but not installed in OV-105. The box failed. The team that maintains the shuttle does not believe there is sufficient evidence to claim that a tin whisker was the cause of the event. This fact illustrates the difficulty of assignment of cause, which is more common than not.

Preventing Whisker-Induced Failures: When using the term *failure*, one must be clear as to what system failed, and in what way it violated its *work requirement*. Violating a work requirement is just as serious a situation as a failure, especially in critical systems such as the space shuttles, nuclear power plants, weapon systems, and medical devices. To be clear, the Shuttle Endeavor (OV-105) works fine, and so *that* system did not fail.

Why did this happen? Why did this NASA approver not know about tin whiskers? The decision to use pure tin and regard whiskering as "only theoretical" was a mistake based on ignorance of the actual threat of whiskering. The NASA approver and contractor were distinguished professionals with long experience in space systems, but they were unaware that tin coatings can grow whiskers. Matte tin coatings of typical thickness usually grow whiskers at a density of some 900 whiskers per square centimeter; or some 14,000 whisker per square centimeter for bright tin on brass. That these cause damage can be rare; it depends on whether there are connectors at sufficient potentials nearby, and whether shorting to these connectors is a problem. Perhaps they *were* correct in this last estimate? None of the shuttles thus far are known to have encountered a whisker-induced problem in flight. *Finding* the damage is rare.

There is another reason. NASA requirements echo the style of requirements used by the military, and by many areas of aerospace. These are directive, of the form 'do this; do not do that,' with no explanations as to what happens if these requirements are contradicted, and no references back to the literature that generated these requirements. NASA has requirements that say to use 3% lead in the tin coating, but they have no pointers to the Bell Labs words that say, "Pure tin coatings have caused entire product lines to fail in service [178]."

So the NASA rep allowed a waiver when asked for it by the manufacturer who wished to optimize *his* process by using pure tin coatings. Probably, the NASA rep had not had experience with tin whisker damage, and did not recognize the very real possibility of this occurring. This style of directing, without any references to reasons, has been costly to NASA [176].

Why are so many people unaware of tin whisker risks? Most people don't care about it, because it hasn't happened to them, not realizing that it is happening to them. Most people address problems that they know they have had before. They do not recognize a steady drizzle of problems caused by metal whiskers. It is hard to *see* whiskers even when whiskers are present.

Do all tin, zinc, or cadmium coatings produce whiskers? Not all of these coatings produce whiskers within the time of use

of the equipment. For example, NASA Goddard's Jay Brusse has what he terms a 'busy box' with a number of tin-plated soldering lugs, each bolted down tightly so there is stress present on part of the lug: only 20% are showing any whiskering at all. Another example: NASA inspected 100 walnut-sized tin plated relays, stored for at least 5 years (no contacting that might rub off whiskers). About 20% were growing whiskers.

No one yet understands how to predict the whiskering probabilities of a given tin coating. The distribution of lengths is close to log-normal, and it is the median value of length that grows at a rate of 0.5 mm to 1.0 mm per year. Leidecker has gotten these values from a number of different reports on experiments dating from the 1950s onward to 2005 (and later). When the tin coating does grow whiskers, and not all do, they may grow only minimal ones [176].

Some whiskers grow faster, some slower. Surface compressive stress seems to play a role, and humidity definitely does. For every datum that is reported about tin whisker growth, it sometimes seems that one can find a report of a contradictory datum. There is a general consensus of opinion among the scientific community that temperature cycling greatly promotes growth, especially cycling above and below the 13.2°C phase-transition temperature of tin. Some find faster growth around room temperature. Leidecker suspects that new whisker growth depends on a cascade of several events, and that these have opposite temperature dependences, and different net impacts, under different circumstances. All other things being equal, they probably grow faster in warmer conditions [176].

Whisker containment is not perfect with conformal coatings, but it is very good. Parylene lasts a few years, and then a tin eruption blows out a divot of it. Elastomers stretch a bit, then crack, and tear. Containment depends in part on inducing Euler buckling [180].

To complicate matters, not all whiskered surfaces cause circuit malfunctions. Size, and geometry can increase risk more than six orders of magnitude. When more than about 100 mV is applied across the metal part of the whisker (i.e., after the tin oxide layer is dielectrically ruptured), then enough current will flow to melt the whisker open, usually within a millisecond or less. Sometimes, this current event is so brief that it escapes being logged as a fault. Other times, the event is able to "latch" an enduring fault (as in alarm circuits), and then the troubleshooter has difficulty finding where the now opened whisker was before the event.

Not all whisker-induced failures can be identified. Very few analysts correctly identify whisker-induced problems. A professional failure analysis can run between \$300 and \$3,000 per job. Almost no broken commercial equipment is ever put through any such analysis. Rather, the failed unit is junked or refurbished without any assignment of the fault. It is characteristically only equipment used in tasks of high importance that gets any analytic attention. Sadly, only a very few analysts are able to correctly recognize whisker induced problems!

Does commercial-grade equipment have this problem? It is typically only the military and space communities that carry out the analysis that is necessary to locate the source of the damage. And then, only a few of the analysts are perceptive as to the real cause.

Not all cases of whisker-induced failures are reported! NASA has logged, in 5 years, 3 to 5 reports per month of tin whisker infestation that required urgent help (almost all reports are from non-NASA sources). Very few manufacturers have allowed NASA to document the problems in detail, or share results publicly due to fear of lost sales, warranty claims, punitive damages, injuries, and embarrassment. There is no desire to share solutions to problems with competitors.

"The hundreds of cases we have documented scale to roughly a few million to a few hundred million cases of whiskering problems over the last fifty years—this seems about right to me," stated NASA's Leidecker [176]. He suspects that about 3% to 30% of electronics systems that are using pure tin plating are growing whiskers, that about 0.5% to 5% of the total are having shorts caused by these whiskers, that about 0.005% to 0.5% of the total are having the cause of these shorts correctly identified, and then about 0.00001% to 0.01% of the total are being publicly named.

The public perception is that there are only a few cases, and that these have happened 'to other folks.' A man operated a computer room in which 75% of the computers blew the fuses in their power supplies in the space of a few hours. It took him several months to trace the cause to zinc whiskers, and during that period those computers were not generating revenue [176]. The whiskers probably had been growing for years beneath the room's raised floor, but hadn't created trouble until a water spill occurred. Air blown into the space between the tiles and the sub floor to dry up the water dislodged the whiskers, which then wafted into the computers through vents in the floor.

Texts that teach newcomers about ways to make systems more reliable do not mention the dangers of whiskering as strongly as they should. A few allude to whiskering, usually as *rare* without distinguishing between *rarely happening*, and *rarely publicly documented*.

A typical company, selling parts with pure tin coatings that are occasionally causing a short, will continue this practice. They will promptly replace any one of their parts that the customer can show has shorted as a result of a whisker. And buyers of these parts will point to this *prompt replace* policy, and to the lack of a publicly documented problem with the use of pure tin coatings, to support the choice of purchasing these relatively inexpensive parts in favor of more expensive parts with whisker-free coatings. No one is charged with tracking injuries or deaths that result from this practice.

Do suppliers give us what we order? If you specify 3% leaded-tin coating, will you be certain that you receive it? NASA and other hi-rel manufacturers find *pure tin coatings* 1.5% to 3% of the time (month to month), even when the contract and Certificate of Compliance say it is to contain a certain percentage of lead. The rate of such findings jumped to 70% for a brief period of time.

There is no prescription for reliably predicting which plated surfaces will grow whiskers, and which will not. Whisker growth is stochastic. Perhaps someday we will learn the controlling parameter(s), and will then be able to apply coatings that are reliably whisker free. Some would say that we now know how to do this: we get stress-free coatings. Leidecker neither agrees, nor disagrees with this remark. He claims that he cannot look at a tin plated surface, make measurements (or

look at production sheets), and make a reliable prediction [176]. In particular, he can't apply a 'stress meter' to the surface.

Are There Mitigations?:

- 1) Apply conformal electrical insulating coatings to block any loose whiskers from shorting electrical conductors/components.
- 2) Apply a 2 mil thick whisker-tough coating which contains whisker growth. When an appropriate coating is used, and is correctly applied everywhere (and does not introduce its own damages), then the risk of shorting can be substantially lowered.
- 3) Re-plate with tin-lead solder, which dissolves any pure tin plating. Corfin Industries, Salem, NH, implemented a robotic hot solder dip (RHSD) for tin whisker mitigation. It is a US Navy-qualified process.
- 4) Ball Grid Array (BGA) reballing for conversion to tin-lead flushes all balls and alloy residue on the pads, and replaces balls with tin/lead solder balls.
- 5) X-Ray Fluorescence (XRF) Analysis, is used to determine lead (Pb) content of termination finishes, and plating thickness.

Tin Deterioration at Low Temperatures: There's another problem with tin called *tin pest*. Tin pest is an autocatalytic, allotropic transformation of the element tin which causes deterioration of tin objects at low temperatures. Tin pest has also been called tin disease, or tin leprosy. It was observed in medieval Europe that the pipes in church pipe organs were affected in cool climates. As soon as the tin began decomposing, the process sped up, and seemed to feed on itself.

At 13.2°C (about 56°F) and below, pure tin transforms from the (silvery, ductile) allotrope of β -modification white tin to brittle, α -modification *grey tin*. Eventually it decomposes into powder, hence the name tin pest. The decomposition will catalyze itself, which is why the reaction seems to speed up once it starts; the mere presence of tin pest leads to more tin pest. Tin objects at low temperatures will simply disintegrate.

The tin crystal has anisotropic coefficients of expansion, so any temperature change generates a compressive stress somewhere that drives tin atoms to travel, then dropping into the lower energy state of a crystal [179]. Tin atoms are itinerant at room temperature, even left to themselves!

Conclusions: For high reliability electronics, such as for NASA, military, aerospace, or medical applications, specify on your equipment *no pure tin, or zinc, or cadmium plating*, or at least try to mitigate whiskers with conformal coatings. Check your incoming materials at the document-level, and use explicit assays. NASA strongly prefers *no pure tin, or zinc, or cadmium* on their equipment. Their rules forbid the use of these materials, and they check their incoming materials at the document-level using explicit assays. They sometimes find that they have one or more of these forbidden materials anyway, despite their rules and checks.

Then, NASA has to decide whether to scrap the delivered equipment, or to take it apart and rebuild it, or to *fly as is*. NASA is working to develop science-based methods for aiding the managers who must make these decisions.

There is a tongue-in-cheek qualification test which all parts manufacturers (such as Analog Devices and National Semiconductor [181]) use to claim that their RoHS parts do not grow tin

whiskers. iNEMI [182] proposed a tin whisker test method in 2003. Since that time, JEDEC [183] has developed a test method which is based largely on the iNEMI proposal. This JEDEC test method passed ballot, and was released in May 2005 as JESD22A121. The JEDEC acceptance criterion, JESD201, was released in March 2006.

JESD201 is a 4,000 hour test. How many hours are in a year? 8,760. This is a guarantee that tin-plated parts will not develop tin whiskers within six months. Does that make you feel good about RoHS reliability in lead-free heart pacemakers? Air bag deployment electronics? Auto braking systems and speed controls? Railroads, airplanes, and air traffic control electronics?

The Joint Boston—New Hampshire—Providence IEEE Reliability Society Chapter has just initiated a project titled *RoHS6 Pushback*. RoHS6 may be technologically feasible for simple boards with simple electronic parts. As the complexity increases, the risks become large. The long term reliability is not assured. The issues and risks need to be quantified and shared.

Unless we discover the magic bullet replacement for 3% lead in tin solder, within the next 5 years we will start to see significant, random, next to impossible to diagnose failures. Reliability in electronics will be a myth.

P. Solutions to Sneak Circuit Analysis (SCA) of Very Large Equipment/System Designs

Provided by Scott Schulman (sschulman@omnicon-group.com)

Project Leader—Systems and Software The Omnicon Group Inc. (www.OmniconGroup.com)

Performing a Sneak Circuit Analysis on a large or complex system has traditionally been a labor intensive task. Because of the sheer cost of the huge amount of time that it typically takes to complete this kind of analysis, this process is often overlooked, or de-prioritized in order to meet schedule, and budgetary constraints. When it is viewed in relation to high cost, high risk, or safety critical applications, this is a process that can help to avoid serious errors that are not a malfunction per se, but rather are undiscovered/unintentional design flaws that may execute an undesired function, or inhibit execution of a desired function. These undesired effects can lead to loss of life/limb, property, or mission failure.

A typical Sneak Circuit analysis would involve a large team of engineers that are intimately familiar with all of the circuitry elements, and the design of the whole system. As more components are added to a design, the labor required to perform the analysis goes up exponentially, as there are more potential unintentional effects with each new circuit pathway added.

After performing many such analyses for our customers with mission and/or safety critical systems, The Omnicon Group developed a unique approach to dealing with this overwhelming task. Using a combination of fourth generation computer languages, databases, simulation and modeling tools, and graphical displays, this daunting man-power extensive undertaking can now be cut down to size. The techniques that we have developed are summarized in the body of this document.

The process begins by performing an initial analysis of the design. In this phase, a list of all of the unique component types is compiled, placing them into one of three major categories:

switch, relay, or diode. In reality, there are generally far more component types in any given design, but The Omnicon Group has found that these components are the one's responsible for Sneak conditions more than 99% of the time. Other components may contribute to failed designs, but these effects are generally limited to failure of the components themselves. As such, these cases are generally handled by a standard failure modes analysis (FMEA/FTA), which we view as a companion to the SCA.

The next step involves writing a software module to simulate the behavior of each specific component type (i.e., single pole/single throw switch, double pole/double throw relay, etc.). This software is not application specific, and may be reused over again on many different efforts. The main consideration in creating the simulation is how the device operates (as designed), along with the circuit connection potential (e.g., single pole/single throw switch, single pole/double throw switch, double pole/single throw switch, etc.). Relays are basically modeled as switches that are automatically activated (no manual interaction), and may be either latching or non-latching (return to "default state") after voltage has been removed.

At this point in the process, all of the components are imported into a database that is tailored for streamlining the circuit simulations and analysis. The database is created from a standard parts net-list. A series of tools is then used to manually apply circuit designations (such as function, for example "firing circuit lockout," or "door safety switch"), and to link each instance of a component to a specific software simulation for that component. The main software application has a set of built in rules that it applies to all simulations to identify potential hazard situations. A Boolean expression generator (custom written to interface to our database format) is then used to specify any custom criteria from the components and states within the database. This allows for easy checking of these hazards during the main part of the simulation. An example of such a custom condition could be 'door command open relay energized while door safety switch is engaged.' These Boolean expressions are then stored in the database.

The heart of this process is a simulation. The simulation works in the following manner.

- The simulation reads all circuit components from the master database (every SCA has its own database, unique to the design being studied).
- Then the simulation builds an internal graphical representation consisting of all of the circuit components, their ports (interconnections), as well as paths to power, and ground.
- It then identifies which components are manual (switches), versus automatic (relays).
- Then it identifies circuit paths that are unidirectional (have a diode limiting current flow to one direction).
- Using the library of component simulation modules, the process then links the simulations to specific instances of each circuit node. This state becomes the simulation default, and the simulation returns to this state after each iteration.
- The simulation manipulates all combinations of manual actions (switch activations). The simulation then recursively walks all of the nodes, applying power, and/or grounding conditions to the rest of the components (as dictated by the states of the manual switches). When the simulation en-

counters a relay that is activated as the result of its coil having a complete path from power to ground, it manipulates the state of the relay. This propagation continues until all components reflect the current state of the system. Using its built-in rules, the simulation then checks for potential problems. It also checks every node for states, and/or conditions specified by the Boolean expression generator. Any problem areas found cause a textual report to be printed out, as well as a graphical representation (picture) of the circuit components/ports/paths.

Following the completion of the simulation, analysts use the error reports and graphical representations of the hazards to perform a manual verification, and determine the criticality of the sneak identified by the tool. Because each error report/graph is unique, the analysts can divide up the investigation as time and staff permits without any potential for overlap. The graphical representations of the circuit focus the analysts' attention directly on the problem area. Using this approach, The Omnicon Group has found that the level of effort required to perform a SCA has been reduced 75% as compared to performing one via more traditional methods.

Q. Design Constraints That Make Software Trustworthy

Provided by Lawrence Bernstein (lbernstein1946@verizon.net)

C.M. Yuhas

Do you lose data when your software system crashes and comes back up again? Too often the answer is yes. Reliable software behavior must be achieved as people come to depend on systems for their livelihoods; and, as with emergency systems, their very lives. Software is fundamental to computerized systems, yet it is rarely discussed as an entity whose quality can be controlled with specific techniques. This technology on which systems are built has itself got a weak theoretical foundation. Until some very difficult questions can be resolved to provide that foundation, constraints on software design can result in a more trustworthy product.

Most current software theory focuses on its static behavior by analysing source listings. There is little theory on its dynamic behavior, and its performance under load. Often we do not know what load to expect. Dr. Vinton Cerf, commonly known as a father of the INTERNET, has remarked that "applications have no idea of what they will need in network resources when they are installed." [184] As a result, we try to avoid serious software problems by over-engineering, and over-testing.

Software engineers cannot ensure that a small change in software will produce only a small change in system performance. Industry practice is to test and retest every time any change is made in the hope of catching the unforeseen consequences of the tinkering. Forbes Magazine pointed out that a three-line change to a 2-million line program caused multiple failures due to a single fault [185]. There is a lesson here. It is software failures which need to be measured. Design constraints that can help software stability need to be codified before we can hope to deliver reliable performance. Instabilities arise in the following circumstances.

- 1) Computations cannot be completed before new data arrive.
- 2) Rounding-off errors build or buffer usage increases to eventually dominate system performance.

- 3) An algorithm embodied in the software is inherently flawed.
- 4) Data become corrupted, and need to be reacquired from the source.

There are six constraints that can be imposed today on software development that will help prevent these circumstances. Though more study of design constraints is needed, that lack is no reason to neglect what can be done.

First Constraint: Software Rejuvenation: The first constraint is to limit the state space in the execution domain. Today's software runs non-periodically, which allows internal states to develop chaotically without bound. Software rejuvenation is a concept that seeks to contain the execution domain by making it periodic. It is an idea that is ready for prime time after ten years of research, and limited use. An application is gracefully terminated, and immediately restarted at a known, clean, internal state. Failure is anticipated, and avoided. One way to describe this is, rather than running a system for one year with all the mysteries that untried time expanses can harbor, run it only one day, 364 times. The software states would be re-initialized each day, process by process, while the system continued to operate. Increasing the rejuvenation period reduces the cost of downtime, but increases overhead. One system collecting on-line billing data operated for two years with no outages on a rejuvenation interval of one week [186].

An internal Bell Laboratories experiment showed the benefits of rejuvenation [186]. A 16,000 line C program with notoriously leaky memory failed after 52 iterations. Seven lines of rejuvenation code with the period set at 15 iterations were added, and the program ran flawlessly. Rejuvenation does not remove bugs; it merely avoids them with incredibly good effect.

The First International Workshop on Software Aging and Rejuvenation met (WoSAR) in November, 2008 [187]. After more than ten years of research work in software aging and rejuvenation, this was the first international event to bring together researchers and practitioners involved with the theoretical and experimental aspects of software aging and rejuvenation. Dr. Kishor Trivedi reported that stochastic analytic models of software rejuvenation for single node, and clusters have been studied for evaluation and optimization showing the importance of this approach. The studies include estimating time-to-resource-exhaustion, for the purpose of model validation, and on-line control of rejuvenation scheduling. Micro-rebooting strategies look promising [188].

Second Constraint: Software Fault Tolerance: If we cannot avoid a failure, then we must constrain the software design so that the system can recover in an orderly way. Each software process or object class should provide special code that recovers when triggered. A software fault tolerant library with a watchdog daemon can be built into the system. When the watchdog detects a problem, it launches the recovery code peculiar to the application software. In connection processing systems, this usually means dropping the connection, but not crashing the system. In administrative applications where keeping the database is key, the recovery system may recover a transaction from a backup data file, or log the event and rebuild the database from the last checkpoint. Designers are constrained to explicitly define the recovery method for each process and object class using a standard library.

Third Constraint: Hire Good People, and Keep Them: This might have been the first constraint because it is so important, but any software shop can adopt the first two constraints as they set about improving the quality of their staff. Hiring good people is not easy. The Bureau of Labor Statistics [189] 2008–9 handbook states, "Computer software engineers are one of the occupations projected to grow the fastest, and add the most new jobs over the 2006–16 decade." They report that there are 507,000 software applications engineers in the US in 2009, and there will be a need for 733,000 by 2016.

One company projects an average of 16 weeks to bring someone up to speed: 4–8 weeks to fill a job, and another 6 to 8 weeks to train the new hire in the ways of the company. This is not news, but the high correlation between defects in the software product and staff churn is chilling.

George Yamamura of Boeing's Space and Defense Systems reports [190] that defects are highly correlated with personnel practices. Groups with 10 or more tasks, and people with 3 or more independent activities, tended to introduce more defects into the final product than those who are more focused. He points out that large changes were more error-prone than small ones, with changes of 100 words of memory or more being considered large. This may have some relationship to the average size of human working memory. The high .918 correlation between defects and personnel turnover rates is telling. When Boeing improved their work environment and development process, they saw 83 percent fewer defects, gained a factor of 2.4 in productivity, improved customer satisfaction, and improved employee moral. Yamamura reported an unheard of 8 percent return rate when group members moved to other projects within Boeing.

Fourth Constraint: Limit the Language Features Used: Most communications software is developed in the C or C++ programming languages. Les Hatton describes the best way to use C and C++ in mission-critical applications [191]. Hatton advocates constraining the use of the language features to achieve reliable software performance, and then goes on to specify instruction by instruction how to do it. He says, "The use of C in safety-related or high integrity systems is not recommended without severe, and automatically enforceable constraints. However, if these are present using the formidable tool support (including the extensive C library), the best available evidence suggests that it is then possible to write software of *at least* as high intrinsic quality and consistency as with other commonly used languages." [191] For example, a detailed analysis of source code from 54 projects showed that once in every 29 lines of code, functions are not declared before they are used.

C is an intermediate language, between high level and machine level. There are dangers when the programmer can drop down to the machine architecture, but with reasonable constraints and limitations on the use of register instructions to those very few key cases dictated by the need to achieve performance goals, C can be used to good effect. The alternative of using a high level language that isolates the programmer from the machine often leads to a mix of assembly language, and high level language code which brings with it all the headaches of managing configuration control, and integrating modules from different code generators. The power of C can be harnessed to assure that source code is well structured. One

important constraint is to use function prototypes, or special object classes for interfaces.

Fifth Constraint: Limit Module Size and Initialize Memory: The optimum module size for the fewest defects is between 300 to 1,000 instructions [192]. Smaller modules lead to too many interfaces, and larger ones are too big for the designer to handle. Structural problems creep into large modules.

All memory should be explicitly initialized before it is used. Memory leak detection tools should be used to make sure that a software process does not grab all available memory for itself, leaving none for other processes. This creates gridlock as the system hangs in a wait state because it cannot process any new data.

Sixth Constraint: Reuse Unchanged: A study of 3000 reused modules showed that changes of as little as 10 percent led to as much as 60 percent rework in the reused module. It is difficult for anyone unfamiliar with a module to alter it, and this often leads to redoing the software rather than reusing it. For that reason, it is best to reuse tested, error-free modules as is.

Conclusion: Software developers know that their systems can exhibit unexpected, strange behavior, including crashes or hangs, when small operational differences are introduced. These may be the result of new data, execution of code in new sequences, or exhaustion of some computer resource such as buffer space, memory, hash function overflow space, or processor time. Fixes and upgrades create their own errors. The fact that the only recourse has been exhaustive re-testing limits the growth of software productivity in enhancements to existing systems and modules. Experienced software managers know to ask ‘What changed?’ when a system that has been performing reliably suddenly and catastrophically fails. Under current methods of software production, systems are conditionally stable only for a particular set of input, and a particular configuration.

The point is that feedback control theory must be the watchword of software professionals if trustworthy software systems are to be a reality. One way to do this is to constrain the dynamic behavior of software by following design rules. The problem is that we do not have the all rules we need. Even NASA, which can create the best software in the world, must admit to eleven mission failures due to software defects. That is not good enough.

R. Malicious Code

Provided by W. Eric Wong (ewong@utdallas.edu)

Vidroha Debroy (vxd024000@utdallas.edu)

Department of Computer Science, University of Texas at Dallas

Malicious code is as big a problem today as it ever was, if not larger still. Software is becoming increasingly more complex; and many software systems themselves do not operate in isolation, but rather are connected, and in fact sometimes dependent on other systems. An attack on a software system therefore is a potential attack on any other system that it may interact with, which further magnifies the damage. Many approaches have been proposed to deal with malicious code, and its adverse effects; and these approaches have all met with varying degrees

of success. A large part of the problem is that prevention & resolution strategies are always a step behind the creation, and rapid deployment of malicious code. Each manifestation of malicious code usually requires its own fix, and therefore there is no miracle cure that can help detect and prevent, if not nullify, all malicious code. To be able to analyze any piece of software, and deem it free of all malicious code, is as difficult as any other un-decidable problem. Now that we are aware of what we cannot do, let us try to briefly describe malicious code in general so that we can address what it is that we can do.

“Malicious code is any code added, changed, or removed from a software system to intentionally cause harm or subvert the system’s intended function.” [193]. It is however important to acknowledge that, when fighting malicious code, we care not of its intention, but rather of its effect on the software. Code inserted with the most benign of intentions can have the most malicious of effects. Take, for example, programmer negligence that manifests itself in the form of a buffer overflow. Previously, some of the more important sources of malicious code were third party renovation and remediation, off the shelf commercial/non-commercial systems that may spread pre-existing malicious code, and disgruntled employees/contractors, or anyone else that might have access and the ability to insert malicious code into the system. However, with the popularity of the Internet, and the growing inter-connectivity of computers, systems are vulnerable to attacks, with or without human intervention, from just about anywhere regardless of physical distance or connectivity. Due to such connectivity, an attack can be propagated to a large number of machines in a relatively small amount of time, which may in turn propagate the attack to other machines causing a chain reaction. This ripple effect makes it equally as difficult to re-trace the attack back to its source, and there is no reason to believe it shall be easier to do so in the near future.

Several classifications exist to help narrow down the type of malicious code that one might be dealing with. The general categorization of malicious code has been along the lines of worms, viruses, Trojan horses, time bombs, backdoors, etc. [194]. The literature on malicious code has several definitions and examples of each category. Further classification might be based on the mode of propagation, the nature of the attack, the portion of the system targeted, etc. For example, the presence of malicious code may cause different levels of damage to the typical operations of a system, such as disruption of a non-critical subsystem, disruption of a critical subsystem, crashing of the entire system, granting unauthorized access, re-directing sensitive data, deleting sensitive data, etc. Risk-based models exist that try to decide on an appropriate course of action based on risk evaluations for each category. Identification of low or no risk components allows concentration on essential, high risk components. Furthermore, a methodology that indicates application areas that are prone to attacks allows for selective analysis of such areas based on their vulnerability. A combination of these models might cause a tradeoff between areas with high proneness but low risk, and those of high risk but low proneness. However, if there are areas of high risk and high proneness, then that is where the maximum of our efforts should go to handle malicious code. Typically, these areas consist of only a small per-

centage of the entire system. Intense effort focused on such areas will pay the largest dividends.

Malicious code is quite hard to test for. Let us first assume that we are developing a piece of software, and one of our disgruntled programmers inserts a piece of malicious code (such as a time bomb) into it. This code does not cause the software to deviate from its specification in any way for a pre-determined amount of time, or until a counter variable reaches a certain value. No test case that checks to see if an output matches an expected output will be able to detect such malicious code as its effects are unobservable, at least for the time being. Given that we cannot detect the effect of the code, a test case would have to be able to detect the actual presence of the malicious code for us to even know that it exists in our software. Alternatively, we may be able to simulate the passing of system time, or increment each counter variable present to its maximum value to detect the time bomb. However, each of these requirements would require a massive overhead to design and execute a large number of test cases that might possibly reveal the inserted malicious code. It should therefore come as no surprise to us that so many vulnerabilities of software to attacks are exposed well after the software has been tested. That being said, it is also useful to point out the inherent similarities that exist between malicious code detection, and fault localization and debugging. Each area that might come under attack can be assigned a numerical score to evaluate its risk. Therefore, we can impose an order in which to test various areas, and have a rough idea of how much we want to test them based on their numerical score. This is similar to fault localization where statements are ranked in order of their suspiciousness (computed by some heuristic [195], [196]) such that statements with higher suspiciousness are examined first. This kind of analysis is also very similar to the analysis of safety, and/or security critical systems, such as nuclear power plants, or flight controller software. In the case of such safety dependent systems, a software hazards analysis is often done to identify failure modes that could lead to an unsafe state [197]. Finding and eliminating malicious code at the source level has the overwhelming advantage that no damage is done to the data or the system, with the exception of any damage incurred while detecting the malicious code.

Several approaches do exist that perform various kinds of analyses on source code, or on the corresponding executable. Some rely on structural features of executables that are likely to indicate the presence of inserted malicious code. The underlying premise is that typical application programs are compiled into one binary, homogeneous from beginning to end with respect to certain structural features; any disruption of this homogeneity is a strong indication that the binary has been tampered with [198]. Others have employed data-mining techniques [199] to identify patterns to detect malicious binaries, and machine learning techniques such as support vector machines [200] to detect computer viruses. A large chunk of the research work on malicious code detection focuses on static analysis of the code. Static analysis deals with examining program code to determine properties without actually executing any of the code in question. In [201], the approach to detect malicious code is based on program slicing. High-risk patterns are defined, and then used as the

basis of a forward and backward static program slice. In [202], static analysis techniques are applied to binary code. First, the binary code is translated into an intermediate form, then the intermediate form is abstracted through flow-based analysis as various relevant graphs, and finally these graphs are checked against security policies. However, static analysis techniques have some inherent limitations in that they make certain assumptions that could be un-checkable statically, such as behavior with respect to array bounds, and pointer aliasing. Some such limitations are pointed out in [203] where it is demonstrated that static analysis techniques alone might no longer be sufficient to identify malware. However, relatively little work has been done on utilizing dynamic analysis either alone, or in conjunction with static analysis, to effectively detect malicious code.

Dynamic analysis aims to test and evaluate a program by actual execution of code in real time, quite possibly with some input. Dynamic analysis allows us to artificially create situations where the software is more likely to fail, and thereby assess how well our program does what it is supposed to do practically as opposed to theoretically. It is true that static analysis holds some advantage over dynamic analysis. First, static analysis does not require any overhead in terms of test case execution, and test case processing. Second, any results provided by static analysis hold invariantly, and are test case independent. The results of dynamic analysis can in some cases be very closely linked to the choice of test cases employed in one's suite. However, dynamic analysis using dynamic slicing can reveal program properties in terms of program behavior that cannot be revealed by static analysis alone. Some malicious patterns might exist that cannot be exposed by static analysis techniques, but might be revealed by one simple execution. All things being equal, the solution is fairly obvious: static analysis techniques and dynamic analysis techniques must work together in tandem. The amount of each analysis, and the depth of the analysis, would of course depend on the resources available. In [204], an automatic malicious code analysis system is proposed that tries to integrate the advantages of static and dynamic analysis, as well as that of network behavior analysis. Such techniques are likely to prove very useful in the detection of malicious code as they take into account more than what can be done by any singleton approach. The application of combined static and dynamic analysis techniques to software is expected to be a rich area of research for some time to come.

While the aforementioned deals with analysis of the code to identify malicious code, there exist other techniques to deal with it. A host can also protect itself from malicious code by re-writing the code, rendering it harmless, monitoring the code and stopping it before it does any harm, and auditing the code and taking appropriate policing action if the code does do some harm [193]. Techniques such as appropriate security policies, solid encryption, code-signing, etc., are also fairly popular. Of late, another consideration is that most malicious code in large scale software systems is placed by insiders with access to code. The field of biometrics analyzes characteristics and traits of personnel, and this information is used to evaluate how much access they should have to critical portions of a system. However, this

approach is less along the lines of detecting malicious code, and more along the lines of detecting malicious coders.

Finally, no discussion could be considered complete without at least talking about some of the major obstacles and concerns regarding malicious code today.

- 1) To develop new models, and extend current models to detect malicious code that takes into account both static and dynamic analysis techniques, and to formulate the model such that it is cost effective and highly accurate.
- 2) To develop better approaches that allow for tolerance of malicious code. Take steps to avoid system failure in the presence of malicious code such that its malicious effect can be mitigated, and its propagation arrested.
- 3) To develop lightweight techniques that can dynamically update a system such that it is not affected by the same attack again.
- 4) To develop suitable testing criteria and test case generation techniques for testing with the intent of revealing malicious code.

These are expected to be the key areas of research interest in the field of malicious code prevention, detection, and handling for some time to come.

S. Preparing the Ground for Next Generation Software Engineering

Provided by Don O'Neill (ONeillDon@aol.com)

Former President

Center for National Software Studies

State of the Industry: The May 2005 Report of the 2nd National Software Summit (NSS2) entitled "Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness" [205] lays out a ten-year concept plan with the vision of "Achieving the ability to routinely develop trustworthy software products and systems, while ensuring the continued competitiveness of the U.S. software industry." The plan includes 11 significant initiatives within four major program areas:

- 1) Improving Software Trustworthiness
- 2) Educating and Fielding the Software Workforce
- 3) Re-Energizing Software Research and Development
- 4) Encouraging Innovation Within the U.S. Software Industry

New Issues, and Challenges: New issues are now emerging surrounding the production, fielding, and operation of net-centric systems of systems that are

- 1) essential to the competitiveness and security of the nation's critical infrastructure,
- 2) essential to the defense and security of the Global Information Grid, and
- 3) essential to the offense and security of Cyber Power strategies.

Unclaimed Benefits, and Unmet Needs: However, there remain unclaimed benefits, and unmet needs stemming from earlier neglect [4]. The immediate goal of practical Next Generation Software Engineering is to drive systems and software engineering to do *more with less*. . . *fast*. Four practical objectives are identified to advance the goal using smart, trusted technologies:

- 1) drive user domain awareness;
- 2) simplify, and produce systems and software using a shortened development life cycle;

- 3) compose and field trustworthy applications and systems from parts;
- 4) compose and operate resilient systems of systems from systems [207].

More specifically:

- 1) *Driving user domain awareness* calls for synthesizing and integrating mission, systems, software, and user need; improving user domain awareness maturity, and conducting user domain awareness assessments; and exploiting NGSE technology through interactive virtual user experience and simulation.
- 2) *Simplifying and producing systems and software using a shortened development life cycle* calls for eliminating bottlenecks through automation of labor-intensive activities; accelerating delivery through Wiki-based requirements, incremental development, and Agile approaches; exploiting NGSE technology through formality in requirements expression, and smart compilers; and measuring speed, and trustworthiness [206].
- 3) *Composing and fielding trustworthy applications and systems from parts* calls for managing rapid release through aspect-based commitment management, fact-based aspect and attribute assurance, and real-time risk management; focusing on supplier assurance through process maturity, global supply chain management, and configuration management; exploiting NGSE technology through attribute-based architecture, smart middleware, interoperability, intrusion detection, intrusion protection, and intrusion tolerance; and measuring frequency of release, and trustworthiness [206].
- 4) *Composing and operating resilient systems of systems from systems* calls for exercising control before, during, and after adversity; focusing on situation awareness through intelligent middlemen and information sharing; exploiting NGSE technology through coordinated recovery time objectives, distributed supervisory control, and operation sensing and monitoring; and measuring control, and resilience [207].

In managing the investment needed to meet these objectives, capability portfolio investments are best organized by management, process, and engineering. In this way, user domain awareness, shortened life cycle, systems from parts, and systems of system from systems provide a natural spiral of incremental activities where current work in progress systematically builds on preceding work accomplished in multiple dimensions. The manner by which a community of interest addresses these practical Next Generation Software Engineering objectives is influenced by the domain engineering paradigms, management and engineering processes, fielding and operating practices, government regulations, and public expectation to which it responds.

Conclusion: Driving user domain awareness towards more harmonious cooperation among people and machines in systems acquisition is an imperative. Without this awareness throughout the life cycle, and across the functional domains of acquisition management, program management, systems engineering, and software engineering, the gap between user expectation and user satisfaction will continue to grow, and mission execution will suffer. With this awareness, user engineering, software engineering, and systems engineering will be better aligned; the synergy between user considerations, and software will

be better expressed in Next Generation Software Engineering approaches; and the intersectional innovation resulting from cross discipline clash will impact systems acquisition, and the missions it supports.

T. Software Security Engineering: A Key Discipline for Project Managers

Provided by Julia H. Allen (jha@sei.cmu.edu), senior member of the technical staff within the CERT Program at the Software Engineering Institute (SEI).

Sean Barnum, Principal Consultant at Cigital and technical lead for their federal services practice.

Robert J. Ellison, senior member of the technical staff in the Secure Software and Systems Group within the CERT Program at the SEI.

Gary McGraw, CTO of Cigital, Inc

Nancy R. Mead, senior member of the technical staff in the Secure Software and Systems Group within the CERT Program at the SEI.

Material from this article has been taken from the preface and Chapter 8 from the book, SOFTWARE SECURITY ENGINEERING [978-0-321-50917-8]. 2008 Pearson Education. Reproduced by permission of Pearson Education, Inc.

The goal of software security engineering is to build better, defect-free software. Resources are now available that provide software project managers with sound practices that they can evaluate and selectively adopt to help reshape their own development practices. Software developed and assembled using these practices should contain significantly fewer exploitable weaknesses.

“Software is ubiquitous. Many of the products, services, and processes organizations use and offer are highly dependent on software to handle the sensitive and high-value data on which people’s privacy, livelihoods, and very lives depend. National security—and by extension citizens’ personal safety—relies on increasingly complex, interconnected, software-intensive information systems—systems that in many cases use the Internet or Internet-exposed private networks as their means for communication and transporting data” [212].

“Dependence on information technology makes software security a key element of business continuity, disaster recovery, incident response, and national security. Software vulnerabilities can jeopardize intellectual property, consumer trust, business operations and services, and a broad spectrum of critical applications and infrastructures, including everything from process control systems to commercial application products” [212]. And in today’s operational environment, software is under an increasing quantity and complexity of attack.

“The integrity of critical digital assets (systems, networks, applications, and information) depends on the reliability and security of the software that enables and controls those assets. However, business leaders and informed consumers have growing concerns about the scarcity of practitioners with requisite competencies to address software security [208] They have concerns about suppliers’ capabilities to build and deliver secure software that they can use with confidence and without fear of compromise. Application software is the primary gateway to sensitive information. According to the Deloitte survey of 169 major global financial institutions, *2007 Global Security Survey: The*

Shifting Security Paradigm [209], current application software countermeasures are no longer adequate. In the survey, Gartner identifies application security as the number one issue for chief information officers (CIO)” [212].

“The absence of security discipline in today’s software development practices often produces software with exploitable weaknesses. Security-enhanced processes and practices—and the skilled people to manage them and perform them—are required to build software that can be trusted to operate more securely than software being used today” [212]. Bridging the capability gap will require addressing today’s shortage in both practitioners skilled in how to execute software security practices, and managers who have the ability to understand, select, and direct their application.

“That said, there is an economic counter-argument, or at least the perception of one. Some business leaders and project managers believe that developing secure software slows the process, and adds to the cost, while not offering any apparent advantage. In many cases, when the decision reduces to ‘ship now,’ or ‘be secure and ship later,’ ‘ship now’ is almost always the choice made by those who control the money, but have no idea of the risks. Information to combat this argument, including how software security can potentially reduce cost and schedule,” [212] is becoming available based on earlier work in software quality, and the benefits of detecting software defects early in the life cycle, along with documented experiences such as Microsoft’s Security Development Lifecycle.

The Goal of Software Security Engineering: To address these challenges effectively, it is important that software development leaders are familiar with, and competent in the discipline of software security engineering. “Software security engineering is using practices, processes, tools, and techniques that enable you to address security issues in every phase of the software development life cycle (SDLC). Software that is developed with security in mind is typically more resistant to both intentional attack, and unintentional failures. One view of secure software is software that is engineered “so that it continues to function correctly under malicious attack” [210], and is able to recognize, resist, tolerate, and recover from events that intentionally threaten its dependability. Broader views can overlap with software security (for example, software safety, reliability, and fault tolerance). These include:

- proper functioning in the face of unintentional failures or accidents,
- inadvertent misuse and abuse, and
- reducing software defects and weaknesses to the greatest extent possible regardless of their cause” [212].

“The goal of software security engineering is to build better, defect-free software. Software-intensive systems that are constructed using more securely developed software are better able to

- continue operating correctly in the presence of most attacks by either resisting the exploitation of weaknesses in the software by attackers or tolerating the failures that result from such exploits
- limit the damage resulting from any failures caused by attack-triggered faults that the software was unable to resist or tolerate and recover as quickly as possible from those failures” [212].

Software Security Practices: “No single practice offers a universal silver bullet for software security. Software security engineering provides software project managers with a variety of sound practices and resources that they can evaluate and selectively adopt to help reshape their own development practices. The objective is to increase the security and dependability of the software produced by these practices, both during its development and its operation.”

It is the responsibility of the software development manager to leverage available guidance in the “identification and comparison of potential new practices that can be adapted to augment a project’s current software development practices, greatly increasing the likelihood of producing more secure software and meeting specified security requirements. As one example, assurance cases can be used to assert and specify desired security properties, including the extent to which security practices have been successful in satisfying security requirements” [212].

“Software developed and assembled using software security practices should contain significantly fewer exploitable weaknesses. Such software can then be relied on to more capably recognize, resist or tolerate, and recover from attacks and thus function more securely in an operational environment. Project managers responsible for ensuring that software and systems adequately address their security requirements throughout the SDLC can review, select, and tailor guidance from” resources such as the Build Security In (BSI) Web site [213], and the recently published book *Software Security Engineering: A Guide for Project Managers* [212].

Five key principles of software security engineering are as follows [212].

- 1) “Software security is about more than eliminating vulnerabilities, and conducting penetration tests. Project managers need to take a systematic approach to incorporate the sound software security practices into their development processes.” Examples include security requirements elicitation, attack pattern and misuse/abuse case definition, architectural risk analysis, secure coding and code analysis, and risk-based security testing.
- 2) “Network security mechanisms and IT infrastructure security services do not sufficiently protect application software from security risks.”
- 3) “Software security initiatives should follow a risk management approach to identify priorities”, understanding that software security risks will change throughout the development lifecycle. Risk management reviews and actions are conducted during each phase of the SDLC.
- 4) “Developing secure software depends on understanding the operational context in which it will be used.” This context includes conducting end-to-end analysis of cross-system work processes, working to contain and recover from failures using lessons learned from business continuity, and exploring failure analysis and mitigation to deal with system and system of system complexity.
- 5) “Project managers and software engineers need to learn to think like an attacker in order to address the range of things that software should *not* do and how software can better resist, tolerate, and recover when under attack.” The use of attack patterns and misuse/abuse cases throughout the SDLC encourages this perspective.

Two Key Resources: In May 2008, Addison-Wesley published the book *Software Security Engineering: A Guide for Project Managers* [212] under both their *Software Security Series*, and their *SEI Series in Software Engineering*. This book explores software security engineering from the project manager’s perspective, offering valuable contextual explanations for software security, descriptions of a varied set of potential practices and resources available, and guidance for selecting and deploying them appropriately. This book can serve as a referential resource for software development leaders looking to get a handle on software security.

“Since 2004, the U.S. Department of Homeland Security Software Assurance Program has sponsored development for the BSI Web site [213], which is one of the significant resources used in developing *Software Security Engineering*. BSI content is based on the principle that software security is fundamentally a software engineering problem, and must be managed in a systematic way throughout the SDLC” [212].

“BSI contains and links to a broad range of information about sound practices, tools, guidelines, rules, principles, and other knowledge to help project managers deploy software security practices and build secure and reliable software. Contributing authors to *Software Security Engineering* [212] and the articles appearing on the BSI site [213] include senior staff from the Carnegie Mellon Software Engineering Institute (SEI) and Cigital, Inc., as well as other experienced software and security professionals” [212].

Readers can consult BSI for additional details, ongoing research results, and information about related Web sites, books, and articles.

Start the Journey: “As software and security professionals, we will never be able to get ahead of the game by addressing security solely as an operational issue. Attackers are creative, ingenious, and increasingly motivated by financial gain. They have been learning how to exploit software for several decades; the same is not true for software engineers, and we need to change this. Given the extent to which our nations, our economies, our businesses, and our families rely on software to sustain and improve our quality of life, we must make significant progress in putting higher quality and more secure software into production.” [212] The practices described in *Software Security Engineering*, and on the (BSI) Web site serve as a useful starting point.

“Each project manager needs to carefully consider the knowledge, skills, and competencies of their development team, their organizational culture’s tolerance (and attention span) for change, and the degree to which sponsoring executives have bought in (a prerequisite for sustaining any improvement initiative). In some cases, it may be best to start with secure software coding and testing practices given that these are the most mature, have a fair level of automated support, and can demonstrate some early successes, providing visible benefit to help software security efforts gain support and build momentum. On the other hand, secure software requirements engineering and architecture and design practices offer opportunities to address more substantive root cause issues early in the life cycle that if left unaddressed will show up in code and test. Practice selection and tailoring are specific to each

organization and project based on objectives, constraints, and the criticality of the software under development” [212].

“Project managers and software engineers need to better understand what constitutes secure software and develop their skills to think like an attacker so this mindset can be applied throughout the SDLC. The above resources describe practices to get this ball rolling, such as attack patterns and assurance cases. Alternatively, if you have access to experienced security analysts, adding a few of them to your development team can get this jump started” [212].

“Two of the key project management practices are (1) defining and deploying a risk management framework to help inform practice selection and determine where best to devote scarce resources and (2) identifying how best to integrate software security practices into the organization’s current software development life cycle” [212].

John Steven states [211]

“Don’t demand teams to begin conducting every activity on day one. Slowly introduce the simplest activities first, then iterate.

[Have] patience. It will take at least three to five years to create a working, evolving software security machine. Initial organization-wide successes can be shown within a year. Use that time to obtain more buy-in and a bigger budget.”

“Clearly there is no one-size-fits-all approach. Project managers and their teams need to think through the choices, define their tradeoff and decision criteria, learn as they go, and understand that this effort requires continuous refinement and improvement” [212].

U. Some Progress in Software Testing Technology

Provided by Phillip A. Laplante (plaplante@gv.psu.edu), Robert Bucholz, and Albert Elcock, Penn State

Several important applied software testing methodologies have been developed and validated through experimentation by our research group. For each of these technologies, we describe the current status of the projects, usable results, limitations of the work, and future research possibilities.

Estimating Total Software Defects Using Capture-Recapture Models: Used by software engineers since the 1970s to estimate the number of defects in software code, the capture-recapture method was first proposed by Laplace in 1786 [214] for biological populations. The model can be described by the following scenario. Suppose a ranger wishes to estimate the number of wolves in his park. He captures, tags, and releases as many wolves as possible during a fixed period of time called a “capture event”. After the event, the wolves are released, and they redistribute throughout the park. The ranger then conducts a second capture event. Suppose that n_1 , and n_2 wolves are captured during the first, and second events respectively; and m of those wolves are common to both capture events (as determined by the tags). Then the total number of wolves, N , can be estimated using the Lincoln-Peterson Estimator [215],

$$N = n_1 \cdot n_2 / m \quad (1)$$

Of course, in between the first and second capture events wolves are born and die so that the population is never constant. And this approach does not address what to do if a wolf is captured more than once in a given event. But N still represents a useful estimator of the population.

In 1972, Harlan Mills proposed deliberately planting n_1 defects in software under test, conducting a code inspection (which uncovers n_2 defects), identifying the m duplicates, and then using (1) to predict the total number of defects present [216]. Instead of seeding deliberate errors, Eick proposed using two inspectors to inspect the same code (finding n_1 , and n_2 defects, respectively), identifying the m common defects found, and then estimating total defects using (1) [217].

A problem with both of these approaches, however, is that different inspectors do not have identical abilities in finding defects, which might cause one type of defect to be over-represented, and another under-represented. Further, once the software has entered the post-inspection lifecycle, it may be impractical to continuously re-inspect the software after each change.

We have been experimenting with an alternative capture-recapture model employing user reported defects entered into a bug repository to estimate the total number of defects that exist in the software. By harvesting user reported defects, dynamic estimates of software defects contained in each release can be made. We have validated this approach with several mature open-source software projects.

Our methodology utilizes the errors reported by users into a defect database or bug repository. To obtain an estimate, the first n_1 unduplicated defects are tagged, representing the first capture event. The next n_2 defects reported in the repository represent the second capture event. The m duplicate entries between the two events are then identified. Then the total number of defects in the software is estimated using (1). Because we do not have the limitations of capturing wild animals over some fixed period of time, it is convenient to set the size of the first and second capture events (the number of defects counted) to be equal.

But what is an appropriate size for the ideal capture, and recapture events? We have found that the ideal population size is based on a defect’s probability of having a duplicate reported within the same release. For the open source defect management system Bugzilla project, we found the ideal capture size to be between 30 and 40 unique defects. This situation can be seen in Table I.

We validated this technique, and obtained similar results on several other open source projects, and one closed source projects.

Our capture-recapture model for open and closed source bug repositories has some limitations.

- A sufficient number of defects need to be reported in both the first, and second capture events; and there must be duplicate defects. More work is needed to determine appropriate necessary and sufficient conditions.
- The predictive model does not take into account defect severity. Additional research and experimentation is needed to see if the technique will work with defects sorted by severity (in essence estimating the population of wolves, rabbits, foxes, squirrels, etc.)
- Certain defects are more likely to appear as duplicates because they are critical or annoying. The model’s sensitivity to these factors needs to be further investigated.

TABLE I
CAPTURE-RECAPTURE POPULATIONS CONSTRAINED FROM 30 THROUGH 40 DEFECTS

Release	Capture event size	Number of duplicates found	Predicted Defects	Total Defects Reported	Estimation Error
2.14	40	7	228.5	215	0.06
2.16	30	6	150	199	0.25
2.18	35	4	306.25	256	0.19
2.19	30	3	300	256	0.17
2.20	35	2	612.5	557	0.09
2.22	30	5	180	151	0.19

- Because some errors are easier to find than others, what is the effect on predictive capability?
- Data collection was manual, and difficult. Users notoriously are inconsistent in the way they report errors, making the identification of duplicates (which is crucial to our technique) very challenging. This problem may be mitigated with automated tools, and we have begun to build and test such a tool. But more work is needed to perfect these tools.

Finally, our validation experiments were conducted on a limited number of projects. This promising technique needs to be tested against more, and varied project types.

Testing Without Requirements: Open source software is software that is available in public repositories for use by anyone provided that the provisions of a license are followed. Open source software is increasingly being used in industry, and even critical infrastructure systems, both to build software, and to embed within the software. However, there is little evidence that most open source software is tested, in the traditional sense, against a set of rigorous requirements. In fact, for most open source software, no requirements specification exists. Then how can one verify this software rigorously? The solution is to create a set of ‘behavioral requirements’ using available artifacts to document implemented product features, as well as expected behavior. The behavioral requirements specification, which looks much like a standard software requirements specification, is used as a basis for traditional software testing.

Since 2006, more than 85 open source projects have been tested using a methodology developed by Elcock & Laplante [218]. In fact, in many cases, significant errors were found, reported, and confirmed by open source communities. Because our technique reverse engineers software specifications, it also can be used with close source (commercial) software when the existing software specification is known to be incomplete, out-of-version, or incorrect in some way.

The approach to constructing the behavioral specification is a deductive one based on available information for the software application. This information is often found in open source repositories including

- software requirements or software design documents, even if incomplete, out-of-version, or known to be incorrect;
- user manuals;
- help files;
- release notes;
- bug reports;
- support requests;

- application forums;
- experimentation with, and use of the application under test; and
- ephemera at the application’s site or elsewhere.

Having collected and organized all available information and artifacts, best practices are then used to write the behavioral specification. Guidelines found in IEEE Standard 830–1998, *Recommended Practice for Software Requirements Specifications* [219] can be used, for example. The system is then tested using the behavioral specification, and traditional testing approaches.

When testing the software using the behavioral specification, it can be expected that some test cases will fail. The problem then is determining whether the test case has been incorrectly implemented, a true error has been uncovered, or if there is a defect in the reconstituted specification. Resolving this situation requires repeated retesting, re-examination of the specification, and meticulous documentation [218].

While this methodology has been validated on many small open source projects, further validation is required with larger projects and closed legacy systems. It would also be desirable to develop tools to automatically generate the behavioral specification document.

Bug Fix Assignment: Another challenging problem, which has received little attention, is that of assigning reported errors to maintenance engineers for repair according to an appropriate scheduling algorithm. The order in which errors are fixed matters because users, managers, maintenance engineers, and project sponsors all may have different priorities, and resource constraints. Several different repair assignment policies can be used along with appropriate reward mechanisms including

- first come first served (FCFS),
- priority fixing (highest priority bugs are fixed first),
- separation of concerns (bugs are clustered and repaired according to functionality),
- random assignment,
- clustering by related problem (errors are grouped together based on their behavior),
- effort assignment (more difficult or easier problems are dealt with first), and
- intelligent assignment (using any of several possible artificial intelligence schemes).

In addition, the behavior of maintenance engineers can be affected by the reward mechanisms that are used. In a true case, for example, software maintenance engineer bonuses depended

TABLE II
MANAGEMENT QUALITY GOAL, SUGGESTED METRIC(S), AND EMERGENT NEGATIVE MAINTAINER BEHAVIOR(S) FOR VARIOUS ERROR RESOLUTION POLICIES [220]

Policy	Management Goal	Suggested metric(s)	Possible negative maintainer behavior (s)
FCFS	Fairness	<ul style="list-style-type: none"> Number of errors resolved per time period 	<ul style="list-style-type: none"> Modification of time stamps Queue jumping Forced "hurry up" periods Careless rushing
Priority	"Important" errors get fixed sooner	<ul style="list-style-type: none"> Some linear combination of errors resolved and weights for each priority class 	<ul style="list-style-type: none"> Downgrading of serious errors Upgrading of less serious errors Customer coercion
Separation of concerns	Right person(s) to resolve each error	<ul style="list-style-type: none"> Number of errors resolved per individual or group 	<ul style="list-style-type: none"> Unhealthy competition Turf battles
Random	Not recommended	<ul style="list-style-type: none"> None suggested 	<ul style="list-style-type: none"> None Suggested
Clustering	Optimization of focus	<ul style="list-style-type: none"> Median time to resolve 	<ul style="list-style-type: none"> Careless rushing
Effort	Controlling maintainer resource allocation	<ul style="list-style-type: none"> Median time to resolve Effort based 	<ul style="list-style-type: none"> Careless rushing Effort mis-estimation
Intelligent	None suggested	<ul style="list-style-type: none"> Dependent on assignment logic 	<ul style="list-style-type: none"> None suggested

on reducing the mean time from 'new' to 'closed' for open problem reports for certain types of reported errors. Unfortunately, bugs could be 'closed' by re-labeling them as 'user misunderstanding,' 'to be fixed in next release,' or by downgrading the seriousness of the bug. The effect was that, while bonuses increased, customer satisfaction did not [220].

We used simulations to observe the effects of assignment policy on error backlog and repair time to help inform our understanding of resultant behavior on the part of managers and maintenance engineers. Table II summarizes some relevant issues in bug repair assignment policy, management goal, possible metrics to be used, and potential negative behaviors that may emerge on the part of maintenance engineers.

One area that has received some attention is the use of automated algorithms with machine learning to make repair assignments. In any case, more studies with respect to the appropriate criteria for selecting assignment policy, reward mechanisms, and management goals need to be undertaken.

V. Communications Network Reliability

Provided by John Healy, (johnhealy@verizon.net)

Communications is one of the primary sectors of the Critical Infrastructure Protection program aimed at assuring the reliability and security of vulnerable, interconnected infrastructures of the United States. Communications network reliability, a joint industry/government initiative, is the focal point for maintaining and improving the reliability of communications services. The focus on communications network reliability began in 1991 after several catastrophic network failures of the signaling network that resulted in major metropolitan areas, including Washington DC for about 8 hours, losing the ability to process telephone calls. These failures resulted in the Federal Communications Commission chartering the Network Reliability Council (NRC), a federal advisory committee composed

of high level executives from each of the major telecommunications companies [221]. One of the recommendations coming out of the NRC was the need for ongoing data collection of information on major network failures. As a result, the FCC instituted network outage reporting. Whenever a large number of customers could not make phone calls for at least 30 minutes, an outage report was generated, and sent to the FCC.

In 2005, the FCC expanded network outage reporting to cover wireless communications companies, satellite providers, paging providers, facility owners, and emergency network providers. Instituted were new reporting thresholds for the services covered by the rules. In simplified terms, outages become reportable when the product of the number of users affected, and the number of minutes the outage lasts exceeds 900,000 [222]. The FCC analyzes these data, and works with individual companies to address causes of network outages. Network outage reporting is currently a primary way to gauge communications network reliability, and drive towards network improvement. Communications networks are composed of thousands of complex pieces of equipment and the network outage reporting process is a systematic way to measure and analyze the reliability of communications networks.

The Network Reliability Steering Committee (NRSC), a subcommittee of the Alliance for Telecommunications Industry Solutions (ATIS), was established to analyze outage reporting data and to refine Best Practices that could prevent outages or alleviate their effects. The NRSC is composed of representatives from major wireline and wireless carriers and suppliers of telecommunications equipments. The NRSC meets quarterly to discuss trends in network reliability. The current mission of the NRSC is

"The NRSC strives to improve network reliability by providing timely consensus-based technical and operation

expert guidance to all segments of the public communications industry” [223].

The FCC provides summaries of outage information at NRSC meetings. The FCC analyzes counts of outages in numerous categories to identify areas where there has been reliability improvement, and areas where reliability has deteriorated. They examine durations of outages, as well as the effects of the outages. The NRSC then has the option to set up subcommittees to analyze categories of network outages when the trends for this category are out of statistical control. These subcommittees are composed of experts in the category of outages. In 2008, teams addressed outages in wireless networks, large facility outages, and outages in emergency services networks. Outages in emergency services networks are particularly important because an outage could prevent many 911 calls from getting through to the appropriate emergency services providers.

In 2008, the FCC utilized a new system for tracking the status of network equipment during a disaster such as a hurricane. The Disaster Information Reporting System (DIRS) was first used during several national security exercises, as well as during the major hurricanes in 2008 including Gustav and Ike. Unlike the outage reporting process referred to previously, DIRS is a voluntary information collection process. Using DIRS, the FCC collected and analyzed information on the status of cell sites, digital switches, digital loop carriers, Public Safety Answering Points (PSAP), interoffice facilities, broadcast stations (AM, FM, TV), and cable TV systems. Hundreds of companies provided information on a daily basis. Not only was information collected on whether equipment was functioning, but information was also collected on the power status of the equipment including whether the equipment was on back-up generators. Because of DIRS and FCC outreach efforts, communications providers, Public Safety Answering Points, hospitals, and other organizations that are vital to recovering from a disaster had a conduit to express their needs for assistance, and/or to convey in a consistent manner status of their equipment.

The FCC distributed reports that summarized the status of communication assets in the disaster area to the Department of Homeland Security (DHS), and agencies that participate directly in emergency response activities connected with communications. These reports provided trend charts which tracked the effectiveness, and speed of the restoration efforts. Maps showed visually where service continued to be impacted.

ACKNOWLEDGMENT

The author would like to thank his mentor Dr. Henning Leidecker, NASA Goddard Space Flight Center, for his guidance, contributions, and technical support. His encouragement is gratefully acknowledged.

REFERENCES

- [1] M. Rosenwald, “The financial lobe: Coping with panic and fear in markets,” September 29, 2008 [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/discussion/2008/09/24/DI2008092401851.html>, accessed October 29, 2008
- [2] M. Castels, *The Information Age, Economy, Society and Culture, Volume I: Rise of the Network Society*, 2nd ed. : Blackwell Publishing, 2000, pp. 77–215.
- [3] G. Hurlburt, “A taxonomy of market automation initiative areas,” [Online]. Available: <http://www.bobsguide.com/>, accessed October 28, 2008, Compiled from bobsguide.com.
- [4] J. R. Hagerty and R. Simon, “Housing pain gauge: Nearly 1 in 6 owners “under water”,” *Wall Street Journal*, p. A5, October 8, 2008 [Online]. Available: <http://online.wsj.com/article/SB122341352084512611.html?mod=relevancy>, accessed October 29, 2008
- [5] ISDA, “International swaps and derivatives association,” [Online]. Available: <http://www.isda.org/statistics/recent.html#2008mid>, accessed October 29, 2008
- [6] Wikipedia, “Credit default swap” [Online]. Available: http://en.wikipedia.org/wiki/Credit_default_swap, accessed October 29, 2008
- [7] W. Buffet, Berkshire Hathaway Inc., “Berkshire Hathaway Inc. annual report 2002,” [Online]. Available: <http://www.berkshirehathaway.com/letters/2002pdf.pdf>, accessed October 29, 2008
- [8] The Bible, King James Version, Genesis, 41:33–36.
- [9] T. W. Ewing *et al.*, “H.R.5660: Commodity Futures Modernization Act of 2000: To reauthorize and amend the Commodity Exchange Act to promote legal certainty, enhance competition, and reduce systemic risk in markets for futures and over-the-counter derivatives, and for other purposes,” [Online]. Available: <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.05660>, accessed October 27, 2008
- [10] ISDA, *op. cit.*
- [11] F. Capra, *Hidden Connections: A Science for Sustainable Living*. : Random House, 2002, pp. 138–141.
- [12] International Swaps and Derivatives Association (ISDA), “ISDA outlines strategic vision for transforming operational processing of OTC derivatives marketplace,” December 10, 2003 [Online]. Available: <http://www.Isda.Org/Press/Press2003index.Html>, Accessed October 28, 2008
- [13] S. Hansell, “Bits: Business, innovation, technology, society: How Wall Street lied to its computers,” *The New York Times*, September 18, 2008 [Online]. Available: <http://bits.blogs.nytimes.com/2008/09/18/how-wall-streets-quants-lied-to-their-computers/?scp=1&sq=How%20Wall%20Street%20Lied%20to%20Its%20Computers&st=cse>, accessed October 29, 2008
- [14] N. N. Taleb, *The Black Swan: The Impact of the Highly Improbable*. : Random House, 2007.
- [15] G. L. Crovitz, “Information age: The 1% panic,” *The Wall Street Journal* October 13, 2008 [Online]. Available: <http://online.wsj.com/article/SB122385689217827341.html>, accessed October 29, 2008
- [16] Capra, pp. 142–149, *op. cit.*
- [17] S. Hansell, “How Wall Street lied to its computers,” *New York Times* Sept. 18, 2008 [Online]. Available: <http://bits.blogs.nytimes.com/2008/09/18/how-wall-streets-quants-lied-to-their-computers/>, accessed February 11, 2009
- [18] R. Newman, “Greenspan vs. Buffet,” *U.S. News and World Report* October 27, 2008 [Online]. Available: <http://www.usnews.com/blogs/flowchart/2008/10/27/greenspan-vs-buffett.html>, accessed February 11, 2009
- [19] H. Kurtz, “Media notes: The press, a few dollars short,” *The Washington Post* October 6, 2008 [Online]. Available: [washingtonpost.com](http://www.washingtonpost.com) [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/article/2008/10/06/AR2008100600620.html>, accessed October 26, 2008
- [20] A. Faiola, E. Nakashima, and J. Drew, ““Economy Watch: The CRASH: Risk and Regulation” What Went Wrong: How did the world’s markets come to the brink of collapse? Some say regulators failed. Others claim deregulation left them handcuffed. Who’s right? Both are. This is the story of how Washington didn’t catch up to Wall Street,” *The Washington Post* October 15, 2008 [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/article/2008/10/14/AR2008101403343.html>, accessed October 29, 2008
- [21] R. Ewing, p. 232, *op-cit.*
- [22] Associated Press, “Greenspan admits “mistake” that helped crisis,” October 23, 2008 [Online]. Available: <http://www.msnbc.msn.com/id/27335454/>, accessed November 1, 2008
- [23] Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press, 2006, pp. 133–176.
- [24] T. K. Landauer, D. S. McNamara, S. Dennis, and W. Kintech, *Handbook of Latent Semantic Analysis*. Mahwah, NJ: Lawrence Erlbaum Associates, 2007.
- [25] T. K. Landauer *et al.*, pp. 35–56, *op. cit.*
- [26] J. A. Stieb, “A critique of positive responsibility in computing,” *Science and Engineering Ethics*, vol. 14, no. 2, pp. 219–233, June 2008.
- [27] K. W. Miller, “Critiquing a critique,” *Science and Engineering Ethics*, vol. 14, no. 2, pp. 245–249, June 2008.
- [28] T. Edsall, “Man versus machine,” November 2, 2008 [Online]. Available: http://www.huffingtonpost.com/2008/11/02/man-versus-machine_n_140115.html
- [29] J. Womack, D. Jones, and D. Roos, *The Machine That Changed the World*. New York: Simon & Shuster, 1990.

- [30] J. Womack, *Deconstruction the Town of Babel*. : LEI, October 2004.
- [31] J. Womack and D. Jones, *Lean Thinking*. New York: Simon & Shuster, 2003.
- [32] Lean Enterprise Institute, "New survey: Middle managers are biggest obstacle to lean enterprise," October 2007.
- [33] M. Imai, *Gemba Kaizen*. New York: McGraw Hill, 1997.
- [34] J. F. Carroll, "[Dir. NRO]; Memorandum To Chairman—JCS on "Requirement for a Second Black Shield Mission Over North Korea," Washington, D.C., January 29, 1968, National Reconnaissance Office, Originally Classified—TS, Declassified and Released, 10 July 2000.
- [35] J. Miller, *Lockheed Martin's Skunk Works: The Official History*. Leicester, England: Midland Publishing, 1995.
- [36] J. Remakand and J. Ventolo, Jr., *A-12 Blackbird Declassified*. St. Paul, MN: MBI Pub. Co, 2001.
- [37] R. H. Graham, *SR-71 Blackbird: Stories, Tales, and Legends*. St. Paul, MN: MBI Publishing Co, 2002.
- [38] J. T. Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Boulder, CO: Westview Press, 2002.
- [39] J. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Books/Random House, 2002.
- [40] D. R. Jenkins, *Lockheed SR-71/YF-12 Blackbirds*. North Branch, MN: Specialty Press, 2004.
- [41] P. Crickmore, *Lockheed Blackbird: Beyond the Secret Missions*. Oxford, UK: Osprey Publishing, 2004, [Revised Edition].
- [42] J. Remak and J. Ventolo, Jr., *The Archangel and the OXCART: The Lockheed A-12 Blackbirds and the Dawn of Mach III Reconnaissance*. Vancouver, B.C., Canada: Trafford Publishing, 2008, and Crickmore, Paul; "Lockheed SR-71 Operations in the Far East," Osprey Publishing, Oxford, UK, 2008.
- [43] D. W. Irvin, *Reconnaissance is Black*. Paducah, KY: Turner Publishing Co, 2000, USAF.
- [44] C. L. Johnson, History of The OXCART program Lockheed Aircraft Corporation—Advanced Development Projects, Burbank, CA, Report# SP-1362, July 1, 1968, Declassified and Released—July 2007 // CIA.
- [45] AIME-Navy Day Forum, "Metallurgy in the Navy," ONR/DoN (Washington, D.C.), Presented on February 15, 1960, New York. // DDC-S&TI # AD-420059, Unclassified.
- [46] "Titanium: Past, Present and Future—Report of the Panel on Assessment of Titanium Availability: Current and Future Needs of the Committee on Technical Aspects of Critical and Strategic Materials," in *National Material Advisory Board (NMAB), Commission on Engineering and Technical Systems, National Research Council [NMAB Pub 392]*. Washington, D.C.: National Academy Press, 1983.
- [47] TML Report No. 46—Titanium Metallurgical Laboratory Battelle Memorial Institute, Columbus, Ohio, , June 21, 1956.
- [48] E. Wenk, Jr., "Repairing radar for the ship of state," in *Science and Technology Advice to the President, Congress and the Judiciary*, W. T. Golden, Ed., 2nd ed. Piscataway, NJ: Transaction Publishers—Rutgers, 2008, (Third Printing).
- [49] R. Mathews, "Guiding principles," in *Conference on 'The Next Generation Information Environment (NGIE)'*, Hamilton, New York, June 1997, U.S. Department of Defense & Air Force Research Laboratory (AFRL).
- [50] R. Mathews, *Special Session on Integration & Interoperability of National Security Information Systems*. Cambridge, MA: The Institute of Electrical and Electronics Engineers (IEEE), VOLPE Center, June 9, 2006.
- [51] R. Mathews, "Some Myths Regarding Interoperability," in *An Interoperability Orientation—Presented at "Sciences and Technologies for Health," the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS) in conjunction with the biennial Conference of the French Society of Biological and Medical Engineering (SFGBM)*, Lyon, France, August 23–26, 2007, [EMBC 2007], sponsored by: European Office of Aerospace Research and Development (EOARD), Air Force Office of Scientific Research (AFOSR), United States Air Force Research Laboratory (AFRL).
- [52] S. Keene, Reliability, Law of Least Astonishment and the Interoperability Imperative April 2008, IEEE—Reliability Society, IEEE/RS Annual Technical Report (2007).
- [53] L. Kun, G. Coatrieux, C. Quantin, R. Beuscart, and R. Mathews, "Improving outcomes with interoperable EHRs and secure global health information infrastructure," in *International Council on Medical & Care Compenetics (ICMCC) 2008*, London, UK, June 9–11, 2008.
- [54] R. Mathews and C. Spencer, "National security strategy for U.S. water," *IEEE—Engineering in Medicine and Biology Magazine*, vol. 27, no. 6, November–December 2008.
- [55] M. D. Griffin, "NASA and engineering integrity," in *Wernher von Braun Memorial Symposium*, Huntsville, AL, October 21, 2008, [NASA Administrator], American Astronautical Society, [emphasis not in the original].
- [56] Final Report of the Return to Flight Task Group: Assessing the Implementation of the Columbia Accident Investigation Board—Return-to-Flight Recommendations National Aeronautics and Space Administration (NASA), Washington, D.C., , July 2005, [emphasis not in original].
- [57] Associated Press, "NASA head unsure global warming is a problem—Climate scientist dismisses remarks as showing 'Arrogance and Ignorance'," Washington, D.C., May 31, 2007 [Online]. Available: <http://www.msnbc.msn.com/id/18964176/>
- [58] L. Kun and R. Mathews, *Interoperability: A Review of Activities to Ensure the Reliability of the U.S. Electric Power Grid*. Piscataway, NJ: IEEE [E-Book], 2007.
- [59] F. Bacon, *Advancement of Learning*, J. Devey, Ed. New York: American Home Library Co, 1902.
- [60] CBS/AP, "Pluto demoted, no longer a planet—Astronomers OK new guidelines cutting planets in solar system from 9 to 8 Prague, Czech Republic, Aug. 24, 2006 [Online]. Available: <http://www.cbsnews.com/stories/2006/08/24/tech/main1931722.shtml>
- [61] *The Correspondence of Erasmus: Letters 1535-1657 [Vol. II], [Correspondence To: The Illustrious Krzysztof Szydlowiecki, Palatine and Prefect of Cracow, and Chancellor of The Kingdom of Poland] Transl.: A. Dalzell*. Toronto, Canada: University of Toronto Press, 1994.
- [62] C. L. Hays, "What Wal-Mart knows about customers' habits," *New York Times* November 14, 2004 [Online]. Available: <http://www.nytimes.com/2004/11/14/business/yourmoney/14wal.html>
- [63] comScore, "qSearch 2.0—Core search report," November 2008, [Total U.S. Home/Work/University Locations], Contact: Andrew Lipsman, Senior Analyst, comScore, Inc., 11950 Democracy Drive, Suite 600, Reston, VA 20190.
- [64] J. F. Gantz, *The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011*. Framingham, MA: IDC, March 2008, [Project Director].
- [65] F. W. Bain, *On The Realisation of The Possible and The Spirit of Aristotle*. London, England: James Parker and Co, 1899.
- [66] N. Maxwell, "Do Philosophers Love Wisdom?," *The Philosophers' Magazine*, no. 22, 2nd Quarter, 2003.
- [67] M. J. Adler and M. Weismann, *How to Think about the Great Ideas: From the Great Books of Western Civilization*. Peru, IL, USA: Open Court Publishing (Carus), 2003, (6th printing).
- [68] G. B. Shaw, *Man and Superman—A Comedy and a Philosophy*. Cambridge, MA: The University Press, 1903.
- [69] "The apology of Socrates," in *The Dialogues of Plato*, 3rd ed. Oxford, England: Oxford University Press, 1892, vol. 2, Translated by Benjamin Jowett.
- [70] Plato, "[H]ow little does the common herd know of the nature of right and truth . . ." in *The Dialogues of Plato*. New York: Scribner, Armstrong & Co., 1874, vol. 1, [Translated by Benjamin Jowett, w/ Analyses and Introductions].
- [71] *The Quiver*. London, Paris, New York: Cassell, Petter & Galpin Co., Ltd., 1877, vol. XII, [in Divine Conviction].
- [72] F. Bacon, "Plutarch," in *The Works of Francis Bacon*. London, England: , vol. III, p. 1740, J. Walthoe, D. Midwinter, etc., [. . . "men of weak abilities set in great place, that they were like little statues set on great bases, made to appear the less by their advancement."].
- [73] W. Smith, *A History of Greece, From the Earliest Times to the Roman Conquest; With Supplementary Chapters on the History of Literature and Art*. New York: Harper, 1897, [Revised by George W Greene].
- [74] H. H. Bauer, "The progress of science and implications for science studies and for science policy," *Perspectives on Science*, vol. 11, no. 2, Summer, 2003.
- [75] W. D. Carey, "Science and public policy," *Science, Technology, & Human Values*, vol. 10, no. 1, Winter, 1985.
- [76] N. S. Young, J. P. A Ioannidis, and O. Al-Ubaydli, "Why current publication practices may distort science," *PLoS Med.*, vol. 5, no. 10, October 2008, 10.1371/journal.pmed.0050201, e201. Published online October 7, 2008.
- [77] M. Bundy, "The scientist and national policy," in *Knowledge and Power: Essays on Science and Government*, S. A. Lakoff, Ed. New York: The Free Press, 1966.
- [78] R. N. Proctor, *Value-Free Science?: Purity and Power in Modern Knowledge*. Cambridge, MA: Harvard University Press, 1991.
- [79] D. K. Price, "Endless frontier or bureaucratic morass?," in *Daedalus: Journal of the American Academy of Arts and Sciences*. : MIT Press, Spring, 1978, vol. 107.
- [80] J. Habermas, *Knowledge and Human Interests*, 2nd ed. London, UK: Heinemann, 1972.
- [81] S. Grundy, *Curriculum: Product or Praxis*. , UK: RoutledgeFalmer, 1987.
- [82] *2020: A New Vision—A Future for Regenerative Medicine*. Washington, D.C.: U.S. Department of Health and Human Services, 2003 [Online]. Available: <http://www.hhs.gov/reference/newfuture.shtml>, additionally, Boyle, Philip J; "Shaping Priorities in Genetic Medicine," *The Hastings Center Report*, Vol. 25, No.3, 1995

- [83] D. J. Kevles, "The national science foundation and the debate over postwar research policy, 1942–1945: A political interpretation of science—The endless frontier," *Isis*, vol. 68, no. 1, March 1977.
- [84] V. Bush, "Science: The endless frontier," *Trans. Kansas Academy of Science*, vol. 48, no. 3, December 1945.
- [85] "The United States commission on national security/21st century," Washington, D.C., January 2001, [Hart-Rudman Commission].
- [86] T. Galama and J. Hosek, U.S. Competitiveness in Science and Technology RAND, Santa Monica, CA, Report MG674, 2008.
- [87] M. A. Tuve, "Basic research in private research institutes," in *Carnegie Institution—The Symposium on Basic Research*, New York City, May 1959.
- [88] *The Knowledge Economy: Is the United States Losing Its Competitive Edge?*. Washington, D.C.: The Task Force on the Future of American Innovation, February 16, 2005 [Online]. Available: <http://www.futureofinnovation.org/>, Supplementally: "Offshore Outsourcing and America's Competitive Edge: Losing Out In The High Technology R&D and Services Sectors" [A White Paper], Senator Joseph Lieberman, United States Senate, Washington, D.C., May 2004; Farrell, John A: "Signs America's scientific edge is slipping," Sunday—Final Edition, The Denver Post, March 26, 2006
- [89] D. Wolffe, Ed., in *Symposium on Basic Research*, New York City, May 14–16, 1959, Sponsored by National Academy of Sciences, American Association for the Advancement of Science & The Alfred P. Sloan Foundation, Caspary Auditorium—Rockefeller Institute.
- [90] "Compete—New challenges, new answers," Washington, D.C., November 2008, Council on Competitiveness [Chairman: Charles O. Holliday, Jr., President: Deborah L. Wince-Smith].
- [91] R. Mathews, "Guiding principles," in *Conference on 'The Next Generation Information Environment (NGIE)'*, Hamilton, New York, June 1997, [Co-Chair], U.S. Department of Defense & Air Force Research Laboratory (AFRL).
- [92] "The importance of new knowledge," in *Symposium on Basic Research*, D. Wolffe, Ed., Id.
- [93] "Merle Tuve' presentation," in *Symposium on Basic Research*, D. Wolffe, Ed., Id.
- [94] W. Triplett, "Is political manipulation of science getting worse?," *Congressional Quarterly (CQ) Researcher*, vol. 14, no. 28, August 20, 2004, [Citing Patrick Michaels at University of Virginia].
- [95] J. Marburger, III, "Policy, Politics and Science in the White House," in *Center for Science and Technology Policy Research, University of Colorado*, Boulder, CO, February 14, 2005 [Online]. Available: http://sciencepolicy.colorado.edu/scienceadvisors/marburger_transcript.html
- [96] C. Mooney, *The Republican War on Science*. New York: Basic Books [Perseus], 2005 [Online]. Available: http://www.economist.com/printedition/PrinterFriendly.cfm?Story_ID=2571867, Additionally, "Science and the Bush administration: Cheating nature?" [The Bush administration has been accused of manipulating science. It is now fighting back], The Economist Newspaper, April 7th 2004
- [97] Available at the Union of Concerned Scientists web-site and their project on scientific integrity, at: [Online]. Available: http://www.ucsusa.org/scientific_integrity/
- [98] Union of Concerned Scientists, "Scientific integrity in policymaking: An investigation into the Bush administration's misuse of science," Cambridge, MA, March 2004.
- [99] L. Peters, "Science literacy: The Chinese get it," *The Seattle Times*, March 26, 2006.
- [100] D. G. Brown, *The Last Log of the Titanic*. Crawfordsville, IN: R.R. Donnelly & Sons, 2001, And McCarty, Jennifer H and Foecke, Tim; "What Really Sank the Titanic," Kensington Publishing Corp., New York, 2008. Supplemental: Campbell, Harry Huse; "The manufacture and properties of iron and steel," McGraw-Hill, New York, NY, 1903.
- [101] W. D. Carey, "Intergovernmental relations: Guides to development," *Public Administration Review*, vol. 28, no. 1, Jan.–Feb. 1968, [U.S. Bureau of the Budget], American Society for Public Administration.
- [102] W. D. Carey, "Science policy," in *Science and Technology Advice to the President, Congress and the Judiciary*, W. T. Golden, Ed., 2nd ed. Piscataway, NJ: Transaction Publishers—Rutgers, 2008, (Third Printing).
- [103] W. D. Carey, "Passing thoughts on science and resource allocation," *American Psychologist*, vol. 22, no. 3, Mar. 1967, American Psychological Association.
- [104] E. Zio, "Soft computing methods applied to condition monitoring and fault diagnosis for maintenance," in *Proceedings of the Summer Safety and Reliability Seminars*, Gdansk/Sopot-Jelitkowo, Poland, July 22–29, 2007.
- [105] D. Roverso, M. Hoffmann, E. Zio, P. Baraldi, and G. Gola, "Solutions for plant-wide on-line calibration monitoring," in *Proceedings of ESREL 2007*, Stavanger, Norway, June 25–27, 2007, vol. 1, pp. 827–832.
- [106] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, pp. 601–611, 1976.
- [107] M. Marseguerra, E. Zio, P. Baraldi, I. C. Popescu, and P. Ulmeanu, "A fuzzy logic—Based model for the classification of faults in the pump seals of the primary heat transport system of a candu 6 reactor," *Nuclear Science and Engineering*, vol. 153, no. 2, pp. 157–171, 2006.
- [108] J. Reifman, "Survey of artificial intelligence methods for detection and identification of component faults in nuclear power plants," *Nuclear Technology*, vol. 119, no. 1, pp. 76–97, 1997.
- [109] A. Doucet, On Sequential Simulation-Based Methods for Bayesian Filtering University of Cambridge, Dept. of Engineering, CUED-F-ENG-TR310, 1998, Technical Report.
- [110] A. Doucet, J. F. G. de Freitas, and N. J. Gordon, "An introduction to sequential Monte Carlo methods," in *Sequential Monte Carlo in Practice*, A. Doucet, J. F. G. de Freitas, and N. J. Gordon, Eds. New York: Springer-Verlag, 2001.
- [111] G. Kitagawa, "Non-Gaussian state-space modeling of nonstationary time series," *Journal of the American Statistical Association*, vol. 82, pp. 1032–1063, 1987.
- [112] Institute for Healthcare Brochure on the March 5–6, 2009 Seminar Reducing Hospital Mortality.
- [113] Institute for Healthcare Improvement, Improving the Reliability of Healthcare, Cambridge, MA, Innovation Series 2004.
- [114] D. Raheja and M. Allocco, *Assurance Technologies Principles and Practices*. Wiley, 2006, pp. 167–168.
- [115] P. Pronovost, D. Needham, and S. Berenholtz, "An intervention to decrease catheter-related bloodstream infections in the ICU," *The New England Journal of Medicine*, vol. 355, no. 26, pp. 2725–2732, December 28, 2006.
- [116] K. Mohanram and N. Touba, "Partial error masking to reduce soft error failure rate in logic circuits," in *Proc. IEEE Int'l Symp. on Defect and Fault-Tolerance*, Boston, MA, USA, 2003, pp. 433–440.
- [117] K. Mohanram and N. Touba, "Cost-effective approach for reducing soft error failure rate in logic circuits," in *Proc. IEEE Int'l Test Conf.*, Charlotte, NC, USA, 2003, pp. 893–901.
- [118] A. K. Nieuwland, S. Jasarevic, and G. Jerin, "Combinational logic soft error analysis and protection," in *Proc. Int'l On-Line Test Symp.*, 2006.
- [119] R. Garg, N. Jayakumar, S. Khatri, and G. Choi, "A design approach for radiation-hard digital electronics," in *Proc. IEEE/ACM Design Automation Conf.*, 2006, pp. 773–778.
- [120] Z. Pan and M. A. Breuer, "Basing acceptable error-tolerant performance on significance-based error-rate (SBER)," in *Proc. IEEE VLSI Test Symp.*, 2008.
- [121] I. Chong and A. Ortega, "Hardware testing for error tolerant multimedia compression based on linear transforms," in *Proc. IEEE Int'l Symp. on Defect and Fault Tolerance in VLSI Systems*, 2005.
- [122] H. Chung and A. Ortega, "Analysis and testing for error tolerant motion estimation," in *Proc. IEEE Int'l Symp. on Defect and Fault Tolerance in VLSI Systems*, 2005.
- [123] I. Polian, B. Becker, M. Nakasato, S. Ohtake, and H. Fujiwara, "Low-cost hardening of image processing applications against soft errors," in *Proc. Int'l Symp. on Defect and Fault Tolerance*, Arlington, VA, USA, 2006, pp. 274–279.
- [124] J. Hayes, I. Polian, and B. Becker, "An analysis framework for transient-error tolerance," in *Proc. IEEE VLSI Test Symp.*, Berkeley, CA, USA, 2007.
- [125] S. A. Seshia, W. Li, and S. Mitra, "Verification-guided soft error resilience," in *Proc. Design, Automation and Test in Europe Conf.*, 2007.
- [126] M. May, M. Alles, and N. Wehn, "A case study in reliability-aware design: A resilient LDPC code decoder," in *Proc. Design, Automation and Test in Europe Conf.*, 2008.
- [127] X. Li and D. Yeung, "Application-level correctness and its impact on fault tolerance," in *Proc. Int'l Symp. on High Performance Computer Architecture*, 2007.
- [128] D. Nowroth, I. Polian, and B. Becker, "A study of cognitive resilience in a JPEG compressor," in *Proc. IEEE/IFIP Int'l Conf. on Dependable Systems and Networks*, Anchorage, AK, USA, 2008.
- [129] S. J. Keene, "Validating measurement data," *Evaluation Engineering*, November–December 1969.
- [130] M. E. Mann, R. S. Bradley, and M. K. Hughes, "Global-scale temperature patterns and climate forcing over the past six centuries," *Nature*, vol. 392, pp. 779–787, 1998.
- [131] McIntyre and McKittrick, "Corrections to the Mann et. al. (1998) proxy data base and Northern Hemispheric average temperature series," *Energy & Environment*, vol. 14, no. 6, pp. 751–771(21), November 1, 2003.
- [132] [Online]. Available: <http://info-pollution.com/mandm.htm>
- [133] [Online]. Available: <http://hotair.com/archives/2008/11/16/hottest-october-on-record-was-really-a-september/>
- [134] [Online]. Available: <http://www.snopes.com>
- [135] [Online]. Available: <http://en.wikipedia.org/wiki/Snopes>
- [136] [Online]. Available: <http://patterico.com/2007/05/29/snopes-wrong-again-on-flight-327/>
- [137] [Online]. Available: http://en.wikipedia.org/wiki/ANOVA_Gage_R&R

- [138] E. B. Sloane, "IEEE and medical device standards: The 21st century healthcare informatics industry & IEEE's leadership roles and opportunities," presented at the IEEE Standards Association Standards Board, March 2008.
- [139] C. W. Johnson, "The interaction between safety culture and uncertainty over device behaviour: The limitations and hazards of telemedicine," 2003 [Online]. Available: <http://www.dcs.gla.ac.uk/~johnson/papers/ISSC2003/telemedicine.pdf>
- [140] National Academy of Engineering Report, "Building a better delivery system: A new engineering/health care partnership," 2005.
- [141] Food and Drug Administration, Center for Devices and Radiological Health, "General principles of software validation; final guidance for industry and FDA staff," January 2002.
- [142] Medical News Today, "FDA finds many possibly life-threatening medical equipment malfunctions result from software problems," July 2008.
- [143] "Addressing the elusive use error: Meeting regulatory expectations for identifying and controlling medical device use-related hazards," R. A. North, 2008, Compliance Online Webinar.
- [144] P. H. Chung *et al.*, "An extended hierarchical task analysis for error prediction in medical devices," 2003 [Online]. Available: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1479951>
- [145] I. Lee and G. J. Pappas *et al.*, "High-confidence medical device software and systems," *IEEE Computer*, April 2006.
- [146] D. Chi and P. C. McIntyre, *APL*, vol. 85, p. 4699, 2004.
- [147] G. Bersuker, P. S. Lysaght, C. S. Park, J. Barnett, C. D. Young, P. D. Kirsch, R. Choi, B. H. Lee, B. Foran, K. van Benthem, S. J. Pennycook, P. M. Lenahan, and J. T. Ryan, "The effect of interfacial layer properties on the performance of HF-based gate stack devices," *J. Appl. Phys.*, vol. 100, p. 094108, 2006.
- [148] P. S. Lysaght, A. J. Barnett, G. I. Bersuker, J. C. Woicik, D. A. Fischer, B. Foranb, H.-H. Tseng, and R. Jammy, "Chemical analysis of HfO₂/Si (100) film systems exposed to NH₃ thermal processing," *Journal of Applied Physics*, vol. 101, p. 024105, 2007.
- [149] J. T. Ryana, P. M. Lenahan, G. Bersuker, and P. Lysaght, "Electron spin resonance observations of oxygen deficient silicon atoms in the interfacial layer of hafnium oxide based metal-oxide-silicon structures," *Appl. Phys. Lett.*, vol. 90, p. 173513, 2007.
- [150] C. D. Young, D. Heh, S. Nadkarni, R. Choi, and G. Bersuker, "Determination of generated electron traps in high-k gate stacks after constant voltage stress," *TDMR*, vol. 6, p. 123, 2006.
- [151] G. Bersuker, N. Chowdhury, C. Young, D. Heh, D. Misra, and R. Choi, "Progressive breakdown characteristics of high-k/metal gate stacks," in *Proc. IEEE IRPS*, 2007, pp. 49–54.
- [152] G. Bersuker, D. Heh, C. Young, H. Park, P. Khanal, L. Larcher, A. Padovani, P. Lenahan, J. Ryan, B. H. Lee, H. Tseng, and R. Jammy, "Breakdown in the metal/high-k gate stack: Identifying the "weak link" in the multilayer dielectric," in *Proc. IEDM*, 2008, p. 791.
- [153] L. Larcher, *IEEE TED*, vol. 50, p. 1246, 2003.
- [154] Merriam-Webster Online Dictionary May 5, 2008 [Online]. Available: <http://www.merriam-webster.com/dictionary/counterfeit>
- [155] T. W. Lee, "Microelectronic FA desk reference," in *Mechanical and Chemical Decapsulation*, 3rd ed. : ASM, 1993, pp. 61–90.
- [156] The United States Mission to the European Union, Feb.22–Apr. 17 2008 [Online]. Available: http://useu.usmission.gov/Dossiers/IPR/Feb2208_Operation_Infrastructure.asp, (This website is produced and maintained by the Public Affairs Office, United States Mission to the European Union).
- [157] "Counterfeit," in *Wikipedia, The Free Encyclopedia*. : , Apr. 16, 2008 [Online]. Available: <http://en.wikipedia.org/wiki/Counterfeit>,
- [158] G. F. Shade and B. Wilson, "Response to Counterfeit Integrated Circuit Components in the Supply Chain, Part I," *Electronic Device Failure Analysis Magazine*, vol. 10, no. 4, pp. 16–22, Nov. 2008.
- [159] B. Grow, C.-C. Tschang, C. Edwards, and B. Burnsed, "Dangerous fakes," *Business Week* 2 Oct. 2008: 1–8. *Business Week*. 2 Oct. 2008. 4 Oct. 2008 [Online]. Available: http://www.businessweek.com/print/magazine/content/08_41/b4103034193886.htm
- [160] US Government, Immigration and Customs Enforcement (ICE), "Value of CBP, ICE seizures of counterfeit goods in FY2007 is up 27%. Nearly \$200 million in goods confiscated as a result of enforcement actions," Press release, Jan. 28–July 11 2008 [Online]. Available: <http://www.ice.gov/pi/news/newsreleases/articles/080128washingtondc.htm>
- [161] B. Jorgensen, "Chip makers step up anti-counterfeiting efforts," *EDN-Electronic Design News Reed Elsevier Inc.*, Oct. 31, 2006, Nov. 11 2008 [Online]. Available: <http://www.edn.com/index.asp?layout=articleprint&articleid=ca6386712>
- [162] "Beware counterfeit electronic components," *DataWeek* 7 Apr. 2004: 1–2. 7 Apr. 2004, Electronics and Communication Technology TechNews Publishing Ltd., Nov. 17, 2008 [Online]. Available: <http://dataweek.co.za/article.aspx?pk1articleid=2922&pk1categoryid=31>
- [163] Counterfeit. BP council, "Counterfeit components: The trends, the threats and one promising solution," Nov. 18, 2008 [Online]. Available: <http://www.bpcouncil.com/apage/609.php>
- [164] J. Miller, "Hidden no more," Mar. 2005, Schofield Media, pp. 24–28, Aug. 15, 2008 [Online]. Available: <http://www.planetxs.com/images/march 2005 usbr article.pdf>
- [165] B. Thompson, Counterfeit Penwall Publishing, Feb. 1, 2005, Nov. 18, 2008 [Online]. Available: <http://www.tmworld.com/article/ca500057.html>
- [166] "Anti-counterfeiting standards task force launched at SEMICON west 2007," *SEMI* Nov. 19, 2008, Aug. 2007 [Online]. Available: <http://www.semi.org/en/p042417>
- [167] R. Pfahl, Jr, "The environmental mandate," in *Circuits Assembly*. : iNEMI CD-ROM, January 2005, Published in, Lead-Free Watch, Countdown to July 1, 2006.
- [168] W. Huang, "Failure probability evaluation due to tin whiskers caused leads bridging on compressive contact connectors," *IEEE Trans. Reliability*, vol. 57, no. 3, pp. 426–430, September 2008.
- [169] L. Nie, M. Osterman, M. Pecht, F. Song, J. Lo, and R. S. W. Lee, "Solder ball attachment assessment of reballed plastic ball grid array packages," in *APEX 2008*, Las Vegas, Nevada, March 30–April 3 2008.
- [170] R. Ooi, T. Chan, C. Siew, A. McAllister, K. J. Blue, and L. H. Ng, "Mechanical shock solder joint reliability (SJR) assessment of the board level adhesive properties," in *SMTA-International (SMTAi), 2007 Conference Proceedings on CD-ROM*.
- [171] K. Rispoli and A. DerMarderosian, "Risk assessment and mitigation of COTS integration in high reliability systems," in *Minnowbrook Microelectronic Conference*, Oct 8–9, 2008.
- [172] K. Rispoli and A. DerMarderosian, "Failure leads to COTS integration strategy," in *2006 International Military & Aerospace/Avionics COTS Conference*, August 22–24, 2006.
- [173] K. Rispoli and A. DerMarderosian, "Power supply reliability—COTS integration, lessons learned," October 15, 2008.
- [174] K. G. Compton, A. Mendizza, and S. M. Arnold, in *Seventh Annual Conference and Exhibition of the National Association of Corrosion Engineers*, New York, March 13–16, 1951.
- [175] S. M. Arnold, "Convention of American electroplating society," in *Technical Proceedings of the 43rd Annual Convention of American Electroplating Society*, 1956, p. 26.
- [176] Author's correspondence with NASA Goddard Space Flight Center (GFSC) scientist Dr. Henning Leidecker, 2007.
- [177] NASA Goddard Space Flight Center [Online]. Available: <http://nepp.nasa.gov/WHISKER/> (A historical and up to date listing of publically reported whisker failures and bibliography of technical papers)
- [178] S. E. Koonce and S. M. Arnold, *Growth of Metal Whiskers*. : , December 8, 1952, Unknown Publisher (only the Letters to the editor at the Bell Telephone Laboratories, Murray Hill, NJ).
- [179] T. A. Woodrow, "Tracer diffusion in whisker-prone tin platings," in *The Proceedings of SMTA International Conference*, Rosemont, IL, September 24–28, 2006.
- [180] H. Leidecker and J. S. Kadesch, "Effects of uranine conformal coating on tin whisker growth," in *Proceedings of IMAPS Nordic, The 37th IMAPS Nordic Annual Conference*, September 10–13, 2000, pp. 108–116.
- [181] [Online]. Available: http://www.national.com/analog/packaging/tin_whiskers
- [182] International Electronics Manufacturing Initiative (iNEMI) [Online]. Available: <http://www.inemi.org/cms/>
- [183] The Joint Electron Devices Engineering Council (JEDEC) [Online]. Available: <http://www.jedec.org/>, For more information, visit a 950+ page bibliography at <http://www.dbicorporation.com/rohsbib.htm>. You can subscribe to a tin whiskers listserv at this website <http://www.freelists.org/list/tinwhiskers>
- [184] V. Cerf, Personal Email Communication.
- [185] P. E. Ross, "The day the software crashed," *Forbes Magazine*, pp. 142–156, April 25, 1994.
- [186] Billdats [Online]. Available: <http://www.morehouse.org/hin/ess/ess08.htm> a reasonably accurate description of the system. The experiment was documented in internal notes.
- [187] in *Workshop on Software Aging and Rejuvenation* [Online]. Available: http://www.csc2.ncsu.edu/conferences/issue/2008/wosar_WS.php
- [188] K. S. Trivedi, "The role of measurements and models in software rejuvenation," keynote address, *WoSAR/ISSRE 2008*, Nov. 11, 2008 [Online]. Available: www.software-rejuvenation.com
- [189] Bureau of Labor [Online]. Available: http://www.bls.gov/oco/ocos267.htm#projections_data
- [190] G. Yamamura and G. B. Wigle, "SEI CMM level 5: For the right reasons," [Online]. Available: <http://www.stsc.hill.af.mil/crosstalk/1997/08/seicmm5.asp>
- [191] L. Hatton, "Safer C: Developing software for high-integrity and safety-critical systems," in *The McGraw-Hill International Series in Software Engineering*. : , 1997, 0-07-707640-0.

- [192] L. Bernstein and C. M. Yuhas, *Trustworthy Systems through Quantitative Software Engineering*. : Wiley-IEEE Computer Society Press, September 2005, Cloth; 0-471-69691-9.
- [193] G. McGraw and G. Morrisett, "Attacking malicious code: A report to the Infosec research council," *IEEE Software*, vol. 17, no. 5, pp. 33–41, Sep. 2000.
- [194] D. M. Kienzle and M. C. Elder, "Recent worms: A survey and trends," in *Proceedings of the 2003 ACM workshop on Rapid malware*, Washington, DC, USA, October 2003, pp. 1–10.
- [195] W. E. Wong, T. Wei, Y. Qi, and L. Zhao, "A crosstab-based statistical method for effective fault localization," in *Proceedings of The First International Conference on Software Testing, Verification and Validation*, Lillehammer, Norway, April 2008, pp. 42–51.
- [196] W. E. Wong, Y. Shi, Y. Qi, and R. Golden, "Using an RBF neural network to locate program bugs," in *Proceedings of the 19th IEEE International Symposium on Software Reliability Engineering*, Seattle, Washington, November 2008, pp. 27–38.
- [197] R. G. Huget, M. Viola, and P. A. Froebel, "Ontario hydro experience in the identification and mitigation of potential failures in safety critical software systems," *IEEE Trans. Nuclear Science*, vol. 42, no. 4, pt. 1–2, pp. 987–992, August 1995.
- [198] M. Weber, M. Schmid, M. Schatz, and D. Geyer, "A toolkit for detecting and analyzing malicious software," in *Proceedings of the 18th Annual Computer Security Applications Conference*, Las Vegas, Nevada, December 2002, pp. 423–431.
- [199] M. G. Schultz, E. Eskin, E. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," in *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, Oakland, California, May 2001, pp. 38–49.
- [200] B. Zhang, J. Yin, D. Zhang, and S. Wang, "Using support vector machine to detect unknown computer viruses," *International Journal of Computational Intelligence Research*, vol. 2, no. 1, pp. 100–104, 2006.
- [201] W. Raymond, L. Karl, and O. Ronald, "MCF: A malicious code filter," *Computers and Security*, vol. 14, no. 6, pp. 541–566, 1998.
- [202] J. Bergeron, M. Debbabi, J. Desharmais, M. Erhioui, Y. Lavoie, and N. Tawbi, "Static detection of malicious code in executable programs," in *Proceedings of Symposium on Requirements Engineering for Information Security*, Indianapolis, Indiana, March 2001.
- [203] A. Moser, C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," in *Proceedings of the 23rd Annual Computer Security Applications Conference*, Miami Beach, Florida, December 2007, pp. 421–430.
- [204] J. Zhang, Y. Guan, X. Jiang, D. H. Duan, and J. Wu, "AMCAS: An automatic malicious code analysis system," in *Proceedings of the 9th International Conference on Web-Age Information Management*, Zhangjiajie, China, July 2008, pp. 501–507.
- [205] Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness Center for National Software Studies, May 2005 [Online]. Available: <http://www.cnsoftware.org/nss2report/>
- [206] T. Rhodes, "Trustworthy information systems—A new NIST research program," in *IEEE Computer Society Presentation*, NIST Gaithersburg, MD, June 24, 2008.
- [207] D. O'Neill, "Maturity framework for assuring resiliency under stress," Build Security In web site. Operated by Software Engineering Institute and Sponsored by Department of Homeland Security, July 2008 [Online]. Available: <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/1016-BSI.html>
- [208] A. Carey, "2006 Global Information Security Workforce Study," Framingham, MA, IDC, 2006 [Online]. Available: <https://www.isc2.org/download/workforcestudy06.pdf>
- [209] "Deloitte Touche Tohmatsu," 2007 Global Security Survey: The Shifting Security Paradigm September 2007 [Online]. Available: [http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecurity-Survey_20070901\(1\).pdf](http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecurity-Survey_20070901(1).pdf)
- [210] G. McGraw, *Software Security: Building Security*. Boston, MA: Addison-Wesley Professional, 2006, 0-321-35670-5.
- [211] J. Steven, "Adopting an enterprise software security framework," *IEEE Security & Privacy* vol. 4, no. 2, pp. 84–87, March/April 2006 [Online]. Available: <https://buildsecurityin.us-cert.gov/daisy/bsi/resources/published/series/bsi-ieee/568.html>
- [212] J. Allen, S. Barnum, R. Ellison, G. McGraw, and N. Mead, *Software Security Engineering: A Guide for Project Managers*. : Addison-Wesley, 2008.
- [213] [Online]. Available: <https://buildsecurityin.us-cert.gov>
- [214] K. H. Pollock, "Modeling capture, recapture, and removal statistics for estimation of demographic parameters for fish and wildlife populations: Past, present, and future," *Journal of the American Statistical Association*, vol. 86, no. 413, pp. 225–238, 1991.
- [215] G. Seber, *The Estimation of Animal Abundance and Related Parameters*, 2nd ed. London: Charles Griffin & Company Ltd., 1982.
- [216] H. Mills, Technical report FSC-72-6015 IBM Federal Systems Division, , 1972.
- [217] S. G. Eick, C. R. Loader, M. D. Long, L. G. Votta, and S. A. Vander Wiel, "Estimating software fault content before coding," in *Proceedings of the 14th International Conference on Software Engineering*, 1992, pp. 59–65.
- [218] A. Elcock and P. A. Laplante, "Testing without requirements," *Innovations in Systems and Software Engineering: A NASA Journal*, vol. 2, pp. 137–145, December 2006.
- [219] *Recommended Practice for Software Requirements Specifications*, IEEE Standard 830-1998.
- [220] P. Laplante and N. Ahmad, "Pavlov's bugs," in *IT Professional*. : , December 2008, to appear.
- [221] A Compendium of Technical Papers Network Reliability Council, National Engineering Consortium, Inc, , 1993.
- [222] 47 C.F.R. Part 4. See also New Part 4 of the Commission's Rules Concerning Disruptions to Communications, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830 (2004); Sections 1, 4(i), 4(o).
- [223] Network Reliability Steering Committee Mission Statement [Online]. Available: <http://www.atis.org/nrsc/>