ROBERT H. ADAMS **Email:** robert.adams@whatifwe.com

CAREER SUMMARY

- **FORTY FIVE YEARS IN SOFTWARE, DIGITAL, ANALOG ENGINEERING** with an emphasis in the development and test of high reliability software. This experience is augmented by free, open source tools that provide a practical, economical means of:
  - Developing software according to enforceable standard processes and methods.
  - Testing software using an aggressive divide-and-conquer approach.
- **EXPERIENCE - HIGHLIGHTS**:
  - **1992-PRESENT: SOLE PROPRIETOR – WHAT IF WE**
    - **Standard Software Parts:** Developed a two step software development process: first, a library of "software parts, and then applications from this library.
      - **Programmable Code Generator (PCG):** Developed the basic Programmable Code Generator for both Windows and Linux operating systems.
      - **Programmable Monte-Carlo Test System:** Developed software test system for measuring the resistance of software parts and modules to use-related programming errors for both Windows and Linux operating systems.
    - **Exportable ELINT:** Developed a Unicode-base Arabic-English Communication Subsystem which converted Unicode into an efficient ASCI representation for transmission over an existing radio-communication system.
    - **Exportable ELINT:** Using the MKS environment developed the Tuner-Antenna Controller and IEEE488 Interface for an exportable ELINT system. Monte-Carlo methods were used to rapidly and thoroughly test the software.
    - **Exportable Cryptography:** Upgraded firmware for an exportable KY58-equivalent Wideband Secure Voice System. Developed IDE for simulating and producing the prom-files for its custom bit-slice processor using the PCG.
    - **French-Arabic Telex Terminal:** Developed software for an MSDOS-based interface board and French-Arabic Windows 3.1. Included a black-box based software PM/FL sub-system augmented by extensive use of state machines.
    - **Television Advertisement Accounting System:** Developed the firmware for 4-slave data collection processors and one master communication processor.
  - **1975-1989, 1991-1992: OCEAN TECHNOLOGY, INC.**
    - **Responsible for:** Wide Band Secure Voice System, Arabsat Secure Control System, Noise and Vibrations Sub-system of MSDC.
    - **Experience:** Exportable cryptography, Signal-data conversion, digital design, analog design, firmware design, bit-slice processors, Assembly, FORTRAN, C, MSDOS, 8085, Z80, AMD 2901.
  - **1961-1975: LOCKHEED CALIFORNIA COMPANY**
    - **Responsible for:** NORAD Feasibility Study, Numerical Functional Analysis Computing Laboratory, 3000-Watt Transistorized Vibration shaker amplifier
    - **Experience:** Bayesian Instrumentation, Monte-Carlo Simulation, Markov Simulation, Multi-Dimensional Splines, IDE Development, Compiler Development, Precedence Analysis, PL/I, FORTRAN, High-Power Analog Design
- **EDUCATION:** B.A. Physics, U.C. Berkeley, 1962.
- **CONFERENCE PUBLICATIONS:** 1985-Oslo, 1987-Prague, 1988-Paris, 1991-Lille.
- **SECURITY CLEARANCE:** Secret – Last Active in January 2004

ROBERT H. ADAMS **Email:** robert.adams@whatifwe.com

HARDWARE / MATHEMATICS

❖ LOCKHEED FUNDED PROJECTS

➢ 1962-1965: Shaker Amplifiers

- **First Amplifier:** Developed the first fully transistorized 3000 watt vibration shaker amplifier with 48 germanium transistors in the output stage. The design was challenged by a parasitic oscillation which was eventually solved experimentally by reducing the frequency range (0-2000 Hz) of the amplifier,
- **Second Amplifier:** Developed a second fully transistorized vibration shaker amplifier using silicon transistors. In order to avoid instabilities, performed a stability analysis of the design using a simple mathematical model of the power transistors. Located the cause of the instability in the original design. The second amplifier was totally turn-key
- **Mathematical Connection:** The source of the parasitic oscillations was not where expected and could not have been found experimentally. No loss in frequency range was necessary and the second amplifier was unconditionally stable.

➢ 1963-1965: Vibration Servo System

- **Background:** The Vibration Level upon a test article was maintained at the proper level by a Vibration Servo System. In an analog-based system, the ability of the traditional servo-system to respond to changes in vibration was constrained by the lowest vibration frequency. This was not suitable for the range of frequencies that was used in most of the tests.
- **Solution:** Developed a prototype analog sample-based vibration servo system. Specifically, the measured vibration amplitude for each cycle was used to correct the vibration amplifier output for the next cycle. The response of the vibration servo system was coupled to the vibration frequency.
- **Mathematical Connection:** The power sequence defining a sampling servo system is much easier to stablize than the equivalent differential equation defining the conventional analog servo system.

❖ OCEAN TECHNOLOGY FUNDED PROJECTS

➢ 1975-1977: Variable Gain Amplifier

- **Background:** One of the components of the MSDC (Monitoring Signal Data Conversion) sub-system was a digitally settable AC-Coupled Variable Gain Amplifier. There was a band-specific maximum transient response time specified for each of the 5-bands of audio frequency.
- **Problem:** The AC-coupling circuitry of the Variable Gain Amplifier was designed for the proper frequency response for the entire spectrum of audio frequencies. Consequently, it did not satisfy the maximum transient response time specification at the high end of the spectrum. A request to relax the specification was being considered by management.
- **Solution:** The AC coupling circuitry was modified to be band specific and the analog gain selectors were relocated so that a change in gain would minimally excite its transient response. As a consequence, the modified VGA satisfied both the frequency response and maximum transient time requirements.
- **Mathematical Connection:** The original designer was not intimate with the differential equations defining the AC coupling circuitry. Mathematical intimacy would have prevented the design inadequacies.

ROBERT H. ADAMS **Email:** robert.adams@whatifwe.com

COMPUTER SIMULATION / NUMERICAL FUNCTIONAL ANALYSIS

❖ LOCKHEED FUNDED PROJECTS

- **1966: MARKOV SIMULATION.** My first computer program was matrix-based statistical mechanics simulation of a sphere of fissionable material (atomic bomb). An estimate of the critical mass was made by running various diameters.
- **1967: PICARD INTEGRATION SIMULATION.** The Markov-base Atomic Bomb experiment was upgraded to a Picard Integration method using a Partial Spline approximation to the probability functions. The results were far superior to those obtained in the discrete Markov Simulation.
- **1967-1969: FUNCTIONAL ANALYSIS COMPUTING LABORATORY.** A comprehensive computing system for the manipulation of multi-dimensional functions approximated by the Partial Spline was developed.
- **1969-1971: BAYESIAN METHODS – NORAD FEASIBILITY STUDY.** Using the Functional Analysis Computing Laboratory, explored the feasibility of using Bayesian methods to improve the capability of NORAD in a full scale attack. "Is Los Angeles under attack and how much time remains" was the question selected for the Bayesian Instrument. First a statistical instrument was defined for this question using a single Synchronous satellite (fly eye). Next the instrument was used to develop the probability of threat from various missile trajectories. The program was quite successful in evaluating single and multiple threats faster than real time on a non-dedicated machine.

❖ PERSONALLY FUNDED PROJECTS

- **1980-1985: STATISTICAL MECHANICS – SEVERELY DISTURBED GAS**
  - **Purpose:** It had become quite apparent that major economic and political problems would occur over the increasing use of petroleum products and that a possible solution was a thermonuclear reactor. Furthermore, ball-lightning, if properly implemented in a deuterium-tritium environment might be a practical solution.
  - **Challenge:** The basic challenge was to be able to perform a statistical mechanics simulation of a highly disturbed gas on a Heathkit-H89 personal computer (Z80 processor, 64k memory, 3-floppy disk drives).
  - **Effort:** To meet the above challenge, the operating system was extensively upgraded and a version of the numerical functional analysis computing laboratory was developed. This program was used to simulate a disturbed gas. The results were presented in Oslo, Norway.
  - **Results:** The experiment clearly demonstrated the power of the personal computer. Unfortunately the results tended to indicate that not enough points were used to represent the functions.
- **1987-1988: FOLLOW-UP ACTIVITY.**
  - **Prague-1987:** The numerical approximation used in the statistical mechanics experiment presented in Oslo was explored for adequacy in the number of points. Found that the discrete time-dependent representation did not converge to the continuous representation as required by the definition of a continuous function.
  - **Paris-1988:** Found a potential explanation of the findings presented in Prague. Specifically, Demonstrated that one can not prove that time is either continuous or discrete. Specifically, the use of time-dependent differential equations of motion cannot be justified.

ROBERT H. ADAMS **Email:** robert.adams@whatifwe.com

CRYPTOGRAPHY / DATA AUTHENTICATION

❖ LOCKHEED FUNDED PROJECTS

- **1972: CRYPTO PROPOSAL:** US Government representative informally requested an "encoding / decoding" algorithm. A multiple random generator / multiple encryption algorithm was prototyped and proposed.

❖ OCEAN TECHNOLOGY FUNDED PROJECTS

- **1977-1978: VOICE SCRAMBLER.** Developed a voice scrambler based on a high-speed FFT signal processor. Specifically, the input voice signal was divided into a large number of frequency bands by an FFT; the frequency bands were randomly reorganized, and then scrambled signal was reconstructed by an inverse FFT. This voice-scrambler concept was prototyped and successfully tested.
- **1978-1982: WIDE-BAND SECURE VOICE SYSTEM.**
  - **Need:** US companies were selling airplanes to non-NATO allies; these planes needed an exportable voice encryption system to replace, form, fit and function, the non-exportable KY-58.
  - **Algorithm:** 16 kilobit/sec CVSD digitized voice was encrypted by a multi-level pseudo-random generator defined by 128-bit cryptographic key and a 32-bit session-key.
  - **Hardware:** A bit-slice processor was specifically developed for this application. The 4-mhz processor clock and 1 clock-cycle per instruction capability were more than adequate for all of its cryptographic and communication requirements.
  - **Epilogue:** As of this date**,** The Wideband Secure Voice System with the original hardware design is still being built for new customers.

❖ PERSONALLY FUNDED PROJECTS

- **1994-2003: CRYPTOGRAPHIC AUTHENTICATION**
  - **Basic Principles:** Data authentication is an instrumentation process the capabilities of which are improved by multiple independent measurements. This can be accomplished by encrypting the data and parity bits with a pseudo-random generator.
  - **Correct Machine:** There are unique, readable pieces of hardware that can be used as the cryptographic key for the defining random generator. This will insure that a program will run and data will be processed only on a specific machine.
  - **Correct Program:** A state machine requires a large quantity of non-unique, numerically different tokens. These tokens permit the development of functionally identical, but numerically different programs. These tokens can be used as a cryptographic key that attaches data to a specific version of a program.
  - **Network Fuse:** Using a rapid continuous encrypted packet exchange as the communication method in a critical network will greatly decrease its vulnerably to viruses and hackers. Specifically, the packets will be cryptographically authenticated. Any machine that disturbs this continuous packet exchange or fails to properly authenticate each packet will be disconnected from the network.
  - **Correct Data Types:** Unique tokens can be assigned to specific data types. These tokens can be used as a component of the authentication cryptographic key. In addition, tokens representing data can be combined with state-machine process tokens to authenticate the specific step of the process.

ERROR FREE SOFTWARE

❖ LOCKHEED FUNDED PROJECTS

- **1971-1975: Precedence Analysis.** Precedence Analysis provides a means of developing error-free language translators and compilers. A Lockheed-developed compiler writer was upgraded to develop error-free application programs. It was successfully used to manage the process defining several applications.

❖ PERSONALLY FUNDED PROJECTS

- **1992-1993: Medicare Progress Notes Editor.** The goal of this effort was to be able to prepare a custom Medicare Progress Notes Editor in about 10 minutes at the customer's site. A program that wrote this program was developed and successfully used in preparing several custom editors. The primary challenge was verifying that these editors were error-free.
- **1993-2001:**
  - **Software Error Detection.** Software "breaks" irretrievably when it makes an erroneous write. Formal error detection methods were developed which would anticipate an erroneous write, prepare a report, and terminate execution of the program.
  - **Programmable Code Generator:** Using the Macro-processing capability of the assembler as a starting point, a Programmable Code Generator was developed for C, C++. Experience with the custom editor revealed the need to build five source/header files simultaneously.
  - **Multi-dimensional State machine:** It was determined during the development of the Programmable Code Generator that a multi-dimensional state-machine could be used to manage both the process and the data.

❖ EDO-CCS FUNDED PROJECTS

- **2001-2004: ELINT SOFTWARE DEVELOPMENT**
  - **Development Methods:** Both the extensive use of state-machines and the memory-cycling techniques were used as the primary error-prevention methods in the hardware management sub-system of an ELINT system. These techniques trapped all write errors before occurring, resulted in self-documenting source files, and caused coding errors to be detected early in checkout.
  - **Monte-Carlo Debug Method.** A Monte-Carlo Simulator for both hardware simulation and stimulation was developed and used to economic advantage to produce a sub-system with no errors at delivery.
- **2003: ISO-9001.** An ISO-9001 Meeting revealed that PCG and a project's library of software parts could satisfy the enforceable standard methods and procedures requirement of ISO-9001. Also, the ability of developing the libraries of software Parts with the PCG provided the responsible organization with complete control of their standard methods and procedures as required by ISO-9001.

❖ PERSONALLY FUNDED PROJECTS

- **2003-2005: Monte-Carlo Test Systems:** A Monte-Carlo based test system was deveolped to satisfy the ISO-9001 requirement to evaluate the quality of the work-products in the software development process. This system was designed to not only test a product for correct operation, but also to evaluate its ability to detect an error in execution and to resist an error during the design of the product.

ROBERT H. ADAMS **Email:** robert.adams@whatifwe.com

CURRENT PROJECTS

- **PROGRAMMABLE DEVELOPMENT ENVIRONMENT:** The Macro Processor and Monte-Carlo Test system are being combined into an integrated programmable development environment: Included in the upgrade are the following features:
  - The ability to combine multiple macro libraries into a project library. This will enable the division of a large project into manageable tasks and the development and marketing of standard libraries.
  - The number of output files is increased from five to sixteen.
  - The ability of preparing the "make" file needed for compilation.
- **STANDARD PARTS LIBRARY:** Baseline standard parts libraries for C, C++, C#, J#, and Visual Basic are currently being prepared and tested A layered approach is being used which will increase the benefits for each layer added. Layer benefits include:
  - Being able to enforce format standards
  - Transparency over the five output languages.
  - Transparent application of standard error detection methods.