

## **Robert Alan Martin**

### **Education**

B.S.E.E, Electrical Engineering, Rensselaer Polytechnic Institute, 1981  
M.S.E.E, Electrical Engineering, Rensselaer Polytechnic Institute, 1982  
M.B.A., Business Administration, Babson College, 1990

### **Work History**

2015 - Present: Steering Committee member, Industrial Internet Consortium  
1982 - Present: Member of Staff, The MITRE Corporation, Bedford, MA  
1981 - 1981: Software Developer, General Electric,  
Electrical Utilities Systems Engineering Department, Schenectady, NY  
1980 - 1982: Electrical Laboratory Engineer, Rensselaer Polytechnic Institute,  
Center for Interactive Computer Graphics, Troy, NY  
1979 - 1980: Coop Student, Eastman Kodak, Area 2 Engineering, Rochester, NY

### **Work Experience**

Robert Martin is a Senior Principal Secure Software & Technology Engineer in the Cyber Solution division's Trust & Assurance Cyber Technology department which provide support across all of The MITRE Corporation's projects and sponsors as well as a member of the Industrial Internet Consortium Steering Committee. Robert has dedicated his career to working on solving some of the world's most difficult problems in systems and software engineering – including cybersecurity, Y2K, Industrial IoT, and application security and assurance. Much of his work has focused on the interplay of cyber risk management, and quality assessment and assurance.

For the past 35 years, Robert's efforts have been focused on the measurement and management of the risks from the use of software-based technologies as well addressing the new challenges of the Industrial Internet of Things (IIoT), CyberPhysicalHuman issues, quality assessment, and assurance. Within these efforts, Robert has applied his expertise to international cybersecurity initiatives over the past 20 years and is one of the creators of the the Common Vulnerabilities and Exposures (CVE), the Common Weakness Enumeration (CWE), the Common Quality Enumeration (CQE), and the Common Attack Pattern Enumeration and Classification (CAPEC) community initiatives along with being responsible for coordinating the industry engagement and adoption efforts for these initiatives, which each have large active vendor and research communities.

Robert is a frequent international speaker on the various security and quality issues surrounding information technology systems, has published numerous papers on these topics, authored over 30 different standards on various aspects of cybersecurity and assurance, in the ITU-T, ETSI, OMG, The Open Group, Underwriter Laboratory (UL), and ISO, as well as being the chair of the OMG Structured Assurance Case Metamodel Task Force.

Robert is currently engaged in the Industrial Internet Consortium, helping craft key portions of the Industrial Internet Reference Architecture, the Industrial Internet Security Framework, and the Vertical Taxonomy Landscape documents.

2001 - Present: Robert is a driving force in industry-wide efforts to bring the standardization of names and definitions to the world of software security issues across software source code, software design, and software architecture, as well as driving efforts to establish norms of practice in how we understand and share information about how software systems are attacked and how we can better discuss, describe and share information about malware. Robert has helped create and lead the Common Vulnerabilities and Exposures (CVE), the Common Weakness Enumeration (CWE), Common Quality Enumeration (CQE), the Malware Attribute Enumeration and Characterization (MAEC), and the Common Attack Pattern Enumeration and Classification (CAPEC) Initiatives, five international, community-based efforts amongst industry, government, and academia that form a portion of the foundation of the software assurance activities in much of industry and academia across the globe. These initiatives are transforming the way enterprises deal with securing their software-based infrastructure.

These efforts are part of the Software and Supply Chain Assurance initiatives and are being adopted by the bulk of the tool industry and educational providers working this topic as well as being a common foundation for work across NIST, DHS, NSA, GSA, and the various services and agencies in the DoD. These efforts, along with Robert's previous work in quality and vulnerability management are being adopted throughout industry and government as well as being adopted internationally and incorporated into ITU, ETSI, UL, and ISO standards efforts.

Robert is also the co-author of the SANS/CWE Top 25 list that is the basis of contract language regarding software security errors agreements for many in industry as well as the co-author of the Common Weakness Scoring System (CWSS), a standard methodology for prioritizing the weakness to their impact to the intended organizational mission that an application is supporting. CWSS is now an international standard, ITU-T X.1525, along with CVE (ITU-T X.1520), CWE (ITU-T X1524), and CAPEC (ITU-T X.1544).

1995 - 2000: At the culmination of his five years of Y2K leadership and coordination efforts, Robert served as the Operations Manager of the Cyber Assurance National Information Center, a 24x7 cyber security watch center within the President's Y2K Information Coordination Center. Robert also led the development of guidance for dealing with Y2K and the consequence management activities leading up to the culmination of Y2K as well as being the primary author for the Y2K check-list that was used throughout the DoD, Intelligence community, and private industry for managing and recording compliance of their Y2K efforts.

Under Mr. Martin's coordination, MITRE became a recognized leader in addressing the Y2K problem in both the military and commercial environments through its participation in national and international conferences, publications in widely read journals and professional magazines, and the development of a Y2K compliance approach in use throughout the Department of Defense. Mr. Martin was directly involved in all of MITRE's Y2K efforts. He managed the MITRE Y2K Website that received over 425,000 hits per month. Software Magazine called the site one of the top websites devoted to the year 2000 problem.

1992-Present: Robert developed a standardized software quality and risk assessment process (the Software Quality Assurance Evaluation (SQAE)) that has been used over to help over 200 of MITRE's Air Force, Army, and FAA customers improve their software risk identification, software risk measurement, and software acquisition methods as well as the quality, cost, and timeliness of their delivered software products and has been licensed to several organizations as well as formed the basis of collaborative research within the international software engineering community. This assessment methodology has also been licensed at no cost to over a dozen organizations here and abroad and is the basis of much of the Consortium for IT Software Quality (CISQ) Quality Measure for Maintainability.

1992 - 1994: Directed the MITRE support for system maintenance and evolution aspects of the Air Mission Support System (AFMSS).

1991 - 1992: Directed and coordinated documenting the architectural approach and desired characteristics for information systems to satisfy the broad requirements of national and theater level command, control, and communications. This effort addressed identified problems in World-Wide Military Command and Control System (WWMCCS) system's inflexibility, technical obsolescence, and lack of functionality. The effort detailed how to incorporate Open Systems compliant COTS components and improved security into WWMCCS and provided a guide for the Army, Navy, Air Force, Marine Corps, Defense Information Systems Agency (DISA), and Defense Nuclear Agency (DNA), and their contractors for planning upgrades to capabilities in their WWMCCS-related programs.

1990 - 1995: Managed department laboratory equipment and facilities which consisted of SpareStations, IBM RS-6000, VAXstations, IBM PC 386-clones, and Apple Macintoshes running a secured version of Unix.

1990 - 1992: Coordinated Air Force LAN design and installation efforts including systems engineering support in the evaluation of the LAN designs provided to the Air Force by their LAN contractor, as well as participation in Site Visits and Design Reviews at the Air Force sites.

1989 - 1993: Technical support to the Air Force and DISA in administrating the Workstation contract including support at conferences with users, providing guidance on the correct technical configurations for workstation orders, verification of the contractual compliance of the Workstation, evaluation of product substitution proposals, evaluation of all candidate software updates, participation in the security certification efforts of the Government, providing technical and programmatic guidance on TEMPEST product issues, providing guidance on configuration management issues, technical support in the development of the Liquidated Damages Settlement, and providing useful information for inclusion in the monthly WWS newsletter.

1988 - 1993: Directed and coordinated the various activities related to the integration of the new Workstation into the WWMCCS environment. The main emphasis of this task was education, information dissemination, and guidance on the use of the new technology. The concepts of workstation and LAN security, POSIX operating systems, multi-user UNIX systems, Network Services like GOSIP, NFS, and the DOD Protocols (Telnet, FTP, and SMTP), and development tools for X-Windows, MOTIF, 'C', and Ada were all new to the programs, projects, and personnel of WWMCCS. Mr. Martin dealt with the incorporation of the use of the Workstation into the operational security policies and procedures at each command. A central issue in this

area was the security issues related to the attachment of the Workstation to a LAN, security of the LAN, and Network management of the LAN.

1988 - 1990: MITRE lead on Air Force/DISA Secure Workstation acquisition including development of the Specification and other acquisition documents. Mr. Martin led the technical analysis and support to the Workstation Program Manager, Buyer, and Contracting Officer for the acquisition. Mr. Martin directly supported the Program Manager, the Source Selection Evaluation Board Chairman, the Source Selection Advisory Council, the Government Lawyer, Contracting Officer, and the Source Selection Authority through all phases of the Source Selection process including Negotiations and the subsequent contract protests before the GAO.

1988 - 1991: Led the team that developed a File Transfer capability for the WWMCCS Honeywell GCOS mainframe using the Kermit file transfer protocol including a User and Programmer Guide. A fully documented version of the host-based Kermit File Transfer capability was provided and approved for use as a WWMCCS Standard software in July 1990.

1986 - 1987: Investigated DBM technology and the possibility of its use in the WIS program including an in-depth look at Teradata, Britton Lee, and Sybase database management systems.

1986 - 1988: Participated in multi-organization "Design Teams" as the Air Force technical lead to resolve the technical and organization specific technical problems encountered during the design effort of the WWMCCS Block B upgrade.

1984 -1986: Investigated the performance of the Automated Message Handling (AMH) system design by developing and running a realistic prototype of IBM's intended use of Model 204, using data and transactions in accordance to those the AMH system was to support in a worst-case situation and measuring the performance against the contractual requirements.

1984 - 1984: Investigated the utility of COTS Database Management Systems for use in WWMCCS replacement through prototype applications developed in the 4GL, Natural, and used the DBMS, ADABAS.

1983 - 1984: Participated in joint requirements analysis and system design for the replacement of WWMCCS that had to support the Military Crisis Planning Process, the Deliberate Planning Process, and the Joint military command and control doctrine and processes.

1983 - 1983: Analyzed the ability of mainframe Commercial Off-The-Shelf (COTS) (circa 1983) to meet the needs of Air Force in modernizing the Air Force WWMCCS components. Documented and illustrated several non-COTS capabilities that would still need to be supplied through development.

1982 - 1983: Participated in a study of WWMCCS Standard Systems versus Air Force and Command-Unique Systems, estimating the software replacement costs for the Air Force.

### **Professional Society or Association Memberships**

Mr. Martin is a member of the Institute of Electrical and Electronics Engineers (IEEE), the IEEE Computer Society, the Association for Computing Machinery (ACM), the National Defense

Industrial Association (NDIA), the International Council on Systems Engineering (INCOSE), the Armed Forces Communications and Electronics Association (AFCEA), a Distinguished Advisor for Consortium for IT Software Quality (CISQ), and serves on the Program Committees of several technical conferences including OWASP's AppSec conference, the International Workshop on Assurance Cases for Software-intensive Systems, the International Conference on IT Security Incident Management and IT Forensics, and the International Symposium on Engineering Secure Software and Systems (ESSoS), as well as being an ISC2 Certified Software Security Lifecycle Professional.

### **Publications (selected)**

- Assuring Trustworthiness in an Open Global Market of IIoT Systems via Structured Assurance Cases, Journal of Innovation issue 9, Sep 2018.
- Evaluating the Security of Industrial IoT Testbeds, IIC's Journal of Innovation issue 7, Mar 2018.
- The Industrial Internet of Things and Why You Should Care, The SciTech Lawyer volume Vol. 14, issue No. 3, Mar 2018.
- There is No One-Size Fits All Approach to the CyberPhysicalHuman World, MITRE Cybersecurity Blog, Jan 2016.
- More Ancient Wisdom for the CyberPhysicalHuman World of Today, MITRE Cybersecurity Blog, Jan 2016.
- Coming Closer and Closer to You, MITRE Cybersecurity Blog, Dec 2015.
- Non-Malicious Taint: Bad Hygiene is as Dangerous to the Mission as Malicious Intent, CrossTalk Magazine, volume 27, issue 2, Mar 2014.
- The Software Industry's "Clean Water Act" Alternative, IEEE Security & Privacy volume 10, issue 3, May 2012.
- Practicing Standards-Based Security Assessment and Management, IANewsletter, volume 13, issue 1, Dec 2010.
- Systems Assurance as a Team Sport, CrossTalk Magazine, Vol 23 No 2, Mar 2010.
- Making Security Measurable and Manageable, CrossTalk Magazine, Vol 22, No. 6, Sep 2009.
- Being Explicit About Security Weaknesses, CrossTalk Magazine, Vol. 20 No. 3, Mar 2007.
- Transformational Vulnerability Management Through Standards, CrossTalk Magazine, Vol 18 No. 5, May 2005.
- The Evolution Path for Industrial Software Quality Evaluation Methods Applying ISO IEC 9126:2001 Quality Model: Example of MITRE's SQA Method, Software Quality Journal, 13, 17-30, 2005.

- Managing Vulnerabilities in Networked Systems, IEEE Computer Magazine, volume 34, issue 11, Nov 2001.
- The Vulnerabilities of Developing on the Net, CrossTalk Magazine Vol 14, No 4, Apr 2001.
- Managing Software Quality Throughout the Lifecycle, MITRE 1998 Software Engineering and Economics Conference, Jan 1998.
- Year 2000 compliance: a discussion on compliance certification, Computer Software and Applications Conference, 1997. COMPSAC'97. Proceedings., The Twenty-First Annual International, Aug 1997.
- Dealing with dates: Solutions for the year 2000, IEEE Computer Vol 30, Issue 3, 44-51, May 1997.
- Providing a Framework for Effective Software Quality Measurement: Making a Science of Risk Assessment, INCOSE International Symposium 6 (1), 1158-1165, Jul 1996.
- Using Product Quality Assessment to Broaden the Evaluation of Software Engineering Capability, Software Engineering Process Group Conference, "Broadening the Perspective for the Next Century," Research Gate, May 1996.
- Providing a framework for effective software quality assessment, First Annual MITRE Software Engineering & Economics Conference, CiteSeer, Apr 1996.
- Workstation Segment Specification for the World-Wide Military Command and Control (WWMCCS) Information System (WIS), ESD-TR-89-197, DTIC, Jul 1989.