**ARTICLES & NEWS**
- Chair Message - **Nicole Radziwill**
- SQP Journal Article - Beyond CMMI Level 5 - **Naomi Honda**

**ANNOUNCEMENTS**
- SQP Journal Seeks Volunteers – **Sue Carroll**
- Participate in the development of IEEE P730 – **Sue Carroll**

**COLUMNS**

**Medical Device Software**
- Improving Performance in Medical Device Software Engineering – **David Walker**

**Get Certified**
- Try the 4th Quarter CSQE Quiz – **Linda Westfall**

**Standards**
- Fall 2009 Standards Report - **Theresa Hunt**

**From the Regions**
- Region 6 Pacific Northwest – **Tom Gilchrist**
- Region 10 Michigan – **Louise Tamres**

**CONFERENCES & WEBINARS**
- Synopsis of the 2009 FAA National Software Conference - **Mike Kress**
- 2010 Institute for Software Excellence - St Louis - May 24-26

**QUESTIONS OR COMMENTS?**

See:
- Software Division Web Site
- Software Division Management

Or Contact:
- Nicole Radziwill, Chair
- Greg Zimmerman, Chair-Elect
- Hank Sobah, Secretary
- Brenda Fisk, Treasurer
- Nicole Radziwill, Newsletter Editor

How can we improve Software Quality Live? Does this issue provide helpful information? Let us know!
Hello to all ASQ Software Division members.

This is my first message to you as Chair of our Division. Although I was scheduled to assume the role in June 2010, I've had to come in early as a result of the illness of our previous Chair, Bill Trest. Bill has been involved in the Division for several years, and in addition to his leadership as Chair, he also facilitated the work of our Regional Councilors. We thank Bill for all of his efforts during this time, and we are pleased that he will be continuing to participate in Division activities on an occasional basis. His kindness, diplomacy, and talents as a software quality specialist will be missed.

Let me first introduce myself. My name is Nicole Radziwill, and I'm currently on the faculty of James Madison University in the Department of Integrated Science and Technology. I have 15 years of experience as a leader at the senior and executive levels of software-intensive organizations, in enterprise software, telecommunications, and for major scientific research facilities. I am an ASQ Certified Manager of Quality and Organizational Excellence (CMQ/OE) and my Ph.D. is in Technology Management with an emphasis in Quality Systems. I look forward to working with everyone in the Software Division over the next few years to catalyze our offerings to members, as well as to stimulate our membership to achieve new breakthroughs in the discipline of software performance excellence.

I'm writing this message from the Hilton in Northbrook, Illinois, where we're getting ready to host the 2009 International Conference on Software Quality. This annual event brings together about 150 software quality professionals for talks, tutorials, and networking. This year, we're proud to host keynoters Bill Curtis (an IEEE fellow speaking on quality control in large, multi-tier applications), Joe Jarzombek (responsible for software quality at the Department of Homeland Security), and Edy Liongosari (from Accenture Technology Labs, fellowship speaking on quality control in large, multi-tier applications), Joe Jarzombek (responsible for software quality at the Department of Homeland Security), and Edy Liongosari (from Accenture Technology Labs, sharing information about how millenials, security and sustainability will be dominating themes in the software quality at the Department of Homeland Security).

Although it’s been a busy 2009, we’re gearing up for an even more exciting 2010. Please plan on meeting with us at the Institute for Software Excellence (ISE), a conference-within-a-conference at the World Conference on Quality and Improvement (WCQI) in St. Louis, Missouri in May 2010. We had a great time at ISE '09 in Minneapolis, and we’re planning on an even more hospitable hospitality suite if you missed the excitement last spring. (And who knows… we might have more "tricks" up our sleeves too!)

Nicole Radziwill
Chair, Software Division
nicole.radziwill@gmail.com

ANNOUNCEMENTS

SQP Journal Seeks Volunteers
By Sue Carroll

Software Quality Professional (SQP) Journal is an ASQ journal supported by the ASQ Software Division. Each issue has 3-4 peer-reviewed articles, book reviews, and a Quality Nugget. If you would like to write an article for the journal – see the author guidelines. If you would like to write a Quality Nugget – it is around 1000 words and should be sent directly to me. The Quality Nugget editor will review it. Please help us out with some practical tips that can be easily used by the readers of SQP. If you would like to volunteer to review articles or books, or write a letter to the editor contact sue_carroll@bellsouth.net.

In each quarterly issue there is an article that is available to non-subscribers. The abstract and a link to the current article is in the Articles section of this newsletter.

 Participate in the development of IEEE P730
By Sue Carroll

I joined the P730 working group when it first started. I started off just reading the listserv mailings. Then I called into the LiveMeeting synopsis of the face-to-face meetings. I have been involved in SQA for over two decades now, so the topic was of great interest to me. I offered to host a face to face meeting at SAS because I knew I would attend and could get other SAS folks involved in the group. We had that meeting in February of this year. I was then able to attend the face to face meetings in Texas and Illinois. During that time, I have really seen the group pull together and earnestly begin the process of constructing the standard.

IEEE P730-1981 was the first IEEE software engineering standard written. That version and the current version of P730 are on software quality plans. That is certainly helpful and gets folks going in the right direction – but SQA is more than planning. The revised standard will cover all aspects of Software Quality Assurance. With the expanded scope we have a need for the SQA experts in all fields to join in this effort and help create a robust standard.

Along with vastly increasing our scope – the new standard must align with the ISO/IEC 12207 standard on Software Life Cycle Processes. This has created a challenge for the group as some activities normally considered part of SQA were considered so important by 12207 that they are pulled out of the SQA clause of the standard and are put into separate sections. These include reviews, audits, V&V, and SCM to name a few. The group has come up with ways to address SQA from a 12207 point of view but still provide guidance on these other aspects of SQA.

Would you like to see what we are doing? The web portal for IEEE P730 Working Group is http://www.computer.org/portal/web/sqa. This site is open to all to see our ongoing work. When you navigate to our page – there will be grey menu items starting with SQA Home. Go to File Library. In that area there are folders for Copyright Standards (open to active members only), Deliverables, and General (meeting minutes and action items). Go into Deliverables and there are folders for Annexes, Sections, and Section 5.2. If you scroll down the page, this section also contains the draft standard and other documents.

Annexes are information the group agrees will be helpful to SQA professionals to do their job. Current plans are to include two normative annexes:
- the elements of an SQA plan
- a table that links all clauses of ISO/IEC 12207 to SQA activities.

Then there will be informative annexes on:
- CMMI Development Product and Process Quality Assurance
- Software Audits and Reviews
- Support of SQA Organizations above ISO 15504 Capability Level 2
- Cross-reference to SQA Practices Referenced by Certification Schemes
- Support of Industry Specific SQA Standards

The sections folder is for all text written for the standard in every section but 5.2. This includes the introduction, the SQA process and outcomes. There will also be a section on the relationship with IEEE Std 12207-2008. Processes many consider part of the role of SQA. These include:
- Software Documentation Management Process
• Software Configuration Management Process
• Software Verification Process
• Software Validation Process
• Software Review Process
• Software Audit Process
• Software Problem Resolution Process
• Software Qualification Testing Process

What is section 5.2? It is the 12207 text about SQA with each clause (usually only a sentence or two) put in a section with text added to explain the concept. The group has done a lot of work in this section. We have researched other standards and methodologies to find details about each concept. This added to the experience of the group has made these sections rich with content.

If you would like notice about upcoming meetings, join our listserv. Send email to me, sue_carroll@bellsouth.net and I’ll add you to the list and you’ll get notified about upcoming meetings. We invite your participation and the contribution of your experience!

Future IEEE P730 Working Group meetings:
1. Phone/LiveMeeting in early January 2010.
2. February 17-19, 2010: face to face meeting in Cary, NC. If you can’t join us, we’ll have Phone/LiveMeeting updates daily.
3. Phone/LiveMeeting in April.
4. June 2010: face to face meeting in Cambridge, MA with Phone/LiveMeeting updates daily.

We need people who are passionate about software quality to help develop the next version of this important standard. You can participate by attending WG meetings or remotely via LiveMeeting. You can help draft sections, review drafts, or just read the listserv, just like my first involvement in the group. IEEE membership not required. Previous standards experience not required.

Improving Performance in Medical Device Software Engineering with CMMI

By David Walker

The Capability Maturity Model Integration * (CMMI®) has been successfully applied for process improvement in various product development environments for almost 10 years, with its predecessor, the Software Capability Maturity Model (CMM- SW) used successfully in the 1990s. The Software Engineering Institute has provided reports on the successful use of the CMMI in aerospace, defense, government, financial, and insurance industry sectors. Little is known of adoption in medical device engineering.

This paper summarizes the comparison performed between the CMMI and the regulations and standards that drive software intensive medical device product development. The primary perspective is for medical device software engineering,

where the most significant opportunity lies. This paper shows what is missed when medical device engineering teams chase ISO 13485 and IEC 62304 compliance without using CMMI to effectively manage processes.


David Walker is the immediate past chair of the ASQ Software Division. He represents ASQ’s interests in medical device software standards development through membership on the AAMI Medical Device Software Standards Committee.

CSQE Quiz for 4th Quarter 2009

By Linda Westfall
Copyright © 2009 Linda Westfall. All Rights Reserved

Note: The items in these quizzes are NOT from the past CSQE examinations NOR were they created as part of the CSQE exam development process.

1. Which of the following would be an appropriate use for the ISO 9001 Standard?
   a. As an outline for establishing a template for a software quality assurance plan
   b. As a checklist for verifying the completeness of a project’s work breakdown structure
   c. As requirements for establishing and maintaining a quality management system
   d. As evaluation criteria for conducting a software configuration management audit

2. Plans for which of the following activities would be documented as part of a project’s software quality plan?
   a. Focus groups
   b. In-process audits
   c. Design modeling
   d. Process tailoring

3. Storyboards are most appropriately used during:
   a. Project planning
   b. Design specification
   c. Peer reviews
   d. Requirements elicitation

4. Retrospectives are held in order to ensure that:
   a. lessons learned are captured and transitioned into process improvements.
   b. project goals and objectives are met before project closure.
   c. the software meets its requirements before the product is shipped.
   d. variances between planned and actual performance do not exceed acceptable levels.

5. The output from which of the following quality analysis tools would be most likely to be used as input into creating a Pareto chart?
   a. Control chart
   b. Histogram
   c. Run chart
   d. Check sheet

6. Which of the following is dynamic analysis technique used for evaluating software products?
   a. Proofs of correctness
   b. Testing
   c. Code analyzers
   d. Peer reviews

7. Which of the following would typically NOT be included in an automated build script?
   a. The location of code components in the configuration libraries
   b. A traceability matrix linking source code to test cases
   c. The compiler option settings to be used
   d. Pointers to included macros, libraries and files

See answers on next page.
Answers to the Certified Software Quality Engineering Quiz for 4th Quarter 2009

1. Answer C is correct. The ISO 9001 standard defines the specific set of quality management system requirements.
   CSQ Body of Knowledge Area: IV.C

2. Answer B is correct. Quality plans define the specifics of how a project intends to implement the organization's quality management system in order to meet the quality goals and objectives of the organization and of that project.
   According to the IEEE Standard for Software Quality Assurance Plans, the software quality plan should include plans for all of the reviews and audits (or pointers to separate plan documents) that will be held as part of this project.
   CSQ Body of Knowledge Area: IIA.3

3. Answer B is correct. Similarly to the panels in a comic strip, a storyboard graphically illustrates who the characters are in a story and describes the order of what happens to those characters and how it happens.
   Storyboards are mainly used in requirements elicitation to describe the human user interfaces. Pictorial sequences can many times be easier for stakeholders to visualize and interpret than written steps. This can aid in understanding and provide a basis for discussion about what needs to happen and how.
   CSQ Body of Knowledge Area: IIA.3

4. Answer A is correct. Retrospectives are a technique for the elimination of repeated mistakes by providing a mechanism for capturing and analyzing lessons learned in order to identify improvement opportunities.
   CSQ Body of Knowledge Area: IV.B.3

5. Answer D is correct. Check sheets are tools used in data collection. In their simplest form, check sheets make the data collection process easier by providing prewritten descriptions of categories or events that should be counted either from historic data or as events occur in the future. The data collected on a check sheet can be used as input into creating a Pareto chart or a histogram.
   CSQ Body of Knowledge Area: V.C.3

6. Answer B is correct. Dynamic analysis includes methods of performing V&V by evaluating a software component or product by executing it and comparing the actual results to expected results. Testing and simulations are forms of dynamic analysis.
   CSQ Body of Knowledge Area: V.A.1

7. Answer B is correct. The build process is automated using a command file called a build script, which specifies:
   • The components of the build (source and derived)
   • Their versions
   • Their locations in the configuration libraries
   • The build tools, including compilers, assemblers, linkers, loaders, and build scripts
   • Their versions
   • The required setting for options and environmental parameters
   • Pointers to the appropriate macros, libraries, and other files to be included
   • Their versions
   • Their locations in the configuration libraries
   CSQ Body of Knowledge Area: VII.B.2

Linda Westfall is president of The Westfall Team, which provides training and consulting in software engineering, quality and project management.
For more information please visit our web site at www.westfallteam.com

FALL 2009 STANDARDS REPORT

By Theresa Hunt

The U.S. TAG met in Pittsburgh September 9-11, 2009. This report provides a graphic overview of the current SC7 standards collection, presents the results of recent ballots, and provides the proposed meeting schedule.

For more information please visit our web site at www.westfallteam.com

CSQ Body of Knowledge Area: III.C.2

Recent Ballots
• At the September 9-11, 2009 U.S. TAG meeting in Pittsburgh the Software Division voted to agree with the U.S. National Body (USNB) to DISAPROVE with comments the following ballots:
  • FPDISP 29110-4, Software Engineering - Lifecycle Profiles for Very Small Enterprises (VSE) - Part 4: VSEP Basic Profile Specification
  • Combined CD Registration and CD Ballot of WD 29155-1, Software and systems engineering - IT
The TAG voted to agree with the U.S. National Body (USNB) to APPROVE the following ballots:

- FDIS ISO/IEC 25045 Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Evaluation module for recoverability

Recently approved New Work Items (NWIs) and active study groups:

- ISO/IEC NP 26521 Software and Systems Engineering - Tools and methods of requirements engineering and management for product lines
- ISO/IEC NP 29169 Information technology -- The application of conformity assessment methodology to process capability and organizational maturity
- ISO/IEC NP 90003 Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software
- ISO/IEC NP 90006 Information Technology -- Guidelines for the application of ISO 9001:2000 to IT service management.
- ISO/IEC DIS 26500 Information technology -- Application management -- Requirements for application management

2010 – Active Study Groups:
- Framework for Software Processes Methodology
- Agility
- Service Oriented Architecture (SOA)
- IT Enabled Services (ITES)
- Embedded Systems
- System Integration
- Guidance for Process Description
- Tools and Methods of Software Testing
- IS Governance for Cloud Computing
- IS Governance for Service Providers
- IS Governance for IT Audit
- IS Governance for Enterprise Architecture
- Software Engineering Certification Schemes

Upcoming Meeting Schedule
JTC1 plenary schedule (The SC7 annual plenary session is scheduled in or around the May timeframe for the purpose of collaboration and coordination among life cycle projects):
- 2010 – Niigata, Japan (May 23-28)
- 2011 – Paris, France
- 2013 – Canada (to be confirmed)

Interesting items on the Lima Peru meeting agenda

- There is an agenda item to produce next draft of project 29154 Software Engineering -- Certification of Software Engineering Professionals – Guidelines and Examples.
- There is an agenda item to produce first draft for PDTR INCOSE Systems Engineering Handbook, version 3.
- There will be a discussion on the status of the work of the study group that will analyze existing certification schemes.
- Also there will be several Life Cycle Process Harmonization Advisory Group (LCPHAG) meetings that week. The LCPHAG works to improve harmonization throughout the SC7 set of standards.

If you are interested in participating in the review of standards please contact me at TheresaHunt@cfl.rr.com or Theresa.Hunt@Navy.mil.
The following links will provide you with a snapshot of the latest activities in the regions.

**Region 6 Pacific Northwest** – Tom Gilchrist

If you are in the Seattle area on the third Thursday of every month (except December), The Seattle Area Software Quality Assurance Group (SASQAG) holds monthly public meetings in the Seattle area. SASQAG also supports certification and study groups. If you are in the area and want to attend, please look at www.sasqag.org for upcoming events, directions, and meeting time.

October 26-28, 2009, the annual Pacific Northwest Software Quality Conference was held (http://www.pnsqc.org/) in Portland, Oregon. The title of this year’s theme, “Moving Quality Forward”, was slightly ambiguous on purpose—consider these two possibilities:

- Moving the profession of software quality ahead - making it more of a recognized field, like civil engineering.
- Moving the validation and verification tasks further upstream in the software development life cycle and even moving them into other functions of the organization (e.g. finance, legal, service, sales, and marketing).

PNSQC had a new venue for PNSQC 2009 — the World Trade Center Portland.

This venue offered an environment more conducive for intimate networking and interaction among attendees. The distinctive facility, located in the heart of downtown Portland, offers a breathtaking setting and spectacular backdrop overlooking the Willamette River and Tom McCall Waterfront Park.

The Seattle SPIN (Software Process Improvement Network) is holding meetings on the first Tuesday, five months a year. The organization is driven with a single, clear-cut goal in mind: change an organization in a way that improves that organization's ability to develop software. If you are interested in more information on SeaSpin, you can go to [http://www.seaspin.org](http://www.seaspin.org)

**AS9115 Software Quality Program for Aerospace Organizations** – This standard is a supplement to AS9100 for those organizations that supply software as an end item or as part of a product. The supplement is not mandatory unless called out by the software acquirer. It provides the acquirer/auditor greater granularity and specificity when auditing the software. This gives the customer greater assurance that the principles and disciplines of AS9100 will be enforced for software development as well as hardware. The supplement is in the final ballot review.

The authors are meeting in Washington D.C. in Aug to reconcile all international comments. Mike Kress is the leader of the AAQG team on this project and may be reached at [michael.p.kress@boeing.com](mailto:michael.p.kress@boeing.com).

If you have information on local software quality and testing events in your area of Region 6, please send them to me for our events calendar. Visit [http://www.tomtong.com/aaqg](http://www.tomtong.com/aaqg) for information on events around Region 6.

Tom Gilchrist, Region 6 ASQ Software Division

tom@tomtong.com

**Region 10 Michigan, Northeast Indiana & Northwest Ohio** – Louise Tamres

Region 10 covers Michigan and parts of northern Ohio and northwest Indiana. Most of the groups listed here are in southeastern Michigan. Please help me find out about other groups and events in your area. Send me an e-mail to the address shown at the end of this report.

The 4th Great Lakes Software Excellence Conference was held in November in Grand Rapids, Michigan. To find out about the next conference (dates, call for papers), visit the conference web site periodically at www.glsec.org.

The Great Lakes SPIN meetings occur on the second Wednesday or Thursday of every other month from September through May. Locations vary throughout the greater-Detroit area. The GL-SPIN frequently sponsors CMMI and SPICE training programs. Upcoming programs in 2010 include: On January 14, a Panel on embedded topic, with intent to attract EE/ME students. The March 10 program features a presentation on “Natural Laws of Software Development”. The April 8 topic is "Seeing Beyond C", and the May 13 program in titled "SharePoint as an end item as or as part of a product. The supplement is not mandatory unless called out by the software acquirer. It provides the acquirer/auditor greater granularity and specificity when auditing the software. This gives the customer greater assurance that the principles and disciplines of AS9100 will be enforced for software development as well as hardware. The supplement is in the final ballot review.

The authors are meeting in Washington D.C. in Aug to reconcile all international comments. Mike Kress is the leader of the AAQG team on this project and may be reached at [michael.p.kress@boeing.com](mailto:michael.p.kress@boeing.com).

If you have information on local software quality and testing events in your area of Region 6, please send them to me for our events calendar. Visit [http://www.tomtong.com/aaqg](http://www.tomtong.com/aaqg) for information on events around Region 6.

Tom Gilchrist, Region 6 ASQ Software Division

tom@tomtong.com

**Ann Arbor Software Quality Professionals** (AASQP) has suspended its monthly meetings due to low participation. The mailing list remains active as a source of communication and information for software quality professionals in southeastern Michigan. Access is through the Yahoo group [http://tech.groups.yahoo.com/group/aasqp/](http://tech.groups.yahoo.com/group/aasqp/)

ASQ chapters in southeastern Michigan provide programs primarily related to manufacturing. Any programs focusing on software and software quality will definitely be highlighted when available.

Michigan Agile Enthusiasts offers meetings and programs at various locations. As of this writing, the program schedule listed events through November 2009. Find out about their events at [www.agileenthusiasts.ning.com](http://www.agileenthusiasts.ning.com).

Are any software quality professionals in southeastern Michigan interested in CSQE exam preparation or other training courses? If either of these educational opportunities interest you (whether as an attendee or as an instructor), do let me know at [LTamres@computer.org](mailto:LTamres@computer.org).
Synopsis of the 2009 FAA National Software Conference
San Jose CA Aug 18-20, 2009
By Michael P. Kress
Associate Technical Fellow
Boeing Commercial Airplanes

Foreword:
This synopsis is inspired by a practice an old colleague began many years ago of actually reading complete proceedings from conferences and “synopsizing” them down to a few noteworthy highlights for those of us who either didn’t attend or were too busy to read lengthy articles. I continued the practice when he retired. It became very popular on the ASQ Software Division website and also here at Boeing. This synopsis summarizes some of the papers deemed most relevant to the certification, configuration control and conformity processes for airborne software for commercial aircraft.

This year’s event covered approximately 50 papers outlining the advancement of processes, methodologies and regulations within the FAA for airborne software. In addition, Airborne Electronic Hardware, aeronautical data bases were emphasized. Software security was addressed in greater depth than previous workshops. I have added a new feature to this synopsis (IN 50 WORDS OR LESS) to allow the time-strapped reader to decide if he/she is interested in reading further. The complete proceedings are on CD and are available from the author.

NextGen – System of Systems
Ron Stroup
FAA Chief Systems Eng for Air Ground Integration
Mr. Stroup is the Chief Systems Engineer for Airborne and Ground Integration for the FAA’s Air Traffic Organization’s NextGen Integration and Implementation Office. He holds a BS degree in Avionics engineering from Parks College of Saint Louis University and a Master of Science in Information Management from Syracuse University. Mr Stroup served as an Aviation Safety Engineer in the Chicago Aircraft Certification Office from 1989 to 1997 and as the Software Technology Specialist in the Special Certification Office in Fort Worth from 1997 to 2000. He is responsible for overall integration of the Next Generation Air Transportation system.

IN 50 WORDS – The next generation of Air Traffic Management will provide efficiencies that will enhance air travel by reducing departure, arrival and weather delays, improve communication and accuracy, increase airspace density to allowing more aircraft to take off and land safely, and provide greater safety and security.

The presentations in this Synopsis are in no special order, however, I will lead off with this presentation because I found it most exciting.

All of us have been caught up in departure and arrival delays caused by weather, air traffic, ground traffic, gate availability, go-arounds, etc. These are the delays we know about. But there are a lot of behind the scenes inefficiencies in air travel that we never see. Visibility Limited Airfield Parameters, ground based navigation and surveillance, voice (vs. digital) data exchange, human vs. automation assisted Air Traffic Management. And how many of us have flown into airports with no radar in low visibility. (Juneau?) It’s scary.

Seventy percent of all delays are weather related. The NextGen ATM system will be based on SWIM (System Wide Information Management.) SWIM will integrate:

- Airline Operations
- Airspace Management
- Flow Management
- Traffic Management
- Separation Management
- A partial list of NextGen capabilities will include:
- ADS-B Automatic Dependent Surveillance – Broadcast
- CATM – Collaborative Air Traffic Management
- High Density Airspace
- Network Enabled Weather
- Electronic Flight Bag
- Trajectory-based airspace
- Initial surface situation monitoring and reporting
- Point in space metering
- Integrated arrival and departure airspace management
- Improved Area Nav/Required Navigation Performance (RNAV/RNP) procedures.

TIS-B, Traffic Information Services, will provide properly equipped aircraft with position reports from secondary surveillance radar, and FIS-B, Flight Information Services, will provide National weather Service products, temporary flight restrictions, and special use airspace. Safety and security today is “forensics” oriented (learn after the fact); NextGen will be probabilistic and predictive. RNAV/RNP will allow multiple precision paths to the runway, reduce separation requirements thereby increasing airspace capacity, and manage multiple departure paths from each runway thereby increasing departure capacity.

Near term, mid-term, and far term goals are being laid out where near term goals are leveraged on existing technologies including RNAV/RNP, VNAV (vertical navigation), electronic flight bag, and flight information services. Mid to long term goals are stretched out from 2012 – 2018. The FAA is committed to working with industry and sharing risk and cost.

Complex Electronic Hardware (CEH) Tool Qualification
Dr. Brian Butka
Embry Riddle Aeronautical University
College of Engineering
Dr. Butka is an Associate Professor of Electrical and Systems Engineering at Embry-Riddle University. He specializes in design of safety-critical hardware and avionics applications of software defined radio. He has 25 years experience in design, verification, and validation of complex and mixed signal semiconductor devices.

IN 50 WORDS OR LESS – This presentation compares the tool qualification criteria of 178B with that of 254 and also discusses the pros and cons of independently qualifying tools vs. not using tools. It also discusses pitfalls of using metrics or service history for tool qualification.

Dr Butka began with an overview of the process steps in the design, build and verification of CEH. He outlined the generic steps known by various names and definitions. The names he used are:
- Design or schematic entry
- Hardware Description Language (HDL)
- Synthesis
- Place and Route (P&R)
- Timing analysis, Power analysis, time simulation, programming configuration

He noted the difference between the definition of tools in 178B and DO-254, with the 178B definition being simplistic and unhelpful.

“A computer program or a hardware device used to help develop, test, analyze, produce or modify hardware component, subsystem, system or its documentation”

As compared to the 254 definition:
- Design Tools -Tools whose output is part of hardware design and thus can introduce errors. For example, an ASIC router or a tool that creates a board or chip layout based on a schematic or other detailed requirement (used to generate the hardware item or the hardware design, thus an error in the tool could introduce an error in the hardware item)

Verification Tools -Tools used to ensure performance against predeterined standards or requirements. These tools do not introduce errors, but may fail to detect them. For example, an analog or digital circuit simulator or an automated test that measures actual circuit performance may cause the tool to fail to detect an error in the hardware item or hardware design)

He recommends Design tools for Design Assurance Levels (DALs) A, and B and C, and Verification tools for DALs A and B.

He suggests that it may be more challenging and time consuming to independently verify the design tool than to develop the design without the tool.

Dr Butka went on to explore the Pros and Cons of simulation vs actual hardware testing. Actual
hardware testing may have an advantage over simulation because numerous effects are poorly modeled in simulations, such as Crosstalk & Noise, Signal Integrity and Power Integrity.

He recommended considering using quality metrics from various IEEE and ISO standards, such as usability, functionality and efficiency, however cautioned that metrics can be misleading as well. He likened using service history that could be unreliable, such as the trend in housing prices in Florida that grew steadily for 15 years only to crash in 2007.

He cited the well-known and often quoted Ariane rocket failure. On the maiden flight, the inertial navigation system ran into a number that was too large for the destination register to store. The resulting error caused the navigation system to shut down. The backup navigation unit came online, but ran into the same problem. The rocket was destroyed before it crashed into the Earth. The problem was caused by the new rocket being much faster than the previous Ariane. The service history was not relevant.

He concluded with the following recommendations:

The success of the DO-254 design assurance process depends on the expertise of the designers, the requirement writers and the validation team. Design assurance requires:

- Knowledge of the design technology
- Knowledge of the design's application and environment
- Expertise in use of the design and verification tools.

Inexperienced teams should be expected to produce more independent assessment evidence than experienced teams.

**Aviation Safety- The European Union System**

Jean-Luc Delamaide

European Aviation Safety Agency (EASA)

Jean-Luc is the Head of Section "Software and Complex Electronic hardware" of EASA. He joined the EASA in 2005 after 7 years as airborne software specialist within the French NAA (DGAM-DGAC) where he coordinated the A380 SW and CEH aspects of certification. Within the EASA today, his goal is to deal with all aspects related to SW and CEH including certification, research, and rule-making.

IN 50 WORDS OR LESS - EASA is the regulatory agency for most of Europe that is in partnership with National Aviation Authorities. It has working arrangements and Bilateral agreements with all major aviation agencies worldwide. (This is an abbreviated report. See last year’s SYNOPSIS of the Denver FAA Workshop for greater detail).

Jean-Luc showed an organization chart for EASA. Main objectives are pretty much the same as the FAA:

- Product safety oversight
- Organizations oversight
- Safety Oversight
- Development of regulatory material
- Safety assessment and promotion
- International technical coordination.

EASA uses two forms of regulation:

- Implementing Rules (IRs) – mandatory compliance
- Alternative Means of Compliance (AMCs) – provides the presumption of compliance. Interestingly EASA uses a ETSO (European Technical Standard Order).

EASA has “working arrangements” with non-EU CAA’s (Canada, Brazil, China, Israel) and Bilateral agreement FAA and the European Union. They have “Technical Cooperation” with Southeast Asia, China, and India. EASA participates in standards development and industry advisory material with EUROCAE (European Organization for Civil Aviation Electronics) much like the similar relationship the FAA has with RTCA. EASA also participates in the SAE Aerospace Council and ASTM.

EASA uses Certification Memos (much like the FAA uses Issue Papers) for the following areas:

- Software and Airborne Electronic Hardware
- Configuration Files
- Aeronautical Databases
- Model Based Development
- Object Oriented Techniques
- MCDM at the object code level
- Data buses

EASA uses project specific “Certification Memo”. Basic requirements are harmonized with FAA policies and CAST (Certification Authorities Software Team) papers. EASA has a website similar to the FAA http://www.easa.europa.eu

**Understanding Formal Methods for Use in DO-254 Programs**

David Landoll

Mentor Graphics.

David is a member of the Engineering Solutions Group at Mentor Graphics. David’s focus is on companies adopting DO254 and how advanced verification techniques can make CEH safer. He has a BSEE from University of Arizona and an MBA from Santa Clara University.

IN 50 WORDS OR LESS - This presentation explores the pros and cons of using formal methods, covering benefits and putting fear of use (because of mathematical sophistication) in perspective. The article explores the comparative complexity of formal methods for software and hardware and provides guidance for its application.

David’s presentation is focused on Formal Methods applied to Hardware (AEH governed by DO-254). It was a neat tutorial on Formal Methods for those of us who are unfamiliar with FM. Whether some of it was “marketing hype is left up to the reader.

David began with a summary of DO-254 Appendix B. and lamented its complexity. His presentation commendably focused on the “meat” of the Appendix with illustrations and simple examples. David postulates that many fear Formal Methods because of its complexity and mathematical sophistication.

While not denying its complexity for many software applications, he claims it is more easily used for AEH devices. He defines Formal verification Methods as, 

“...The use of exhaustive mathematical algorithms to functionally verify that a design works correctly with respect to its requirements”.

Unlike simulation methods, which are probabilistic, formal methods are exhaustive and virtually guarantee complete results.

EASA uses specific “Certification Memo”. Basic requirements are harmonized with FAA policies and CAST (Certification Authorities Software Team) papers. EASA has a website similar to the FAA http://www.easa.europa.eu

**Understanding Formal Methods for Use in DO-254 Programs**

David Landoll

Mentor Graphics.

David is a member of the Engineering Solutions Group at Mentor Graphics. David’s focus is on companies adopting DO254 and how advanced verification techniques can make CEH safer. He has a BSEE from University of Arizona and an MBA from Santa Clara University.

IN 50 WORDS OR LESS - This presentation explores the pros and cons of using formal methods, covering benefits and putting fear of use (because of mathematical sophistication) in perspective. The article explores the comparative complexity of formal methods for software and hardware and provides guidance for its application.

David’s presentation is focused on Formal Methods applied to Hardware (AEH governed by DO-254). It was a neat tutorial on Formal Methods for those of us who are unfamiliar with FM. Whether some of it was “marketing hype is left up to the reader.

David began with a summary of DO-254 Appendix B. and lamented its complexity. His presentation commendably focused on the “meat” of the Appendix with illustrations and simple examples. David postulates that many fear Formal Methods because of its complexity and mathematical sophistication.

While not denying its complexity for many software applications, he claims it is more easily used for AEH devices. He defines Formal verification Methods as, 

“...The use of exhaustive mathematical algorithms to functionally verify that a design works correctly with respect to its requirements”.

Unlike simulation methods, which are probabilistic, formal methods are exhaustive and virtually guarantee complete results.

David Landoll

Mentor Graphics.

David is a member of the Engineering Solutions Group at Mentor Graphics. David’s focus is on companies adopting DO254 and how advanced verification techniques can make CEH safer. He has a BSEE from University of Arizona and an MBA from Santa Clara University.

IN 50 WORDS OR LESS - This presentation explores the pros and cons of using formal methods, covering benefits and putting fear of use (because of mathematical sophistication) in perspective. The article explores the comparative complexity of formal methods for software and hardware and provides guidance for its application.

David’s presentation is focused on Formal Methods applied to Hardware (AEH governed by DO-254). It was a neat tutorial on Formal Methods for those of us who are unfamiliar with FM. Whether some of it was “marketing hype is left up to the reader.

David began with a summary of DO-254 Appendix B. and lamented its complexity. His presentation commendably focused on the “meat” of the Appendix with illustrations and simple examples. David postulates that many fear Formal Methods because of its complexity and mathematical sophistication.

While not denying its complexity for many software applications, he claims it is more easily used for AEH devices. He defines Formal verification Methods as, 

“...The use of exhaustive mathematical algorithms to functionally verify that a design works correctly with respect to its requirements”.

Unlike simulation methods, which are probabilistic, formal methods are exhaustive and virtually guarantee complete results.

He explained that formal methods are more difficult to apply to software because software deals with “infinite state systems and is dynamic. Formal methods are easier for hardware because there are established coding standards for VHDL. (Very High Speed Integrated Circuits Hardware Description Language), hardware deals with finite states and is static.

David demonstrated with the example of a requirement that “Thrust reversers shall never deploy in flight” Simulation methods check some of the logical paths by which this could happen to gain confidence reversers will not deploy. Formal methods provides complete assurance by verifying all possible behavior of the code.

In the early ’90’s, there was no commercial market formal control. In the late ’90’s, a $5M market developed, by year 2000 the market was $23M, and today the market is $50M. He cited a sampling of the companies using formal methods today including, Alcatel-Lucent, HP, IBM Cisco, Qualcomm, Fujitsu, Saab, Silicon Logic, to name a few.

David summarized with a checklist for the use of Formal Methods:

1. V & V plan should describe formal use model
2. Formal properties must be created and reviewed against requirements (including constraints)
3. The formal model is just the VHDL (or Verilog) code
4. Proofs for each property should be documented, traceable to requirements, and repeatable
5. Tools and assessment process (typically independent output assessment when used with simulation) should be documented
6. Counter-examples as simulation test cases and new or changed properties should be documented
7. Analysis of formal coverage should be documented
8. Analysis of formal coverage should be documented
9. Our post-design lessons learned reviews generally find that we should do more in formal and mixed formal/dynamic verification.”
CONFERENCES & WEBINARS (cont.)

Aircraft Cyber Security Workshop

Chris Riley
Volpe National Transportation Center

Chris Riley has been involved in Security Certifications, Vulnerability Assessment and Penetration Testing of Federal Computer Systems for the past 10 years. He leads RTCA-SC-216 dealing with Airborne Network Security Controls. He advises the FAA on Next Generation Aircraft, Risk Assessment and Robustness testing of Electronic Flight Bags, and has published several white papers on the subject. Chris was the main presenter of this paper co-authored by Ray DeCherio, Kevin Harnett and Vince Rakauskas.

IN 50 WORDS - Intense "deep dive" into the world of cyber security focused on airborne networks and their vulnerabilities. The work of RTCA/DO-216 is summarized.

Chris's Track spanned an entire afternoon on Wed and was repeated on Thursday to allow greater participation for a most important new topic for aircraft safety. There are no existing regulations that provide assurance that cyber security threats will not cause unsafe flight conditions. If left unmitigated, this threat will have a negative effect on flight safety. The threats come from academics, kids, disgruntled programmers and certain nations, China, North Korea and terrorist groups. "Titan Rain" was the name given to series of coordinated attacks on American computer systems since 2003.

To put the problem in perspective, USAF General William Lord, Director of Information is quoted as saying "China has downloaded 10-20 terabytes of data from NIPRNET (DOD's non-classified IP router"). Vulnerabilities consist of viruses, worms, backdoors, malicious code, enumeration, password cracking. These and many others including Bots and spyware, infect supply chains including USB thumb drives, GPS systems, photo frames, VOIP networks, and event phishing and others.

Chris cited several targets for these cyber threats including open source software, dual processor Electronic Flight Bag's, OS's like Linux and Windows, and packet switching networks. Chris did a deep dive on packet switching networks. He described protection mechanisms including encryption, penetration testing, network monitoring, firewalls, stateful packet filters, intrusion detection, file integrity monitoring, proxies, cryptographic "hash" functions, and public key infrastructure protection. He talked about the unique vulnerabilities of wireless because transmissions circumvent traditional firewalls.

The short term plan is to address process shortfalls with special conditions and issue papers. Long term, RTCA-SC-216 will provide processes and methods for certifying the safety and security of airborne networks. He envisions significant increases in security training and greater attention to hiring qualified IT security staff for airline MRO staff, DERs, Aircraft manufacturers, and FAA personnel.

Database Integrity for Aeronautical Data

Brad Miller
FAA Air 130

Brad is an FAA avionics engineer within the Avionics Systems Branch (AIR-130) in Washington DC. He leads policy projects concerning Aeronautical Database integrity, vertical Flight, RVSM Altitude, Electronic Flight Bags, ISO 9000 Quality Management and AC 120-76. He is responsible for publication of numerous documents, including AC 20-153, AC20-159, AC120-76 TSO-C165, and FAA Order 8110.55. He is a graduate of Vanderbilt and a former Navy pilot.

IN 50 WORDS - Covers the latest FAA orders, AC's and DO's dealing with Aeronautical Data bases, including terrain and Airport Moving Maps. Discusses the various ways of getting data approval.

Prior to the issuance of AC20-153, and RTCA/DO-200A, there was no guidance for aeronautical data (navigation, terrain). For government supplied data, the state is responsible for the accuracy and currentness of the data. Aeronautical Information Publication (AIP) provides this data. Downstream parties can assume the data is correct.

Data not received through AIP must be verified. The FAA's approach is to approve the process, not the vast amounts of data.

Currently AC20-153 only addresses navigation data. Approval options for Terrain data are threefold.

1. Acceptance through Flight Standards AFS for airport data is provided in DO-272A. Guidance on DQRs for terrain and obstacle data is provided in DO-276A

2. Put the data under the TC as part of the Cert process

3. Use database LOA to oversee data process

Option 1 does not provide data integrity

Option 2 relies on data approval via Terrain Awareness Standards (TAWS) and approval of that data as part of the design change approval process of TSO-C-151b, a laborious option.

Option 3 uses the new AC20-153 supplier process approval via LOA. Until this LOA can be obtained, data updates will have to be managed through option 2.

Under option 3, the applicant defines the data quality requirements, compatible with the avionics. The FAA audits to verify compliance with DO-200A via AC20-153. The ACO issues the LOA. Major/ minor changes to data are classified within the LOA. The process for nav data has already been harmonized with EASA and the FAA.

There are 2 types of LOA approval

1. Compliance with DO-200 with no aircraft compatibility stated.

2. Process Type 1 data to ensure compatibility with target hardware.

One addition to the AC has been to add Airport Moving Map Database (AMMD) Issues. Applicant must validate data which is not from State AIPs and must define processes, from origination through loading the data, to ensure data quality. International Civil Aviation Organization (ICAO) should include:

- Definition of requirements and conditions for updating (Periodicity, Source, Process, and Verification).
- Restrictions and/or limitations for operating with expired databases.
- Latest edition of ICAO Annex 15 indicates AIP will include:
  - Area 1 (entire territory of a state (Terrain)) and 4 (category II/III) data implemented November 2008, and
  - Area 2 (terminal area) and 3 (aerodrome) data by November 2010.
- Guidance on Data Quality Requirements (DQRs)
the work that is planned for the balance of this year and next. DO-248B (Clarifications to 178B) will be updated to DO-248C and likely renamed. It will address Frequently Asked Questions (FAQ’s, Discussion Papers (DP’s) and Rationale, things that would not be appropriate to invoke at the 178B level. DO-278 (Ground software) will be updated as well. The next meetings are scheduled for Paris in October and Sarasota Fla in Feb 2010. 178C is slated for publication in late 2010.

**Other papers not synopsized here include:**

- RTCA/SC216 – Aeronautical Systems Security-Chuck Royalty - Boeing
- TSO Process Revision – Carol Martineau - FAA
- Software Contributions to Accidents- Dana Schulze NTSB
- Military IMA Certification to Civil Standards – Cheryl Dorsey – Digital Flight
- FAA Order 8110.105 Simple and Complex Electronic Hardware Approval Guidance - Gregg Bartley FAA
- Assignment of Development and Design Assurance Levels, (DALs) - Steve Beland – Boeing
- Electronic Flight Bags - Peter Skaves- FAA
- SC-205 Tool Qualification Supplement – Leanna Rierson Digital Safety.
- DO 297, AC 20-IMA and FAA Order 8110.IMA – Gregg Bartley FAA
- Model Based Development and Support – Kevin Meier, Cessna.

**About the Author:**

Mike Kress is an Associate Technical Fellow within Boeing Commercial Airplanes Global Partners Procurement QA. He has over 34 years experience in military and commercial aviation hardware and software. He has written guidebooks for the U.S. Air Force on trainer and simulator software. He holds a Bachelor’s degree in Electrical Engineering, is a Fellow member of ASQ and holds ASQ CQE and CSQE certifications and is a Registered Professional Engineer. He has led several Boeing and industry advisory groups that have written or contributed toward software standards, most notably RTCA/DO-178B and AS9006. He is currently chair of the AAQG Project 60 team drafting AS9115, the new international aerospace software quality system standard. He is a former ASQ Software Division Regional Councilor and past chair of the ASQ Software Division. He is a member of the U.S. Technical Advisory Group to ISO/IEC TC176 SC7 and is co-editor of ISO standards on COTS software and Data Quality. He is an RAB/QSA registered QMS and Aerospace Industry Experience Auditor.

**2010 Institute for Software Excellence**

The Institute for Software Excellence is in St Louis, MO, May 24-26, 2010.

Here is a tentative list of the topics covered:

- Software Security Assurance: Mitigating Risks to the Enterprise Workshop
- How to use the CMMI to improve processes
- Are you smarter than a CSQE?
- New Developments in Global Medical Device Software Regulations and Standards
- ISO 25012 - An International Standard for Data Quality
- Workshop - Nuts & Bolts of Testing (Test Design Techniques)
- Improving Test Coverage with the Combinatorial Approach
- Global Quality Initiatives at SAP
- Using the Voice of the Customer to Improve Software Quality
- Agile Strategies for Life

Once again, the ASQ Software Division Hospitality Suite will host social events