



Extending Infrastructure Software for High Confidence Systems

by: William M. Thomas, PhD

Tuesday, May 25, 2004

American Society for Quality (ASQ) Section 509 — Software Special Interest Group (SSIG)

Many of the more spectacular failures attributed to software are at least indirectly the result of seemingly minor changes to the operational software. Because of unanticipated interactions within the software and subsequent “breakage” of implicit assumptions when software is changed, software maintenance can produce fragile, error prone software. Even in carefully managed product lines, it can be difficult to determine the impact of such “minor” changes. Adding to this difficulty is the fact that modern, product line focused development approaches are increasingly adopting the use of externally developed software, integrating custom software with COTS and GOTS software, and in general being dominated by integration of existing components and services rather than new development. While such approaches have been shown to offer substantial benefit in application development, they also result in less insight into (and control over) the components being used in an application. Another complicating factor is a push for more and more rapid change of the system (and a desire for greatly reduced cycle time for new system variants).

This inherently brittle approach is of particular significance for High-Confidence Software (HCS), i.e., software where the consequences of failure are high, and therefore the confidence one must have in the software is equally high. However, extensions can be made to component-based software infrastructures (e.g. J2EE, CCM) that can alleviate some of the inherent difficulties of component-based HCS, while still enabling the expected development benefits. This presentation will discuss some of the limitations of component-based development approaches as they apply to HCS, illustrate design patterns that use and extend infrastructure technology to better satisfy HCS assurance needs, and demonstrate how these patterns can be applied to two widely used commercial infrastructure technologies.



Presenter: Bill Thomas is a lead scientist in the Software Engineering Center at the MITRE Corporation, where he has researched software quality modeling, software analysis techniques, and component-based development paradigms. He received a B.S. in Mathematics from Bucknell University and an M.S. and Ph.D. in Computer Science from the University of Maryland.

Sponsored By: The American Society for Quality (ASQ) Section 509 (Washington, DC), Software Special Interest Group (SSIG). Members of the ASQ SSIG include software quality professionals, software engineers, and others interested in applying quality principles to the field of software development. See our web page: http://www.asq509.org/Committee_Software.htm We meet every other month, alternating locations between the FDA Tech Center near Gaithersburg, Maryland and the MITRE facility in Tyson's Corner, Virginia.

Registration:

Please register for the meeting prior to COB Friday, May 21, 2004 by contacting Scott Ankrum at 703-883-6127 or ankrums@mitre.org with the following information:

- Name of attendee
- Position or title
- Name of employer
- Telephone number of attendee
- If married, maiden name of attendee

Cost per person is \$5.00 – Please bring a picture ID. ASQ membership is **not** required to attend.

The Meeting Is Scheduled For:

Tuesday, May 25, 2004
6:30 - 7:30 Networking – Pizza and Sodas
7:30 - 8:30 Program

And Will Be Held At:

FDA Tech. Center
16071-B Industrial Drive (off Shady Grove Road)
Gaithersburg, Maryland

Directions to the FDA Tech Center:

From I-270 N or S, take Shady Grove exit east and proceed to Gaither Road. Turn LEFT on Gaither and proceed to first stop sign. Turn Right on Industrial Drive. You will cross over I-370. Go to the large Industrial building at the end of Industrial Drive and bear left to the end of the building. The meeting will be at the FDA Tech Center, 16071-B Industrial Drive, Gaithersburg, MD.

From Route 355 (Frederick Rd), take Shady Grove West and proceed to Gaither Road. Turn RIGHT on Gaither Road and proceed to first stop sign. Turn Right on Industrial Drive. You will cross over I-370. Go to the large Industrial building at the END of Industrial Drive and bear left to the far end of the building. The meeting will be at the FDA Tech Center, 16071-B Industrial Drive.

