Real-time and Embedded Systems Forum

Spotlight

16 November 2011

Joseph I. Bergmann
Director,
Real-time and Embedded Systems Forum

630 W. Leslie Street
Allentown, PA 18103 USA
www.opengroup.org

Tel +1 610-506-1455
eFax +1 208-246-2893
j.bergmann@opengroup.org
Software with Real-time and High Assurance will make the Boundaryless RT Enterprise deterministic, integrated and flexible.
The Open Group Forum Coverage

Boundaryless Information Flow Reference Architecture

User Interface & Ontology
Messaging
Supply Chain
Security
Identity Mgmt.
Directory
Information Mgmt.
System Mgmt.
Transaction Mgmt.

Messaging Forum
OTTF Forum
Security Forum
Directory Interoperability Forum
Enterprise Management Forum

Dependability through Assuredness™ Predictable Execution
Real-time & Embedded Systems

(C) The Open Group 2011(C)
Real-time & Embedded Systems Forum

- **RTES Vision**
  - Employ widely supported and open real-time standards and enabling technologies to deliver testable and certifiable, cost-effective, mission-capable systems.

- **RTES Mission**
  - Improve the time and cost to market adoption of real-time and embedded solutions by providing a forum where we can share knowledge and integrate open initiatives, and certify approved products and processes.
# Real-time & Embedded Systems Forum Coverage

## Dependability through Assuredness™
- Predictable Execution
- Real-Time & Embedded Systems Work Areas

|----------------------------|--------------------------------------------------|---------------------------------------------|-------------------------------|--------------------------|

THEOpen GROUP
Making standards work®
RTES Forum Activities

- **Work Areas:**
  - Dependability through Assuredness™
  - OA for RT – Architecting to the Edge™
  - TOGAF™ to the Platform
  - Cross Domain Security for RT – MILS™ Architecture
  - RT Java for Safety/Mission Critical Environments – JSR302
  - High Assurance, Safety Critical Environments
  - Safety/Mission Critical Applications
  - MILS™ APIs Standard (POSIX & ARINC 653)
  - Independent Evaluation & Certification Scheme for COTS Components/Systems
  - Component Competition Readiness Levels (CCRLs)
  - IEEE POSIX RTOS Profiles and Certification
  - Secure Mobile Architecture
  - Product Standards and Certification for:
    - SCADA – Smart Grid
    - Medical Devices
    - Consumer Electronics
    - Intelligent Transportation Systems

- **Liaisons/Affiliations:**
  - The Object Management Group
  - IEEE PASC SSWG RT
  - Society of Automotive Engineers
  - NATO Research Task Group on Validation, Verification and Certification of Embedded Systems
  - INCITS CS1
  - US Army COE
  - Navy PEO (IWS) – Open Architecture
  - Process Control Systems Cyber Security Forum
  - ARINC 653 APEX Working Group
  - Association for Enterprise Integrators
  - High Confidence Medical Device Software and Systems Workshop
  - DHS Software Assurance Working Group
  - Network Centric Operations Industry Consortium
  - Center for Advanced Defense Studies
  - OMG SwA Working Group
RTES Forum Members

Current as of 31 October 2011

- AIM
- Aonix
- Architecting-the-Enterprise
- AXE, Inc
- Capgemini S A
- Carnegie Mellon University, Software Engineering Institute
- City University (London)
- Danish Ministry of Science Technology & Innovation
- DDC-I, Inc
- US Department of the Navy
- eFlow
- eValley Inc
- Finite State Machine Labs
- Florida State University
- Fujitsu Limited
- Forschungszentrum Informatik
- Georgia Institute of Technology
- Green Hills
- IBM Corporation
- JAXA
- Kestrel Technology
- Kingdee
- Lockheed Martin Corp.
- LynuxWorks Inc.
- MIT, Embedded Systems Lab
- NASA Goddard Space Flight Center
- Objective Interface Systems
- DUSD/AT&L
- Ohio University
- QNX
- PrismTech
- Pryrrhus software
- Raytheon
- REGIS
- Real-time Innovations
- Teamcall Ltd.
- The Boeing Company
- The Mitre Corp.
- Universidad de Cantabria (Spain)
- University of Idaho
- University of Nagoya
- University of Tokyo
- University of York (UK)
- Verocel, Inc
- Wind River
## Real-time and Embedded Systems Forum Progress

<table>
<thead>
<tr>
<th>Item</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>POC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Work In-process</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Standards for the MilSTM Architecture</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rance DeLong</td>
</tr>
<tr>
<td>APIs</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td>Joe Wlad</td>
</tr>
<tr>
<td>Evaluation &amp; Certification Program</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td>Rance DeLong</td>
</tr>
<tr>
<td>Composability Business Scenario</td>
<td></td>
<td>Finalize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>John Rushby</td>
</tr>
<tr>
<td>Component level specification</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td>Rance DeLong</td>
</tr>
<tr>
<td><strong>High Assurance Procurement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managers Guide – what it is, how to use it</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td>Michael McEvilley</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Edwin Lee</td>
</tr>
<tr>
<td>Procurement Guide – what should be in RFI</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td>Glen Logan</td>
</tr>
<tr>
<td><strong>Dependability through AssurednessSTM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Finalize</td>
<td>Edwin Lee Glen Logan</td>
</tr>
<tr>
<td>Dependability Guide</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td>Edwin Lee</td>
</tr>
<tr>
<td><strong>Architecting to the EdgeSTM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSA Guide – Requirements</td>
<td>Initial</td>
<td>Finalize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Edwin Lee Glen Logan</td>
</tr>
<tr>
<td>OSA Pocket Guide</td>
<td>Initial</td>
<td>Review</td>
<td>Review</td>
<td>Finalize</td>
<td></td>
<td></td>
<td>Edwin Lee</td>
</tr>
<tr>
<td><strong>Safety Critical Java – JSR 302 Specification</strong></td>
<td>On-going</td>
<td>On-going</td>
<td>On-going</td>
<td>Finalize</td>
<td>Release</td>
<td>Update</td>
<td>Doug Locke</td>
</tr>
</tbody>
</table>
Safety Critical on-going standards/project activity in The Open Group Real-time and Embedded Systems Forum
JSR-302: SC Java Current Summary

- Safety Critical Application: Mission, optionally restartable, statically analyzable:

  ![Diagram of execution phases](image)

  **Figure 3.1: Safety Critical Execution Phases**

- Simple application and infrastructure model
- No Garbage Collector, no reflection, no finalizers, no heap memory
- Three Compliance Points (Levels 0, 1, 2)
  - Level 0 provides a cyclic executive (single thread), no wait/notify
  - Level 1 provides a single mission with multiple schedulable objects,
  - Level 2 provides nested missions with (limited) nested scopes
- Specification writing completed
- Initial specification 2Q 2011 – Final Specification 1Q 2012
- Reference Implementation being implemented as open source RTSJ-compliant Java executable on any RTSJ-compliant JVM
- Two companies have built product based on JSR 302 – Aicas and Atego
  - [http://www.aicas.com](http://www.aicas.com)
EC Projects Related to Safety Critical

- Current projects -- Composition with Guarantees for High-integrity Embedded Software Components Assembly (includes Multicore)
  - JEOPARD
  - CHESS
  - CHARTER

- New EC Opportunities
  - Framework Programme for ICT – Provides funding for many technology areas
    - Networking
    - Cloud Computing
    - Security and Trust
    - Identity Management
    - Smart Grid
    - Cognitive Systems
    - Robotics
    - Smart components
    - Nano technologies
    - Etc..
On The Horizon

- Independent Evaluation and Certification Scheme for High Assurance COTS Security Components and Systems to include International Mutual Recognition
- An Open Group “Mils™” Brand
- Complete a Tool Chain for “TOGAF to the Platform” activity to ensure “Dependability through Assuredness™”
- Additional Java Specification Requirements (JSRs) to include Multicore and Security
- Multicore Standard APIs – to be submitted to IEEE PASC
- Assurance Cases/Templates/Patterns WG
- Mils™ Development Practices Working Group WG
- Planning to Respond to an 1Q 2012 Call for Proposals from the EC Under Framework 7 for a High Assurance Security Framework
Proposed RTES Forum Agenda for San Francisco

30 January - 2 February 2012

Monday 30 January 1130-1730 Hours – Conference - Dependability Track – Joint Sponsors Security/RTES Forums
1145-1300 DEOS/Open Systems Dependability -- A new Approach for Huge and Complex Software -- Dr Mario Tokoro - President Sony R&D/ Dr Yutaka Matsuno - University of Tokyo, Introduction Jack Fujieda - The Open Group/ReGIIS
1300-1400 Lunch
1400-1445 DEOS/Open Systems Dependability Panel Discussion – Dr Tokoro, Dr Matsuno, Dr Yamamoto – Nagoya University, Jack Fujieda, Ed Roberts Elparazim – Moderator Dave Lounsbury
1445-1545 Assurance Cases/Templates/Pat terns -- Dylan McNamee - Galois/Ed Roberts - Elparazim
1545-1600 Break
1600-1730 Assurance Cases/Templates/Pat terns Workshop -- Dylan McNamee - Galois/Ed Roberts - Elparazim

Tuesday 31 January 1130-1730 Hours -- Conference - Dependability Track
1145-1300 IT for Mega Disasters -- Dr Jane Liu - Institute of Information Science, Academia Sinica/ Dr Chi-Sheng (Daniel) Shih - National Taiwan University
1300-1400 Lunch
1400-1445 IT for Mega Disasters Panel – Dr Liu, Dr Shih, Representative from FEMA Invited, Moderator, Dave Lounsbury
1445-1530 Open Systems Architecture and Data Rights – Director for Open Architecture (Invited – DASN (RDT&E)
1530-1600 Break
1600-1730 TOGAF to the Platform – Ed Roberts - Elparazim

Wednesday 1 February 0900-1730 Hours – RTES Forum Members Meeting
0900-0930 TOGAF going forward – Dave Hornford (TBC) – Chair Architecture Forum
0930-1230 Mils™ Development Practices Working Group (MDP WG) -- Steve Kuehl – Raytheon -- WG Agenda Details to Follow
1230-1330 Lunch
1330-1730 Mils™ Architecture/Mils API Standards WGs Going Forward including Compositional Certification -- Rance DeLong LynuxWorks -- WG Agenda Details to Follow

Thursday 2 February 0900-1730 Hours – RTES Forum Members Meeting
0900-0945 Update EC Projects -- Scott Hansen - The Open Group
0945-1030 Safety Critical Java Specification Update -- Doug Locke - Doug Locke LLC
1030-1100 Break
1100-1145 Architecting to the Edge -- Glen Logan - US Army
1145-1230 Component Competition Readiness Levels (CCRLs) -- Gerald Walles - US Navy (NAVAIR)
1230-1330 Lunch
1330-1530 Assurance Cases/Templates/Pat terns WG -- Dylan McNamee, Galois
1530-1600 Break
1600-1730 RTES Forum Going Forward -- Joe Bergmann et al. - The Open Group.

Conference Information http://www3.opengroup.org/sanfrancisco2012

(C) The Open Group 2011(C)