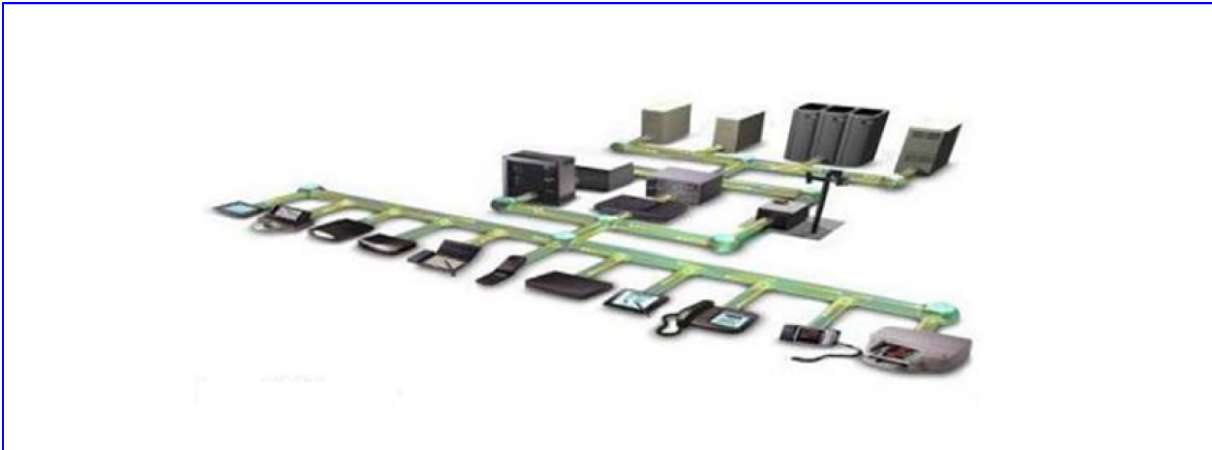# "Dependability through Assuredness ™"

Summary of Boston Sessions presented by the RTES Forum --

20 July Tuesday - 1) Dependability through Assuredness featuring two committee members, Dr. Daniel Jackson from MIT and Dr. John Rushby from SRI for the National Academy of Science's publication "Software for Dependable Systems: Sufficient Evidence?" 2) High Assurance Security, Standardization of MILS APIs, chaired by Rance DeLong from LynuxWorks and Paul Chen from Wind River, MILS Requirement for UAVs, Rob Hoffman from High Assurance Systems, Evaluation and Certification of High Assurance Commercial off the Shelf Products (COTS) and International Mutual Recognition of the Certified Security Products.

21 July Wednesday - 1) Mission Assurance featuring Harriet G. Goldman, Director of Cyber Mission Assurance, serving as the MITRE focal point for Mission Assurance in support of the Department of Defense and Intelligence customers, responsible for raising awareness of the advanced cyber threat across government and industry and developing strategies, technologies and processes to address customer cyber security and mission assurance needs. A Mission Assurance Business Scenario workshop, conducted by Terry Blevins, Chief Architect and Associate Department Head, MITRE, will follow Ms. Goldman's presentation, 3) SYSML Tutorial by Ed Roberts from Elparazim, 4) Progress on the Open Systems Architecture Guidebook, Edwin Lee from Raytheon, 5) A Joint Session with the Security Forum on "Architecting for Uncertainty", 6) Update on the JSR 302 Expert Group Specification for Safety Critical Java.

22 July Thursday - 1) An update on the AFRL HAMES Project by Carolyn Boethcher from Raytheon, 2) High Assurance Security Requirements: for the US Government and Critical Infrastructure by Dr. Ron Ross from NIST and for the Medical Field by Partners HealthCare System. Immediately following the presentations there will be a Workshop/Discussion on High Assurance Requirements facilitated by Rance DeLong, 3) Developing an Approach to Evaluation and Certification for High Assurance Security Commercial Products. 4) A joint session with the Security Forum to progress Secure Mobile Architecture (SMA) including a presentation on a series of use cases, 5) A wrap-up on the activities of the RTES Forum going forward.

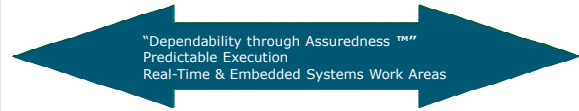## Real-time & Embedded Systems Forum Vision and Mission

❑ **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.
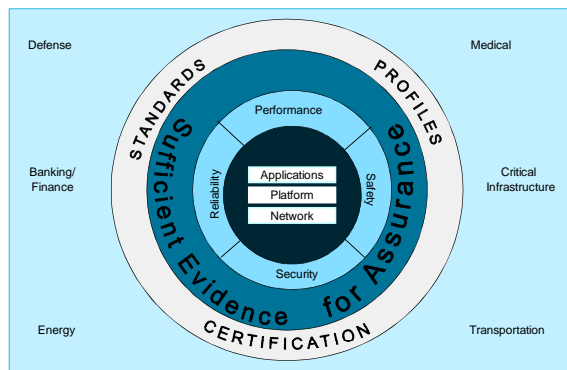
THE O*pen* GROUP

Real-time and Embedded Systems Forum Coverage

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

Open Architecture for RTES	IEEE POSIX® RT Standards, Profiles & Certification	RT (Security & Safety) Critical Systems	Safety Critical RT Java/ JSR302	Secure Mobile Architecture

THE O*pen* GROUP

Real-time & Embedded Systems Forum Perspective

"Dependability through Assuredness™"

"Dependability through Assuredness™"

❑ The Open Group "Dependability through Assuredness™" theme/activity with member partners will facilitate developing an approach to High Assurance and High Robustness across all work areas of the Forum through the use of certifiable interoperable tools based on formal methods and open standards to support a distributed real-time test bed architecture for testing, certification and accreditation of PPs, components and systems across domains.

❑ The various instantiations of assurance testing would support a system and/or system-of-systems for software development, software quality, high robustness security, information assurance, requirements traceability, interoperability, quality of service, aggregated real-time performance, modeling and simulation, formal methods proof, and artifact generation based on current best practices for mission, security and safety-critical systems.

❑ From definition and validation of requirements, through a hierarchy of architectures to development, deployment and post deployment of the system (hardware & software) and/or system-of-systems.

❑ A Business Scenario was conducted to determine the Scope and Goals of the "Dependability through Assuredness™" effort at The Open Group Austin meeting on 27 July 2007.

THE O*pen* GROUP

RTES Forum Members

Current as of 31 March 2010 (45)

❑ 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
❑ eFlow
❑ eValley Inc
❑ Finite State Machine Labs
❑ Florida State University
❑ Fujitsu Limited
❑ Forschungszentrum Informatik
❑ Georgia Institute of Technology
❑ Green Hills
❑ IBM Corporation
❑ Information-Technology Promotion Agency-Japan
❑ JAXA
❑ Kestrel Technology
❑ Kingdee

❑ Lockheed Martin Corp.
❑ LynuxWorks Inc.
❑ MIT, Embedded Systems Lab
❑ NASA Goddard Space Flight Center
❑ Objective Interface Systems
❑ OUSD/AT&L
❑ Ohio University
❑ Panasonic Electric Works
❑ QNX
❑ PrismTech
❑ Pryrrhus software
❑ SYSGO AG
❑ Raytheon
❑ REGIS
❑ Real-time Innovations
❑ Teamcall Ltd.
❑ The Boeing Company
❑ The Mitre Corp.
❑ Universidad de Cantabria (Spain)
❑ University of Idaho
❑ University of York (UK)
❑ Verocel, Inc
❑ Wind River

THE O*pen* GROUP

Real-time & Embedded Systems Forum Structure & Leadership

❑ **Forum Chairs**
  ▪ Chair - Glen Logan
  ▪ Vice Chair – Edwin Lee, Raytheon
❑ **Working Groups/Chairs**
  ▪ **Open Architecture for RTES – Glen Logan/Edwin Lee**
    ▪ Modular Open Systems Architecture –Glen Logan
    ▪ Architecting to the Edge ™ – Edwin Lee
  ▪ **IEEE POSIX RT Standards, Profiles, & Certification - Joe Gwinn, Raytheon**
    ▪ IEEE POSIX 1003.13 – Joe Gwinn
    ▪ IEEE POSIX 1003.26 – Joe Gwinn
  ▪ **RT (Security & Safety) - Critical Systems - Michael McEvilley, MITRE/ Rance DeLong, LynuxWorks/ Edwin Lee, Raytheon**
    ▪ MILS Demos – Ben Calloni, Lockheed Martin
    ▪ Lexicon – Michael McEvilley
    ▪ Standardization – Carolyn Boettcher
    ▪ Protection Profiles – Rob Hoffman
    ▪ MILS Integration – Rance DeLong
    ▪ Compositional Certification – John Rushby, SRI
    ▪ Cyber-Physical Systems – Rance DeLong
    ▪ Commercial approach to Evaluation, Certification and Accreditation – Rance DeLong
  ▪ **Safety Critical RT Java/JSR 302 – Doug Locke, LLC**
    ▪ Specification
  ▪ **Secure Mobile Architecture - Steve Venema, Boeing**
    ▪ SCADA
    ▪ Medical Devices
    ▪ Intelligent Transportation Systems

THE O*pen* GROUP

"Dependability through Assuredness™"

Boston, Hyatt Haborside - Track Agenda sponsored by The Open Group *RTES Forum*: 19-22 July 2010

Monday 19 July:
Open Sessions of interest to RTES Forum Members
- 09:00 – 12:30 Cybersecurity: The Intentional Enterprise in an Uncertain World   .
  www.opengroup.org/boston2010/sub-prog-plenary-1.htm
- 14:00 – 17:30 The Acquisition Cybersecurity (ACS) Initiative   .
  www.opengroup.org/boston2010/acs.htm
- 16:00 – 1630 Mission Assurance, Harriet Goldman, Mitre   .
  See Plenary Security Track www.opengroup.org/boston2010/program.htm

Tuesday 20 July:
09:00 – 09:15 Introduction to the RTES Forum: Overview of the forum mission, work areas and work group   .
.   activities - Joe Bergmann, Forum Director, The Open Group
09:15 – 10:00 MILS Architecture/APIs: Objectives, Vision and Overview of the MILS API Requirement from a   .
.   Minimal Runtime Perspective - Rance DeLong/Paul Chen, Co-Chairs of the MILS API WG
10:00 – 10:30 MILS Architecture/APIs: Facilitated session to identify and prioritize the outstanding Issues   .
.   related to scope and market adoption of a MILS API - Facilitated by Sally Long
10:30 – 11:00 Break
11:00 – 11:15 Update MILS Architecture Requirement for UAVs – Rob Hoffman, CEO High Assurance Systems
11:15 – 12:30 MILS Architecture/APIs: Interactive discussion to begin working through issues identified above
12:30 – 13:30 Lunch
14:00 – 17:30 Parallel Activity: ACS Initiative - See Open Sessions:
13:30 – 14:30 Dependability through Assurance: "Dependability by Design" – Dr Daniel Jackson, MIT
14:30 – 15:30 Dependability through Assurance: "Making the Case" – John Rushby, SRI
15:30 – 16:00 Break
16:00 – 17:00 Dependability through Assurance: Panel Disscussion, Jack Fujieda - ReGIS, Glen Logan -   .
.   Chair RTES Forum. John Rushby – SRI, et al.

Wednesday 21 July:
08:00 – 09:00 Mission Assurance – Harriet Goldman, MITRE
09:00 – 10:30 Mission Assurance Scenario Workshop - Facilitator Terry Blevins, MITRE
10:30 – 11:00 Break
11:00 – 11:30 Report on latest release and support for DODAF 2.0 - Glen Logan, Chair RTESF
11:30 – 12:30 TOGAF RTES Extension and RTES Reference Model Overview - Ed Roberts, Elparazim
12:30 – 13:30 Lunch
13:30 – 15:00 SysML Overview and Tutorial - Ed Roberts, Elparazim
15:00 – 15:30 Open System Architecture & Guidebook Update - Edwin Lee, Raytheon, Vice Chair RTESF
15:30 – 16:00 Break
16:00 – 17:30 "Architecting for Uncertainty" Workshop - Joint session with Security Forum – Mike Jerbic et al.
17:30 – 18:00 Safety Critical Java (JSR 302) Status and Future Plans - Doug Locke, LC Systems Services,Inc
19:00 – 2130 Potential BOF if needed to develop TOGAF to the Platform requirements (i.e.Properties,
.   Constraints, etc.) to support High Assurance and Safety Critical Environments.
Note: The SC Java (JSR302) Expert Group will meet in in Boston 20-22 July. Send requests for information and permission to attend the Expert Group meeting to Doug Locke doug@douglocke.com

This agenda is subject to update.   As of 7 July 2010

"Dependability through Assuredness™" (Continued)

Boston, Hyatt Haborside - Track Agenda sponsored by The Open Group *RTES Forum*: 19-22 July 2010

Thursday, 22 July:
08:00 – 09:00 HAMES Presentation – Carolyn Boethcher, Raytheon
09:00 – 09:45 High Assurance Requirements: Government, Critical Infrastructure – Dr Ron Ross , NIST
09:45 – 10:30 Assurance (Security) Requirements for Medical Devices/Operating Room of the Future –
.   (TBD), Partners HealthCare System
10:30 – 11:00 Break
11:00 – 11:30 Assurance Requirements: Discussion/Workshop - Rance DeLong, et al.
11:30 – 12:30 Developing a Commercial Approach to Evaluation/Certification for High Assurance –
.   Joe Bergmann, Rance DeLong
12:30 – 14:00 Lunch = Optional Session -- AADL Tutorial and Discussion by Ed Roberts
14:00 – 15:30 Secure Mobile Architecture – Joint session with Security Forum - Steve Venema, Boeing
.   Use Cases   -- 1) Automotive: Jack Fujieda, ReGIS
                                          2) SCADA: Joe Weiss, Applied Control Solutions
                                          3) Mobile Collection Devices: Glen Logan, Chair RTES Forum
15:30 – 16:00 Break
16:00 – 17:30 RTES Forum Members meeting – Going Forward, Sally Long, Joe Bergmann, Glen Logan et al.

Note: The SC Java (JSR302) Expert Group will meet in in Boston 20-22 July. Send requests for information and permission to attend the Expert Group meeting to Doug Locke at doug@douglocke.com

This agenda is subject to update.   As of 7 July 2010