



The Real-time and Embedded Systems Forum

Andrew Josey
Director of Certification

Agenda

- ❑ Overview of the Forum
- ❑ Report from Last forum meeting
- ❑ 2002 Plans/Roadmap
- ❑ Other items

The Vision



The Goals

- ❑ To be the *single place* for information exchange
- ❑ To act as an independent broker
- ❑ To develop a series of white papers
- ❑ To identify priorities for standardization
- ❑ To develop test and certification programs to cause growth of the marketplace

Industry Sectors

- ❑ *Industrial controls,*
- ❑ *Aerospace,*
- ❑ *Telecommunications,*
- ❑ *Defense,*
- ❑ *Medical/scientific,*
- ❑ *Automotive control,*
- ❑ *Test, etc*

Market Drivers

- ❑ Hardware performance continues to increase
 - Moore's Law continues
- ❑ Bandwidth is increasing rapidly
- ❑ Computing and communications proliferate beyond the desktop
 - Smart devices are becoming prevalent

Members

- ❑ FDS Embedded Systems Co. Ltd
- ❑ Hewlett-Packard Company
- ❑ IBM Corporation
- ❑ Lineo Inc
- ❑ LynuxWorks Inc
- ❑ The Mitre Corporation
- ❑ MontaVista Inc
- ❑ NASA SEWP Goddard Space Flight Center
- ❑ OAR
- ❑ Regis
- ❑ Rockwell Collins Inc
- ❑ REDSonic, Inc
- ❑ Silicon Graphics Inc
- ❑ Sun Microsystems Inc
- ❑ The Boeing Company
- ❑ The J Consortium
- ❑ The US Department of Defense Defense Informations Systems Agency
- ❑ TimeSys Corporation
- ❑ VenturCom, Inc

The Opportunity

- ❑ Implementors of this technology face the same challenges:
 - the need for fast, predictable response to events such as interrupts and messages
 - the ability to manage system resources to meet processing time constraints
- ❑ Existing standards are necessary yet insufficient
- ❑ We need to identify and remove blockages to adoption
- ❑ A need for test tools and certification

Scope of the Forum

- ❑ Operating system APIs (Application Programming Interfaces)
- ❑ Operating system profile standards
- ❑ Performance APIs
- ❑ Security policy and APIs for Real-time and Embedded Systems
- ❑ Real-time Java®
- ❑ Real-time CORBA ®



Collaborative Activities Are Key

Liaisons

- ❑ IEEE PASC
- ❑ NCITS R1
- ❑ The Object Management Group
- ❑ The US Department of Defense, Open Systems Joint Task Force
- ❑ Society of Automotive Engineers
- ❑ J Consortium
- ❑ Java Community Process
- ❑ UDI Consortium

Forum Co-Chairs

- ❑ Dave Emery, Mitre
- ❑ Lt Col Glen Logan, OSJTF

Report on Working Groups - July 2001

- ❑ 1. Testing and Certification Group
 - Did not meet
- ❑ 2. Real-time Profiling Group
 - Addressed working with the Linux Community on a Profile for Real-time Linux
- ❑ 3. Security for Real-time and Embedded Systems Group.
 - This group has produced charter and draft security profile for real-time and embedded systems

Report on Working Groups

- ❑ 4. Joint Real-time and QoS Working Group
- ❑ 5. New areas addressed by the Forum at the Austin meeting
 - Safety Critical Certification
 - Hard Real-time Java requirements

Working Group Champions

- ❑ Security - Sam Bowser
- ❑ Hard Real-time Java - Robert Allen/LTC Logan
- ❑ RT Profiles - Andrew Josey/Joe Gwinn
- ❑ Testing and Certification - Lt Col Glen Logan
- ❑ Safety Critical - Dave Emery

Security Services for RT

□ Kernel Robustness Attributes:

- **Single process system (POSIX 51/53) is not a robustness kernel**
- **Multiprocessing system (POSIX 52/54) require the following attributes:**
 - **Memory Protection**
 - **Process Management and Creation capability**
 - **Process Privilege Control**
 - **No unknown service call**
 - **Context switching discipline**
 - **Clean registers**
 - **Clean memory**
 - **Provide 'hooks' to report Intrusions**
 - **Provide Files system security as extensions (for POSIX 54)**
 - **Robust Network Protocol Stack (Not defined as a POSIX profile, may be we should someday)**
 - **Resistant to malicious packets**

Security Services for RT

Security Services / Capabilities Extensions beyond the kernel:

- ❑ **Process / Data security functions**
 - **File System Integrity**
 - **File system privacy**
 - **Labeling support**
- ❑ **Network Security functions**
- ❑ **Encryption / Decryption functions**
- ❑ **Authentication functions**
- ❑ **Biometrics functions**
- ❑ **PKI Support Function**
- ❑ **Security logging:**
 - **Intrusion Detection reporting**
 - **Security Logging**
- ❑ **Intrusion Detection Function**

Security Services for RT

- ❑ **Extensibility mechanism:**
 - **(Nothing has been proposed yet)**

Safety Critical WorkPlan Submitted by Dave Emery

Safety Critical Outline WorkPlan, Draft 1

Goal 1: 'model contract' for use of COTS on safety-critical systems.

Right now each COTS vendor and each system developer/prime integrator must negotiate the products and services required of the COTS vendor to support the prime contractor's safety certification requirements. The goal of this task is to produce a 'model contract' with deliverables that both COTS vendors and prime contractors can use to acquire COTS products and services suitable for use in safety-critical systems. This should reduce costs as the COTS vendors will be able to develop to a 'standard' set of deliverables, and the prime contractors will know in advance the kinds of products that COTS vendors will provide.

The approach for this goal is to work with RT OS vendors (e.g. OSE, Wind River) who have already delivered products to primes under the provisions of DO-178b (commercial avionics). With vendor cooperation, we can produce a draft set of 'data item descriptions', that we can take to the commercial avionics community for their review. After a couple of iterations within the DO-178b community, we can then approach other communities, particularly the medical instruments domain, the electric power domain, and the military weapon systems domain. With some luck, we can get a consensus document that can be applied across these domains.

Safety Critical WorkPlan (cont'd)

Goal 2: Common requirements for COTS for use on high assurance safety-critical systems.

Each certification authority, for each domain, has a separate and distinct set of requirements for software to meet its assurance levels. A COTS vendor who wants to support both commercial avionics and medical instruments must develop a product that meets two sets of requirements, DO-178b for avionics and ?? for medical devices.

Building on the (presumed :-) success of the 'model contract' work, we will try to get agreement across several safety-critical domains on the requirements that COTS products must meet to support the various domains.

Note that this is higher risk than Goal 1, as previous attempts to establish common requirements have not been successful. If we can get the communities of interest to come together for COTS, there's a better chance that the financial incentives for COTS use will encourage each of the domains to seek a common solution.

Specific deliverables:

- Task 1: "Recommended Practice" for documenting COTS products for use in Safety-Critical applications. Initially Open Group document, but submitted to the proponents of DO-178b, medical instruments, nuclear power, etc, for consideration by them as a new 'standard'.**
- Task 2: "Standard" requirements for COTS products intended for use in safety-critical applications. Again, initially an Open Group paper, but this will be successful only if it's adopted as a standard by the various proponent agencies.**

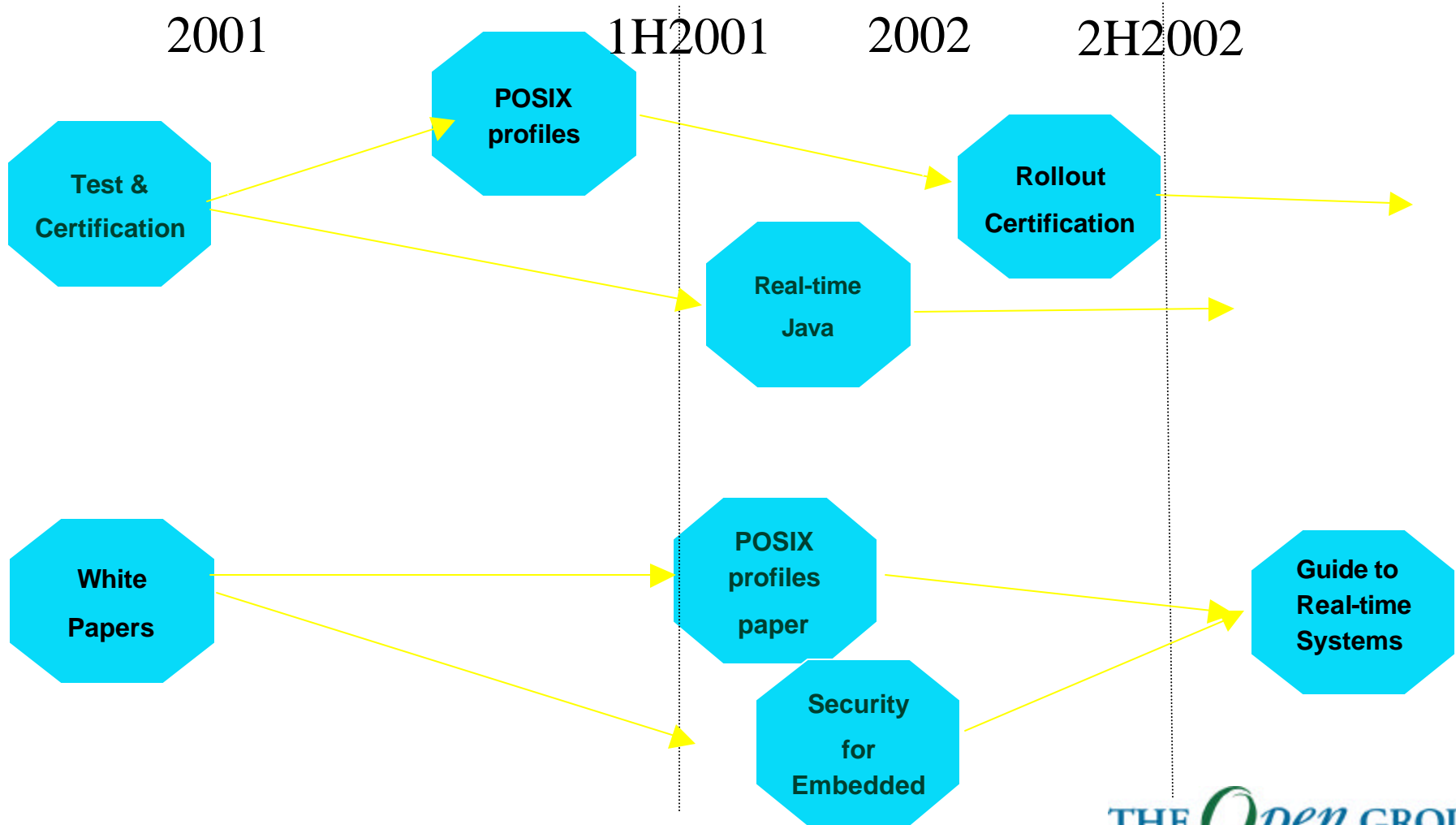
Forum Activities

- ❑ Regular meetings at the Open Group quarterly conferences
 - open plenary session
 - closed working group sessions
- ❑ Initial Working Areas:
 - Testing and Certification
 - Profiles
 - Real-time Security
 - Quality of Service

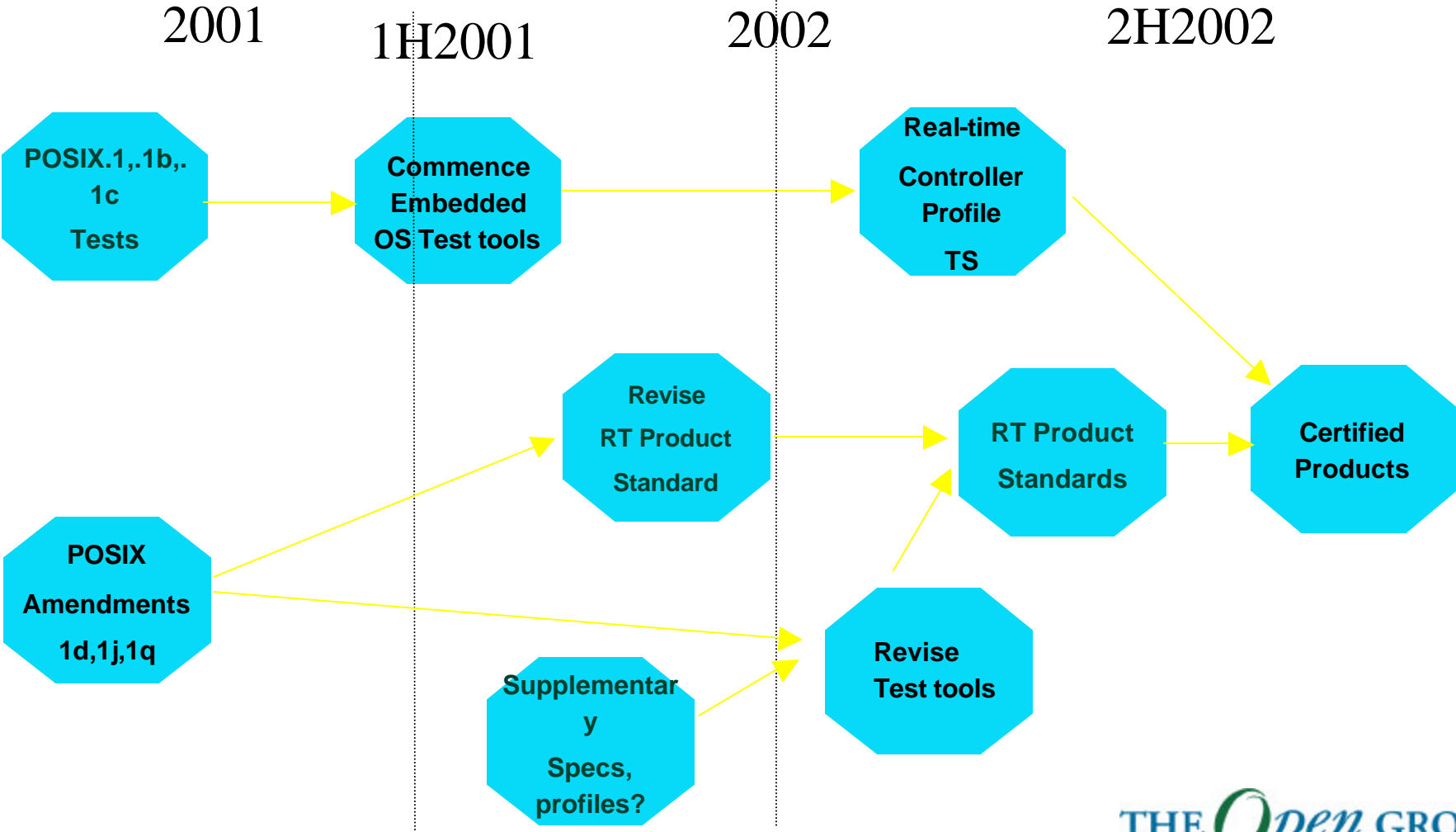
Roadmap

- ❑ The planned deliverables for 2001/2002 are as follows.
 - Test suites for RT POSIX Profiles
 - Certification program for POSIX profiles
 - White Papers
 - POSIX Conformance
 - Security for Real-time and Embedded Systems
 - Security Profile for Real-time and Embedded Systems
 - Additional test and certification program

Roadmap



Roadmap



Next Meetings

- The next conference is in Anaheim in January. Theme of the conference is Safety --- Integrated Information Infrastructure (IN**3**)

Additional Items

- ❑ Beta Testing for Profile 52
- ❑ Hard RT Java Requirements
- ❑ RT requirements for devices in the pervasive computing environment
- ❑ Requirements for additional POSIX 1003.13 Profiles