2003 FAA National Software Conference
COTS RTOS Research and Results

2003 FAA National Software Conference
September 16 - 19, 2003 – Reno, Nevada

COTS RTOS Research & Results

Commercial Off-The-Shelf (COTS) Real Time Operating Systems (RTOS) and Architectural Considerations
DTFA03-01-P-10129

Jim Krodel, Pratt Whitney
East Hartford, CT, USA

Sponsoring Org: FAA AIR120/Technical Standards Branch

1

Outline

Background of this Research

- Three Major Discussion Points
  - PowerPC – Considerations in Complex Micros
  - Partitioning – On a single CPU
  - RTOS's supporting Partitioning
- Integrated Points Of Discussion
  - Health monitor, Security & Safety, etc.
- Next Phase of Research
- Discussion

2

Background

- Multi-phased COTS Study Program
  - Phase 1 & 2
    - COTS HW Report (**DOT/FAA/AR-01/41**)
    - COTS SW Report (**DOT/FAA/AR-01/26**)
      - COTS snapshot (nuclear, medical, elev.), Alternate methods
      - Emerging COTS – **RTOSs** & Communications
  - Phase 3
    - COTS RTOSs (**DOT/FAA/AR-02/118**)
  - Phase 4
    - COTS RTOSs and architectural considerations
      - (**SOON TO BE PUBLISHED**)

http://av-info.faa.gov/software/Reports.htm

3

PowerPC Features – a basis for study

- Memory Models
- Supervisor/User Mode
- Pipes

Pipes

- Cache
- Exceptions

Exceptions

- Interrupts

Timers

- Machine State Register

4

Industry Standards

- POSIX
  - Little hard-real time
- ARINC 653
  - An API model – mapped to many approaches
  - Each approach should represent the A653 semantic model
  - Each A653 implementation will have assumptions that will need to be understood.
    - Task scheduling, use of user/supervisor mode

5

A653 APEX – Application Exec

- Provides API for users to create processes within a partition
- Tasks coexist in a partition and share available processor time assigned to the partition.
- A653 permits applications to adjust their allocated time.
  - Allows high priority processes execution certainty

6

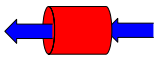
RTOSs That Support Partitioning

- An integral relationship with microprocessor features
  - Timing mechanisms
  - Interrupt mechanisms
  - MMU models
  - Utilization of cache
  - Supervisor/User Mode

7

Other Attributes of RTOSs Supporting Partitioning

- Data Communications



Queues

- Scheduling
  - Within partitions
  - Between partitions

Tasks

- Supervisory Authority of Module Operating System

8

Integrated Points Of Discussion

- Cache Jitter
- Memory & Timing Considerations in Higher Criticality Applications
- I/O Operations
- Board Support Packages (BSPs)
- Worst Case Execution Time (WCET)
  - ...and associated analyses.
- Health Monitoring
- System Integration
- RTOS Robustness Testing
- Linkers for Partitioned Systems
- Security

9

Cache Jitter

- Cache memory typically shared between partitions
- Cache info may contain page address values, data values, and code specific to a partition.
- If cache flushing needed when partitions change time can be compromised via the APEX round-robin scheduler
- A partition could potentially change the internal state of the cache, which may induce a failure of another partition.

10

Memory & Timing Considerations in Higher Criticality Applications

- Memory Managed by MOS
  - (Module Operating System)
  - O/S within partitions
  - Maximum stack sizes allocated.
  - Memory heap that is allocated at initialization
  - Fixed size & protected for such systems.
  - Code Statically allocated for higher criticality systems
- Timing
  - Inter-partition & intra partition
    - Jitter, WCET, Task Scheduling Priority Schemes

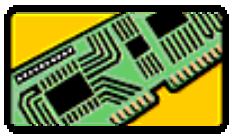
11

I/O Operations

- Kernel control
  - Centralized control
- Partition control
  - Less efficient data to be communicated between partitions
- Trade offs latency vs. efficiency

12

Board Support Package (BSP)



- Initializes the processor
- Initializes memory
- Performs various memory checks
- Initializes devices
- After initialization is complete, the BSP can still function to perform low-level cache manipulations.

13

Worst Case Execution Time (WCET) and Associated Analysis

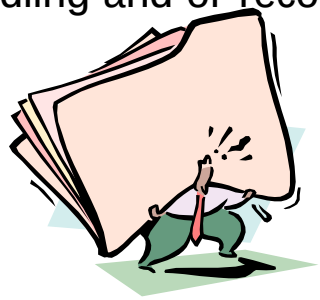
- Complex analysis due to pipelined processor, cache, out of order execution, etc.
  - WAG
  - Basic model
  - Sophisticated model
  - Statistical based analysis

- Flight envelope trials to confirm or adjust model figures
- In system monitors

14

Health Monitoring

- Space
- Time
- Error handling and or recording



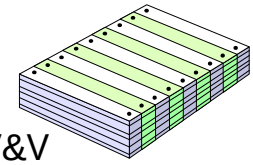
15

System Integration

- A person (organization) must act as an overall IMA system integrator
  - Allocates and integrates the resources
  - Strictly controlled, constraints well known, understood and enforced
  - Tool pedigree

16

RTOS Robustness Testing



- Separate plan OR Part of normal V&V
  - Memory Model review found stack overflow potential
  - Utilized chip page boundary exception handler
- Verification beyond RTOS
  - Partitions, Timing
  - Monitoring, Starvation
  - Queue overflows, and all system processes
  - … including on-chip attributes

17

Linkers for Partitioned Systems

- Vehicle for specifying what SW goes in what partition
  - Robust Linker Verification in order
  - Defined Integrator process needed

18

Security

- Commonality with safety
- Can provide challenges to safety
  - Stringent cache or memory flushing (increases jitter)
  - Deterministic time can be a channel for covert action
  - Some amount of indeterminism may be security-required

19

Next Steps of Study - RTOS &Component Integration

- Partition System Development
  - Design Approaches & Constraints
  - Guidance for RTOS developers, Designers, Integrators, Applications in a Partition
  - Partition System Build Techniques
  - Building a Verifiable System
  - Health Monitoring Activities
  - Incremental Cert. Considerations

20