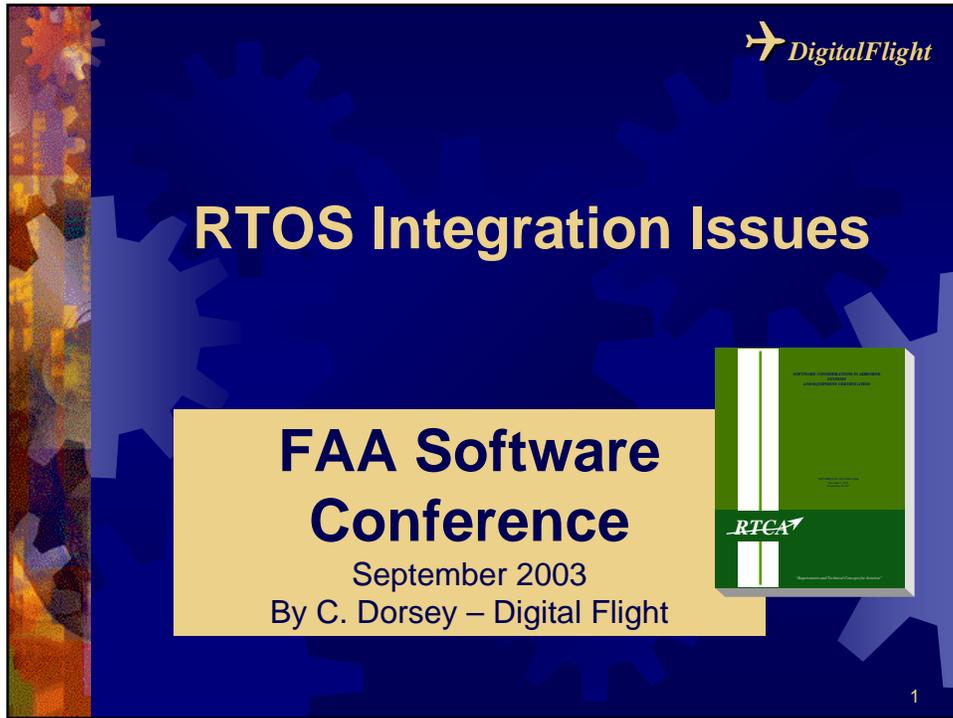


2003 FAA National Software Conference

RTOS Integration Issues



DigitalFlight

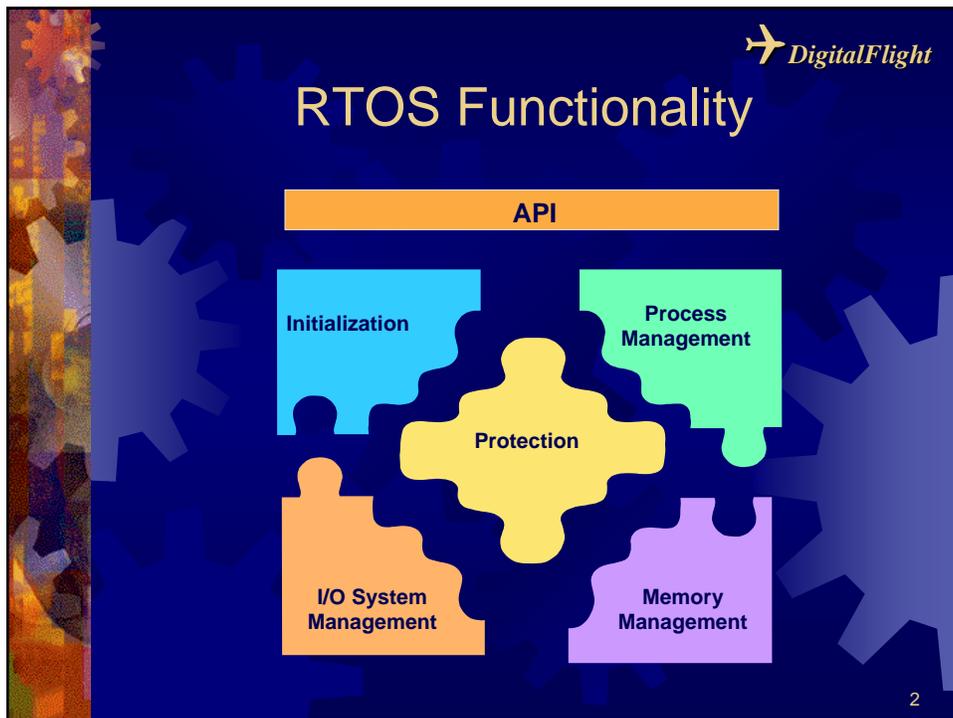
RTOS Integration Issues

FAA Software Conference
September 2003
By C. Dorsey – Digital Flight



1

This slide features a dark blue background with a pattern of interlocking gears. On the left side, there is a vertical strip with a colorful, abstract pattern. The DigitalFlight logo is in the top right corner. The main title 'RTOS Integration Issues' is centered in a large, bold, yellow font. Below it, a yellow rectangular box contains the text 'FAA Software Conference', 'September 2003', and 'By C. Dorsey – Digital Flight'. To the right of this box is a small image of a green book cover with the RTCA logo. A small number '1' is in the bottom right corner.



2003 FAA National Software Conference

RTOS Integration Issues



Defined API Issues

- Who tests that API works correctly?
- Is there a users guide and is it correct?
- What about errors – are they reported back by the API, and then are they dealt with correctly?
- Is the user-defined error handling used by the avionics manufacturer as intended by the RTOS vendor?

API

3



What the API Doesn't Tell You

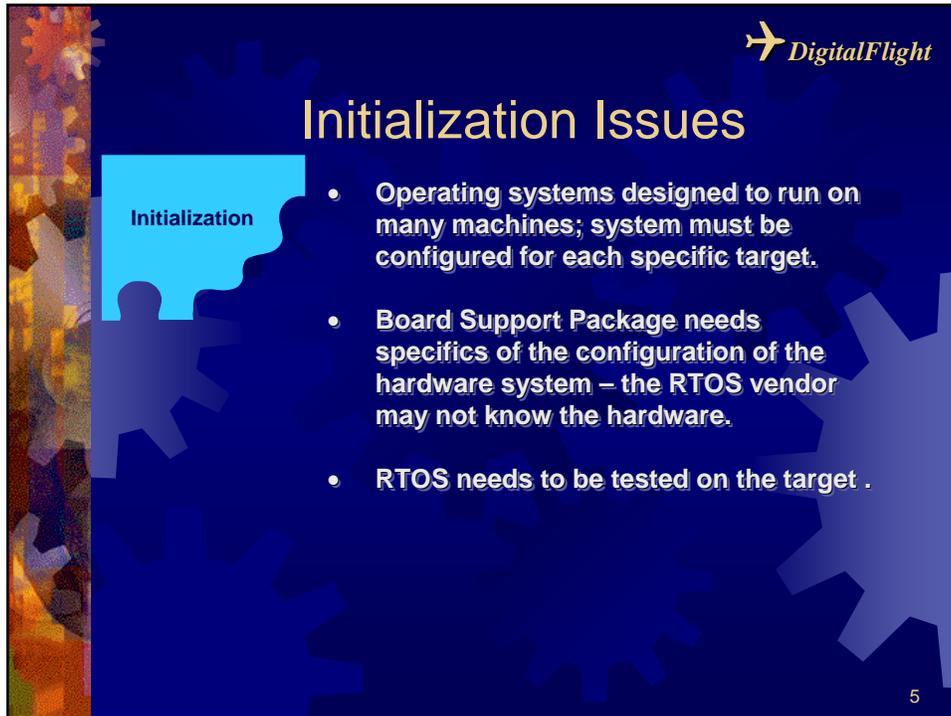
There are more errors in an RTOS than what you see at the API layer!

- Do you have visibility into the development to determine how this lower level error handling works, and supports the API error handler?
- What if the lower level error handling either does not work correctly or disregards the error –is this reported to the application layer?
- What happens if there is an error using the complex data structures, how does this surface at the API level?

4

2003 FAA National Software Conference

RTOS Integration Issues



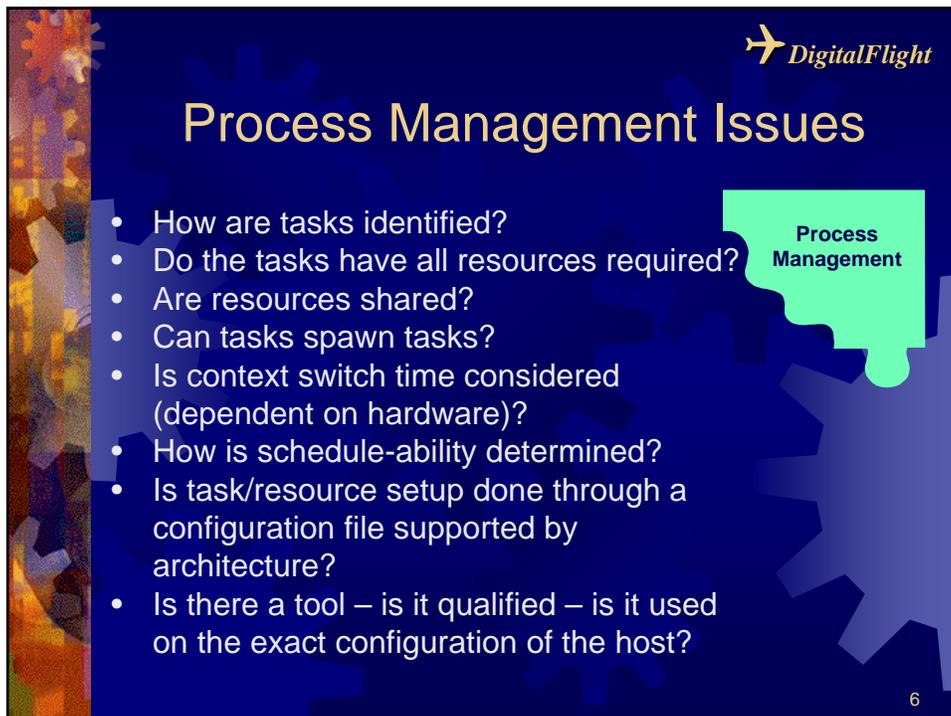
DigitalFlight

Initialization Issues

Initialization

- Operating systems designed to run on many machines; system must be configured for each specific target.
- Board Support Package needs specifics of the configuration of the hardware system – the RTOS vendor may not know the hardware.
- RTOS needs to be tested on the target .

5



DigitalFlight

Process Management Issues

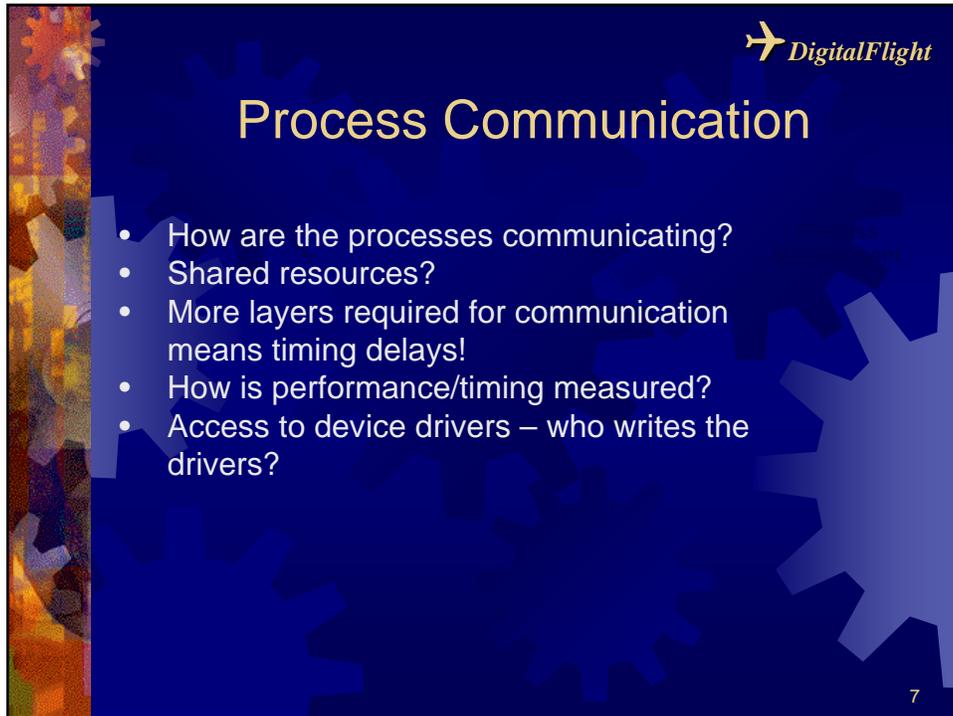
Process Management

- How are tasks identified?
- Do the tasks have all resources required?
- Are resources shared?
- Can tasks spawn tasks?
- Is context switch time considered (dependent on hardware)?
- How is schedule-ability determined?
- Is task/resource setup done through a configuration file supported by architecture?
- Is there a tool – is it qualified – is it used on the exact configuration of the host?

6

2003 FAA National Software Conference

RTOS Integration Issues



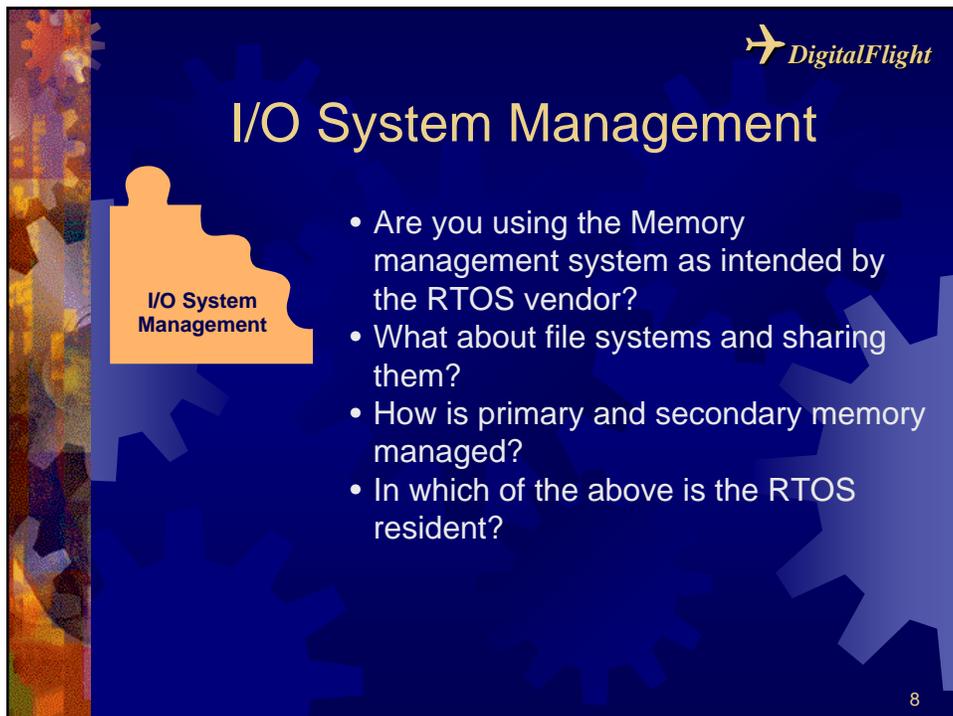
DigitalFlight

Process Communication

- How are the processes communicating?
- Shared resources?
- More layers required for communication means timing delays!
- How is performance/timing measured?
- Access to device drivers – who writes the drivers?

7

This slide features a dark blue background with a pattern of interlocking gears. On the left side, there is a vertical strip with a colorful, abstract gear-like pattern. The title 'Process Communication' is centered at the top in a light yellow font. The 'DigitalFlight' logo is in the top right corner. A list of five bullet points is positioned in the center-left. The number '7' is in the bottom right corner.



DigitalFlight

I/O System Management

- Are you using the Memory management system as intended by the RTOS vendor?
- What about file systems and sharing them?
- How is primary and secondary memory managed?
- In which of the above is the RTOS resident?

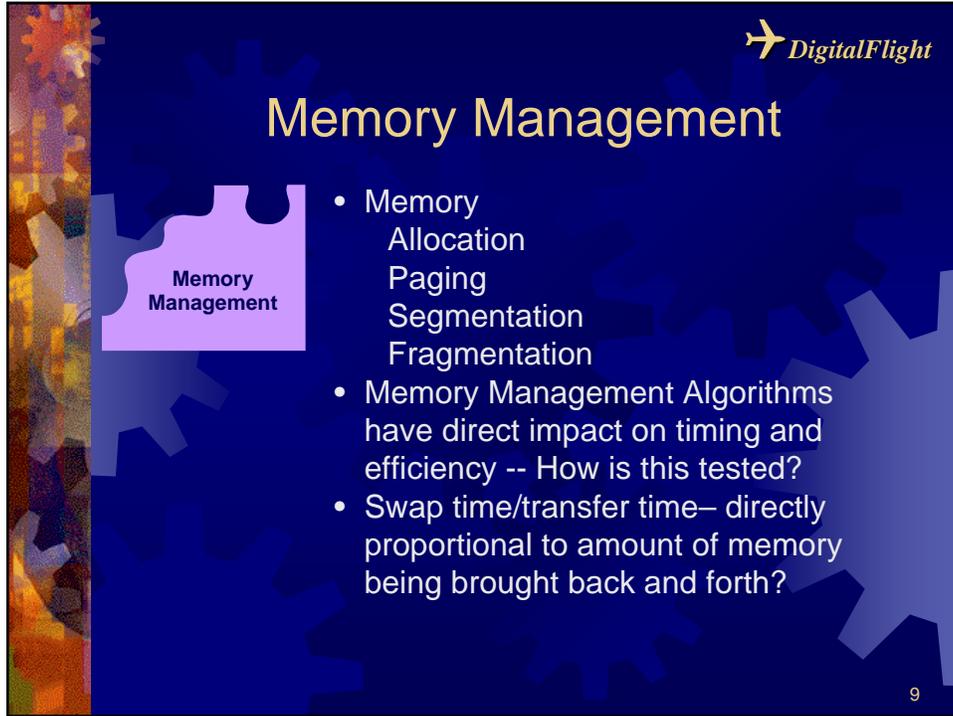
I/O System Management

8

This slide features a dark blue background with a pattern of interlocking gears. On the left side, there is a vertical strip with a colorful, abstract gear-like pattern. The title 'I/O System Management' is centered at the top in a light yellow font. The 'DigitalFlight' logo is in the top right corner. A list of four bullet points is positioned in the center-right. An orange puzzle piece graphic on the left contains the text 'I/O System Management'. The number '8' is in the bottom right corner.

2003 FAA National Software Conference

RTOS Integration Issues



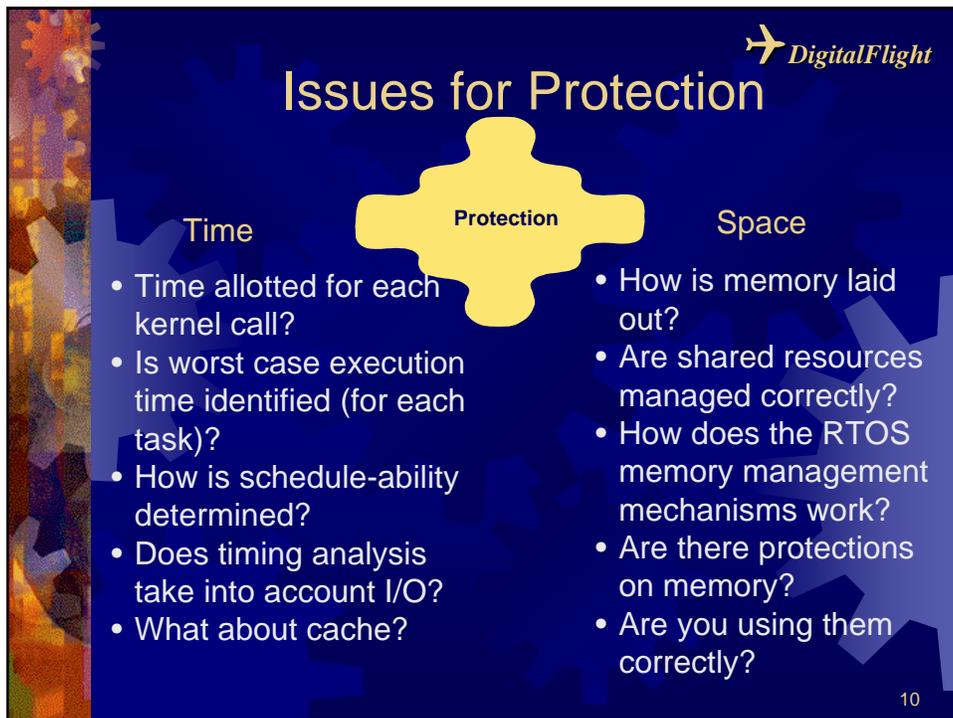
DigitalFlight

Memory Management

Memory Management

- Memory Allocation
Paging
Segmentation
Fragmentation
- Memory Management Algorithms have direct impact on timing and efficiency -- How is this tested?
- Swap time/transfer time-- directly proportional to amount of memory being brought back and forth?

9



DigitalFlight

Issues for Protection

Time Protection Space

- Time allotted for each kernel call?
- Is worst case execution time identified (for each task)?
- How is schedule-ability determined?
- Does timing analysis take into account I/O?
- What about cache?
- How is memory laid out?
- Are shared resources managed correctly?
- How does the RTOS memory management mechanisms work?
- Are there protections on memory?
- Are you using them correctly?

10

2003 FAA National Software Conference

RTOS Integration Issues



Protection In The Time Domain

- Does the RTOS vendors understand RMA?
- Timing is dependent on the actual HW, application, RTOS algorithms -- peak load conditions
- Schedule-ability analysis
- Bounded time kernel calls – how is this computed without the application specific HW configuration?
- Hidden execution time (message passing execution time gets attributed to sender? receiver? both?)
- Long Kernel calls (Close/Kill partition) pass work off to System Tasks
- Non-deterministic resource reclamation
- Cache? - Instruction Cache?
- How is throughput measured?

11



Protection In The Space Domain

- Kernel memory pool for resource allocation allows other partitions to effect resource availability
- Single protected segment for all “Code” requires analysis of errant jumps
- Pre-emptible kernels use task stacks for system calls
- Dynamic installation of device drivers requires privileged user code

12

2003 FAA National Software Conference

RTOS Integration Issues



DO-178B Considerations

- How did the RTOS vendor test?
- How was robustness testing achieved?
- Is the configuration file -- task definition -- set up correctly?
- Does the RTOS use the configuration file correctly?
- Is there trace-ability between API definition and the requirements that implement it – are they all tested?
- What are the assumptions of the RTOS vendor when giving timing benchmarks?

13



Decision To Go With COTS Vendor

- Is the RTOS a re-usable component?
- Will the COTS vendor give other certification customer references?
- Does the User Manual provide the information required for integration, performance characteristics?
- Does the low-level requirements architecture divulge the required information regarding errors that are not apparent at the API interface – or information regarding what “could be the error”?
- If the application must be fail operational does the RTOS support this requirement?

14