

Final Presentation

Real-time operating system for ARM microcontrollers

ESTEC Contract Number: 4000135473/21/NL/GLC/js 1st December 2022 12:30 Michael Ryan, CTO, O.C.E.Technology Ltd





Summary

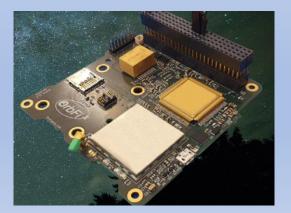
- RTOS for ARM Cortex-M with unique features (named OCEOS)
- Tested to ECSS Category B safety standard
- Tested for Microchip Cortex-M3 SAM3X8ERT & Cortex-M7 SAMRH71
- GSTP contract 4000135473/21/NL/GLC/js
- Duration: 13 months
- Budget: ESA €300k Co-funding €145k
- ESA Technical Officer: Piotr Skrzypek
- OCEOS development kit now on-sale





Embedded System Characteristics (1)

- Fixed Code Base Software not added during system life => can use physical addresses, RTOS doesn't need page tables etc.
- Code must be robust So an RTOS design should... => ensure certain failure modes are impossible
 - e.g. unbounded priority inversion, deadlocks,...
 - => allow behaviour policing by the application (white box)
 - performance data recorded and checkable at any time
 - => automatically check for problems
 - e.g. stack overrun, missed deadlines...
 - => automatically trigger application problem handlers
 => provide calls to deal with problems
 - e.g. kill task, disable task, ...









esa

Embedded System Characteristics (2)

- But things can go wrong So an RTOS design must provide => Fault Anticipation, Detection, Isolation, Reporting, Recovery
 - make it easy for the application to police the system: min time between task start requests max execution times, deadline misses max pre-emptions, max stack usage
 - automatic checks of key components memory area sentinels, stack space
 - automatic logging of anomalies
 - triggers for user defined problem handler functions
 - kill tasks, disable tasks, ...







OCEOS: For Embedded Systems

• Based on 'Stack Resource Policy' (Baker 1991) => single system stack per CPU (not stack per task)

• Deterministic

- => behaviour predictable
- => memory statically allocated
- => timing overheads minimized and quantifiable
- Application task timing recorded for analysis
 => maximum execution times, maximum times to completion.....

 missed deadlines trigger application defined action
- Timed actions independent of scheduling
 => output at specific time, task start request at specific time







OCEOS: RTOS (1)

• Fixed priority

=> task priorities fixed based on task importance

Pre-emption threshold

=> pre-emption only by tasks with higher priority than threshold

Multiple execution instances

=> multiple same task 'jobs' can be queued for execution typically using different data

- Timed actions independent of scheduling
 - => data output at specific time
 - => task start request at specific time







OCEOS: RTOS (2)

- Mutexes
 - => unbounded priority inversion cannot occur
 => deadlocks cannot occur
- Counting semaphores
 => allow wait with timeout
- Data queues
 => allow read with timeout







OCEOS: RTOS (3)

• System time

=> in microseconds, 64 bit

- Context switch timing
 => context switch time minimized
- Interrupts

=> interrupt disabled timing is minimized => high priority timer interrupt reserved for timed actions

Some numbers

255 tasks, 15*255 execution instances (jobs), 63 mutexes, 63 semaphores, 63 data queues



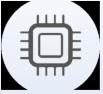




OCEOS: RTOS (4) – USING IT

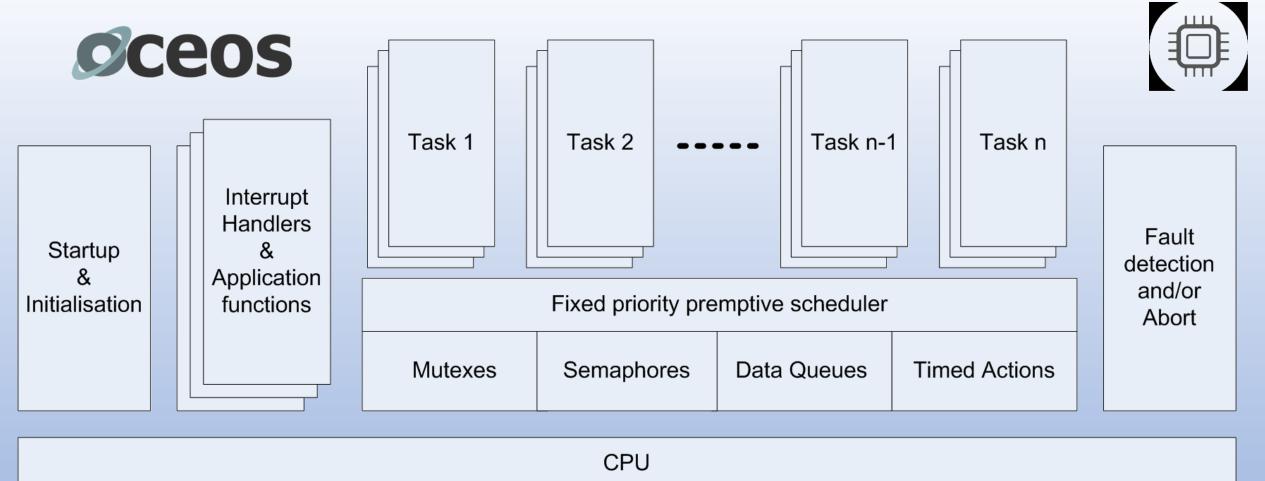
- Library components not used not linked into the executable
- Servant not Master started by application main()
- Step 1 : Create application configuration, pass to oceos_init() what stack space, log entries how many tasks, jobs per task, timed actions, how many mutexes, semaphores, data queues
- Step 2: Create corresponding tasks, mutexes, etc. using oceos_task_create() etc.
- Step 3: Use oceos_init_finish() to complete fixed data and checksum
- Step 4: Pass fixed data and initial task (if any) to oceos_start() dynamic data area is set up scheduling begins











Log & system state Area	Fixed data Area	Dynamic data Area	Single stack





Debug support - DMON

2									0	CEOS Systen	n view										- 0	J ×
😐 er	nabled 🛛 🗕 paused																					
Log ID	TimeStamp	Log Type	Delay	DeadLineMargin	Stack	CWP	SysStateVar	Log Info							Stac	k						
	00.969 602	SC=>T:0	00.000 213		0x6ffffbd0 (39%)	4	0x00000000	â	0	x7000003A												
	02.425 673 LO	g sys ok					0x0000000	0x0000cafe		-												
	02.425 772 US						0x0000000	0x0000caf1	(0x6FFFFF40												
	02.425 865		00.000 075		0x6ffff890 (70%)	1	0x00000000			x6FFFFE46												
	03.111 704	T:9=>T:0		00.146 503	0x6ffff890 (70%)	1	0x00000000		,													
	03.111 858	T:0=>T:3	00.685 982		0x6ffff890 (70%)	1	0x00000000		c	x6FFFFD4C												
	03.249 052	T:3=>T:0		N/A	0x6ffff890 (70%)		0x00000000											$\neg \cap$				
	03.249 111	T:0=>T:8	00.000 088		0x6ffff890 (70%)		0x00000000		c	x6FFFFC52												
	03.437 738	T:8=>T:0		00.040 061	0x6ffff890 (70%)		0x0000000			x6FFFFB58		11 11		11		I II						
	03.437 795	T:0=>T:4	00.188 673		0x6ffff890 (70%)		0x00000000			JXDFFFFB58		UU		U	UL			U				
)	03.780 781	T:4=>T:7	00.000 058		Ox6fff1560 (101%)	-	0x0000000		Stack	x6FFFFA5E												
	04.038 013	T:7=>T:4		00.050 989	0x6ffff560 (101%)		0x0000000		5													
	04.038 084	T:4=>T:5	00.000 110		Ox6ffff560 (101%)	6	0x00000000		(x6FFFF964												
	04.209 567	T:5=>T:4		00.035 675	0x6ffff560 (101%)	6	0x00000000															
	04.209 621	T:4=>T:0		00.192 995	0x6ffff890 (70%)		0x00000000		(x6FFFF86A												
	04.209 683	T:0=>T:6	00.000 146		0x6ffff890 (70%)		0x00000000			x6FFFF770												
	04.288 557	T:6=>T:0		00.017 119	0x6ffff890 (70%)		0x0000000		,													
	04.288 604	T:0=>SC		N/A	0x6ffffbd0 (39%)		0x0000000			x6FFFF676												
	04.288 657	SC=>SL			0x6ffffd20 (27%)		0x0000000															
	06.474 362				0x6ffffca8 (31%)		0x00000040		c	x6FFFF57C								-				
	06.474 428	ISR:9=>SC			0x6ffffca8 (31%)		0x00000040			0x6FFFF482												
	06.474 469	SC=>T:1	00.000 069		0x6ffffad8 (49%)	2	0x00000040	0.0000 (JXDFFFF482	5	g	65		4 9	8 9	20	8	91	10		
	06.474 478 LO 06.509 745			00.035.330	0.0000 10.0000	2	0x00000040	0x0000cafe		.000	.000	.000	.000				8	.000	.000	5.000	0.000	
		G DEADLINE MISSED		-00.053.220	0x6ffffad8 (49%)	2	0x00000040 0x00000040	0x00000001		80	000	000	000 00	8		8 8	8	000	000	000	0 00	
	06.509 814	SC=>T:2	00.035 437		0x6ffffad8 (49%)	2	0x00000040	0x0000001								Time, s			0	0	0	
	07.214 794		00.053 457	00.116 539	0x6ffffad8 (49%)		0x00000040															
	07.214 843	SC=>SL		00.110 535	0x6ffffd20 (27%)		0x00000040						O Max Stack (0x)	5FFFFFF0) C	Stack (0x6FF	FFAD8) C	Min Stack (0x6FFFF570)				
	01.344	-	03.472	626 04.586			06.720 724	4 07.794 53	<	8.866 794	09.943 062	11.058 060	12.117 32	4 12	190 711	14.251 151	15	.316 717	16.378 592	17.435 156	18.522 5	
ntext	01.344	484 02.402 810	05.472	020 04.380	4/9 05.002	911	00.720 724	+ 07.794 35	0 0	5.800 794	09.943 002	11.038 000	12.117 52	4 15,		14.251 151		.510 / 1/	10.578 592	17.455 150	10.522	337
eLine																						
R																						
1							ſ					I I						1				
2										·												
3			· · ·					Log ID		б												
5				· · · ·				Timestamp	: 0'	7.214 794		1										
5 7								Log Type		:2=>SC												
9			-					Stack CWP	: 0: : 2	x6ffffad8	· · ·											
4	· · · ·	· · · ·			· · ·			SysStateVa								· · ·			· ·		· · ·	
	100 C							Margin		0.116 539												
6								_	_	_												
8																						
0				Щ,																		
1.																						
:hedu																						
Sleep																						



Current Status

OCEOS (single core)

 SPARC and ARM versions complete (with additional support for GR716 microcontroller) ESA Flight Level B qualification ready

OCEOSmp (multicore)

- Multicore SPARC & RISC-V in initial test, ARM pending
- Example test results using SPARC quad core Gaisler GR740:
 - 1001 task starts even distribution: Per CPU 251,250,250,250
 - 4096 sample FFT (one task, four jobs in parallel): Speedup factor 3.7

• Availability

- OCEOS single-core development kit on-sale
- OCEOS multicore beta evaluations available soon









- Thanks to ESA for their support
- Thank you for listening
- Any Questions?



www.ocetechnology.com