OCEOSmp

a whitebox RTOS for multicore embedded systems

GR740 User Day

13th December 2022

Michael Ryan, CTO, O.C.E.Technology Ltd

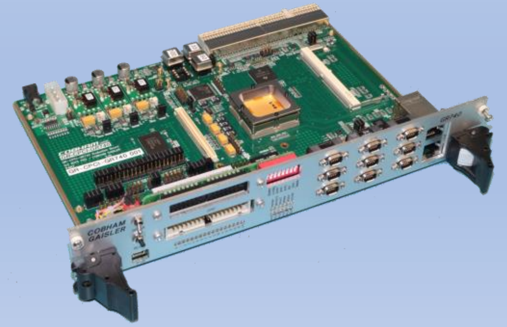
Embedded System Characteristics (1)

- **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, …

  => 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, disable a CPU, …



OCEOSmp on GR-CPCI-GR740

Embedded System Characteristics (2)

- **But things can go wrong** *So an RTOS design must provide*
  => **F**ault **A**nticipation, **D**etection, **I**solation, **R**eporting, **R**ecovery
  - 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
  - make it easy to exploit redundancy:
    run same task on many CPUs, check results agree
  - 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, disable CPU cores,
    restart CPU core, …

OCEOSmp on GR-VPX-GR740

OCEOSmp: For Multi-Core 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
- **Schedulability analysis**
  => simpler to perform
- **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

OCEOSmp on GR712

OCEOSmp: Multi-Core

- **Exclude**
  => exclude some cores from OCEOSmp use, e.g. for use by Linux
- **Reserve**
  => reserve cores for higher priority OCEOSmp tasks
- **Symmetric**
  => after start-up, all cores are equal
- **Work Distribution**
  => task execution instances distributed evenly across cores
  => unless task restricted to a particular core
- **Control**
  => take core out of use, put core back in use

OCEOS on GR716

OCEOSmp: 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 in execution at same time typically using different data
- **Timed actions independent of scheduling**
  => data output at specific time
  => task start request at specific time

OCEOSmp for RISC-V

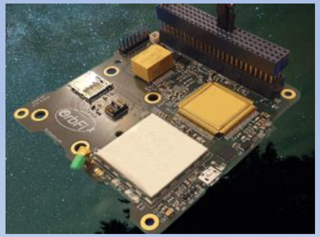
OCEOSmp: RTOS (2)

- **Mutexes**
  => unbounded priority inversion cannot occur
  => deadlock warning, cannot occur if single core
- **Read-Write mutexes**
  => allow multiple simultaneous reads of protected area when not being written, prevent writing if being read
- **Counting semaphores**
  => allow wait with timeout
- **Data queues**
  => allow read with timeout

Solar array drive

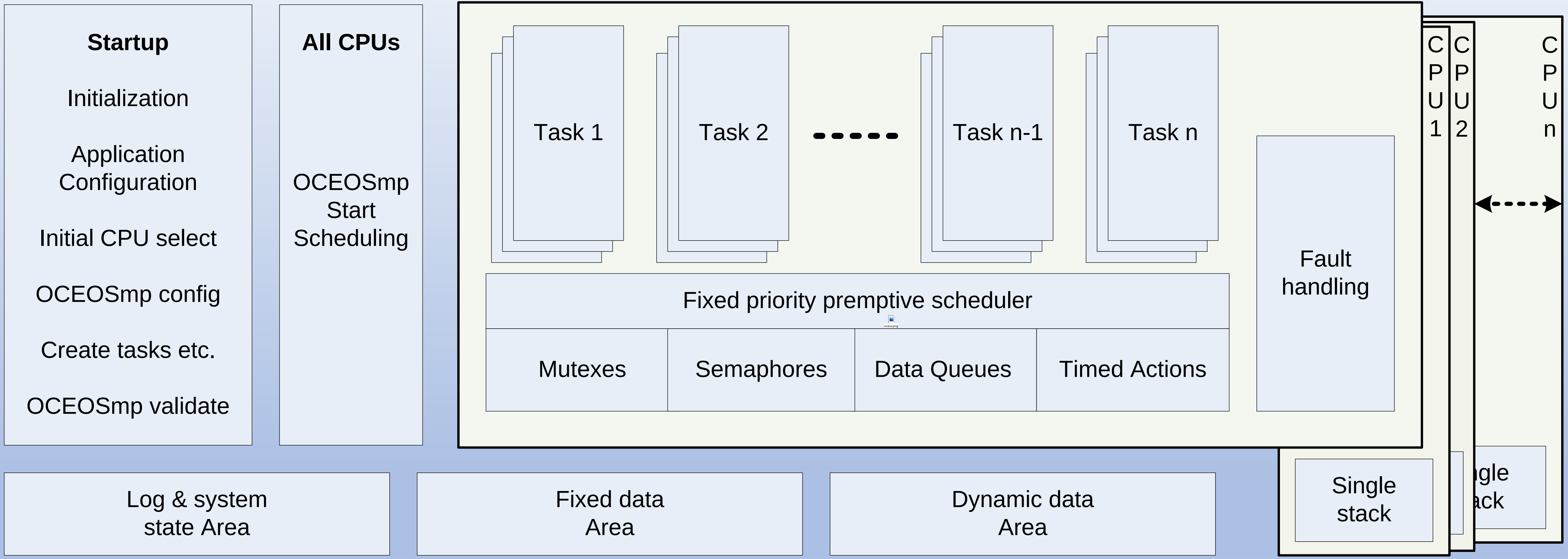
OCEOSmp: RTOS (3)

- **System time**
  => in microseconds, 64 bit
- **Context switch timing**
  => context switching shared across all cores
  => context switch time minimized
- **Interrupts**
  => interrupt disabled timing is minimized
  => high priority timer interrupt reserved for timed actions
- **Some numbers**
  Up to 255 cores, 255 tasks, 15*255 execution instances (jobs),
  63 mutexes, 63 read-write mutexes, 63 semaphores,
  63 data queues, memory < 20KiB



GNSS embedded system using OCEOS

OCEOSmp



Startup

Initialization

Application Configuration

Initial CPU select

OCEOSmp config

Create tasks etc.

OCEOSmp validate

All CPUs

OCEOSmp Start Scheduling

Task 1

Task 2

Task n-1

Task n

Fixed priority premptive scheduler

Mutexes

Semaphores

Data Queues

Timed Actions

Fault handling

Single stack

gle ack

Log & system state Area

Fixed data Area

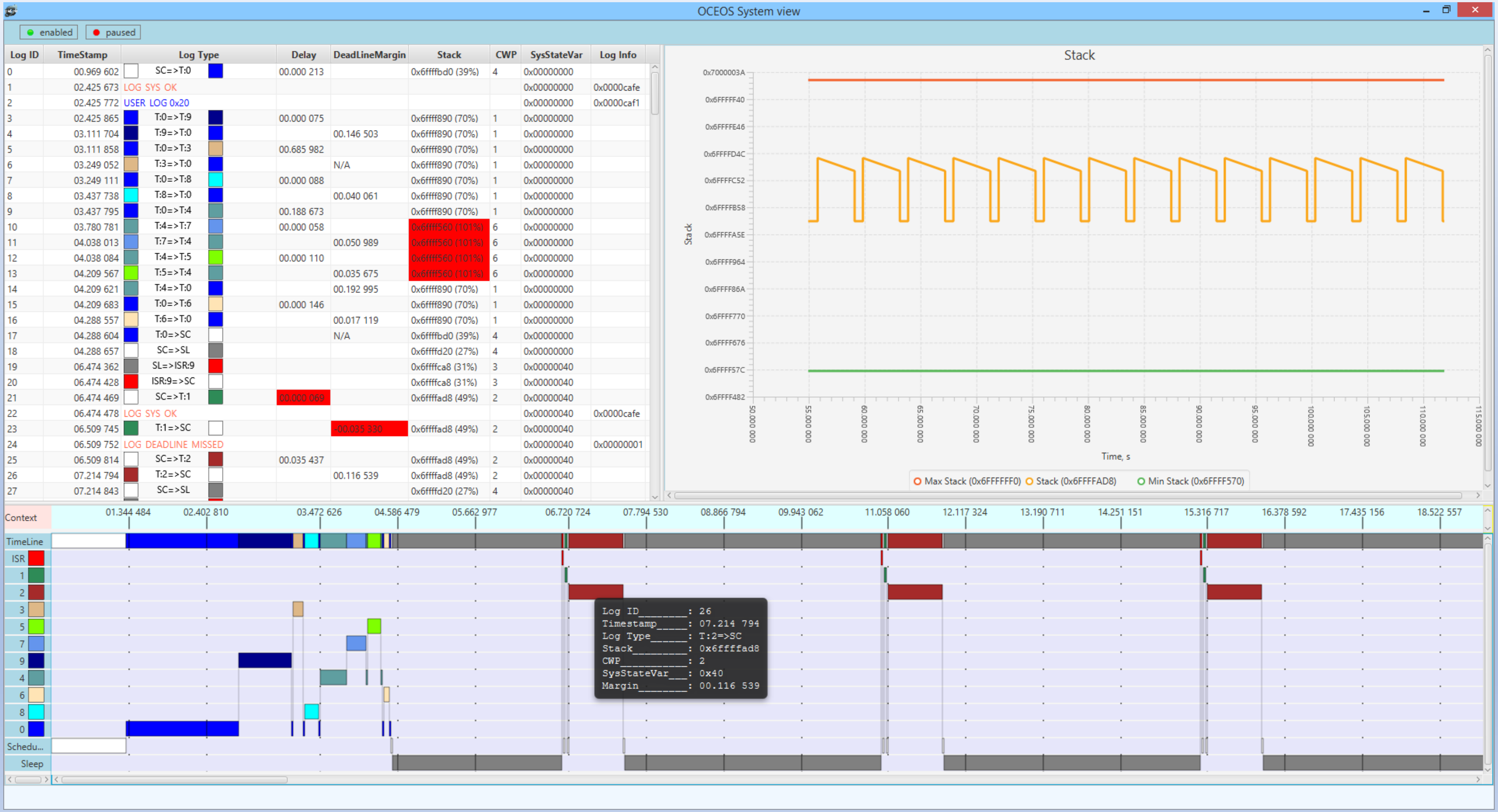
Dynamic data Area

OCEOSmp: 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 cores to use, 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
  multi-core scheduling begins

OCEOS for automobiles

Debug support - DMON

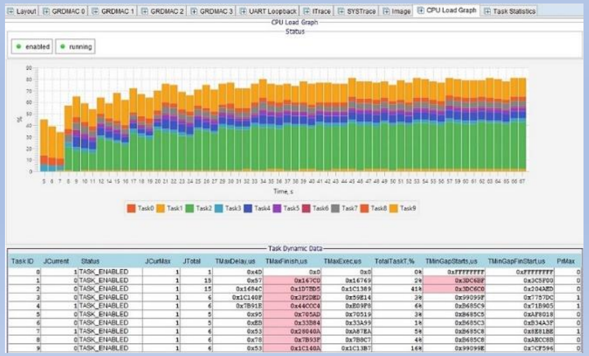


Log ID	TimeStamp	Log Type	Delay	DeadLineMargin	Stack	CWP	SysStateVar	Log Info
0	00.969 602	SC=>T:0	00.000 213		0x6ffffbd0 (39%)	4	0x00000000	
1	02.425 673	LOG SYS OK					0x00000000	0x0000cafe
2	02.425 772	USER LOG 0x20					0x00000000	0x0000caf1
3	02.425 865	T:0=>T:9	00.000 075		0x6ffff890 (70%)	1	0x00000000	
4	03.111 704	T:9=>T:0		00.146 503	0x6ffff890 (70%)	1	0x00000000	
5	03.111 858	T:0=>T:3	00.685 982		0x6ffff890 (70%)	1	0x00000000	
6	03.249 052	T:3=>T:0		N/A	0x6ffff890 (70%)	1	0x00000000	
7	03.249 111	T:0=>T:8	00.000 088		0x6ffff890 (70%)	1	0x00000000	
8	03.437 738	T:8=>T:0		00.040 061	0x6ffff890 (70%)	1	0x00000000	
9	03.437 795	T:0=>T:4	00.188 673		0x6ffff890 (70%)	1	0x00000000	
10	03.780 781	T:4=>T:7	00.000 058		0x6ffff560 (101%)	6	0x00000000	
11	04.038 013	T:7=>T:4		00.050 989	0x6ffff560 (101%)	6	0x00000000	
12	04.038 084	T:4=>T:5	00.000 110		0x6ffff560 (101%)	6	0x00000000	
13	04.209 567	T:5=>T:4		00.035 675	0x6ffff560 (101%)	6	0x00000000	
14	04.209 621	T:4=>T:0		00.192 995	0x6ffff890 (70%)	1	0x00000000	
15	04.209 683	T:0=>T:6	00.000 146		0x6ffff890 (70%)	1	0x00000000	
16	04.288 557	T:6=>T:0		00.017 119	0x6ffff890 (70%)	1	0x00000000	
17	04.288 604	T:0=>SC		N/A	0x6ffffbd0 (39%)	4	0x00000000	
18	04.288 657	SC=>SL			0x6ffffd20 (27%)	4	0x00000000	
19	06.474 362	SL=>ISR:9			0x6ffffca8 (31%)	3	0x00000040	
20	06.474 428	ISR:9=>SC			0x6ffffca8 (31%)	3	0x00000040	
21	06.474 469	SC=>T:1	00.000 069		0x6ffffad8 (49%)	2	0x00000040	
22	06.474 478	LOG SYS OK					0x00000040	0x0000cafe
23	06.509 745	T:1=>SC		-00.035 330	0x6ffffad8 (49%)	2	0x00000040	
24	06.509 752	LOG DEADLINE MISSED					0x00000040	0x00000001
25	06.509 814	SC=>T:2	00.035 437		0x6ffffad8 (49%)	2	0x00000040	
26	07.214 794	T:2=>SC		00.116 539	0x6ffffad8 (49%)	2	0x00000040	
27	07.214 843	SC=>SL			0x6ffffd20 (27%)	4	0x00000040	

```
Log ID_______: 26
Timestamp____: 07.214 794
Log Type_____: T:2=>SC
Stack________: 0x6ffffad8
CWP__________: 2
SysStateVar__: 0x40
Margin_______: 00.116 539
```

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 scheduling in initial test, ARM later
  - 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
  - OCEOSmp - multicore beta evaluations available soon



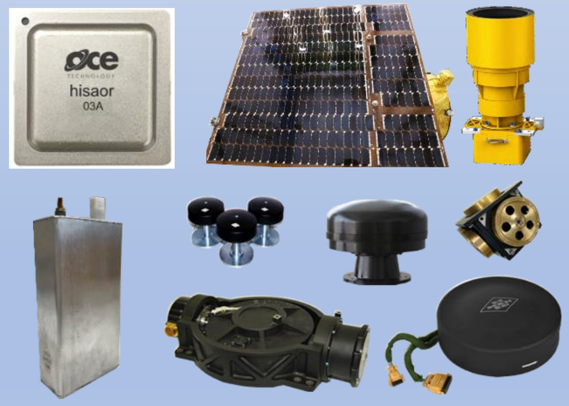
Task Dynamic Data

Task ID	JCurrent	Status	JCurMax	JTotal	TMaxDelay,us	TMaxFinish,us	TMaxExec,us	TotalTaskT,%	TMinGapStarts,us	TMinGapFinStart,us	PrMax
0	1	TASK_ENABLED	1	1	0x4D	0x0	0x0	0%	0xFFFFFFFF	0xFFFFFFFF	0
1	0	TASK_ENABLED	1	15	0x57	0x167C0	0x16769	2%	0x3DC6BF	0x3C5F00	0
2	0	TASK_ENABLED	1	15	0x1684C	0x1D7BD5	0x1C1389	41%	0x3DC6C0	0x204AED	0
3	0	TASK_ENABLED	1	6	0x1C140F	0x3F2DED	0x59E14	3%	0x99099F	0x7757DC	1
4	1	TASK_ENABLED	1	6	0x7B91E	0x44CCC4	0xE09F8	6%	0xB685C9	0x71B905	1
5	0	TASK_ENABLED	1	5	0x95	0x705AD	0x70519	3%	0xB685C5	0xAF8018	0
6	0	TASK_ENABLED	1	5	0xEB	0x33B84	0x33A99	1%	0xB685C3	0xB34A3F	0
7	1	TASK_ENABLED	1	6	0x53	0x28040A	0xA87EA	5%	0xB685C8	0x8E81BE	1
8	0	TASK_ENABLED	1	6	0x78	0x7B93F	0x7B8C7	4%	0xB685C8	0xAECC8B	0
9	0	TASK_ENABLED	1	6	0x53	0x1C140A	0x1C13B7	16%	0x99099E	0x7CF596	0

OCEOS task usage & debug screen

Finally

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



michael.ryan@ocetechnology.com

www.ocetechnology.com