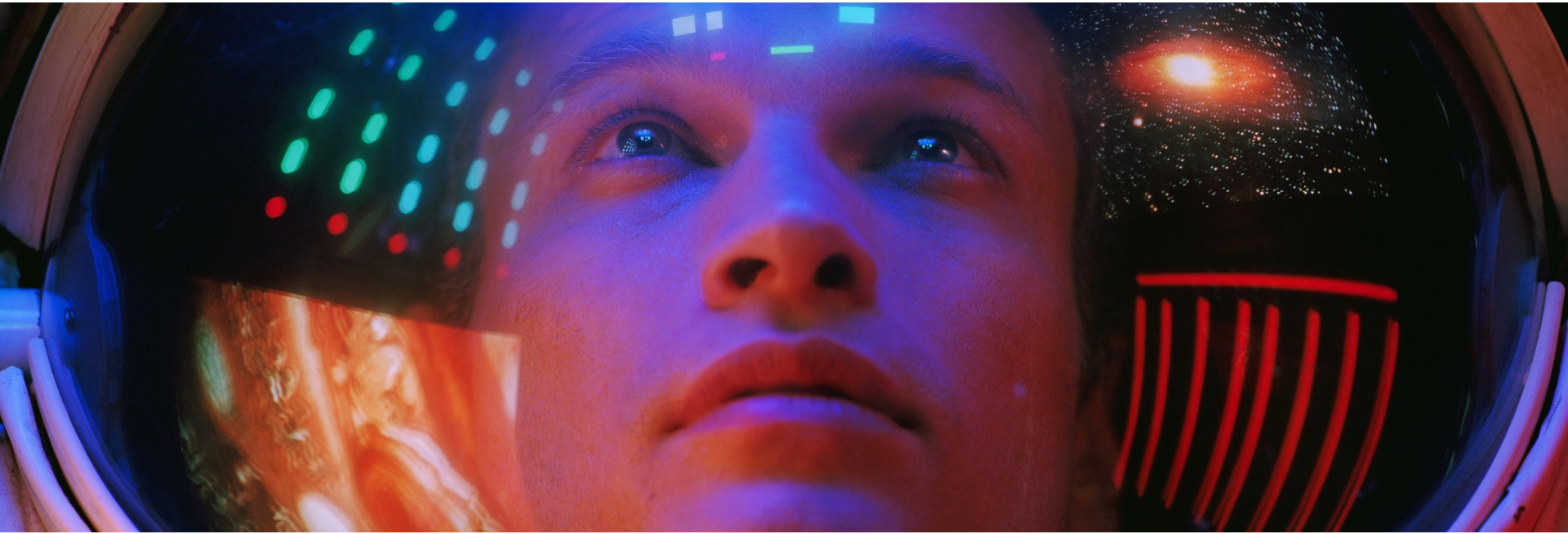
MSE | MASTER OF SCIENCE IN ENGINEERING

MA_EmbReal

Robust Patterns for Reliable Systems (III)

Version: 1.2

Serge Ayer – Luca Haab | 09.05.2023 | Cours MSE



Temporal Isolation

Tasks Temporal Isolation

Recap

Tasks - Monitoring

Recap

- First thing first:
  - Detect a fault happening
- Apply pattern(s)
  - Watchdog – the simplest

Monitoring Tasks - Watchdog

Recap

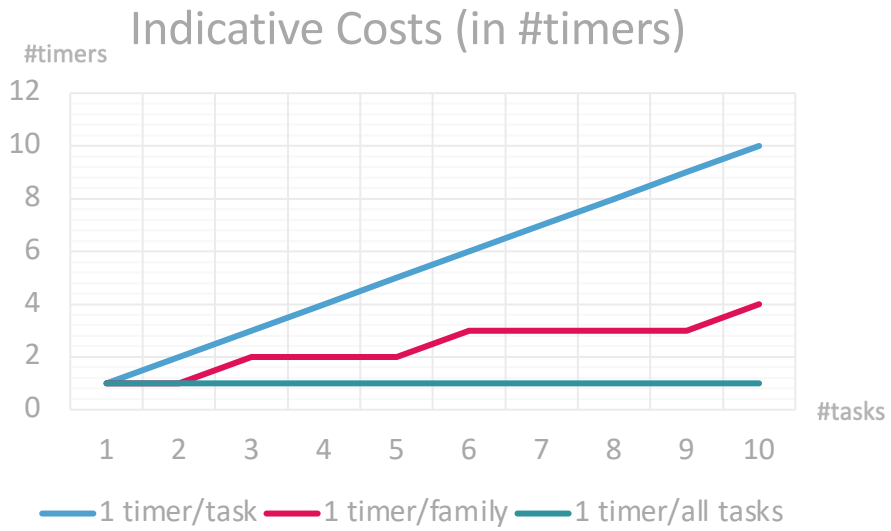
- A task needs to refresh a watchdog
- A consequent action is triggered if not

- Note: multiple tasks with different cadences may undergo watchdog scrutiny

What does this mean for real?

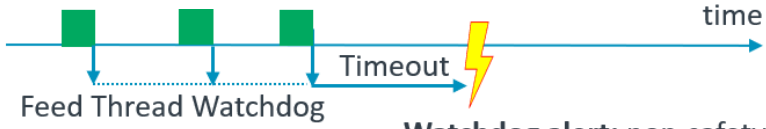
Task Watchdog: Options

- 1 timer per task
- 1 timer per task family
- 1 timer for all tasks



Task Watchdogs: timeout options

Thread 99



Watchdog alert: non-safety operation is stalled.

It can be suspended or restarted without impact on safety functionality

Thread 1

Watchdog alert: safety operation is stalled!

Suspend non-safety threads and track that execution of thread continues

Task Watchdogs: refreshing…

$$watchdog_{value} = task_{next\_execution} - getTick() + task_{period}$$

Where:

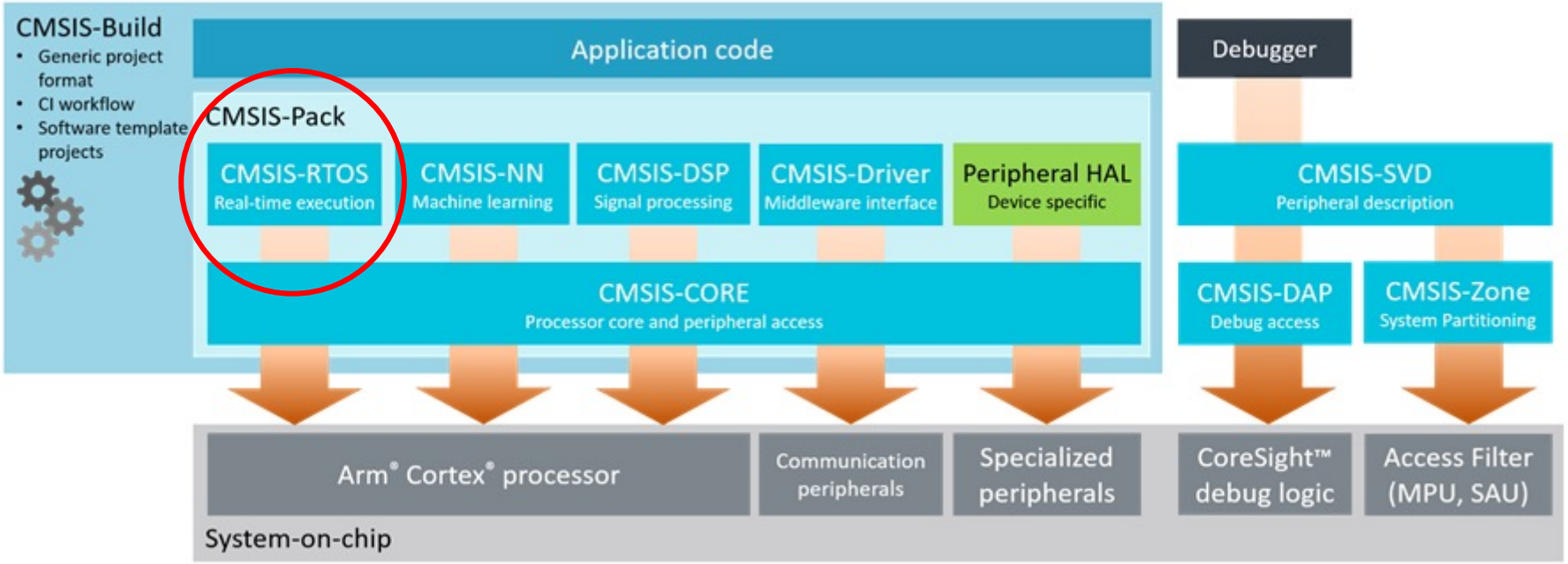
$task_{next\_execution}$: *earliest possible start*

$task_{period}$: *period of the task*

$getTick()$: *current system tick*

Thread Watchdog in CMSIS

- If we were to implement a watchdog in our environment



Hypothesis: you modify Keil RTX

- If you miss features, what would we need?

Let’s get dirty

https://embreal.isc.heia-fr.ch/codelabs/robust-patterns-part2/#modifying-an-rtx-kernel

References

- Robust Communications Software - Extreme Availability, Reliability and Scalability for Carrier-Grade Systems, Greg Utas (ISBN 0-470-85434-0)
- Patterns for Fault Tolerant Software, Robert S. Hanmer (ISBN: 978-1-118-35154-3)
- The Architecture of a Reliable Operating System (https://www.cs.vu.nl/~ast/Publications/Papers/asci-2006.pdf)
- Process isolation with Arm FuSa runtime system: https://community.arm.com/arm-community-blogs/b/tools-software-ides-blog/posts/process-isolation-with-fusa-rts