Mixed Criticality Systems What is it Really?

Geoffrey Nelissen

CISTER – Research Centre in
Real-Time & Embedded Computing Systems

Mixed Criticality Systems (Model) What is it Really?

Geoffrey Nelissen

A bit of personal history

A bit of personal history

2007

The beginning:
Paper of **Vestal**

A bit of personal history

My debut:
I start to work on MCS
using **Vestal's model**

The beginning:
Paper of **Vestal**

A bit of personal history

My debut:
I start to work on MCS using **Vestal's model**

The beginning:
Paper of **Vestal**

Awareness:
I start collaborating with **industrial partners** in EU projects

We were not really understanding each other

A bit of personal history

The beginning:
Paper of **Vestal**

My debut:
I start to work on MCS using **Vestal's model**

Awareness:
I start collaborating with **industrial partners** in EU projects

We were not really understanding each other

An opportunity:
My new **PhD student** works for a company called Critical Software and is an **expert in certification**

A bit of personal history

The beginning:
Paper of **Vestal**

My debut:
I start to work on MCS using **Vestal's model**

Awareness:
I start collaborating with **industrial partners** in EU projects

We were not really understanding each other

An opportunity:
My new **PhD student** works for a company called Critical Software and is an **expert in certification**

An attempt:
We **publish** a paper discussing the **dichotomy** around the notion of criticality

The original message

The original message

Criticality of a component:
measure of the severity of that component's failure

The original message

Criticality of a component:
measure of the severity of that component's failure

- Defines safety requirements that must be fulfilled
- Drives the development and certification process
  ➔ impacts cost and time

The original message

Criticality of a component:
measure of the severity of that component's failure

- Defines safety requirements that must be fulfilled
- Drives the development and certification process
  ➔ impacts cost and time

- Misbehaviour is not limited to the consequence of a deadline miss
  Examples:
  - Wrong output
  - Corruption of blocking of shared resources
  - Buffer overload
  - ...

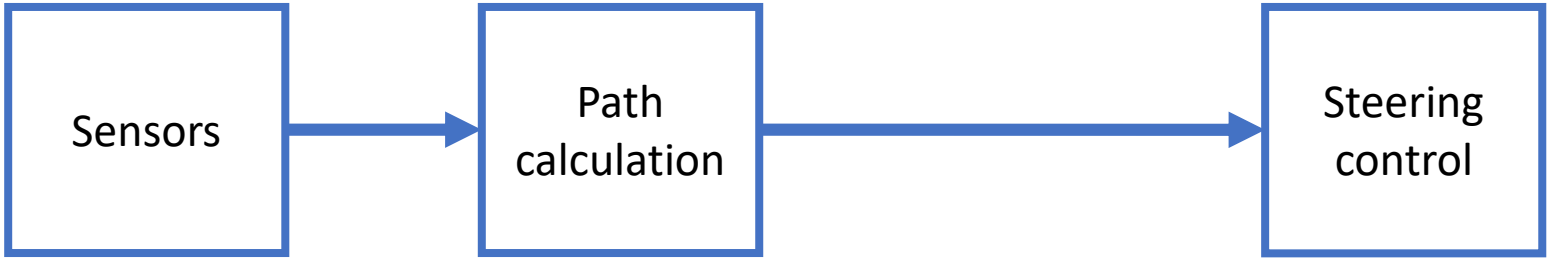
The original message

- **Criticality** is **not** a measure of **importance**

The original message

- **Criticality** is **not** a measure of **importance**

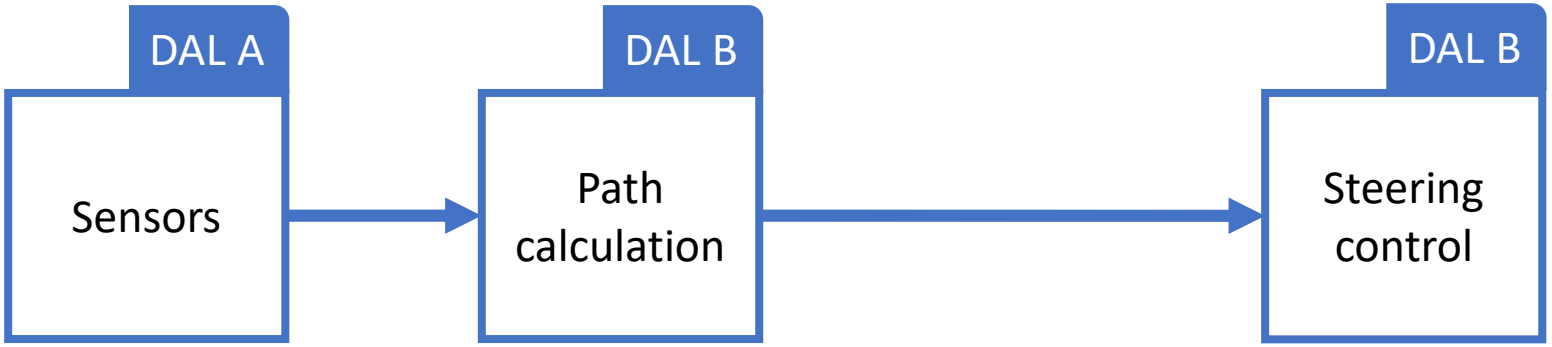
  Example: Auto-pilot



The original message

- **Criticality** is **not** a measure of **importance**

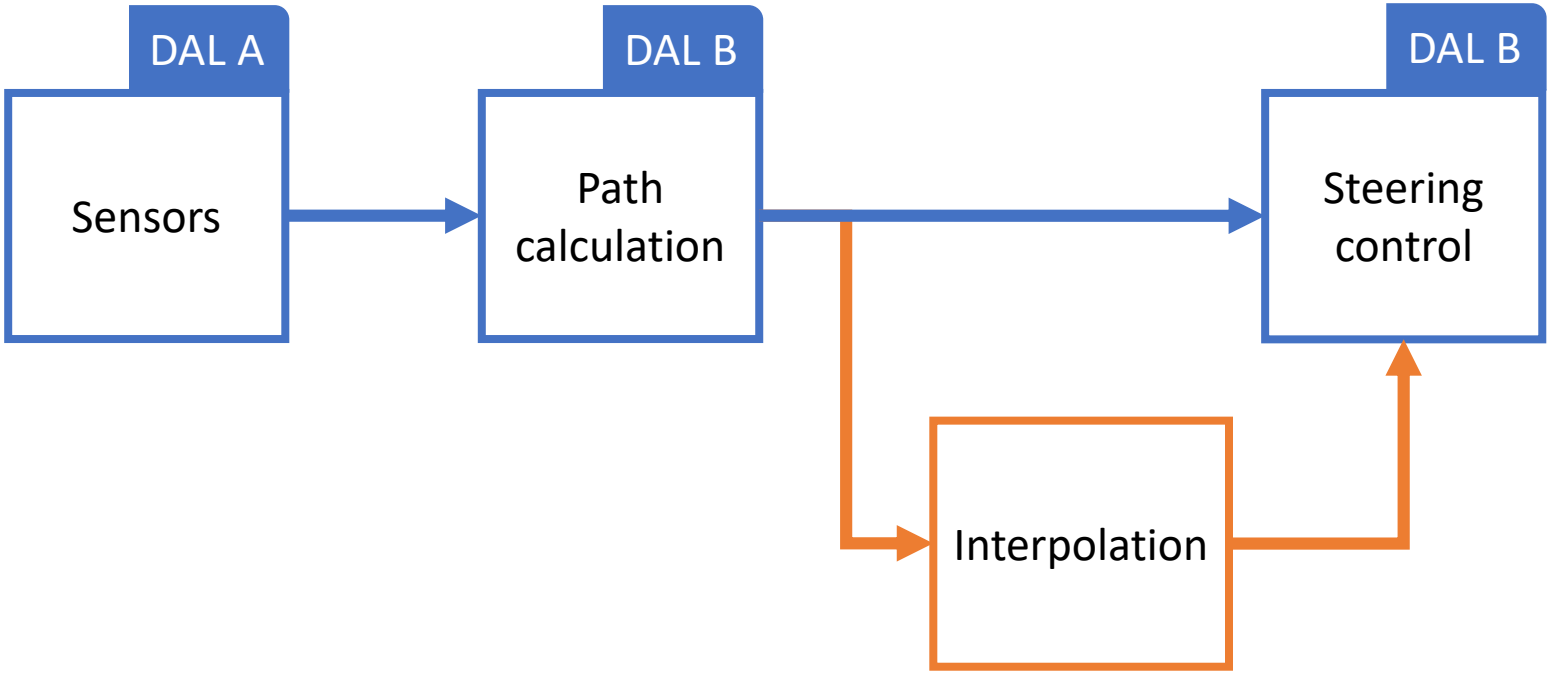
  Example: Auto-pilot



The original message

- **Criticality** is **not** a measure of **importance**

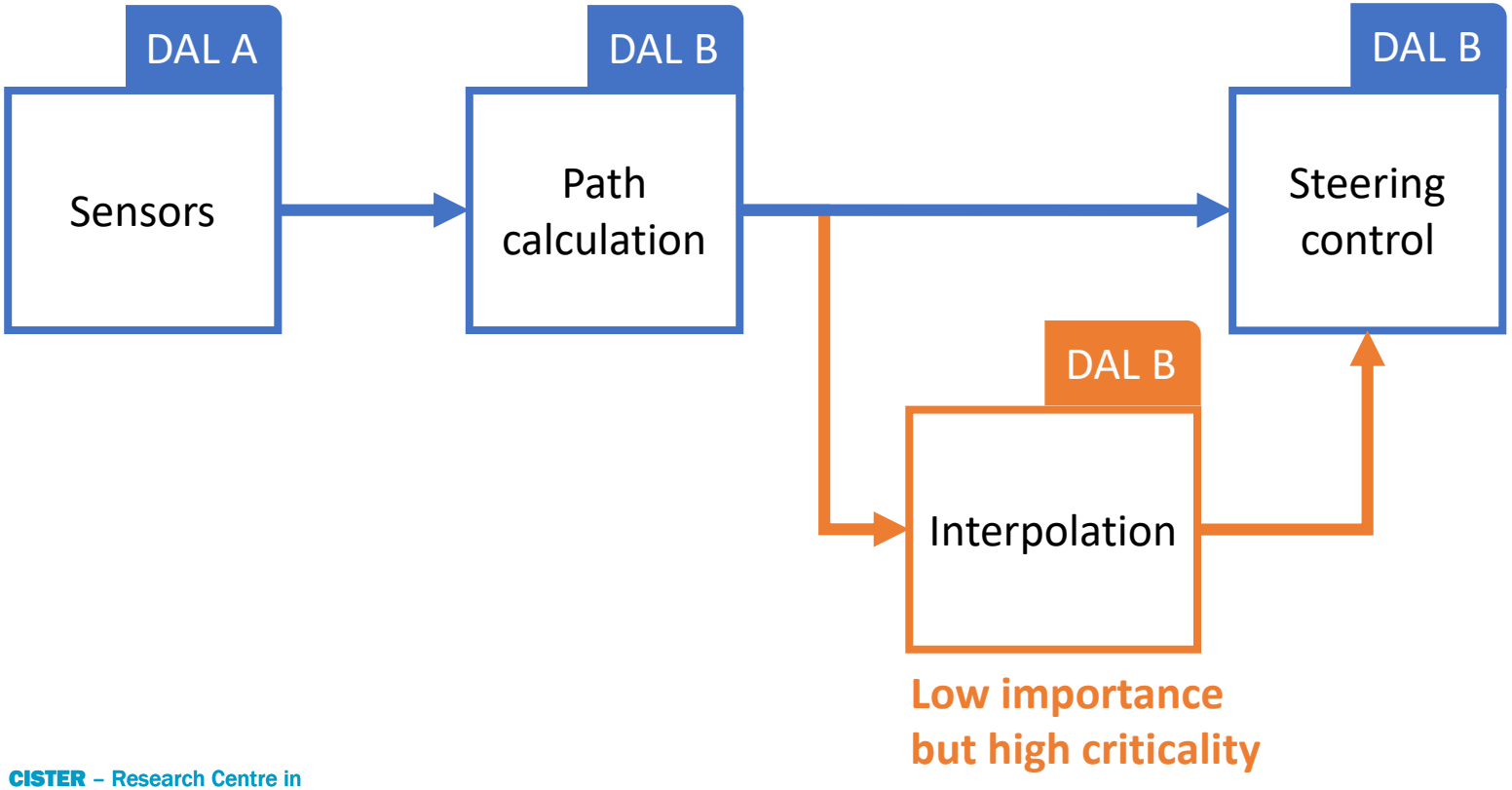
  Example: Auto-pilot



The original message

- **Criticality** is **not** a measure of **importance**

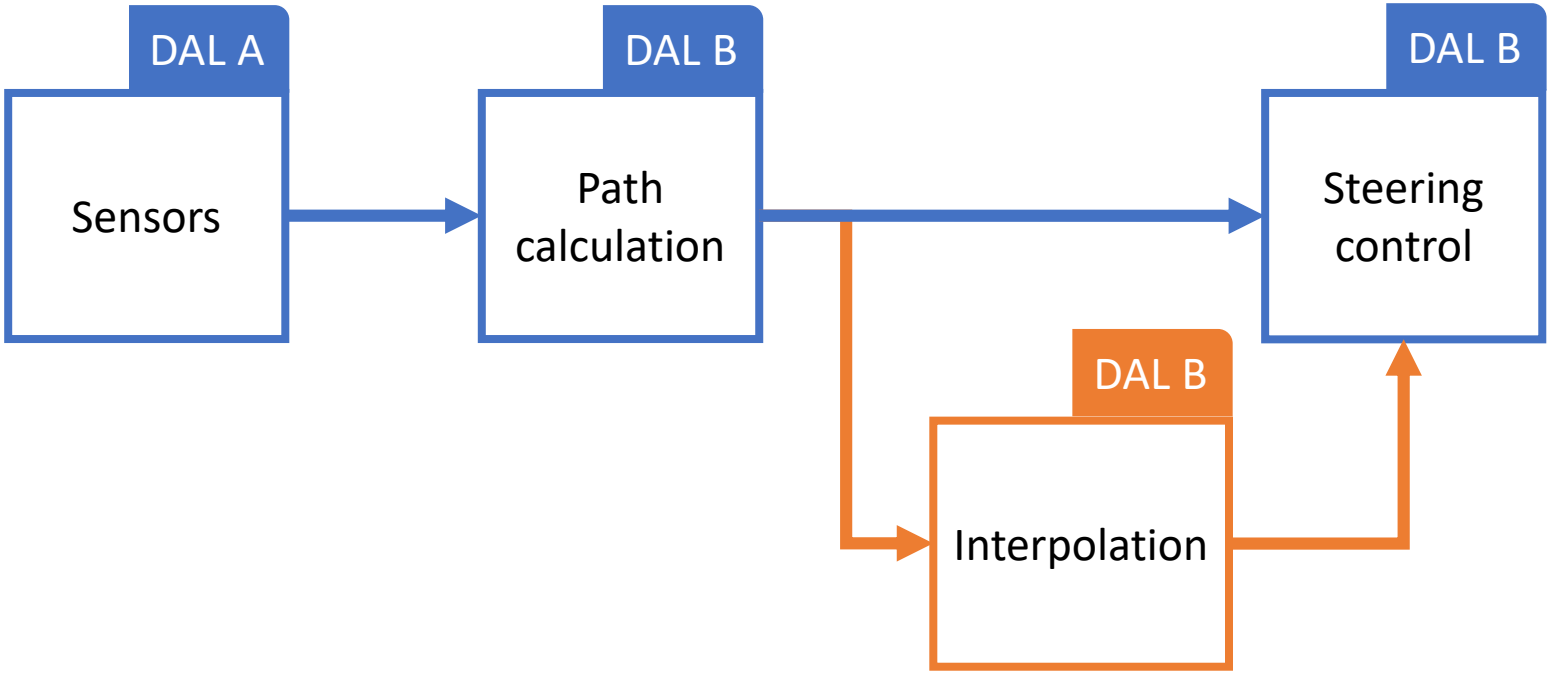
  Example: Auto-pilot



The original message

- **Criticality** is **not** a measure of **importance**

  Example: Auto-pilot

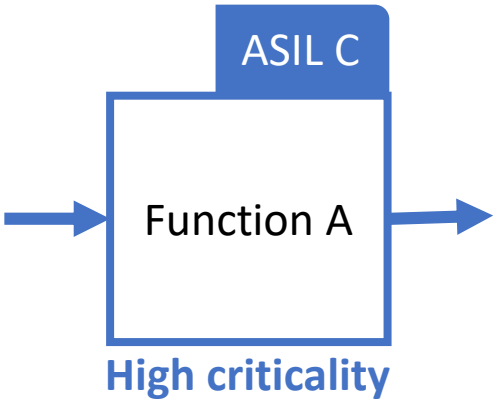


The decision of which function to keep running in case of a fault should not be based on criticality only

The original message

- **Criticality** is **not** a measure of **importance**

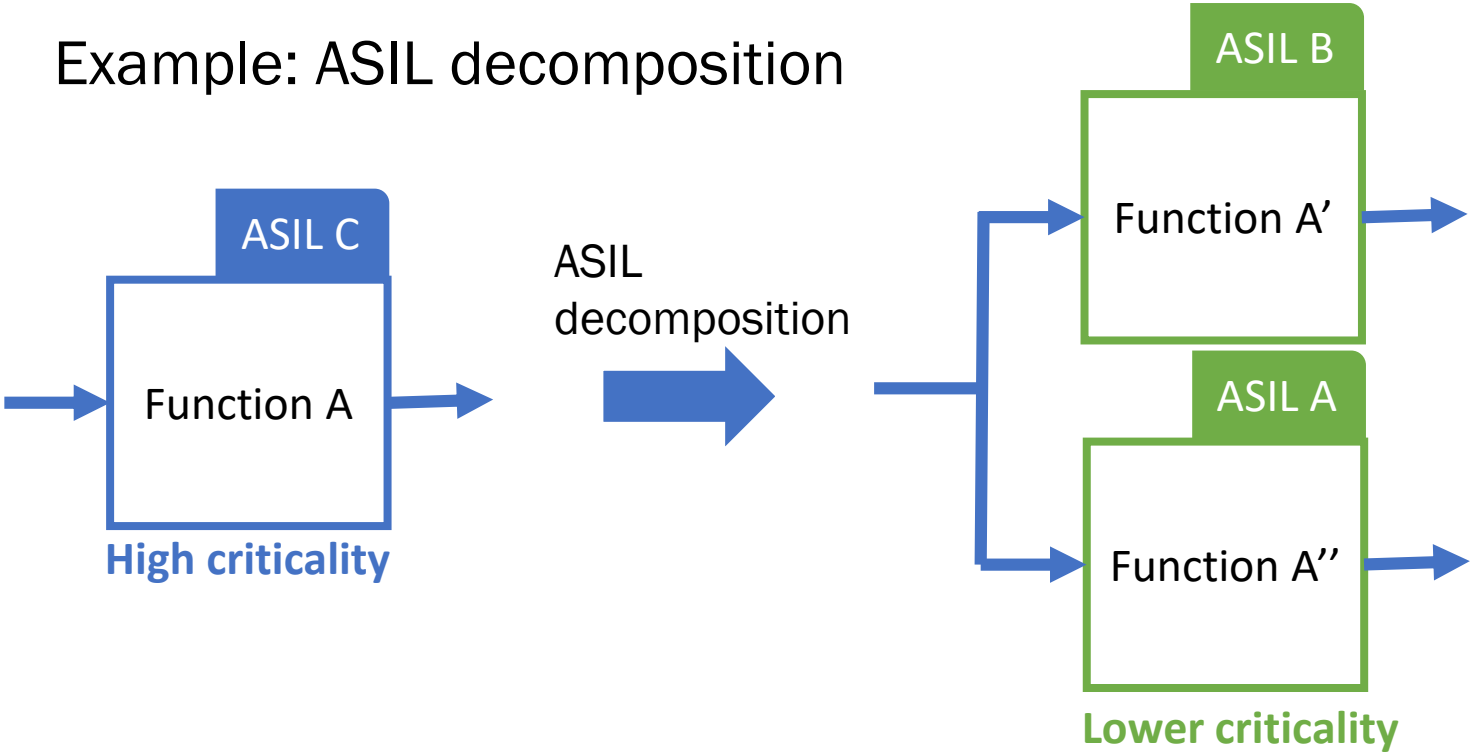
  Example: ASIL decomposition



The original message

- **Criticality** is **not** a measure of **importance**

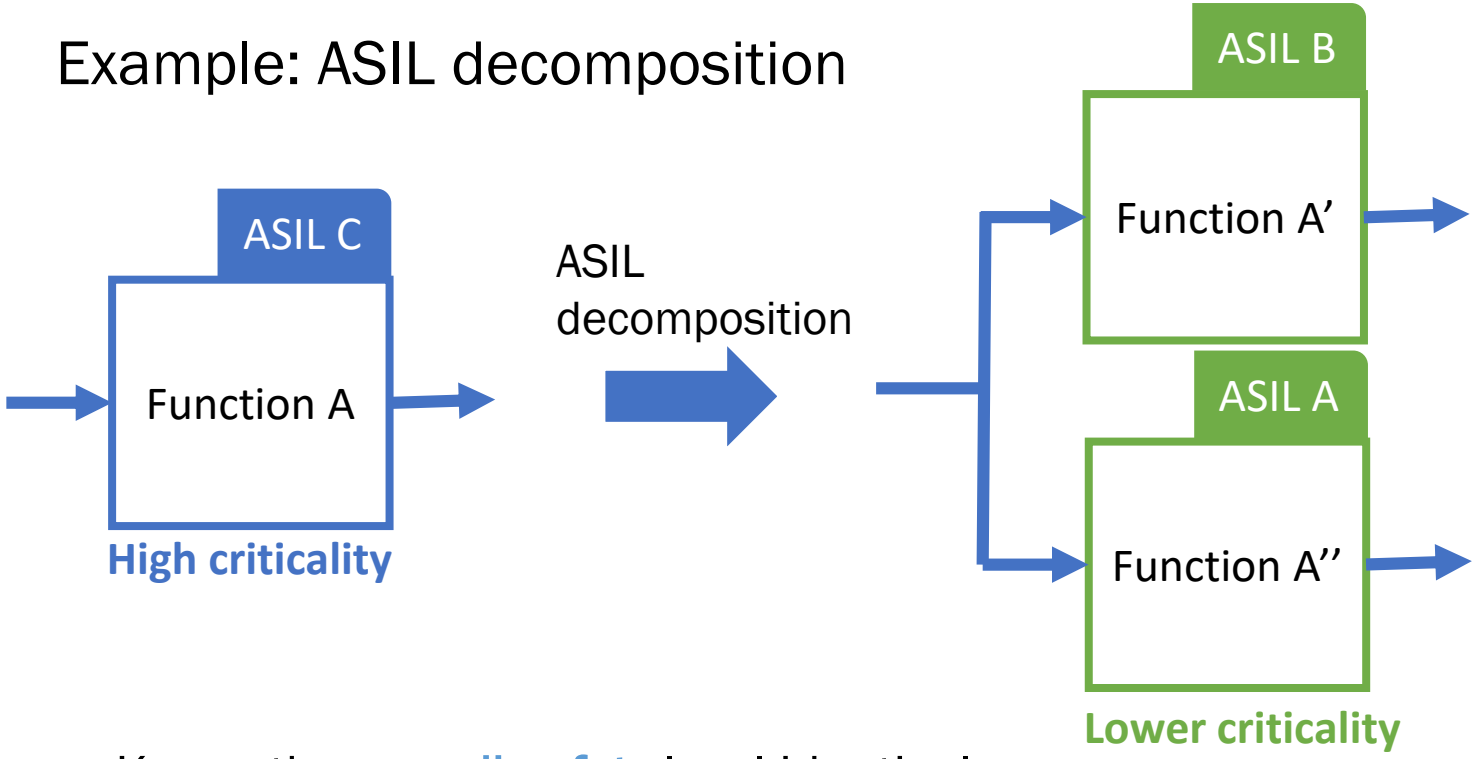
Example: ASIL decomposition



The original message

- **Criticality** is **not** a measure of **importance**

Example: ASIL decomposition

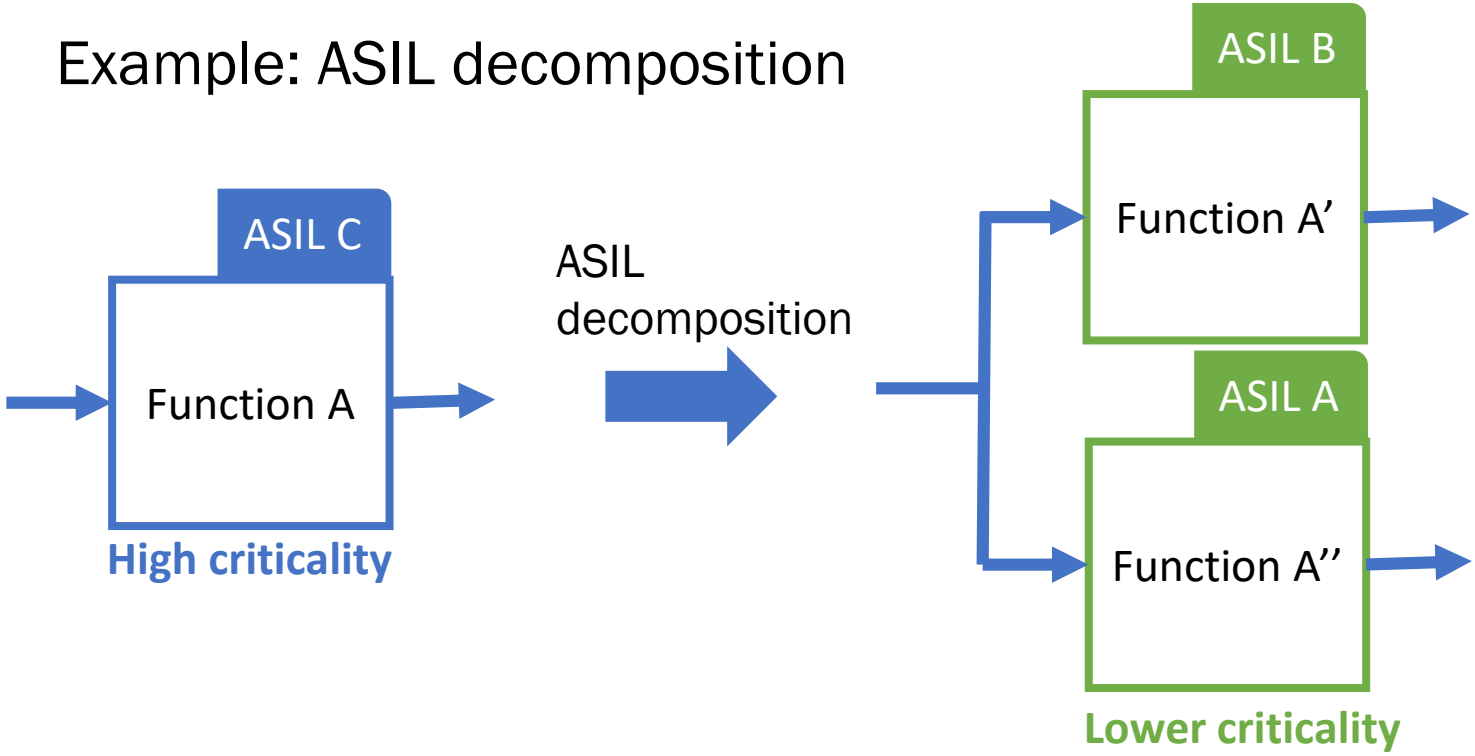


- Keeps the overall safety level identical
- Reduces cost and development effort

The original message

- **Criticality** is **not** a measure of **importance**

Example: ASIL decomposition



If a **safety mechanism** was to stop/penalize all lower criticality tasks whenever **one** of them **fails** ➔ ASIL decomposition would never be acceptable

The original message

- Presented a more industrially-oriented view of mixed criticality
- Raised awareness about the potential misunderstanding

The original message

- Presented a more industrially-oriented view of mixed criticality
- Raised awareness about the potential misunderstanding

- Focused on what the MCS model is not ➔ It was perceived as dimishing the impact of a large body of work
- Did not discuss how to improve the state of things

The goal of this talk

- Analyse the so-called Vestal MCS model
- Understand its key properties
- Discuss its use and applicability

- Objective:
  - Extand/generalize the MCS model
  - Expand its reach to other problems than mixed-criticality systems

Vestal's model

Vestal's model

Tasks	Execution budget		Period	Deadline
	Model 1	Model 2		
Tsk1	C1	C1'	T1	D1
Tsk2	C2	C2'	T2	D2
Tsk3	C3	C3'	T3	D3
Tsk5	C4	0	T4	D4
…				
Tskn	Cn	0	Tn	Dn

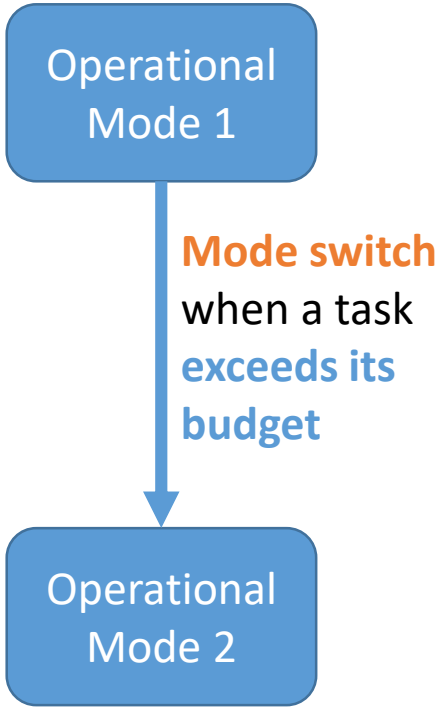
Vestal's model

	Tasks	Execution budget		Period	Deadline
		Model 1	Model 2		
Subset 1	Tsk1	C1	C1'	T1	D1
	Tsk2	C2	C2'	T2	D2
	Tsk3	C3	C3'	T3	D3
Subset 2	Tsk5	C4	0	T4	D4
	…				
	Tskn	Cn	0	Tn	Dn

Two different models for each task to provide different guarantees

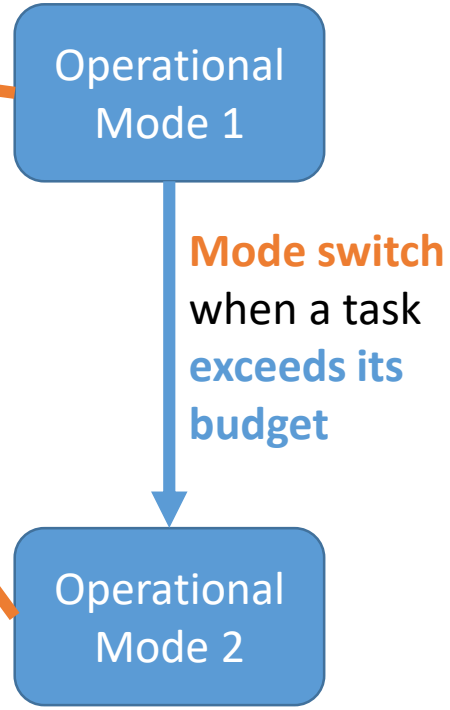
Vestal's model
Multi-mode version

Tasks	Execution budget		Period	Deadline
Tsk1	C1	C1'	T1	D1
Tsk2	C2	C2'	T2	D2
Tsk3	C3	C3'	T3	D3
Tsk5	C4	0	T4	D4
…				
Tskn	Cn	0	Tn	Dn



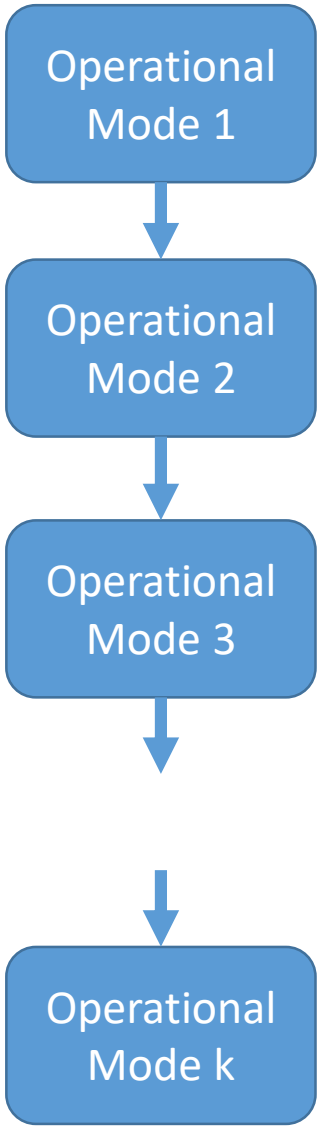
Vestal's model
Multi-mode version

Tasks	Execution budget		Period	Deadline
	System config. 1	System config. 2		
Tsk1	C1	C1'	T1	D1
Tsk2	C2	C2'	T2	D2
Tsk3	C3	C3'	T3	D3
Tsk5	C4	0	T4	D4
...				
Tskn	Cn	0	Tn	Dn



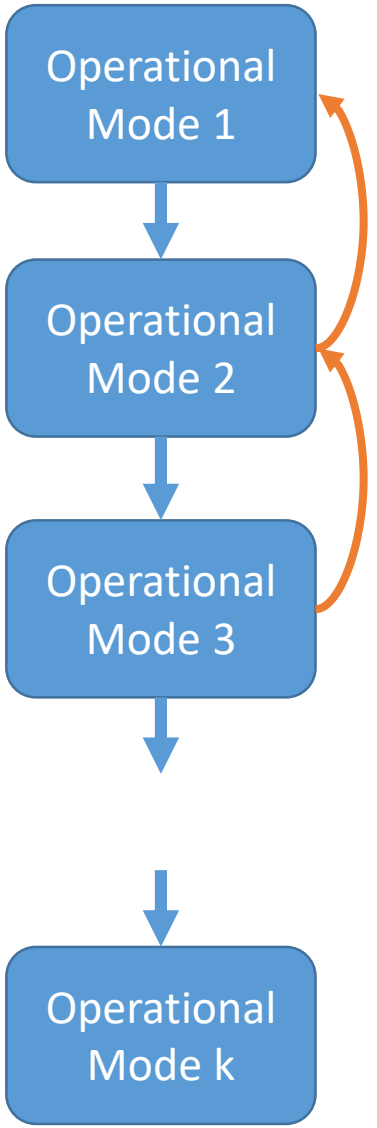
Vestal's model
Multi-mode version - Extensions

Tasks	Execution budget			Period	Deadline
	System config 1	System config 2	System config 3		
Tsk1	C1	C1'	C1''	T1	D1
Tsk2	C2	C2'	C2''	T2	D2
Tsk3	C3	C3'	0	T3	D3
Tsk5	C4	C4'	0	T4	D4
...					
Tskn	Cn	0	0	Tn	Dn



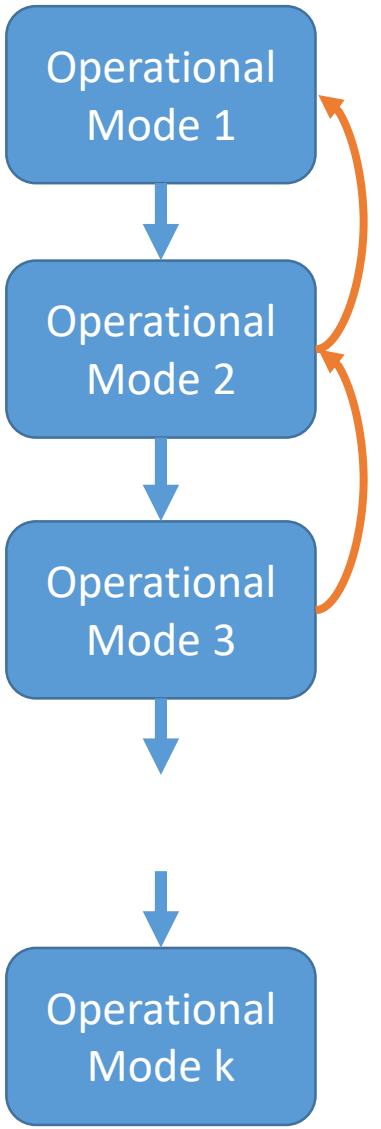
Vestal's model
Multi-mode version - Extensions

Tasks	Execution budget			Period	Deadline
	System config 1	System config 2	System config 3		
Tsk1	C1	C1'	C1''	T1	D1
Tsk2	C2	C2'	C2''	T2	D2
Tsk3	C3	C3'	0	T3	D3
Tsk5	C4	C4'	0	T4	D4
...					
Tskn	Cn	0	0	Tn	Dn



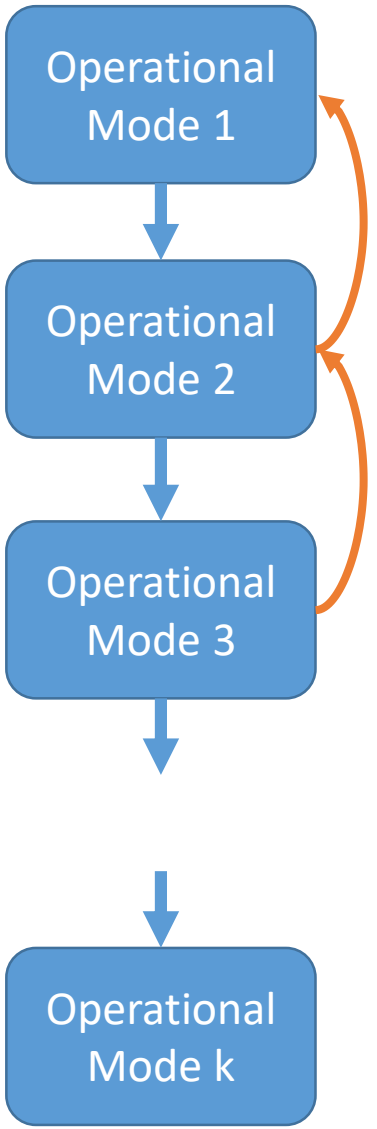
Vestal's model
Multi-mode version - Extensions

Tasks	Execution budget		Period		Deadline
	System config 1	System config 2	System config 1	System config 2	
Tsk1	C1	C1'	T1	T1'	D1
Tsk2	C2	C2'	T2	T2'	D2
Tsk3	C3	C3'	T3	T3'	D3
Tsk5	C4	0	T4	T4'	D4
…					
Tskn	Cn	0	Tn	Tn'	Dn



Vestal's model
Multi-mode version - Extensions

Tasks	Execution budget		Period		Deadline	
	System config 1	System config 2	System config 1	System config 2	Sys. conf 1	Sys. conf 2
Tsk1	C1	C1'	T1	T1'	D1	D1'
Tsk2	C2	C2'	T2	T2'	D2	D2'
Tsk3	C3	C3'	T3	T3'	D3	D3'
Tsk5	C4	0	T4	T4'	D4	D4'
...						
Tskn	Cn	0	Tn	Tn'	Dn	Dn'



Vestal's model Generalisation

Vestal's model Generalisation

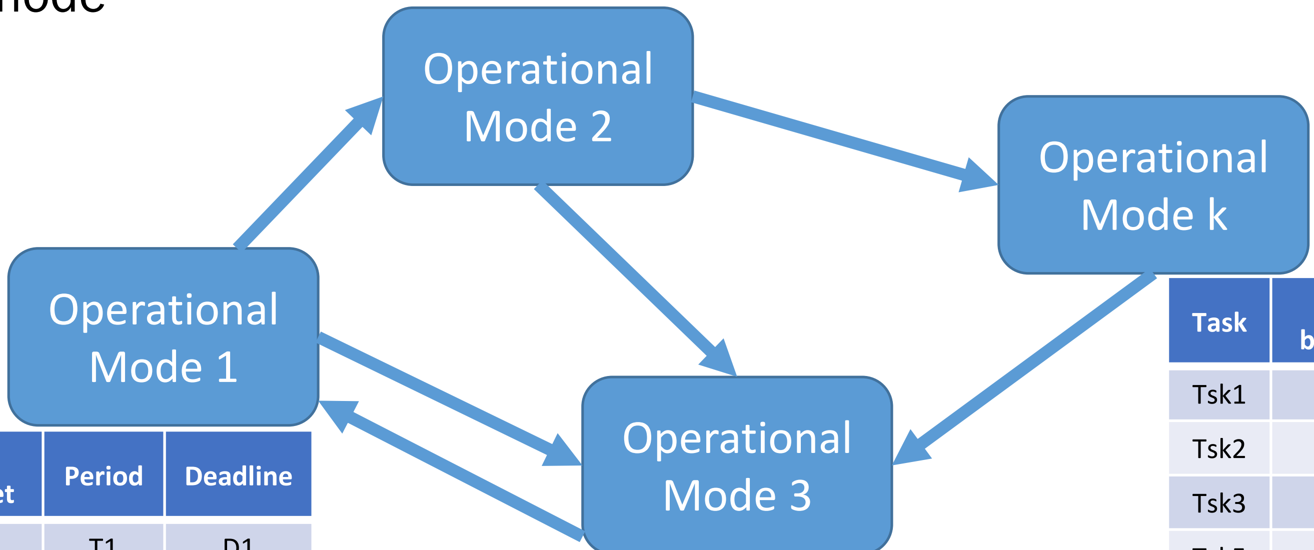
- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, ...) in each mode

Vestal's model Generalisation

- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, ...) in each mode

Vestal's model Generalisation

- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode



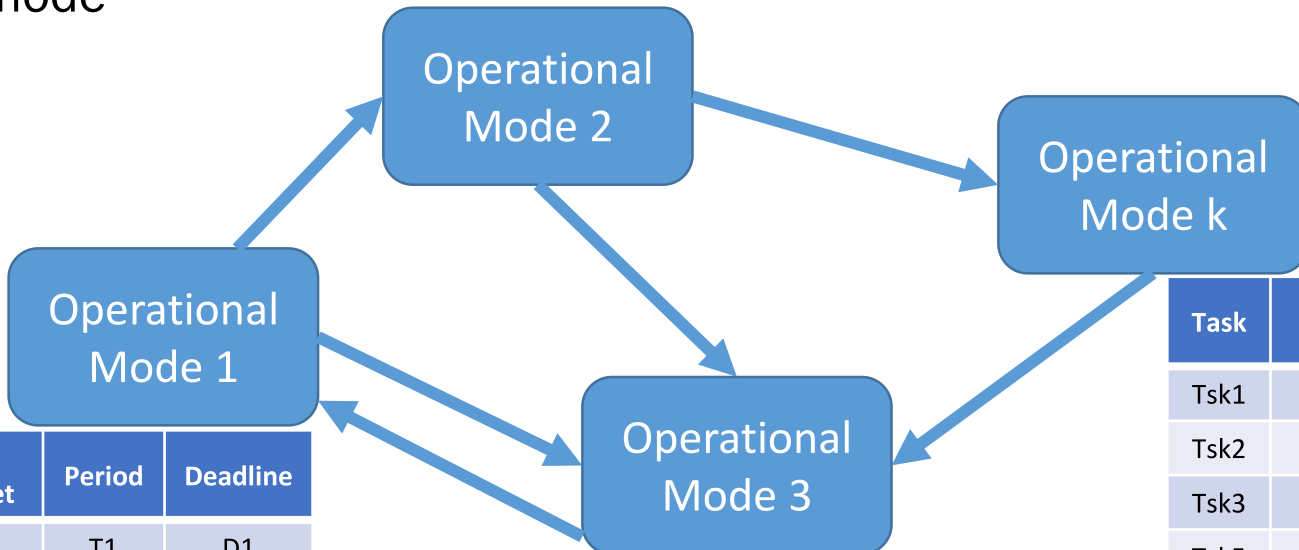
Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Vestal's model Generalisation

- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, ...) in each mode



Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

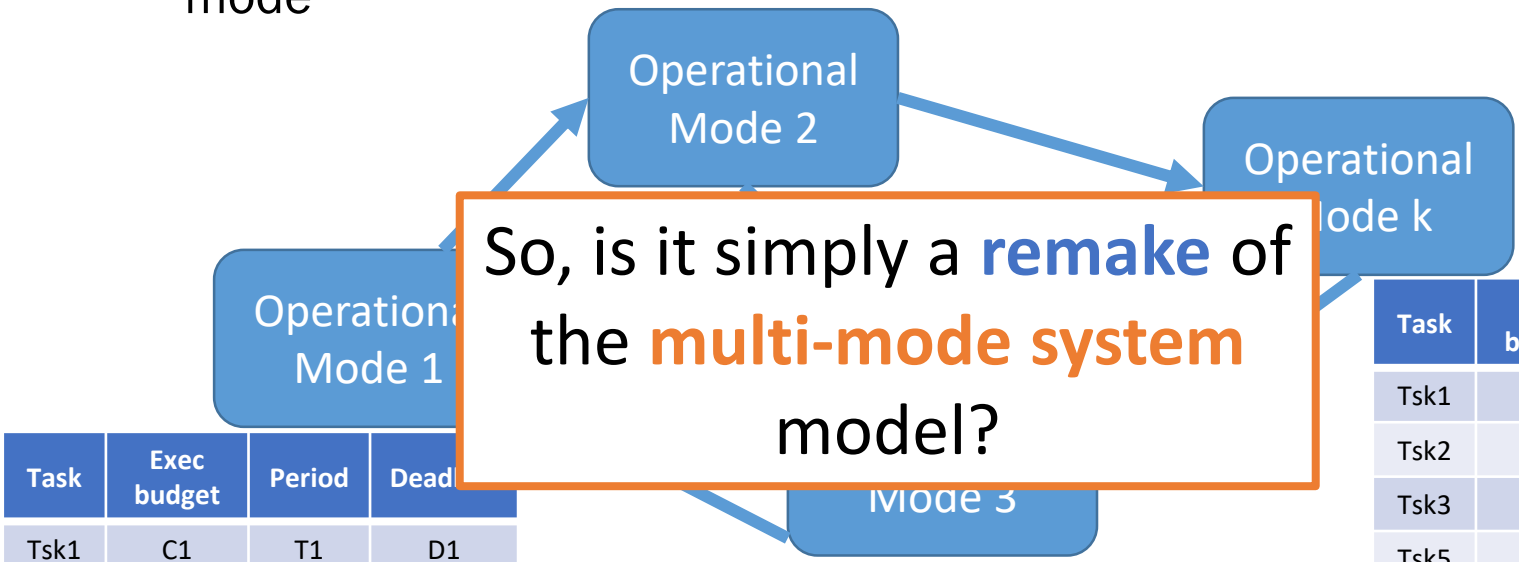
Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Similar to Ekberg and Yi 2014

Vestal's model Generalisation

- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, ...) in each mode



So, is it simply a **remake** of the **multi-mode system** model?

Task	Exec budget	Period	Deadl
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

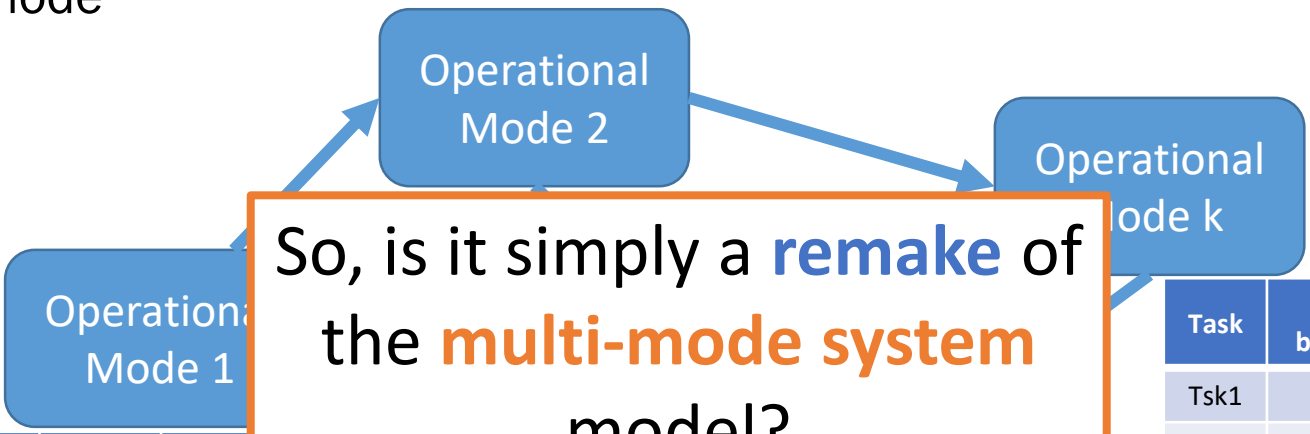
Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Similar to Ekberg and Yi 2014

Vestal's model Generalisation

- Multiple operational modes
- Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, ...) in each mode



Task	Exec budget	Period	Deadl
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

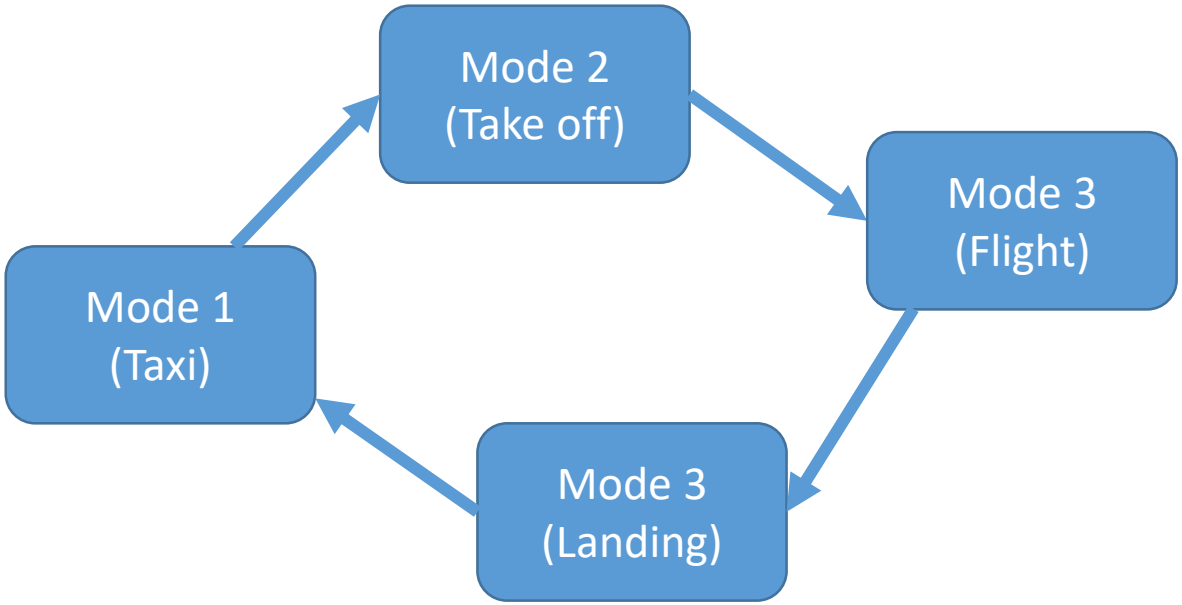
Task	Exec budget	Period	Deadline
Tsk1	C1	T1	D1
Tsk2	C2	T2	D2
Tsk3	C3	T3	D3
Tsk5	C4	T4	D4

Similar to Ekberg and Yi 2014

Difference with multi-mode

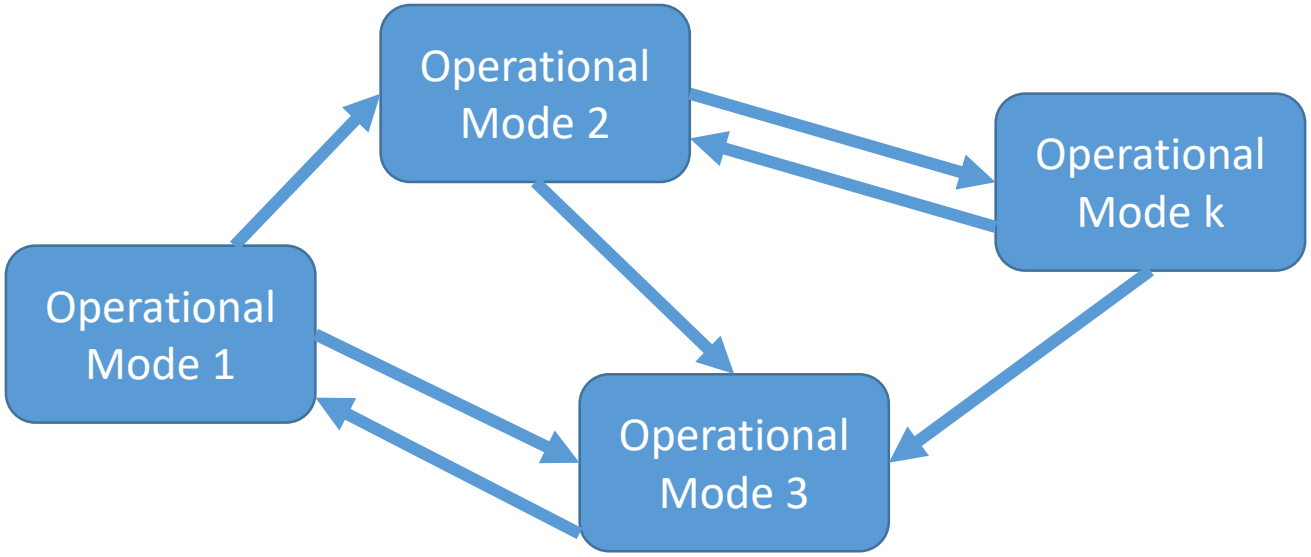
Difference with multi-mode

- Multi-mode system model
  - Mode changes are triggered by external requests
  - The system must adapt with a bouded delay



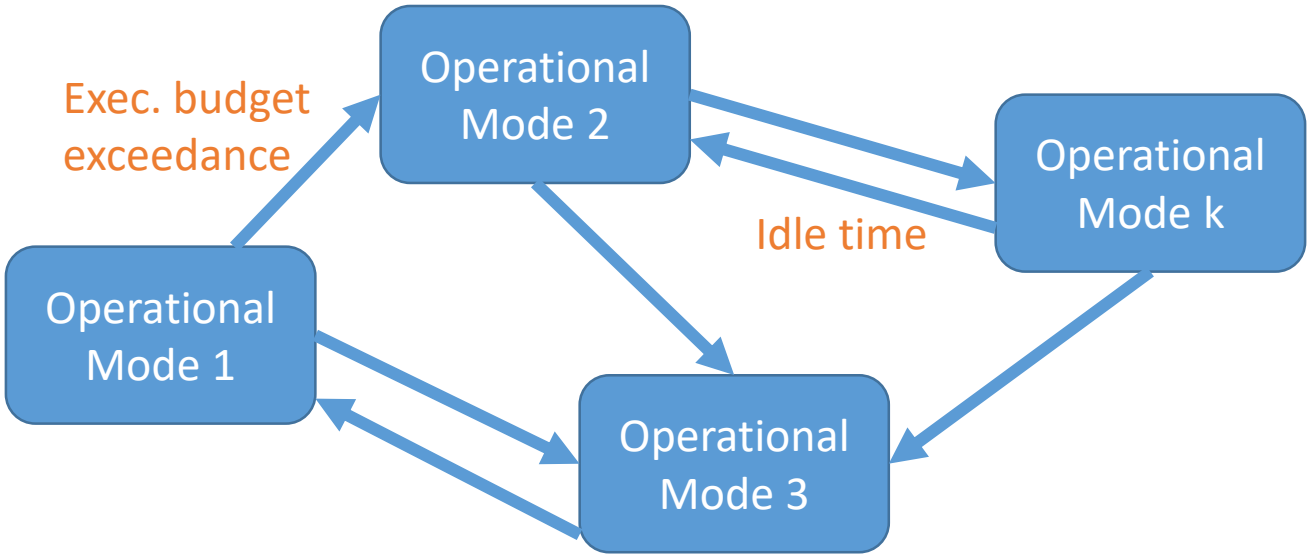
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode



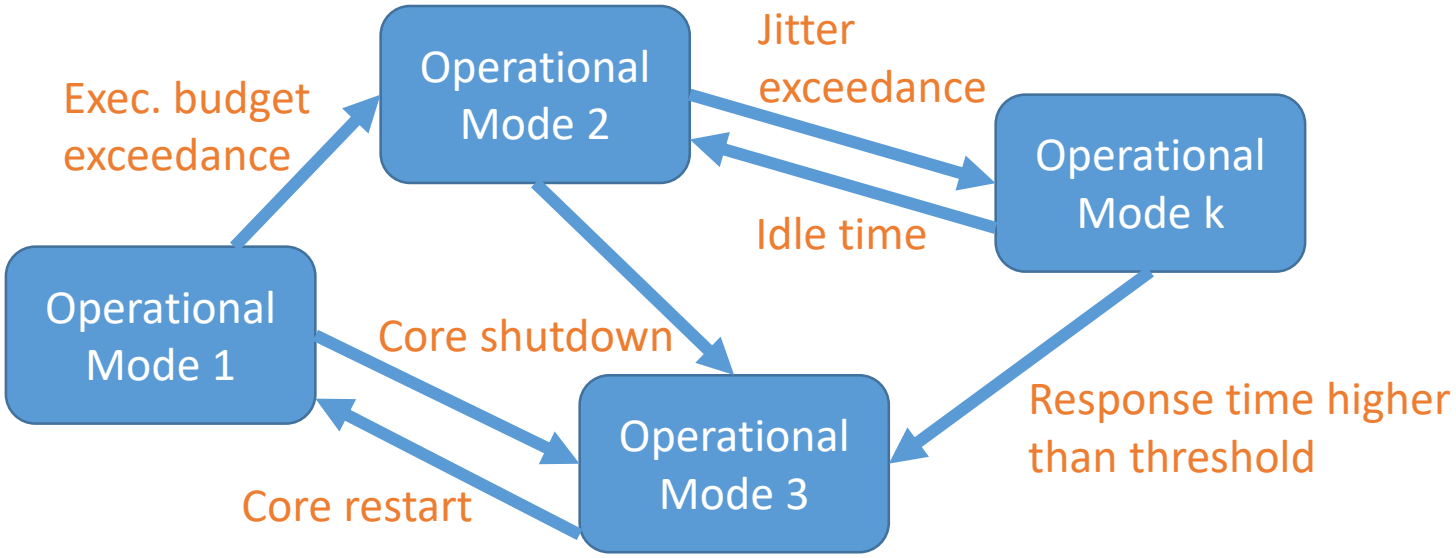
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode



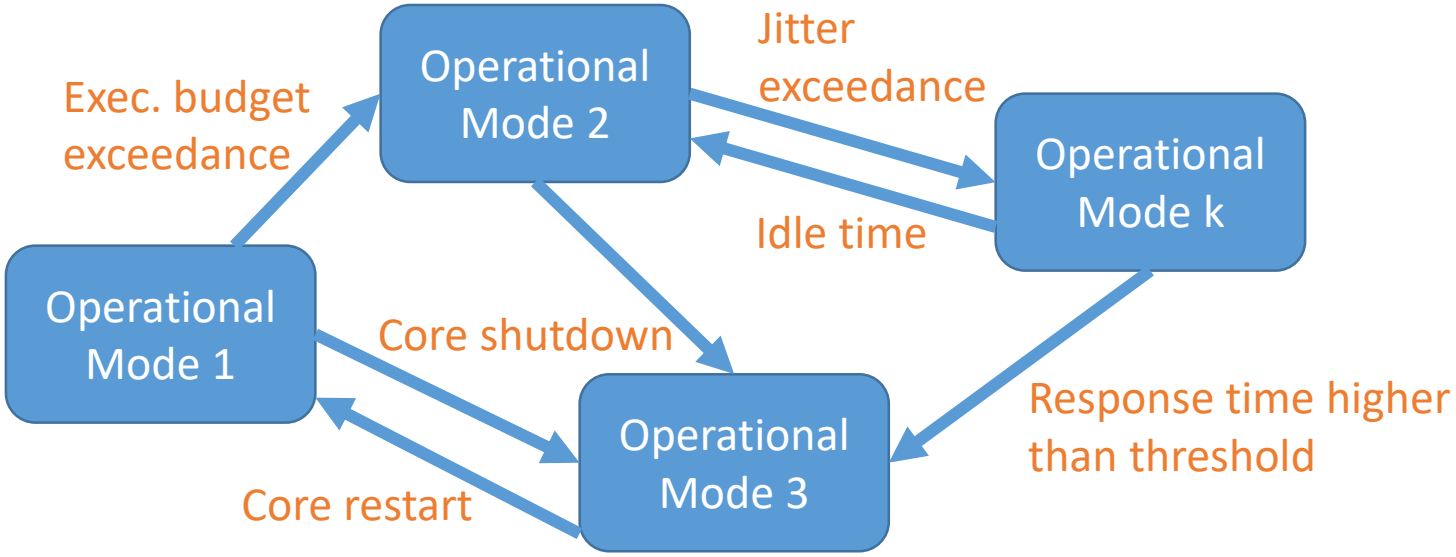
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode



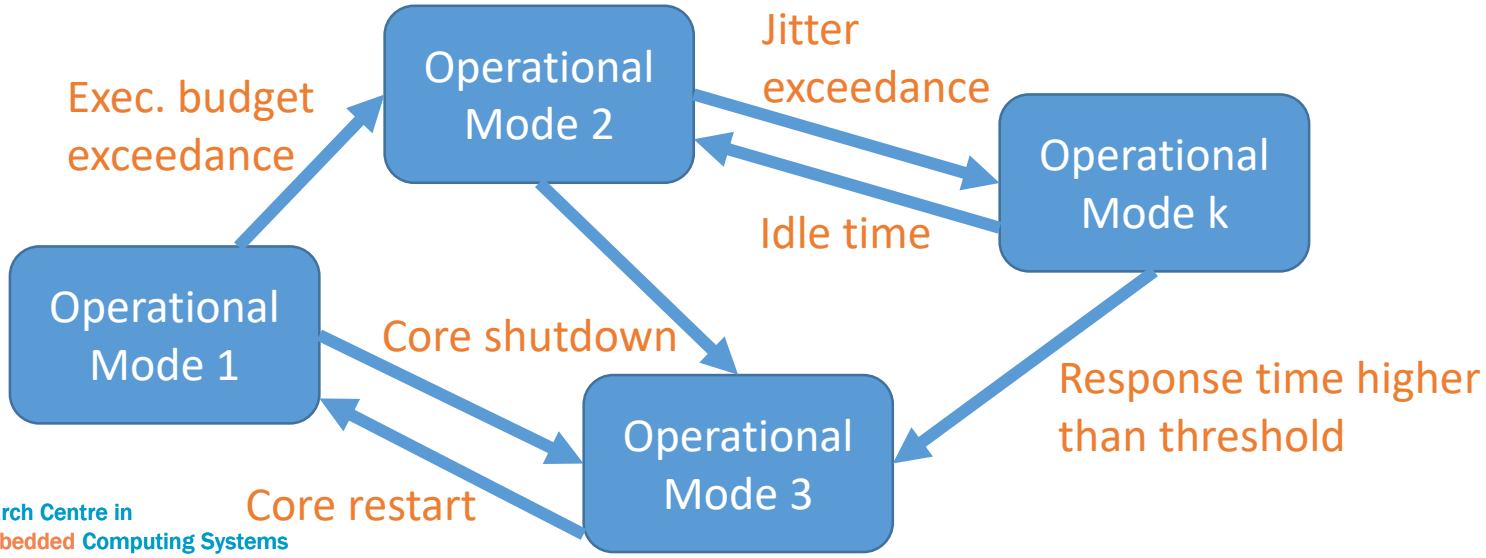
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode
  - The system is self-monitored and self-adapts by self-triggering mode switches



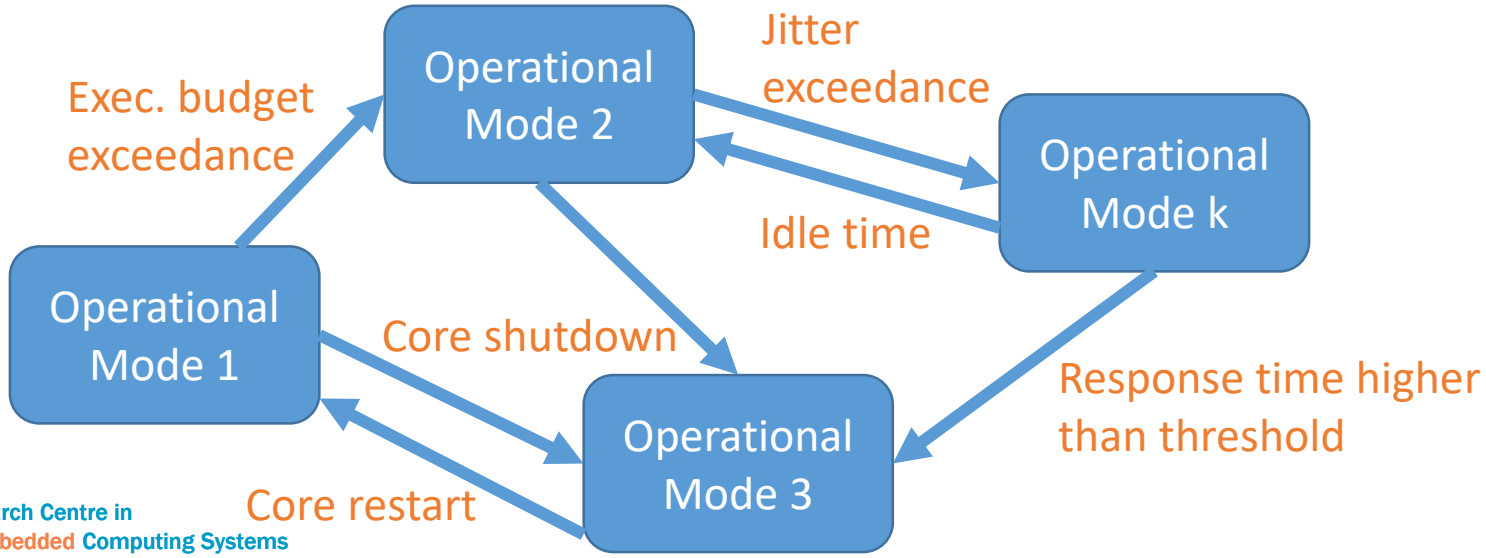
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode
  - The system is self-monitored and self-adapts by self-triggering mode switches
    ➔ we know which system state(s) may trigger a mode switch
    ➔ more efficient analysis/scheduling strategies are possible



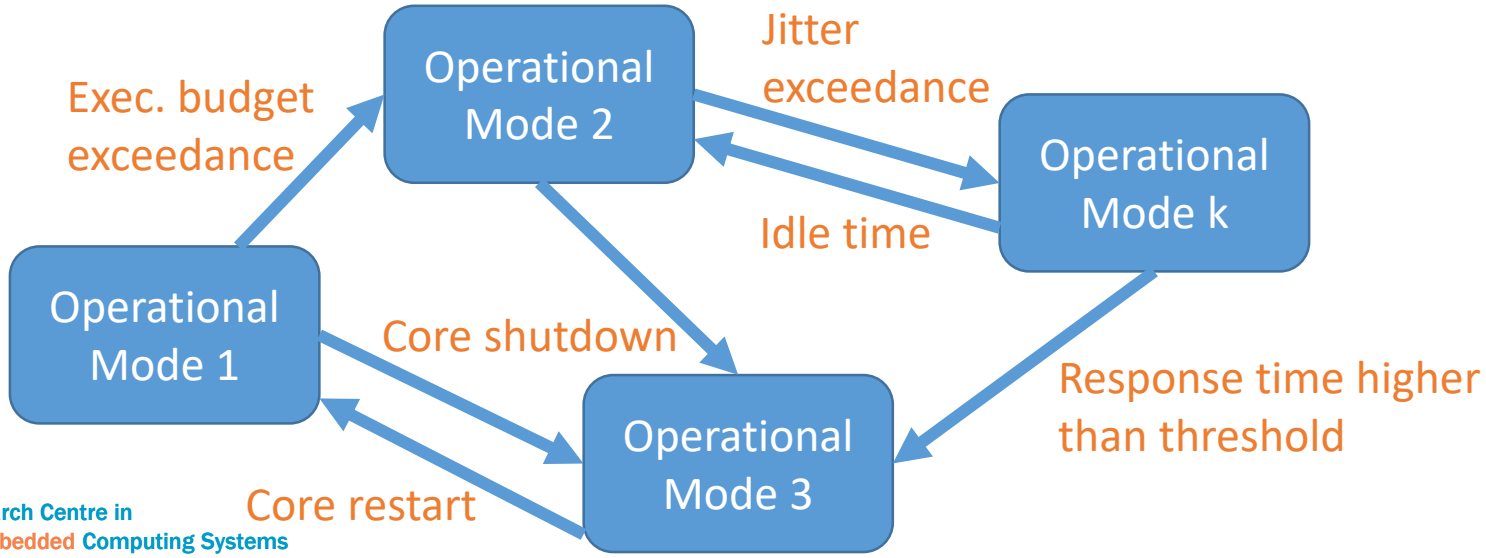
Difference with multi-mode

- Vestal's model generalisation
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode
  - The system is self-monitored and self-adapts by self-triggering mode switches
  - Changes to the system are instantaneous



A new name?

- Self-adaptive system model
  - Multiple operational modes
  - Each task has a different configuration (execution budget, period, deadline, priority, mapping, memory config, executed code, …) in each mode
  - The system is self-monitored and self-adapts by self-triggering mode switches
  - Changes to the system are instantaneous



Applications

Applications

- Safety critical applications

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)
  - May help **reduce the criticality** of some components by
    - showing that counter-measures exist, and
    - proving the limited impact of that component's failure

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)
  - May help **reduce the criticality** of some components by
    - showing that counter-measures exist, and
    - proving the limited impact of that component's failure
- Soft or firm real-time systems

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)
  - May help **reduce the criticality** of some components by
    - showing that counter-measures exist, and
    - proving the limited impact of that component's failure
- Soft or firm real-time systems
  - Model normal operational mode and reactions to system overloads (where bounded deadline misses become acceptable)

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)
  - May help **reduce the criticality** of some components by
    - showing that counter-measures exist, and
    - proving the limited impact of that component's failure
- Soft or firm real-time systems
  - Model normal operational mode and reactions to system overloads (where bounded deadline misses become acceptable)
- Self-optimising systems

Applications

- Safety critical applications
  - Model reactions to faults/failures (HW and/or SW)
  - May help **reduce the criticality** of some components by
    - showing that counter-measures exist, and
    - proving the limited impact of that component's failure
- Soft or firm real-time systems
  - Model normal operational mode and reactions to system overloads (where bounded deadline misses become acceptable)
- Self-optimising systems
  - System optimises its behaviour based on observable parameters (e.g., response time, execution time, inter-arrival time or jitter)

Conclusion

- Yes, Vestal's model may be useful for certification of safety critical systems but …
- … the viewpoint should change
  - The notion of criticality should probably not be the key aspect
  - Emphasis should be made on operational modes, system configurations in those modes and observable properties that trigger mode changes
- The applicability of Vestal's model generalization is not restricted to safety critical systems

Future work and open problems

- Define a generic terminology for the generalized model discussed here
  - No ambiguity
  - No double meanings
- Migrate and extend the existing theory to actual existing problems out there
- Mix the self-adaptive system model with the multi-mode system model
  - i.e., react to both internal observables and external requests

Questions?