Service Adaptions for Mixed-Criticality Systems

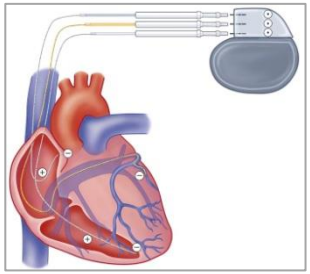
Pengcheng Huang, Georgia Giannopoulou,
Nikolay Stoimenov, Lothar Thiele

January 21, 2014
ASP-DAC, Singapore

ETH Zürich
Computer Engineering and Networks Laboratory

One Fact

- Most complex embedded systems are *mixed-critical*
  - Functionalities of different *safety* criticalities co-exist
  - A reflection of the real world

- Key challenges
  - Uncertainties: WCET, temperature, HW/SW errors…
  - Different assurances for different criticalities

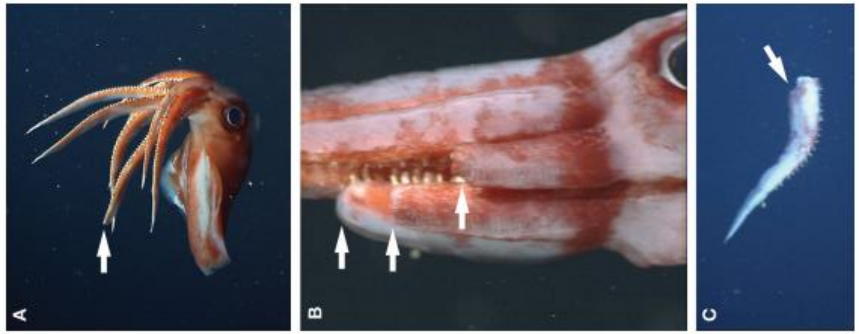
Two Views

- Obstacle
  - Worst-case model for the entire system
  - Resource over-provisioning
- Opportunity
  - Self-organized system that *adapts* to uncertainties, and deliver bounded guarantees to all criticalities
  - Like all life on earth, we evolve to survive from adverse events

Our Motivation

How should the system re-organize under the attack of uncertainties?

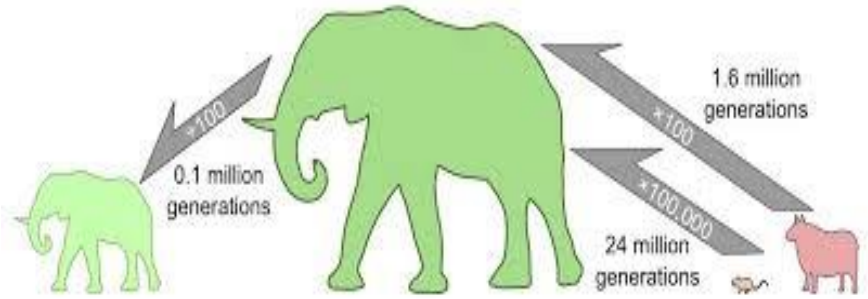
- Some answers by nature



Autotomy: detach less-critical part of a system, *as majority of mixed-criticality systems are designed*

Size evolution: adapt the size of a system (or part of it),

more flexibility and ***why not***

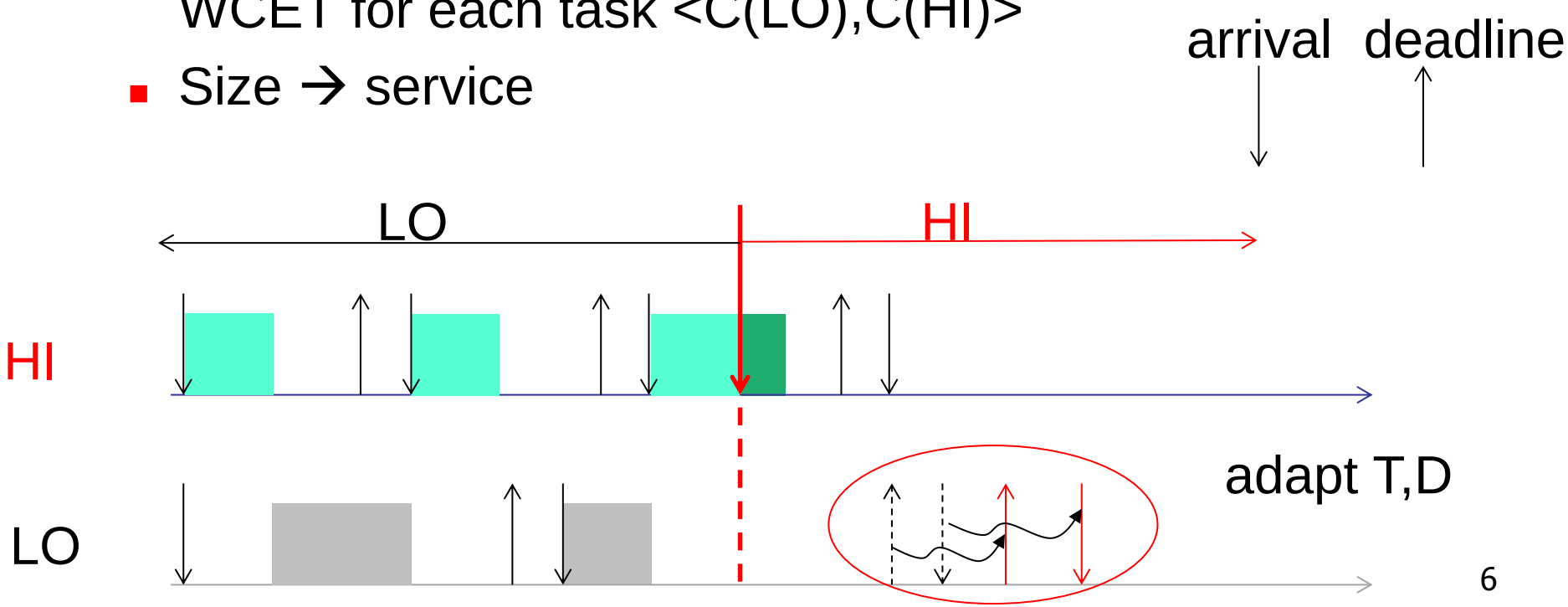


One Problem Formulation

- Our setting up
  - Uniprocessor, Earliest Deadline First (EDF) scheduling
  - Dual-criticality sporadic tasks <T,D,χ>, $\chi \in$ {HI,LO}
  - Uncertainty in WCET: a normal (LO) and a safe (HI) WCET for each task <C(LO),C(HI)>
  - Size → service

One Problem Formulation

- Our setting up
  - Uniprocessor, Earliest Deadline First (EDF) scheduling
  - Dual-criticality sporadic tasks <T,D,χ>, $\chi \in$ {HI,LO}
  - Uncertainty in WCET: a normal (LO) and a safe (HI) WCET for each task <C(LO),C(HI)>
  - Size → service



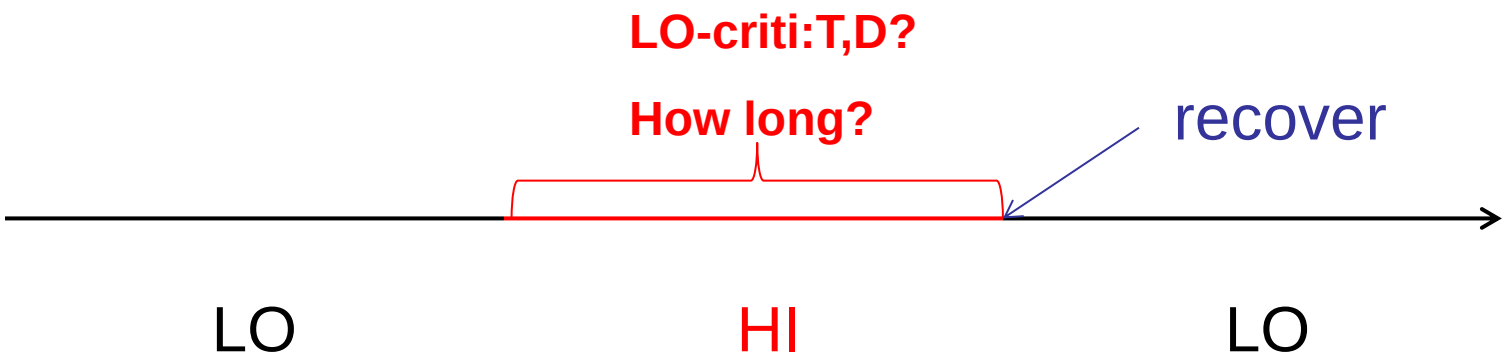
One Problem Formulation

- Our setting up
  - Uniprocessor, Earliest Deadline First (EDF) scheduling
  - Dual-criticality sporadic tasks <T,D,χ>, $\chi \in$ {HI,LO}
  - Uncertainty in WCET: a normal (LO) and a safe (HI) WCET for each task <C(LO),C(HI)>
  - Size → service

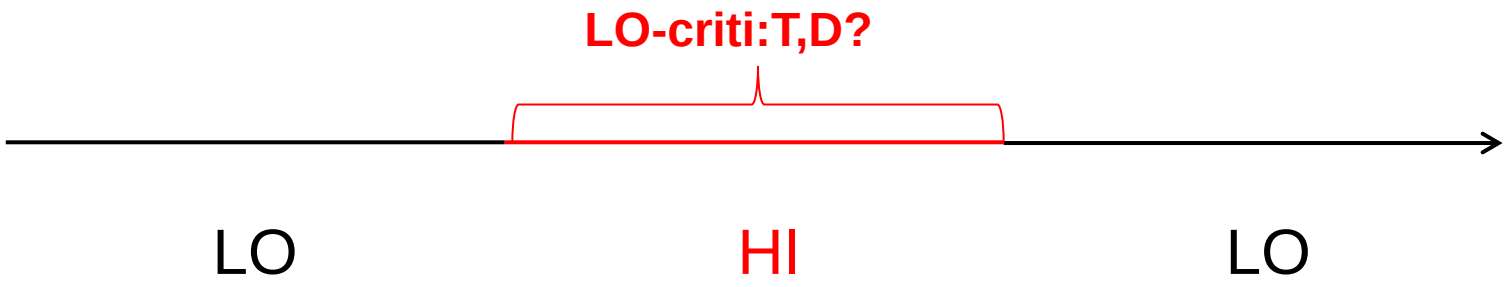
- Desired behavior
  - For HI-crit: they are always guaranteed
  - For LO-crit: receive different services in different modes

Two Aspects of the Problem

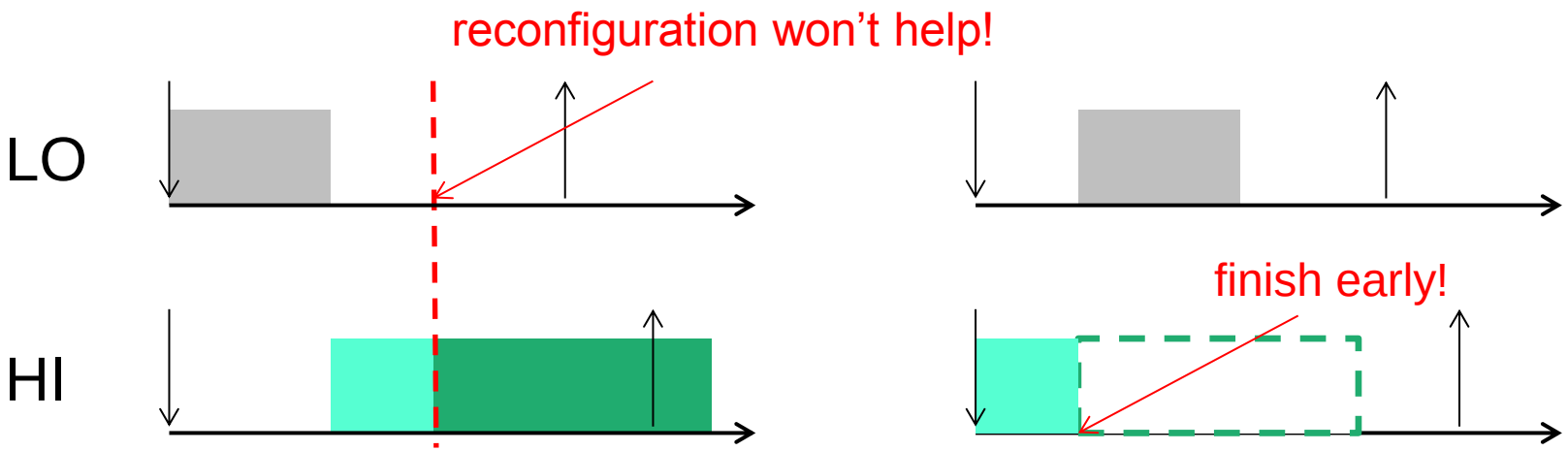
- How should the service of LO criticality tasks be reconfigured?
  - With service adapted for LO criticality tasks, both HI and LO criticality tasks should meet their deadlines
- When can the system be recovered?
  - Safe recovery: no deadline will be missed after that



Service Reconfiguration



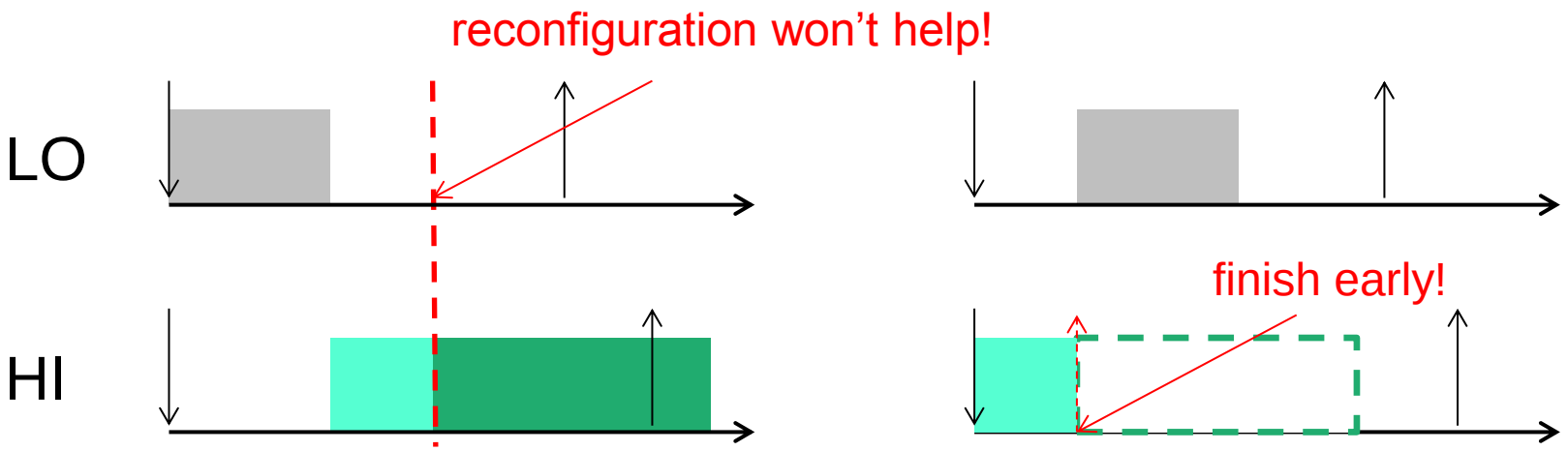
- Only reconfiguration when entering HI may not work
- "Preparation" for reconfiguration



Service Reconfiguration

How to prepare?

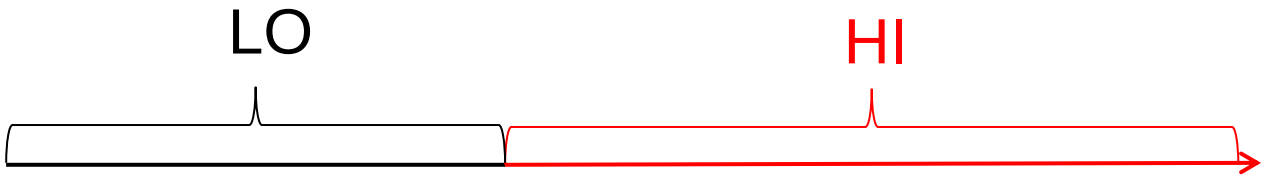
- Preparation Baruah et al. ESA 2011
  - Shorten the deadlines of HI-crit tasks in the LO mode



Service Reconfiguration

Preparation → Reconfiguration?

- Relation
  - Bounded by the schedulability of the system



Schedulable with shortened deadlines for HI-crit tasks

Schedulable with original deadlines for HI-crit tasks, reduced services for LO-crit tasks

Service Reconfiguration

Preparation → Reconfiguration?

- Relation
  - Bounded by the schedulability of the system

$$\mathrm{dbf}_{\mathrm{LO}}(\tau_i,\Delta)=\max\left\{\left\lfloor\frac{\Delta-D_i(\mathrm{LO})}{T_i(\mathrm{LO})}\right\rfloor+1,0\right\}\cdot C_i(\mathrm{LO}).$$

$$\sum \mathrm{dbf}_{\mathrm{LO}}(\tau_i,\Delta)\le\Delta$$

$$\mathrm{RM}(\tau_i,\lambda)=C_i(\mathrm{HI})-C_i(\mathrm{LO})+\min\{D_i(\mathrm{LO})-\lambda,C_i(\mathrm{LO})\},$$

$$\mathrm{dbf}^1_{\mathrm{HI}}(\tau_i,\Delta)=\max\left\{\left\lfloor\frac{\Delta-D_i(\mathrm{HI})}{T_i(\mathrm{HI})}\right\rfloor+1,0\right\}\cdot C_i(\mathrm{HI}),$$

$$\mathrm{dbf}_{\mathrm{RM}}(\tau_i,\lambda,\Delta)=\begin{cases}\mathrm{RM}(\tau_i,\lambda) & \text{if } \Delta\ge D_i(\mathrm{HI})-\lambda,\\ 0 & \text{if } \Delta< D_i(\mathrm{HI})-\lambda.\end{cases}$$

$$\mathrm{dbf}^2_{\mathrm{HI}}(\tau_i,\lambda,\Delta)=\mathrm{dbf}_{\mathrm{RM}}(\tau_i,\lambda,\Delta)+\max\left\{\left\lfloor\frac{\Delta-D_i(\mathrm{HI})-(T_i(\mathrm{HI})-\lambda)}{T_i(\mathrm{HI})}\right\rfloor+1,0\right\}\cdot C_i(\mathrm{HI}).$$

$$\mathrm{dbf}_{\mathrm{HI}}(\tau_i,\Delta)=\sup\{\mathrm{dbf}^1_{\mathrm{HI}}(\tau_i,\Delta),\sup_{0\le\lambda\le D_i(\mathrm{LO})}\{\mathrm{dbf}^2_{\mathrm{HI}}(\tau_i,\lambda,\Delta)\}\}.$$

$$\sum \mathrm{dbf}_{\mathrm{HI}}(\tau_i,\Delta)\le\Delta$$

Demand bound analysis

Service Reconfiguration

Preparation → Reconfiguration?

- Simplification
  - Implicit deadlines
  - All HI criticality tasks, LO Mode: $deadlines \times X \ (0 < X \leq 1)$
  - All LO criticality tasks, HI Mode: $deadlines \times Y$

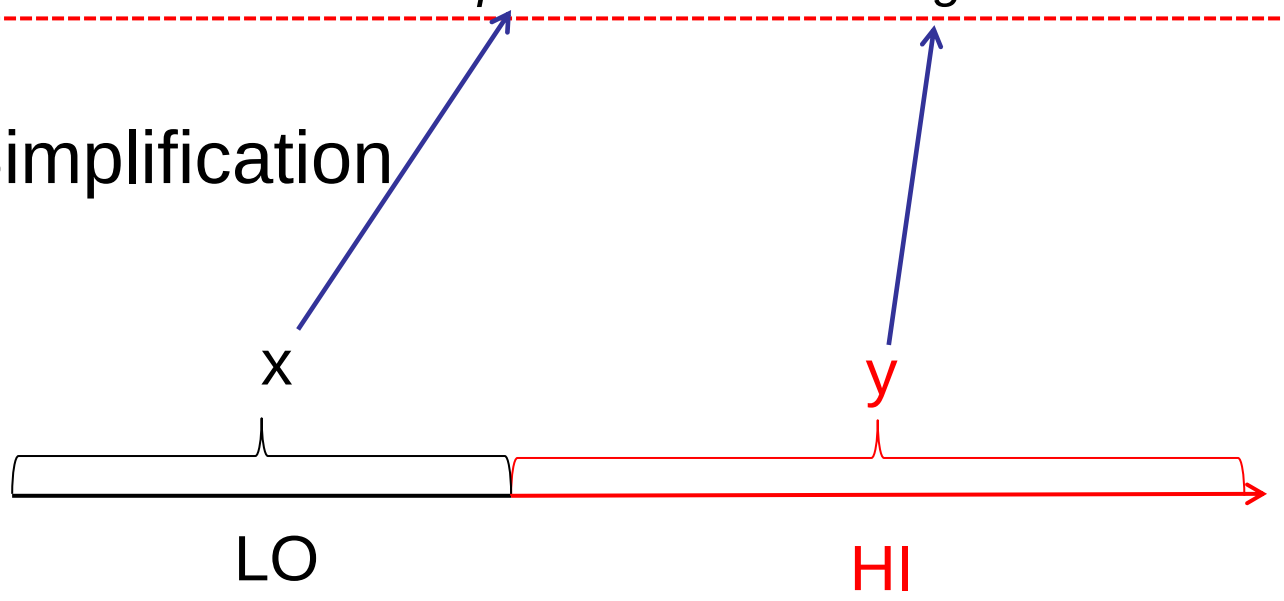
    $periods \times Y \ (Y \geq 1)$

  - Demand bounds can be subsequently *approximated*

Service Reconfiguration

Preparation → Reconfiguration?

- Simplification



$$h(x) = \sum_{\tau_{HI}} \frac{U_i(\mathrm{HI})}{U_i(\mathrm{LO}) + (1-x)},$$

$$l(y) = \sum_{\tau_{LO}} \frac{U_i(\mathrm{LO})}{U_i(\mathrm{LO}) + (y-1)},$$

$$U_i(\chi) = C_i(\chi)/T_i$$

$$y \leftarrow \inf\{y \geq 1 : h(x) + l(y) \leq 1\}$$

Service Reconfiguration

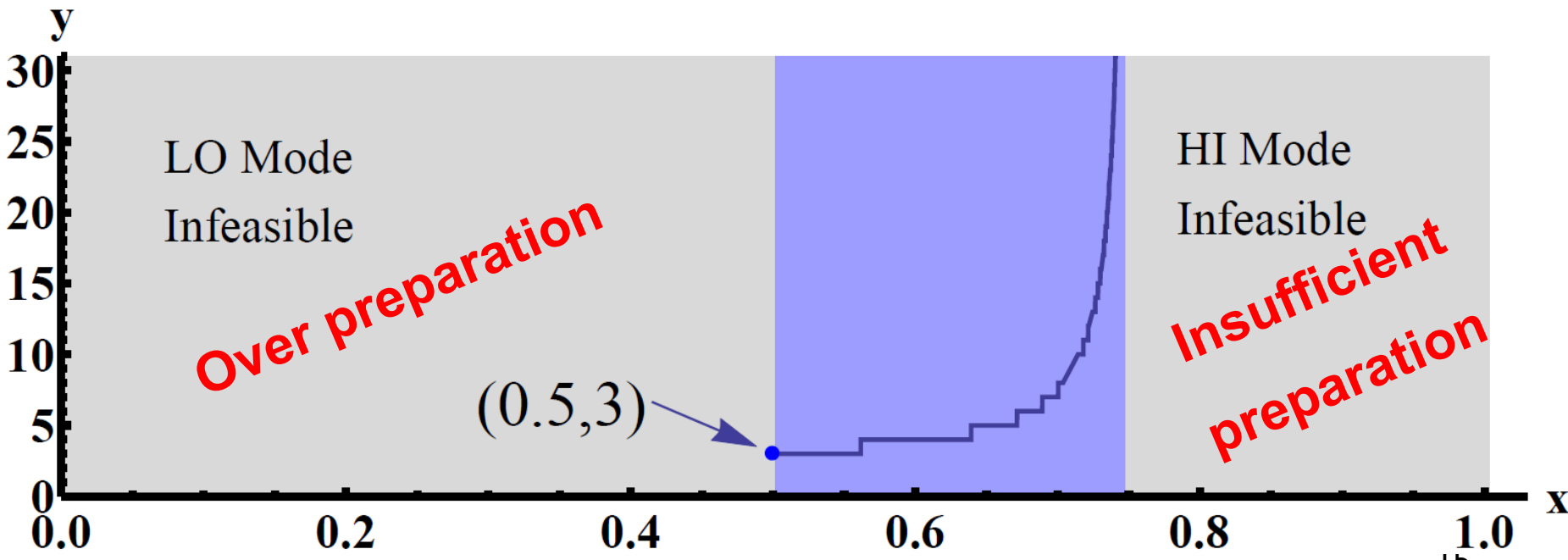
Preparation → Reconfiguration?

EXAMPLE TASK SET

τ	τ_1	τ_2	τ_3	τ_4	τ_5
χ	HI	LO	LO	LO	LO
T/D	60	8	30	90	15
C(HI)	18	4	4	6	3
C(LO)	3	4	4	6	3

Better preparation

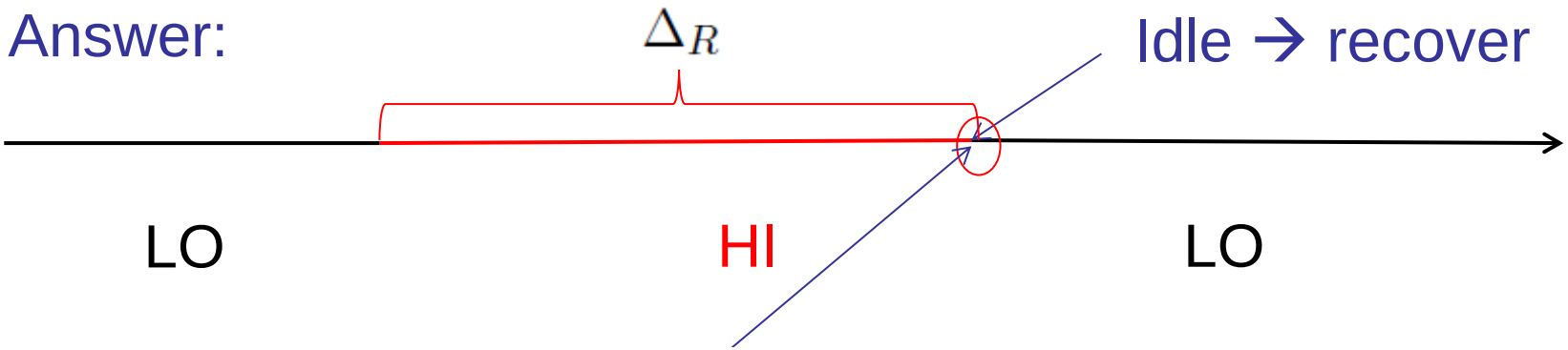
→ Better degraded service



Service Recovery

When recover?

Answer:



All arrived jobs finish!

$$\mathrm{adf}^1_{\mathrm{HI}}(\tau_i,\lambda,\Delta) = \mathrm{RM}(\tau_i,\lambda) + \max\{\left\lceil \frac{\Delta-(T_i(\mathrm{HI})-\lambda)}{T_i(\mathrm{HI})} \right\rceil, 0\} \cdot C_i(\mathrm{HI}),$$

$$\mathrm{adf}^2_{\mathrm{HI}}(\tau_i,\Delta) = \left\lceil \frac{\Delta}{T_i(\mathrm{HI})} \right\rceil \cdot C_i(\mathrm{HI}),$$

$$\mathrm{adf}_{\mathrm{HI}}(\tau_i,\Delta) = \sup\{\mathrm{adf}^2_{\mathrm{HI}}(\tau_i,\Delta), \sup_{0\le\lambda\le D_i(\mathrm{LO})}\{\mathrm{adf}^1_{\mathrm{HI}}(\tau_i,\lambda,\Delta)\}\}.$$

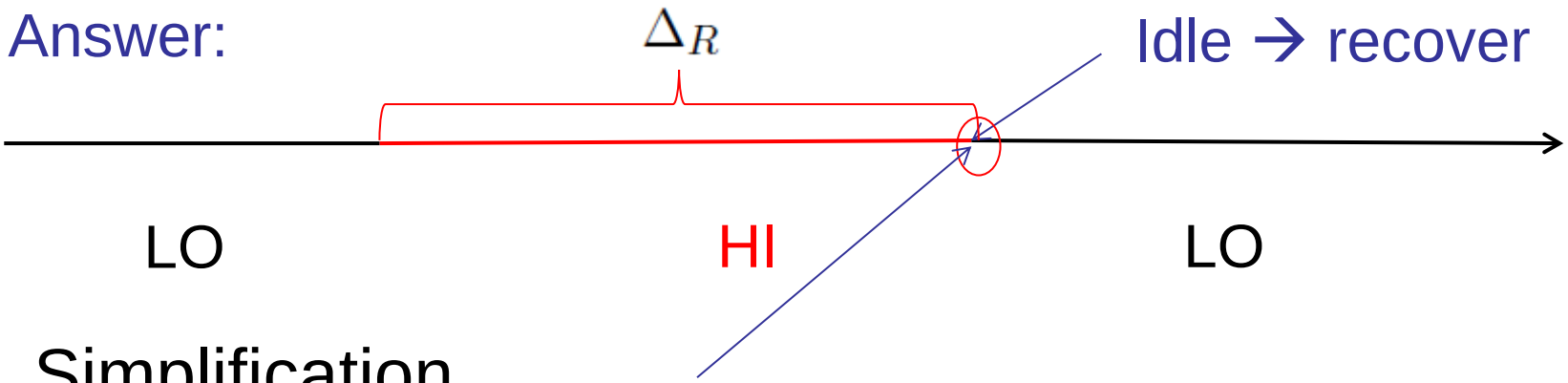
$$\sum_{\tau}\mathrm{adf}_{\mathrm{HI}}(\tau_i,\Delta_R) \le \Delta_R.$$

Service Recovery

Relation: preparation and reconfiguration → recovery?

x and y → Δ_R*?*

Answer:



- Simplification

All arrived jobs finish! ⇨

$$\Delta_R >= \frac{\sum_{\tau} C_i(\chi_i)}{1-h(x)-l(y)}$$

Service Recovery

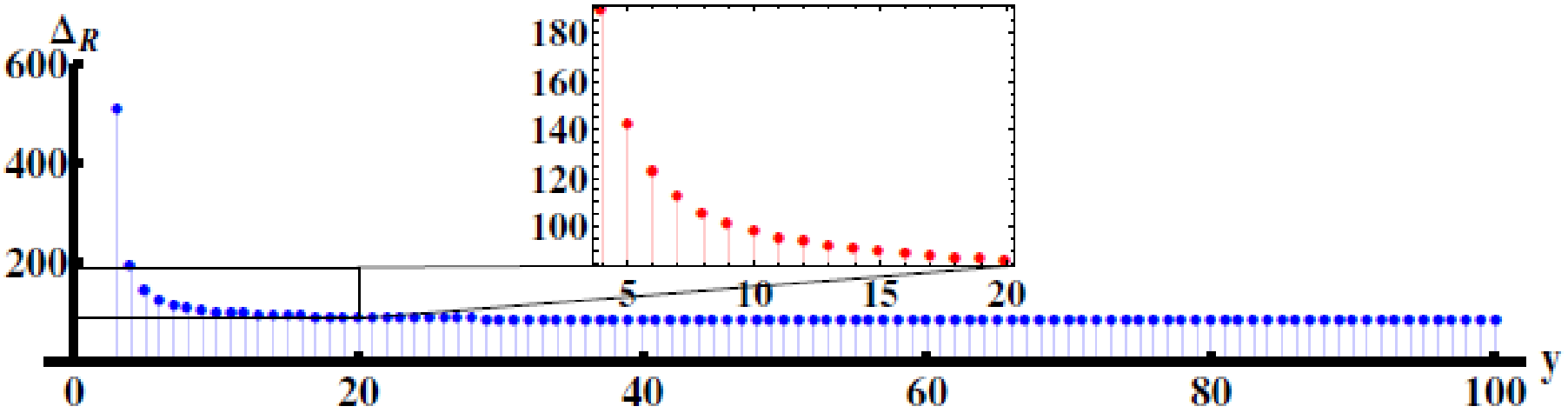
When recover?

EXAMPLE TASK SET

τ	τ_1	τ_2	τ_3	τ_4	τ_5
χ	HI	LO	LO	LO	LO
T/D	60	8	30	90	15
C(HI)	18	4	4	6	3
C(LO)	3	4	4	6	3

Less to guarantee

→ Faster to recover



x set to the minimal value that guarantees LO mode schedulability

Case-Study

- A flight management system (FMS)
  - Subset – 11 tasks
  - DO-178B criticality B (HI) and C (LO)
  - Only know LO criticality WCETs' ranges
  - Scaled by safety factor f_{safe} to get HI criticality WCETs

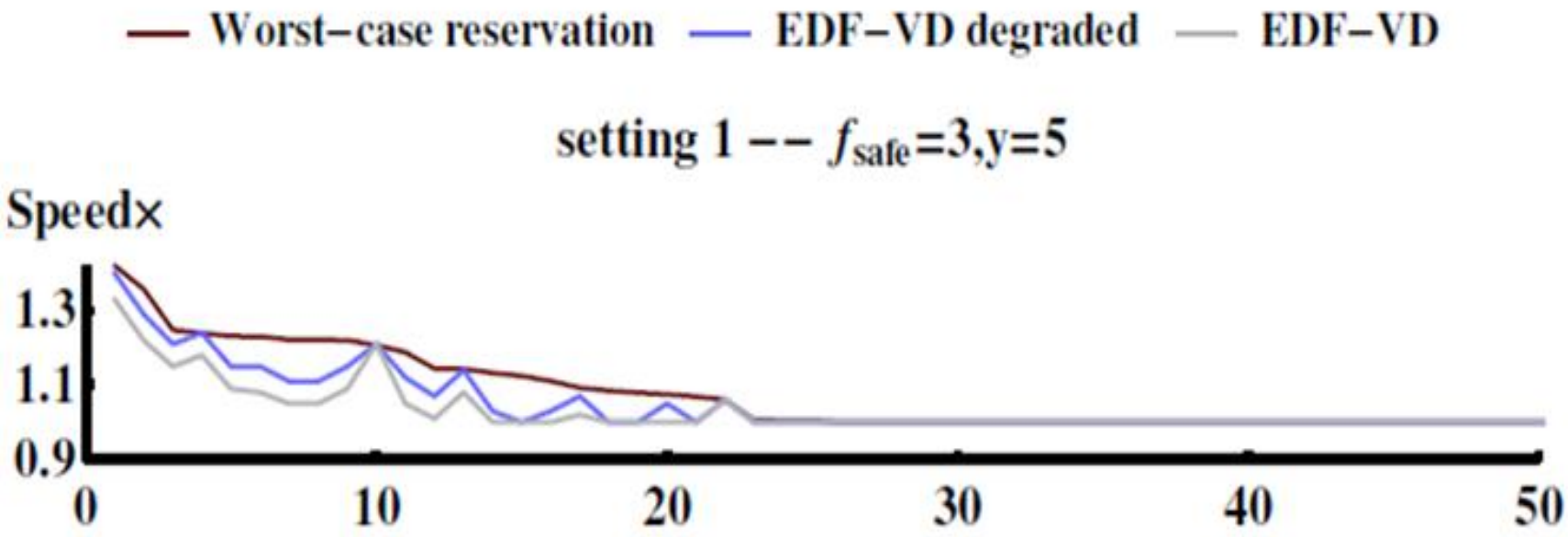
TASK PARAMETERS FOR THE FMS APPLICATION

τ	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
T/D	5000	200	1000	1600	100	1000
C(LO)	{0,20}	{0,20}	{0,20}	{0,20}	{0,20}	{0,20}
χ	B	B	B	B	B	B
τ	τ_7	τ_8	τ_9	τ_{10}	τ_{11}	
T/D	1000	1000	1000	1000	1000	
C(LO)	{0,20}	{0,200}	{0,200}	{0,200}	{0,200}	
χ	B	C	C	C	C	

Case-Study

-50 random FMS instances

-3 algorithms



Resource Efficiency **Flexibility**

Case-Study

1 random FMS instance

$$f_{\text{safe}} = \frac{C(\text{HI})}{C(\text{LO})}$$

$f_{\text{safe}} = 3$			$f_{\text{safe}} = 4$			$f_{\text{safe}} = 5$		
y	x	Δ_R	y	x	Δ_R	y	x	Δ_R
1	1	0	3	0.25	21.6	22	0.25	2.1×10^3
-	-	-	4	0.25	7.8	23	0.25	661.8
-	-	-	5	0.25	5.92	24	0.25	406.1

Increased uncertainty in WCET (larger f_{safe})

⇨

Later to recover

Summary

- Mixed-criticality systems
  - Mixed (safety) critical, uncertainties, heterogeneous assurances
- Self-organizing under WCET uncertainty
  - Service reconfiguration, service recovery
- Demonstrated with a flight management system
  - Resource efficiency, flexibility
- Outlook
  - Different sources of uncertainties, different scheduling policies…


감사합니다
Natick
Grazie
Danke
Ευχαριστίες
Dalu
Obrigado
Thank You
Köszönöm
Tack
Спасибо
Dank
Gracias
谢谢
Merci
Seé
ありがとう

?