Sharif University of Technology
Department of Computer Science and Engineering

Lec. 10:

Mixed-Criticality Systems

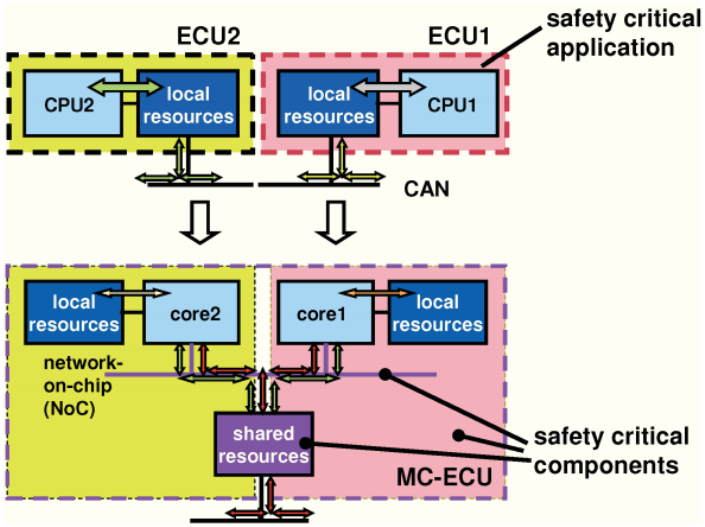
Real-Time Computing

S. Safari

2023

Mixed-Criticality Systems (MCS)

- An increasingly important trend in the design of real-time and embedded systems is the integration of components with different levels of criticality onto a common hardware platform.
- The integration of **various** applications with different **levels of criticality** (importance and safety levels) on a **shared** hardware platform.
- Criticality is a designation of the level of assurance against failure needed for a system component.
  - Reduction of the
    - Overall number of computers,
    - Cables and area
    - Cost
    - Weight
    - Energy consumption



Shared resources lead to mixed criticality systems

MCSs Application

- Typical examples are:
  - Advanced driver assistance systems in the automotive industry
  - Integrated modular architecture in the avionics industry

Standards of Mixed-Criticality Systems

- At the same time, these platforms are migrating from single cores to multi-cores and in the future many-core architectures.
- A mixed criticality system (MCS) is one that has two or more distinct levels (for example safety critical, mission critical and low-critical).
- Perhaps up to five levels may be identified in different standards:
  - DO-178B
  - IEC 61508
  - DO-178C
  - DO254
  - ISO 26262

DO-178B Standard

- DO-178B is a software development process standard, *Software Considerations in Airborne Systems and Equipment Certification*.

Level	Failure Condition	Interpretation
A	Catastrophic	Failure may cause a crash.
B	Hazardous	Failure has a large negative impact on safety or performance, or reduces the ability of the crew to operate the plane due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.
C	Major	Failure is significant, but has a lesser impact than a Hazardous failure (for example, leads to passenger discomfort rather than injuries).
D	Minor	Failure is noticeable, but has a lesser impact than a Major failure (for example, causing passenger inconvenience or a routine flight plan change).
E	No effect	Failure has no impact on safety, aircraft operation, or crew workload.

DO-178B Standard (cont'd)

- Typical names for the levels are ASILs (Automotive Safety and Integrity Levels), DALs (Design Assurance Levels or Development Assurance Levels) and SILs (Safety Integrity Levels).

Design Assurance Level (DAL)

A	A/B	B	C	D	E
Cockpit • Display • Autopilot	**Critical** • Engine control • Flight control • Breaking • Steering	**FMS** • Localization • Trajectory • Guidance • Performance	**Maintenance** • Maintenance • Logging	**Cabin** • Cabin light • Water control • Pressure	**Passenger** • In flight entertainment • Communication

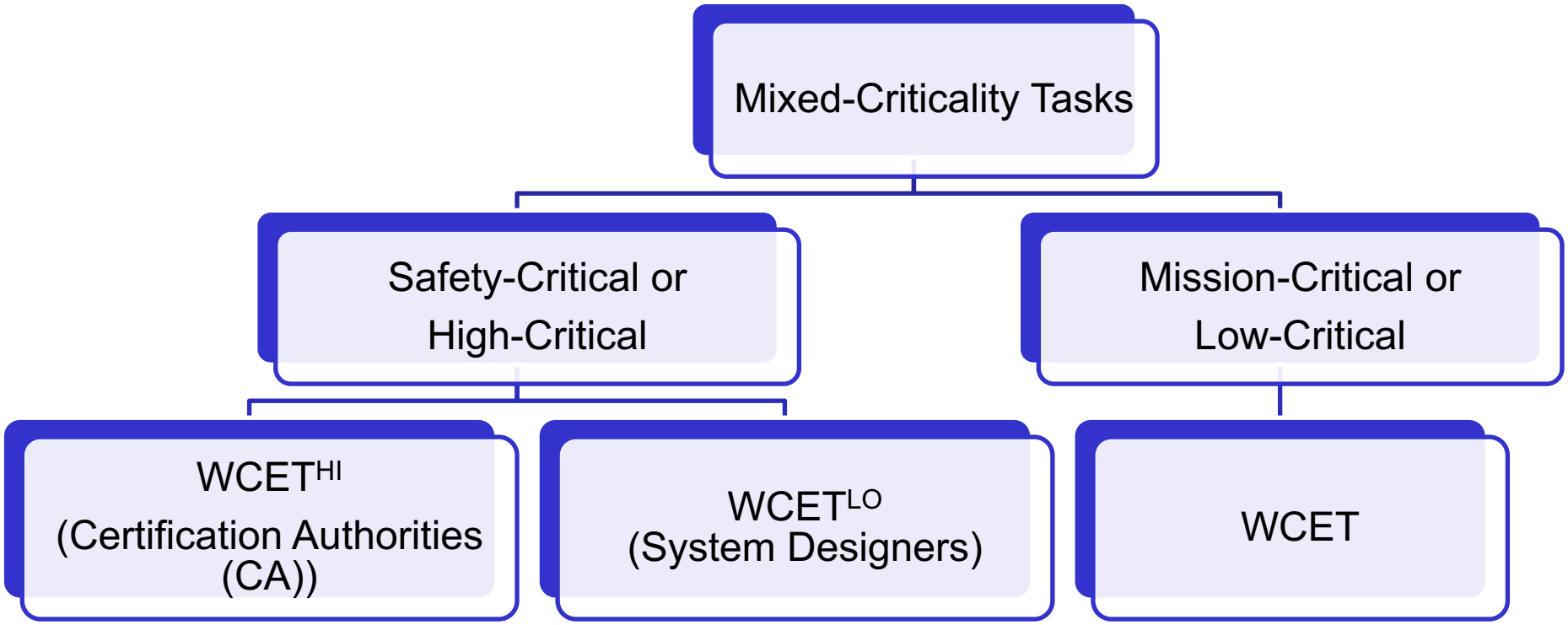
Overview of Mixed-Criticality Systems

- Considering first an example from the domain of unmanned aerial vehicles (UAVs), used for defense reconnaissance and surveillance.
- The functionalities on board such UAVs may be classified into two levels of criticality:
  - Level 1: *flight-critical functionalities*, to be performed by the aircraft to ensure its safe operation.
  - Level 2: *mission-critical functionalities*, concerning reconnaissance and surveillance objectives, like capturing images from the ground, transmitting these images to a base station, etc.
- The mission-critical functionalities must be validated separately by the system designers and it is mandatory that its flight-critical functionalities be certified correct.

Design Challenges of Mixed-Criticality Systems

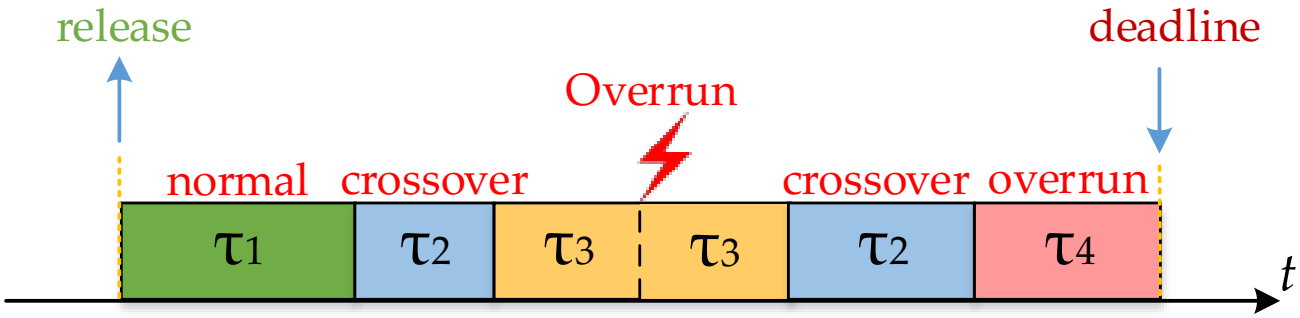
- Design challenges of mixed-criticality systems:
  - Certification
  - Fault-Tolerance
  - Power/Energy/Temperature Management
  - Quality of Service (QoS)
  - Resource sharing

Certification



Overrun & Crossover Tasks

- When an overrun occurs, three types of jobs may exist
  - Normal jobs: have both release time and deadline before the mode switch point.
  - Overrun jobs: are released after the mode switch point.
  - Crossover jobs: which are released before the mode switch point but have later deadlines are candidates for crossover jobs.



Quality of Service (QoS)

Normal

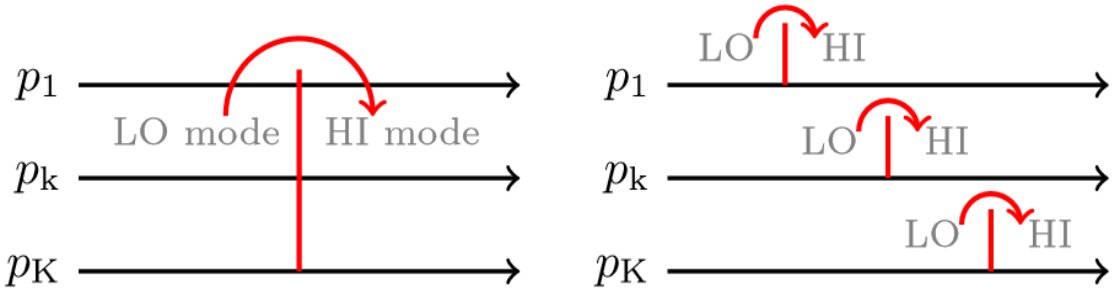
Normal or LO-criticality mode:
- HC & LC tasks → $WCET^{LO}$

Overrun

HC task exceeds its $WCET^{LO}$

Critical

Overrun or HI-criticality mode:
- HC tasks → $WCET^{HI}$



a) Global overrun

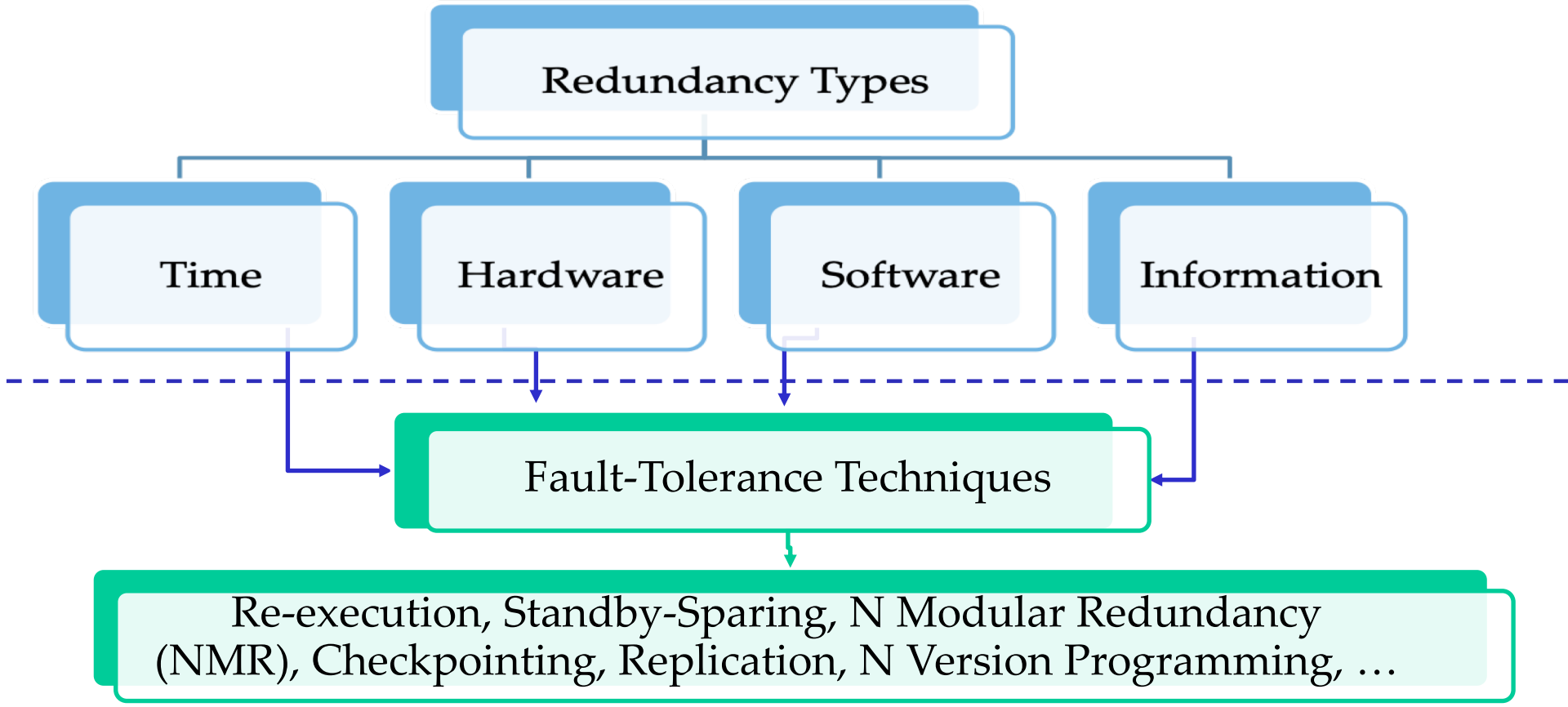
b) Local overrun

- In Critical mode, LC tasks:
  - Drop: EDF-VD
  - Selectively execute
  - Guarantee: ER-EDF

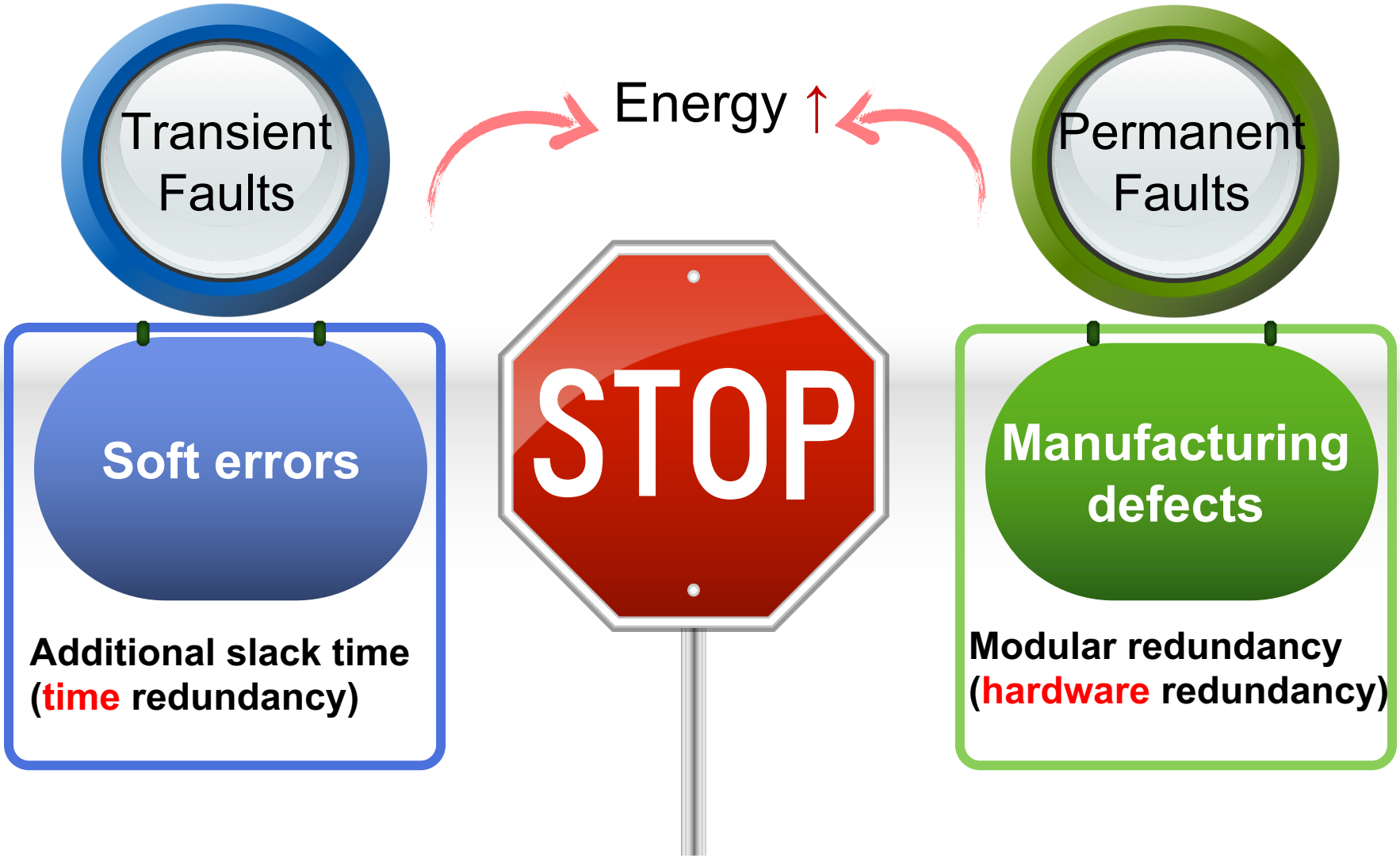
Reliability and Fault-Tolerant Techniques

RTCA DO-178B safety requirements

ζ	A	B	C	D	E
PFH	$< 10^{-9}$	$< 10^{-7}$	$< 10^{-5}$	$\geq 10^{-5}$	-



Reliability vs. Energy



Design Objectives

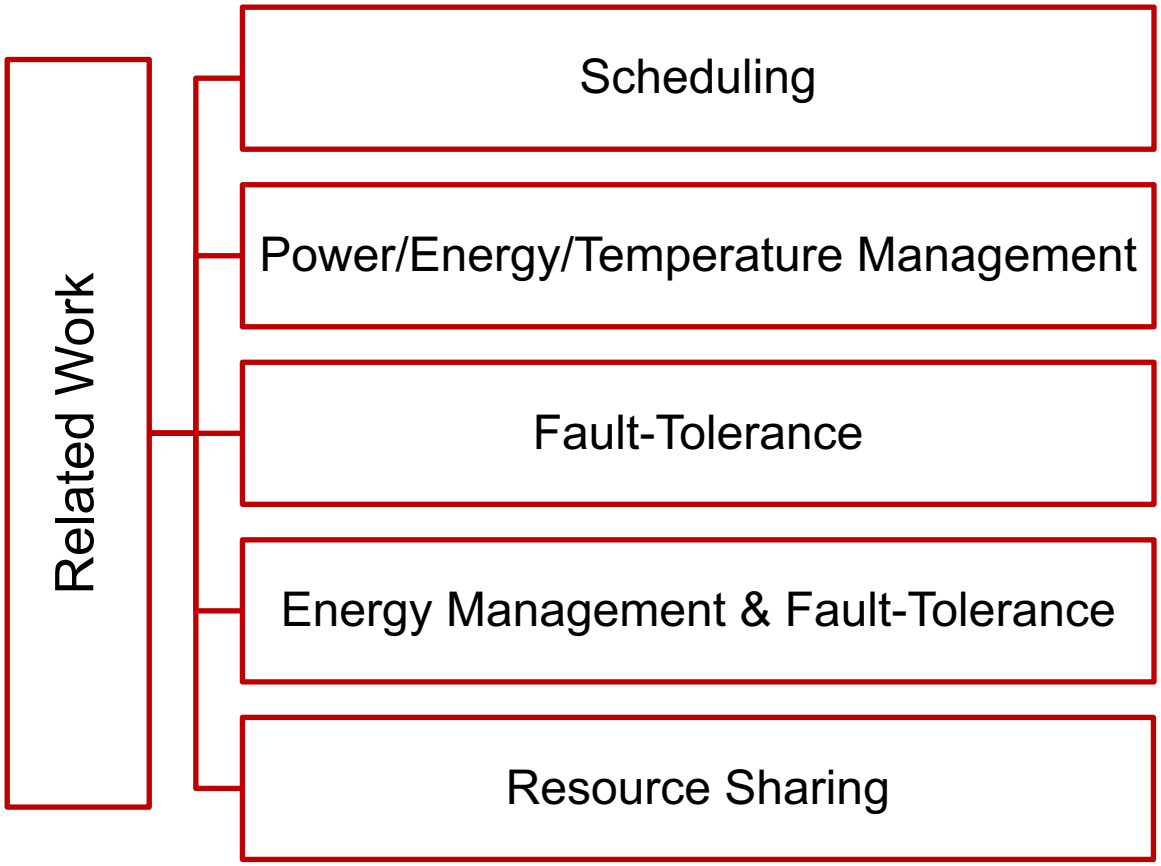
Power/Energy Management

High Reliability

Schedulability (Real-Time Constraint)

QoS

Related Work



Scheduling

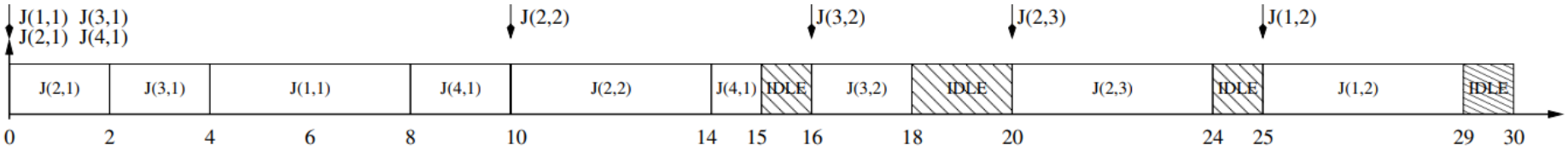
Method	Platform	Scheduling Algorithm	Criticality Level	Energy Management	Method	Fault-Tolerance	Method	QoS
(Vestal07)	Single-core	PFP	Multi	No	-	No	-	Degradation
(Baruah08)	Single-core	Hybrid	Multi	No	-	No	-	Degradation
(Niz09)	Single-core	ZSRM	Multi	No	-	No	-	Drop & Degradation
(Baruah10)	Single-core	EDF, OCBP	Dual	No	-	No	-	Selective
(Park11)	Single-core	CBEDF	Dual	No	-	No	-	Selective
(Santy12)	Single-core	FP	Multi	No	-	No	-	Degradation
(Baruah12) (Baruah15)	Single-core	EDF-VD	Dual	No	-	No	-	Drop
(Ekberg12)	Single-core	EY	Dual	No	-	No	-	Drop
(Socci12)	Single-core	MCEDF	Dual	No	-	No	-	Drop
(Su13a)	Single-core	ER-EDF	Dual	No	-	No	-	Guarantee
(Su14)	Single-core	ER-EDF, EDF-VD	Dual	No	-	No	-	Guarantee
(Huang15)	Single-core	EDF	Dual	No	-	No	-	Drop
(Su17)	Single-core	ER-EDF	Dual	No	-	No	-	Guarantee

Scheduling (cont'd)

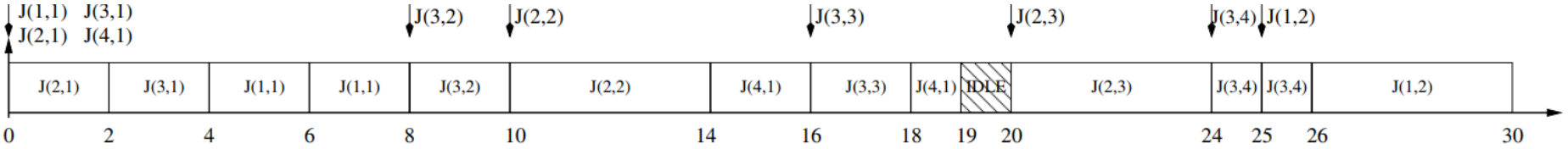
Method	Platform	Scheduling Algorithm	Criticality Level	Energy Management	Method	Fault-Tolerance	Method	QoS
(Mollison10)	Multi-core	CE, BE P-EDF, G-EDF	Multi	No	-	No	-	Selective
(Kelly11)	Multi-core	RMS, Audsley (FP)	Dual	No	-	No	-	Drop & Degradation
(Pathan12)	Multi-core	MSM (FP)	Multi	No	-	No	-	Drop
(Li12) (Baruah14)	Multi-core	EDF-VD, fpEDF	Dual	No	-	No	-	Drop
(Su13b)	Multi-core	ER-EDF	Dual	No	-	No	-	Guarantee
(Gu14)	Multi-core	MPVD	Dual	No	-	No	-	Drop
(Socci15)	Single-core	Graph	Dual	No	-	No	-	Drop

ER-EDF Scheduling

	Basic MC Parameters			Parameters for E-MC		EDF-VD [2]
	ζ_i	c_i	p_i	p_i^{max}	P_i^{ER}	Virtual Deadline
τ_1	ζ^{high}	{4,10}	25	-	-	13.85
τ_2	ζ^{high}	{2,4}	10	-	-	5.54
τ_3	ζ^{low}	2	8	16	{8}	8
τ_4	ζ^{low}	3	30	40	{30}	30



The EDF schedule with maximum periods of low-criticality tasks to ensure their minimal service requirement.



The ER-EDF schedule where the low-criticality task τ3 releases early at time 8, 16 and 24

EDF-VD Scheduling

Task system $\tau = \{\tau_1, \tau_2, \ldots \tau_n\}$ to be scheduled on a unit-speed preemptive processor.

1) Compute x as follows:

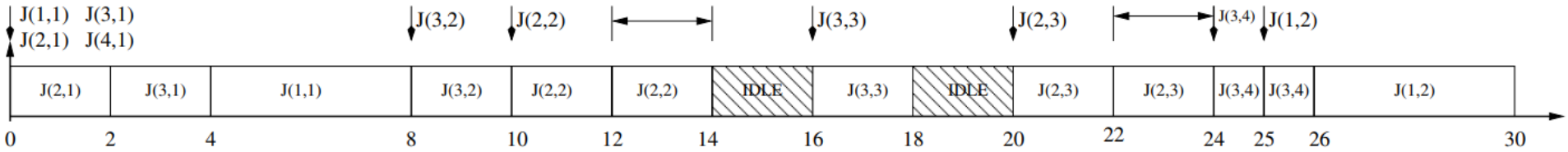
$$x \leftarrow \frac{U_{\text{HI}}^{\text{LO}}(\tau)}{1 - U_{\text{LO}}^{\text{LO}}(\tau)}$$

2) If $\left(x\, U_{\text{LO}}^{\text{LO}}(\tau) + U_{\text{HI}}^{\text{HI}}(\tau) \leq 1\right)$ **then**

$\hat{T}_i \leftarrow x\, T_i$ for each HI-criticality task τ_i
declare success and **return**

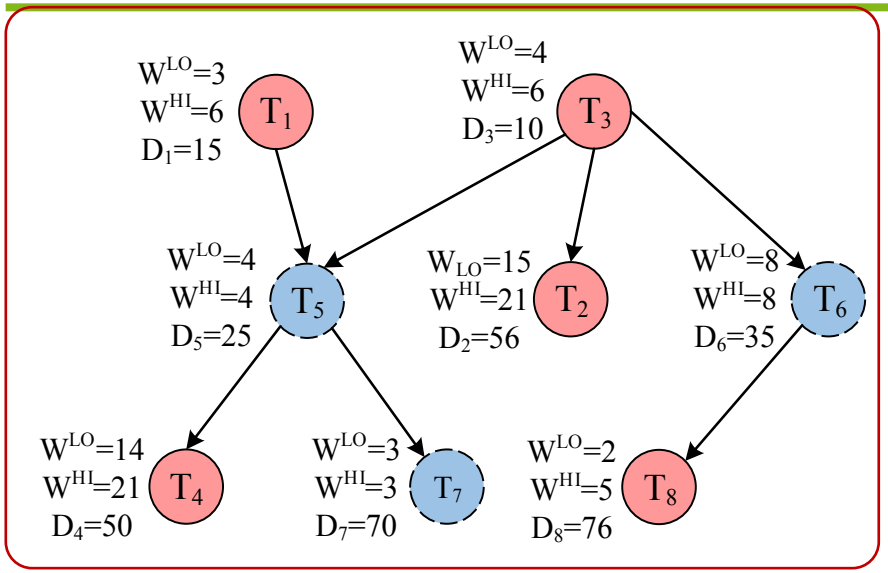
else declare failure and **return**

	Basic MC Parameters			Parameters for E-MC		EDF-VD [2]
	ζ_i	c_i	p_i	p_i^{max}	P_i^{ER}	Virtual Deadline
τ_1	ζ^{high}	{4,10}	25	-	-	13.85
τ_2	ζ^{high}	{2,4}	10	-	-	5.54
τ_3	ζ^{low}	2	8	16	{8}	8
τ_4	ζ^{low}	3	30	40	{30}	30

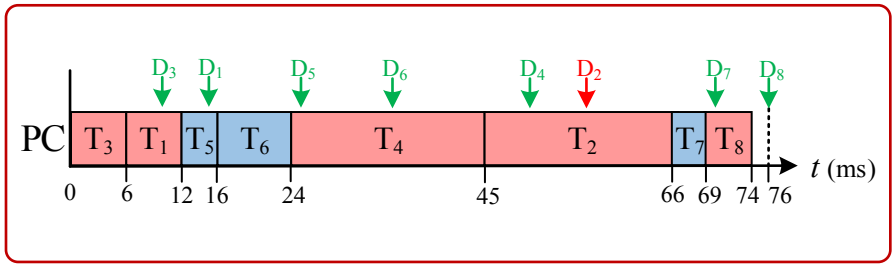


The EDF-VD schedule where low-criticality job *J*(4, 1) is discarded due to high execution mode during interval [12, 14].

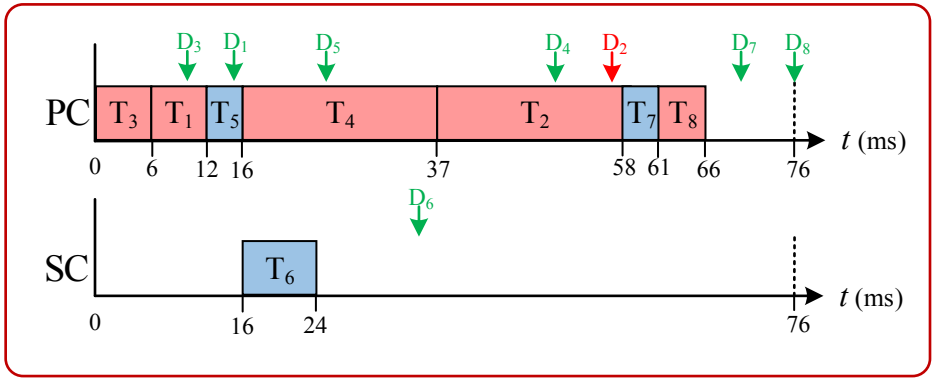
Example of a Mixed-Criticality Task Graph



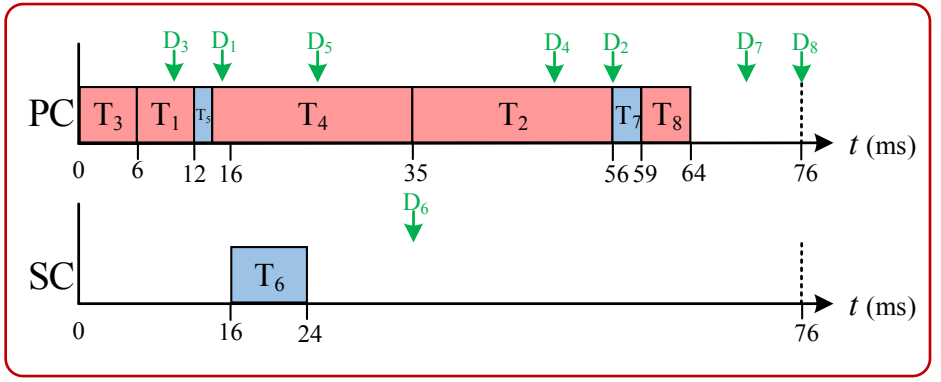
Latest Deadline First (LDF)



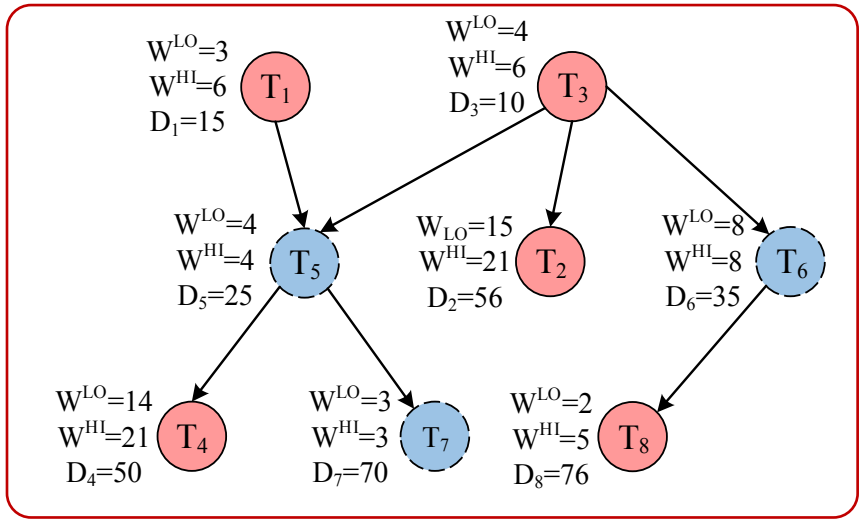
Parallelism

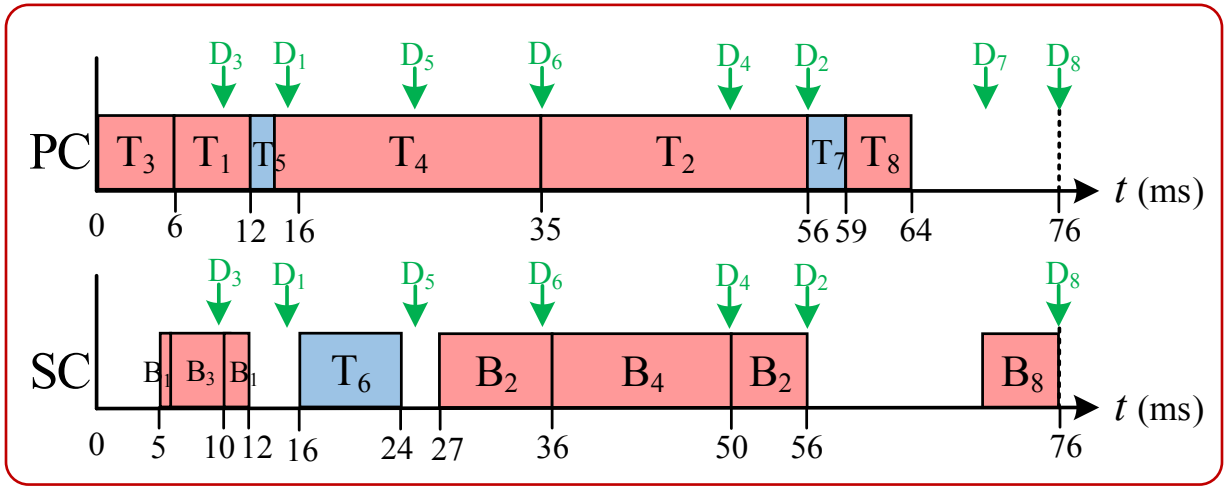


Parallelism & Reduction



Example of a Mixed-Criticality Task Graph





Summary

- Introduction to Mixed-Criticality Systems
- DO-178B Standard
- MCSs Applications
- Objectives of MCSs
  - Certification
  - QoS
  - Power/Energy/Temperature
  - Reliability
  - Resource sharing