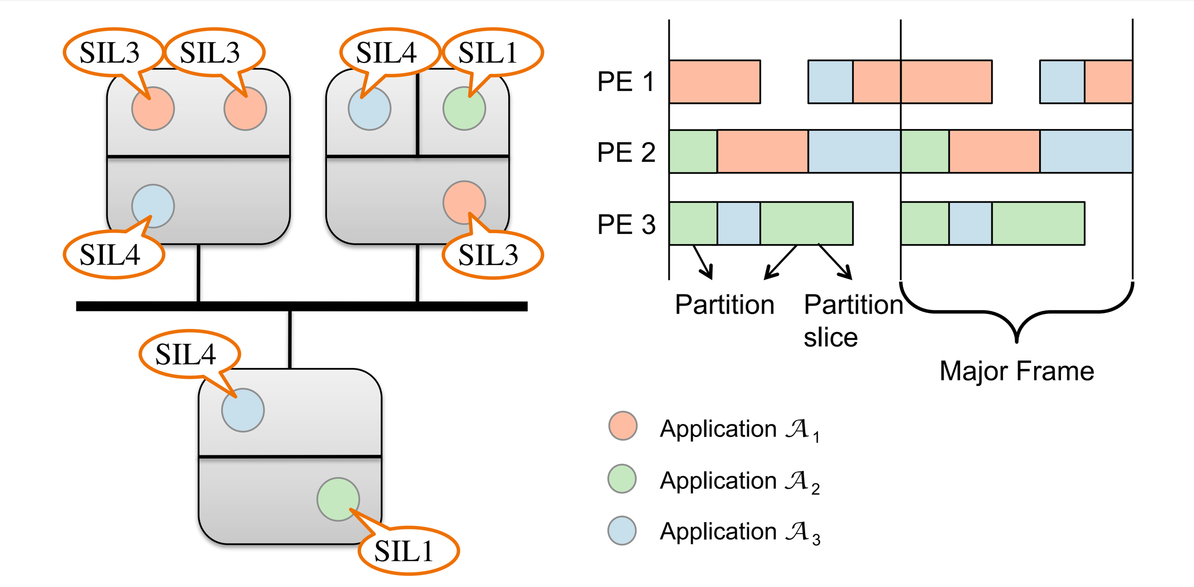
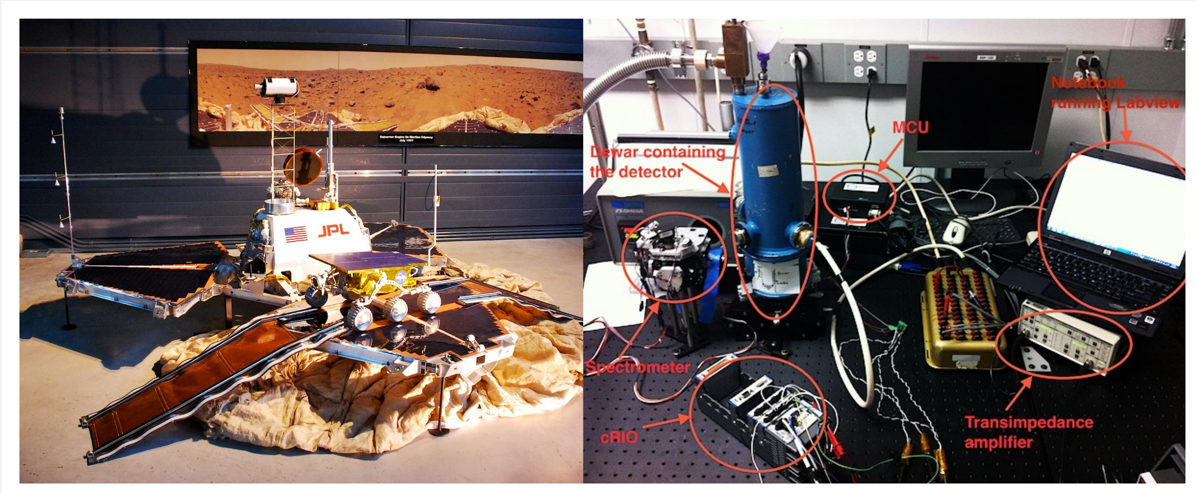
Design of Mixed-Criticality Applications on Distributed Real-Time Systems

Domițian Tămaș-Selicean (dota@dtu.dk). Advisor: Paul Pop

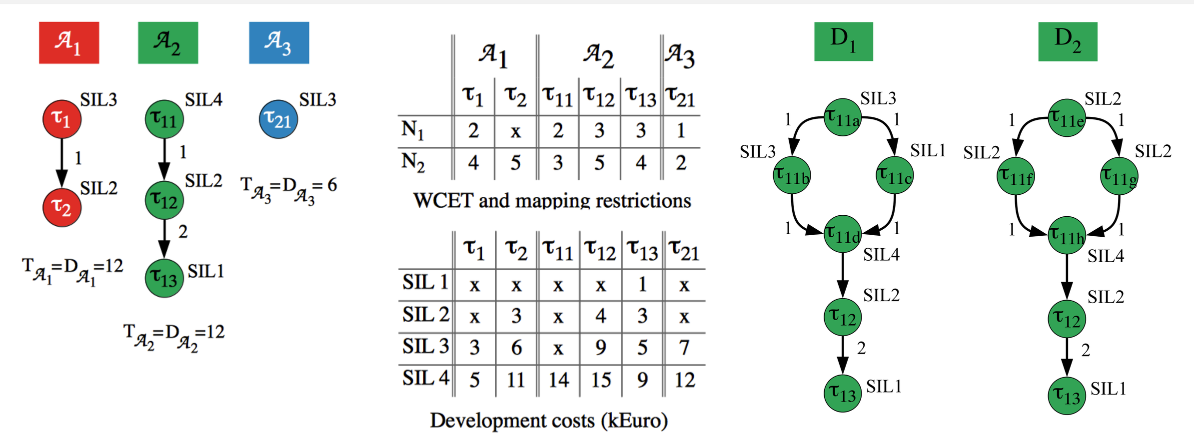
Design optimization at the processor-level



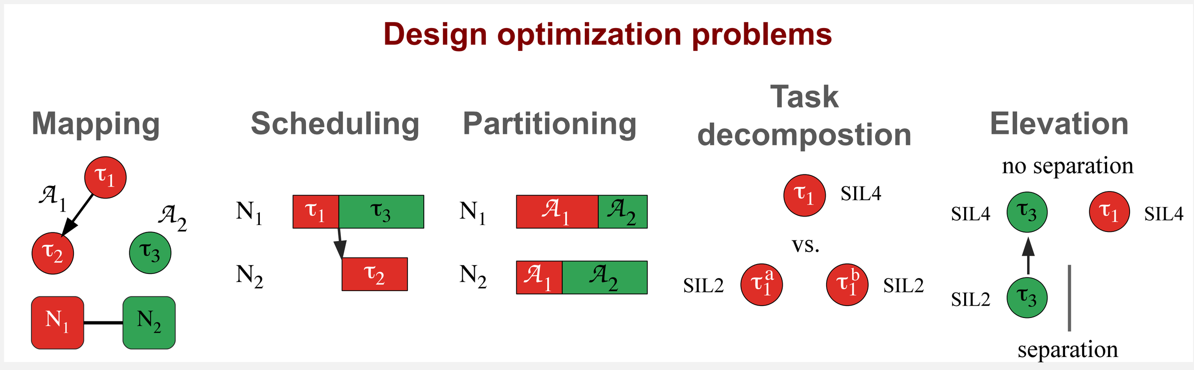
System model. Separation between mixed-criticality applications is enforced by partitioning. Tasks can share a partition only if they have the same SIL.



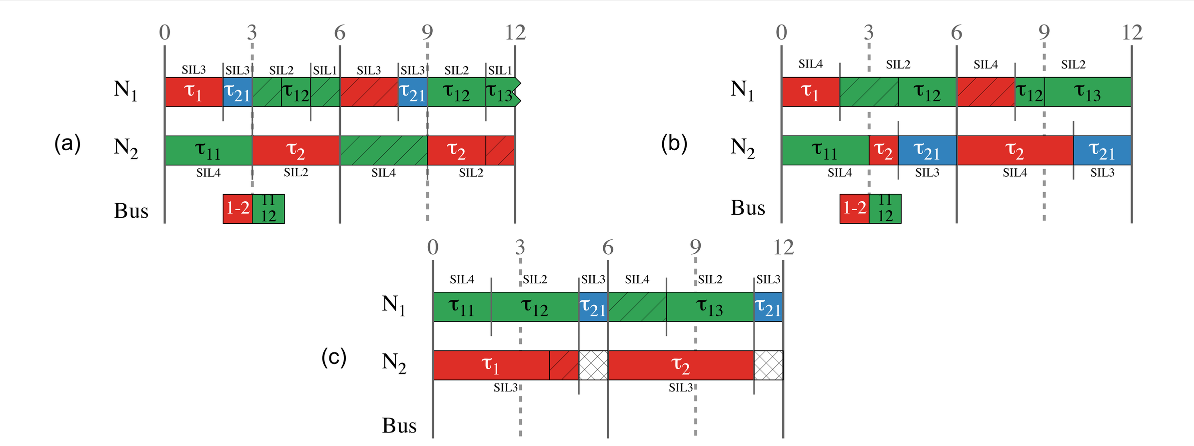
Realistic aerospace case study. Two mixed-criticality applications implemented on the same processor: Mars Pathfinder (MESUR) (left, hard real-time) and CIRIS (right, soft real-time, the controller of a FTIR spectrometer developed during my external stay at the Jet Propulsion Lab, NASA).



Application model. Applications scheduled using static cyclic scheduling or preemptive fixed-priority scheduling. The applications are modeled as directed acyclic graphs (right). The WCET, mapping restrictions and the developments costs for each task are given (center), together with a library of possible task decompositions (right).



Mapping: deciding in which Processing Element (PE) to place a task. **Scheduling**: deciding the start times of static tasks. **Partitioning**: deciding the sequence and sizes of partition slices. **Task decomposition**: deciding how to implement a task to meet the SIL requirements. **Elevation**: implementing a lower SIL task at a higher SIL. We proposed the Tabu Search-based Mixed-Criticality Design Optimization (MCDO) strategy to solve these design problems.



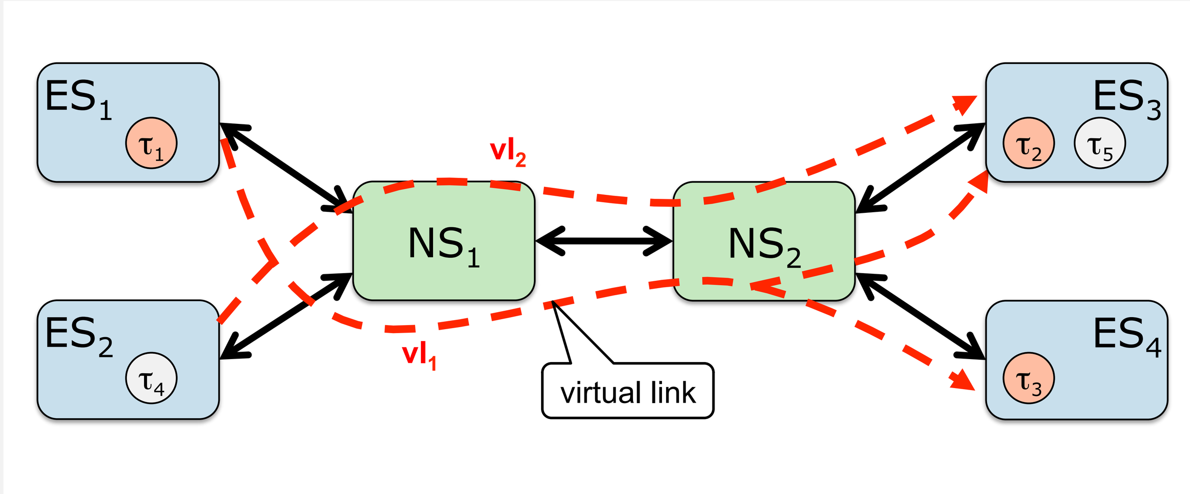
Motivational example

(a) Simultaneous mapping and partitioning optimization, τ_{13} does not fit in the schedule.
(b) Allowing partitioning sharing results in a successful schedule with DC = 44.
(c) Simultaneously optimizing the mapping, partitioning and partition sharing results in a schedulable implementation with DC = 37.

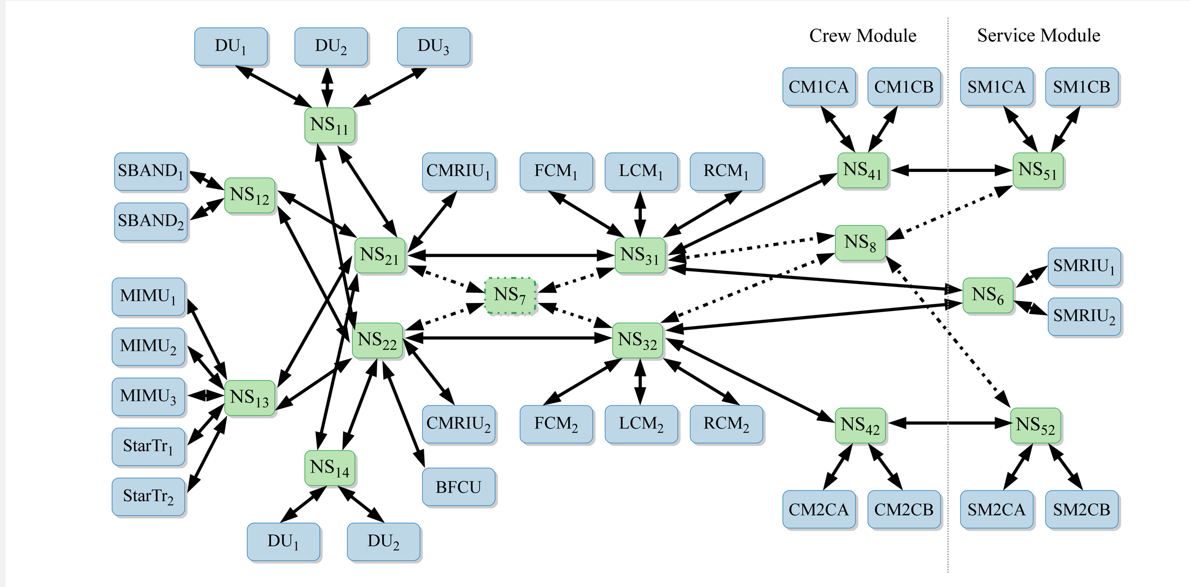
Partition table	Major Frame size (ms)	Total partition slice size (ms)			CIRIS		MESUR Sched. task	
		CIRIS	MESUR-HC	MESUR-LC	No. of interferograms	QoS	MESUR-HC	MESUR-LC
a	125	34	75	16	128	0.800	4 / 4	3 /3
b	120	20	80	20	92	0.575	4 / 4	2 /3
c	200	10	160	30	79	0.493	4 / 4	3 /3
d	120	40	60	20	160	1.000	2 / 4	2 /3
e	100	12	64	24	160	1.000	4 / 4	3 /3

Evaluation results for the realistic case study.
The MCDO strategy targets systems implementing hard real-time applications. We extended MCDO to also take into account soft real-time tasks and we modified the cost function to capture also the quality of service of the soft real-time tasks.
MESUR-HC is the set of high criticality Mars Pathfinder tasks. MESUR-LC is the set of low criticality tasks. The Mars Pathfinder tasks are scheduled using fixed-priority preemptive scheduling. The CIRIS tasks are scheduled using static cyclic scheduling.

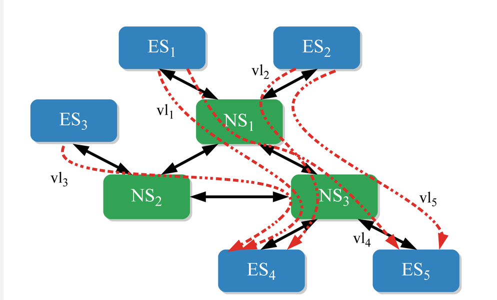
Design optimization at the communication network-level



System model. The network implements the TTEtherent protocol, an Ethernet-based protocol compliant with ARINC 664p7 "Aircraft Data Network" for mixed-criticality applications. TTEthernet enforces separation between messages of different criticalities through the concept of "virtual link".

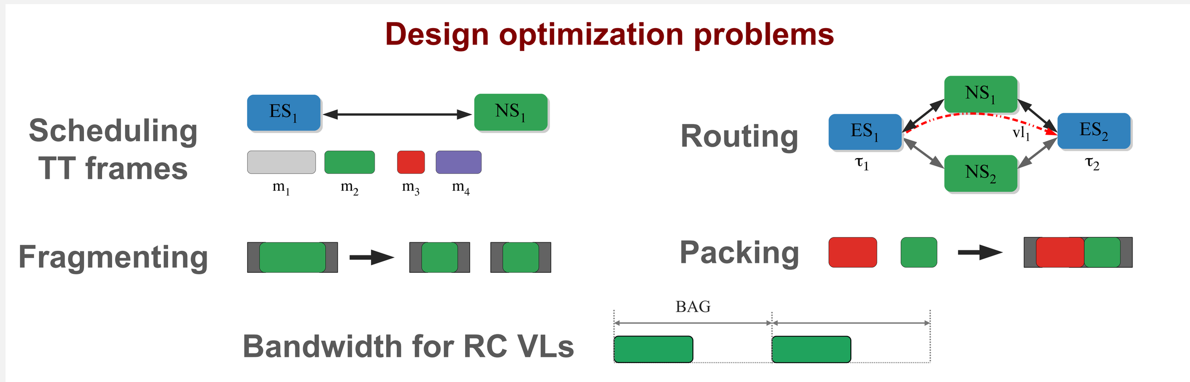


Realistic aerospace case study. Topology of the Orion Crew Exploration Vehicle, 606E baseline.

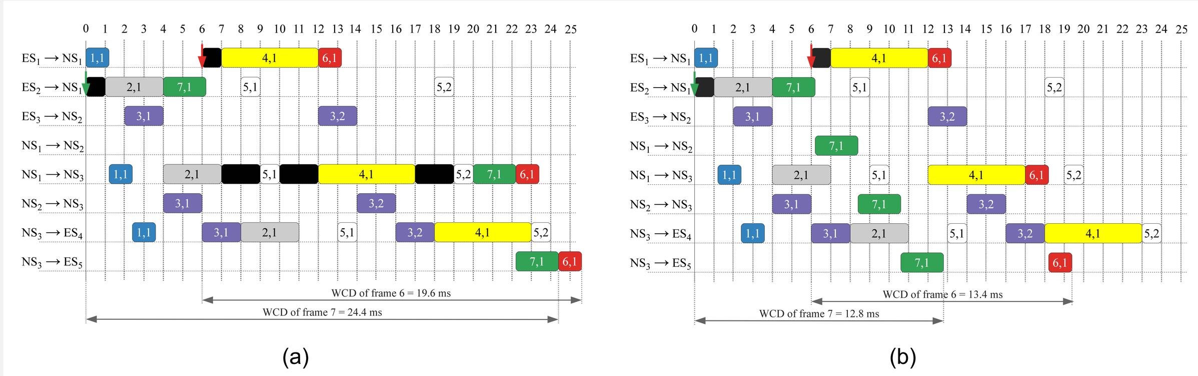


	period (ms)	deadline (ms)	size (B)	C_i (ms)	Source	Dest
$m_1 \in \mathcal{M}^{TT}$	40	40	233	1.2	ES_1	ES_4
$m_2 \in \mathcal{M}^{TT}$	40	40	683	3	ES_2	ES_4
$m_3 \in \mathcal{M}^{TT}$	10	10	433	2	ES_3	ES_4
$m_4 \in \mathcal{M}^{TT}$	40	40	1183	5	ES_1	ES_4
$m_5 \in \mathcal{M}^{TT}$	10	10	183	1	ES_2	ES_4
$m_6 \in \mathcal{M}^{RC}$	40	32	233	1.2	ES_1	ES_5
$m_7 \in \mathcal{M}^{RC}$	20	16	483	2.2	ES_2	ES_5

Application model. TTEthernet offers three traffic classes: Time-Triggered (synchronized), Rate Constrained (unsynchronized) and Best Effort (regular Ethernet traffic). For each message, the engineer specifies the traffic class, the period, deadline, the size, the source and destination end systems.



Scheduling TT frames: deciding the schedules of TT frames in ES and NS devices. **Routing**: deciding the routing of virtual links. **Fragmenting**: deciding if and how to split messages before transmission. **Packing**: deciding which messages to pack into a frame. **Bandwidth for RC VLs**: deciding the Bandwidth Allocation Gap for RC VLs. To solve these design problems we proposed the Tabu Search-based Design Optimization of TTEthernet-based Systems (DOTTS) strategy.



Motivational example

(a) Baseline solution: each message is packed in a frame that is routed on the shortest path. Timely block intervals marked with black.
(b) Routing optimization: routing f_7 via an extra network switch improves considerably the worst-case end-to-end delay (WCD) of both RC frames.

(a)

Topology	ES	NS	Cost	Messages	Frame Instances	Sched.%
orion 1	31	14	124	187	6250	100
orion 2		13	115		7240	100
orion 3		12	106		8804	100

(b)

Benchmark	ES	NS	TT and RC Messages	BE Messages	Frame Instances	$BW^{BE}_{\%}$
be 1	31	12	187	41	8588	100
be 2				63	8500	100
be 3				83	8824	100
be 4				101	8810	100

Evaluation results for the realistic case study.
(a) Perform topology selection to reduce the cost of the system.
(b) DOTTS focuses on hard real-time traffic transported via TT and RC frames. We modified the cost function to take into account BE traffic. Even though the BE traffic is increasing, DOTTS is able to find solutions such that all the TT and RC frames meet their real-time constraints and the BE frames have their bandwidth requirements met.

DTU Technical University of Denmark

recomp Reduced Certification Costs for trusted Multi-core Platforms

Acknowledgements This work has been funded by the Advanced Research & Technology for Embedded Intelligence and Systems (ARTEMIS) within the project "RECOMP", support code 01IS1001A, agreement no. 100202. The external stay was partly funded by the Oticon Fonden and Otto Mønsteds Fond.