Fault-Tolerant Topology Selection for TTEthernet Networks

Voica Gavriluț, Domițian Tămaș-Selicean, Paul Pop

Presenter: Sune Mølgaard Laursen

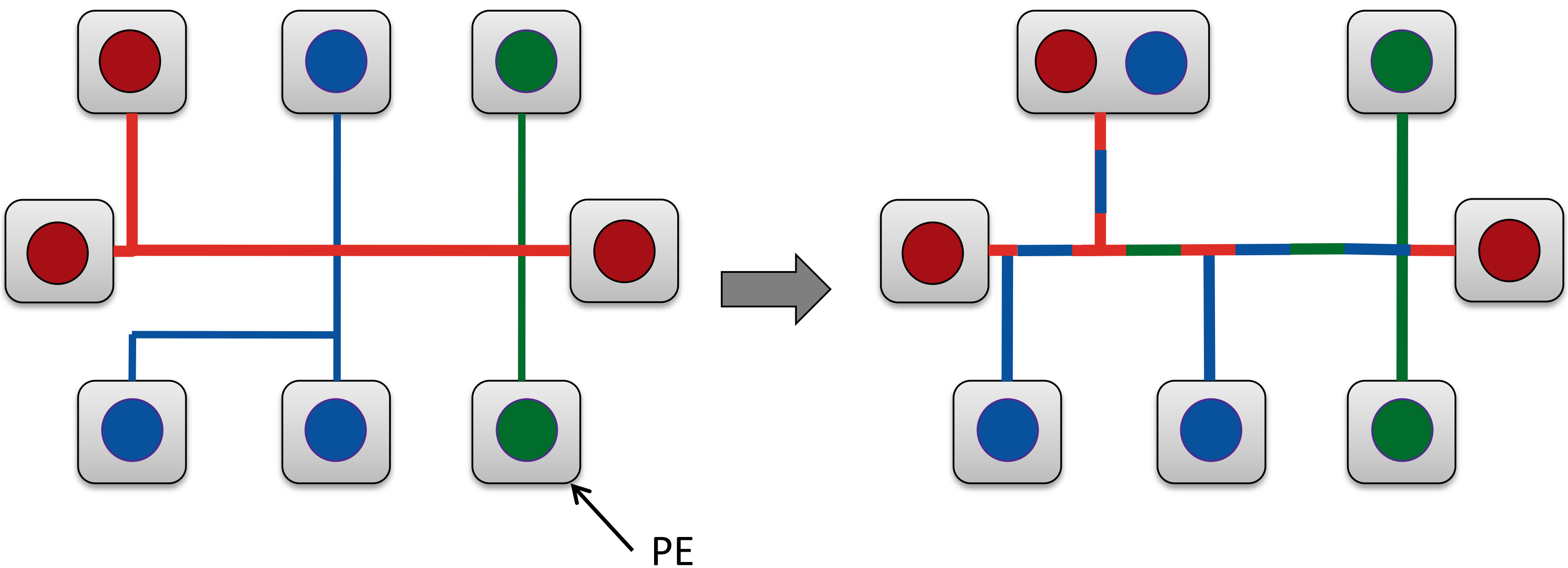
DTU Compute
Department of Applied Mathematics and Computer Science

Background

- Real time applications implemented using distributed systems

Point-to-point connection

Bus connection



- Application $\mathcal{A}_1$ -- highly critical
- Application $\mathcal{A}_2$ -- critical
- Application $\mathcal{A}_3$ -- non-critical

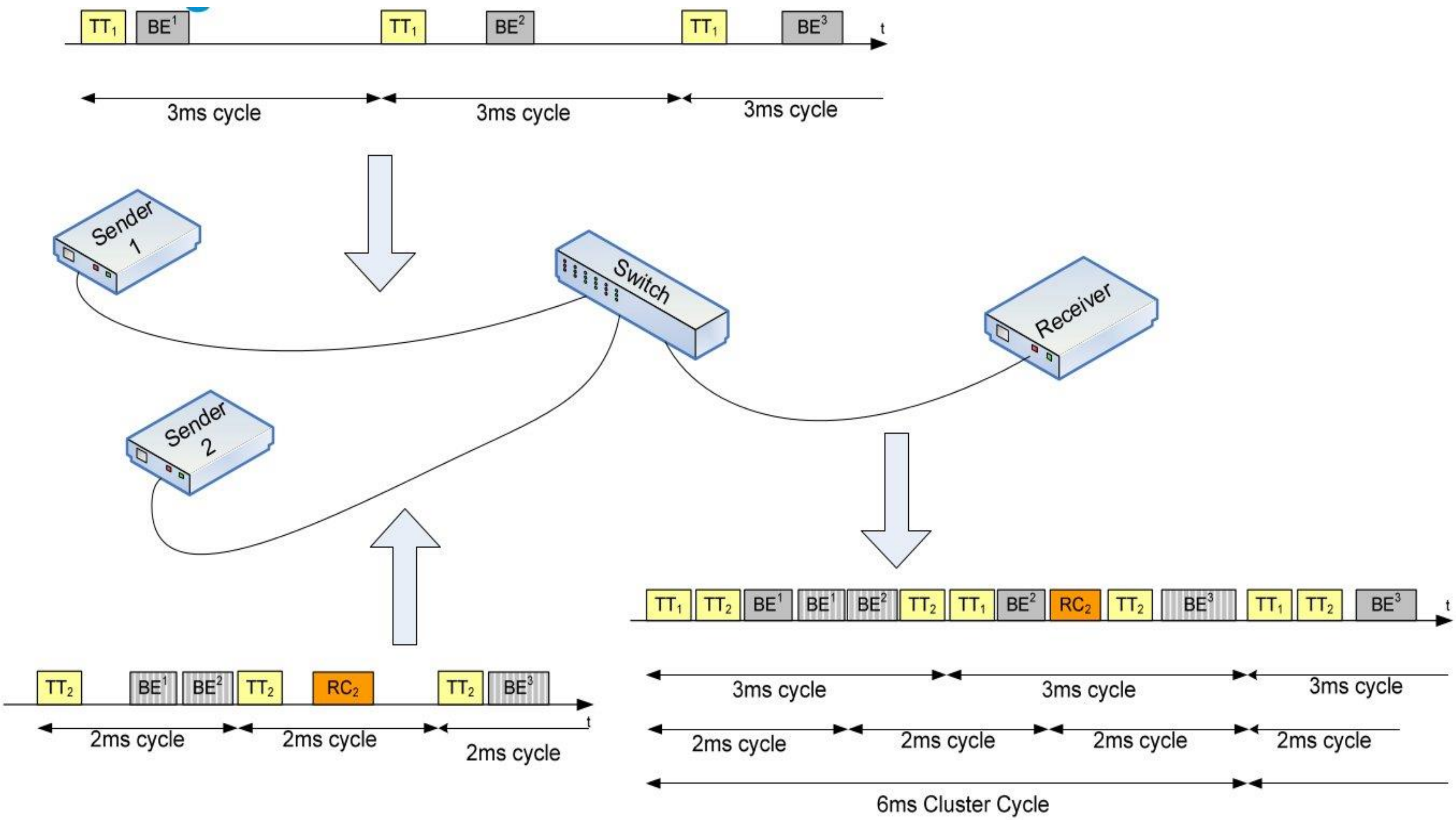
- Reduces wiring and weight
- Mixed-criticality applications share the same network

TTEthernet

- ARINC 664p7 compliant
- Traffic classes:
  - synchronized communication
    - Time Triggered (TT)
  - unsynchronized communication
    - Rate Constrained (RC) – ARINC 664p7 traffic class
    - Best Effort (BE) – no timing guarantees

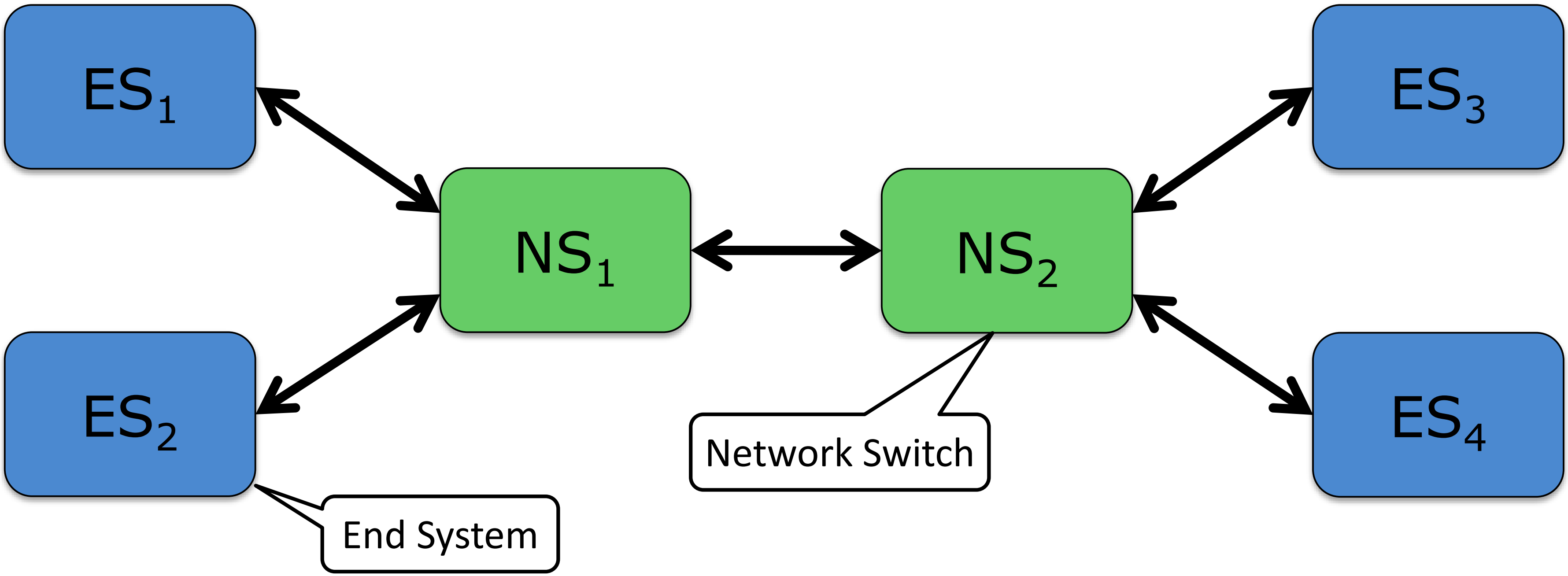
- Standardized as SAE AS 6802
- Marketed by TTTech Computertechnik AG
- Implemented by Honeywell on the NASA Orion Constellation

TTEthernet

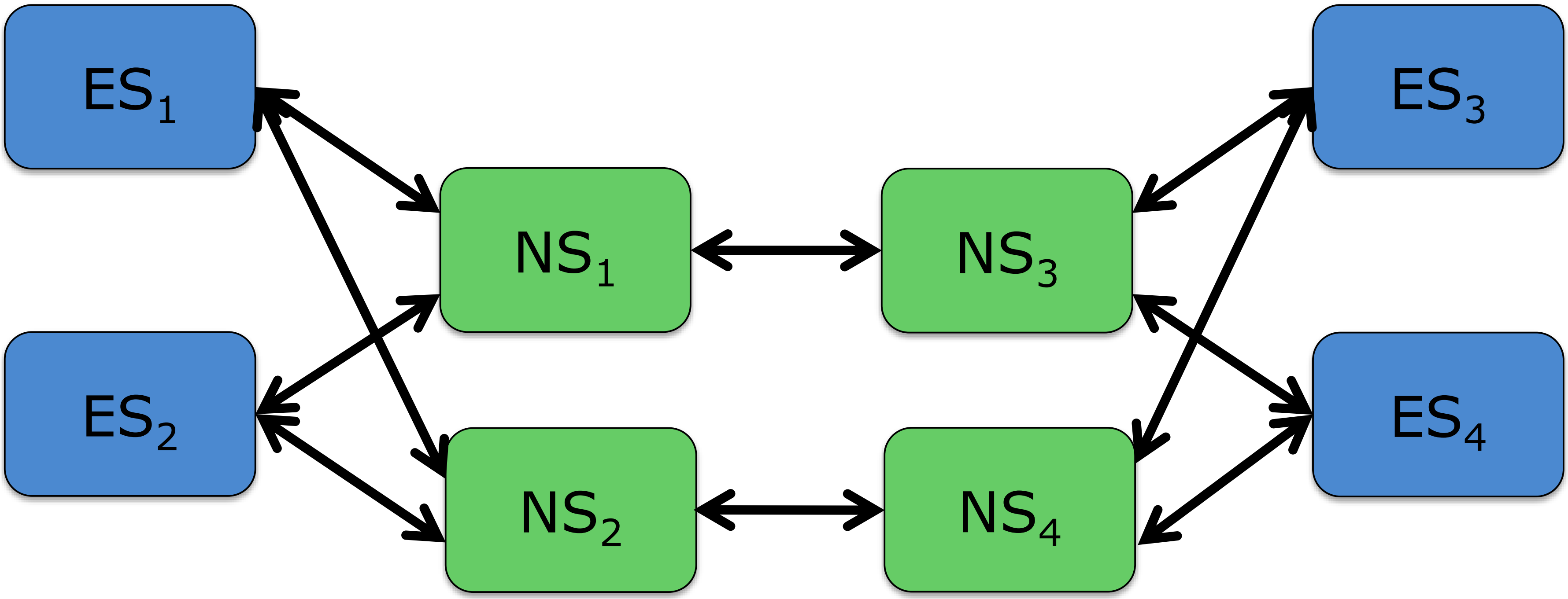


TT1
BE1
TT1
BE2
TT1
BE3
t
3ms cycle
3ms cycle
3ms cycle
Sender 1
Switch
Receiver
Sender 2
TT2
BE1
BE2
TT2
RC2
TT2
BE3
t
2ms cycle
2ms cycle
2ms cycle
TT1
TT2
BE1
BE1
BE2
TT2
TT1
BE2
RC2
TT2
BE3
TT1
TT2
BE3
t
3ms cycle
3ms cycle
3ms cycle
2ms cycle
2ms cycle
2ms cycle
2ms cycle
6ms Cluster Cycle

Motivation



Motivation



- Fault-Tolerancy is costly!

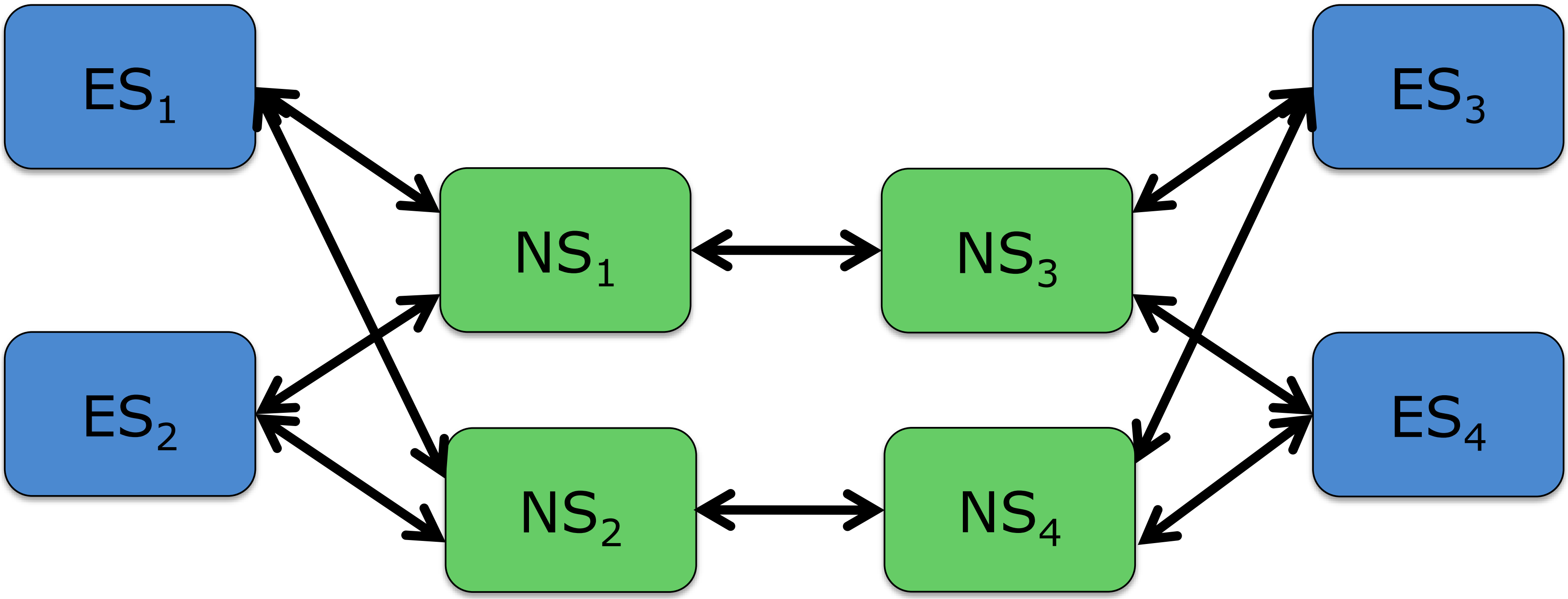
Problem formulation

- **Given**
  - Architecture model
    - The set of End Systems (ESes)
    - Cost and maximum number of ports for ESes and Network Switches
  - Application model
    - Set of TT and RC messages
    - Size, deadline, period and "redundancy level" RL for each message
- **Determine**
  - The network topology: Number of NSes, the physical links and interconnections
  - Network configuration
    - Assignment of frames to virtual links; routing of virtual links
    - Bandwidth for each RC virtual link
    - Set of TT schedule tables S
  - Such that
    - Architecture cost is minimized, applications are fault-tolerant, considering the specified redundancy levels, and the timing constraints of all frames, both TT and RC are satisfied.

Optimization strategy

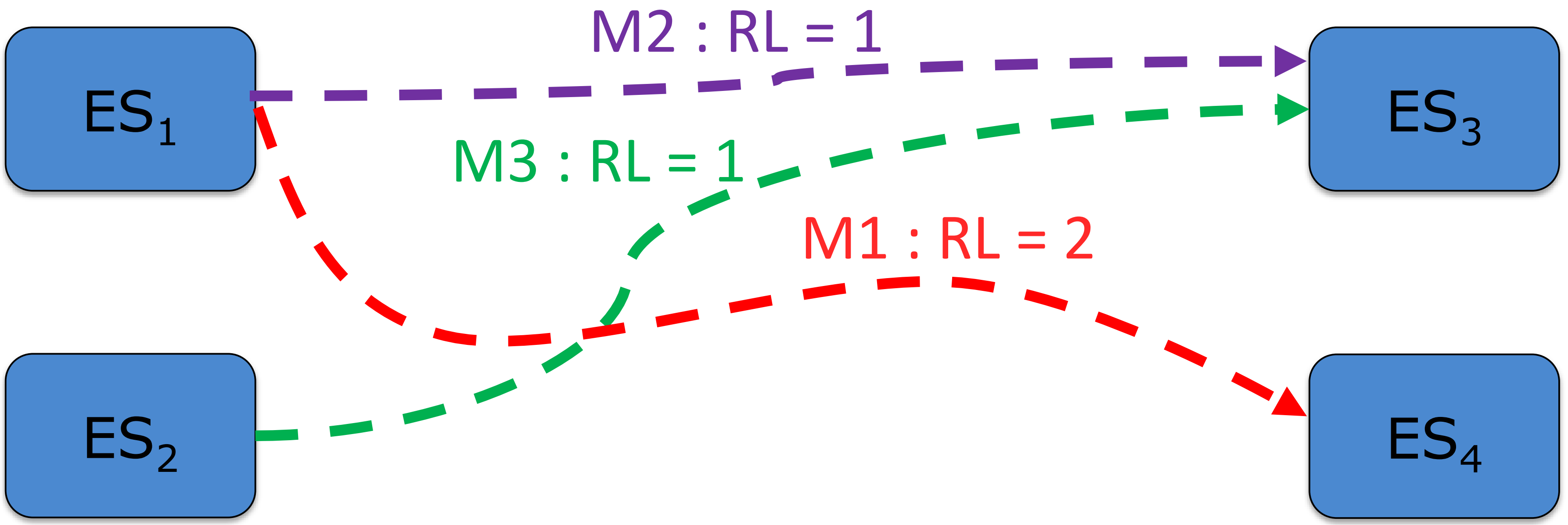
- Redundant Architecture Selection (RAS)
  - Based on a Simulated Annealing metaheuristic
  - Searches the solution space to minimize the cost function
    - *Penalty Weight* × *Degree of Schedulability* + *Architecture cost*
      - The “Degree of Schedulability” is positive if there are messages which are not schedulable, otherwise it is 0
      - The Penalty Weight is a large value, which “penalizes” the cost function in case the messages are not schedulable
      - The schedulability of RC messages is determined with the techniques from: *Tamas-Selicean, D., P. Pop, & W. Steiner (2015). Timing analysis of rate constrained traffic for the TTethernet communication protocol. In International Symposium On Real-time Computing (ISORC)*
  - Uses “design transformations” to modify the current solution during the search, e.g., insert/delete NS, insert/delete a physical link, or reroute a VL

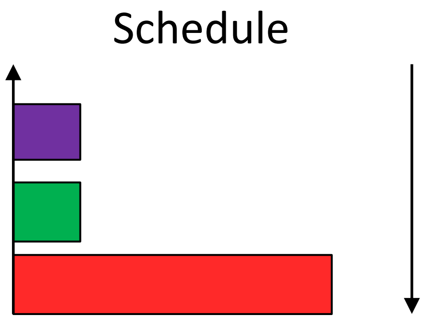
Example



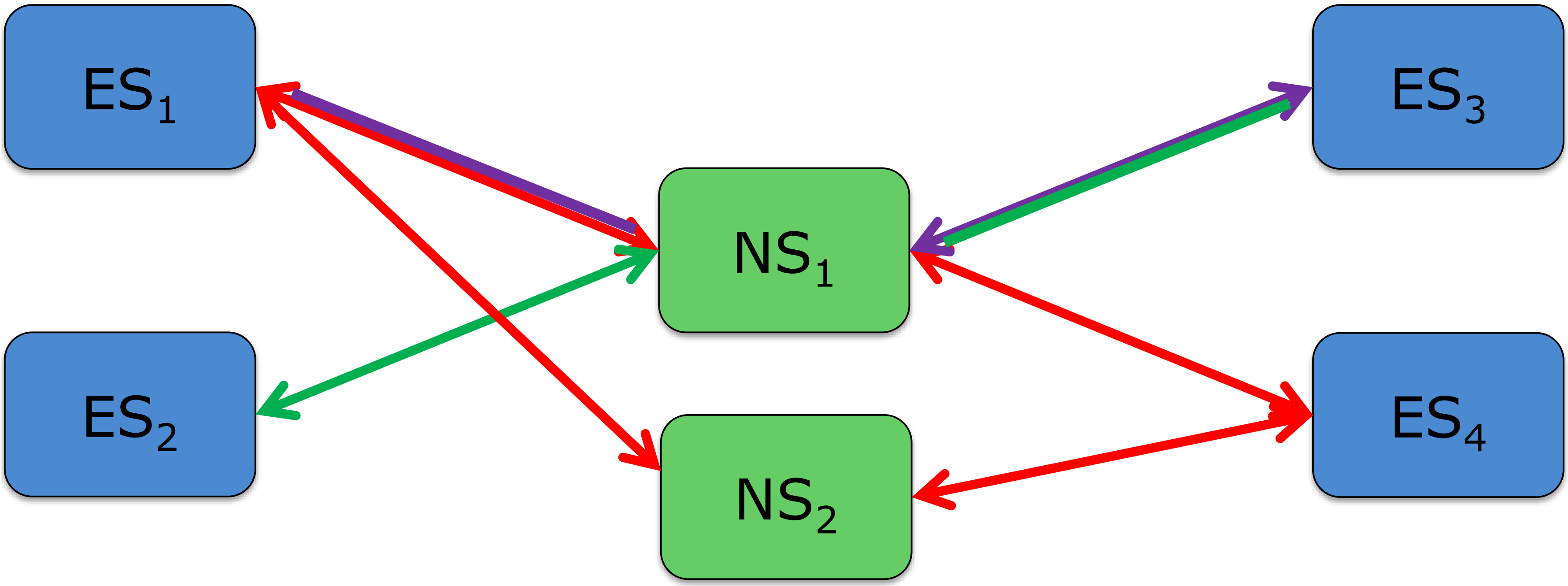
Cost = 180

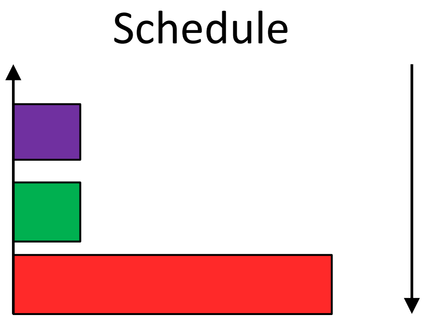
Example





Intermediate Solution

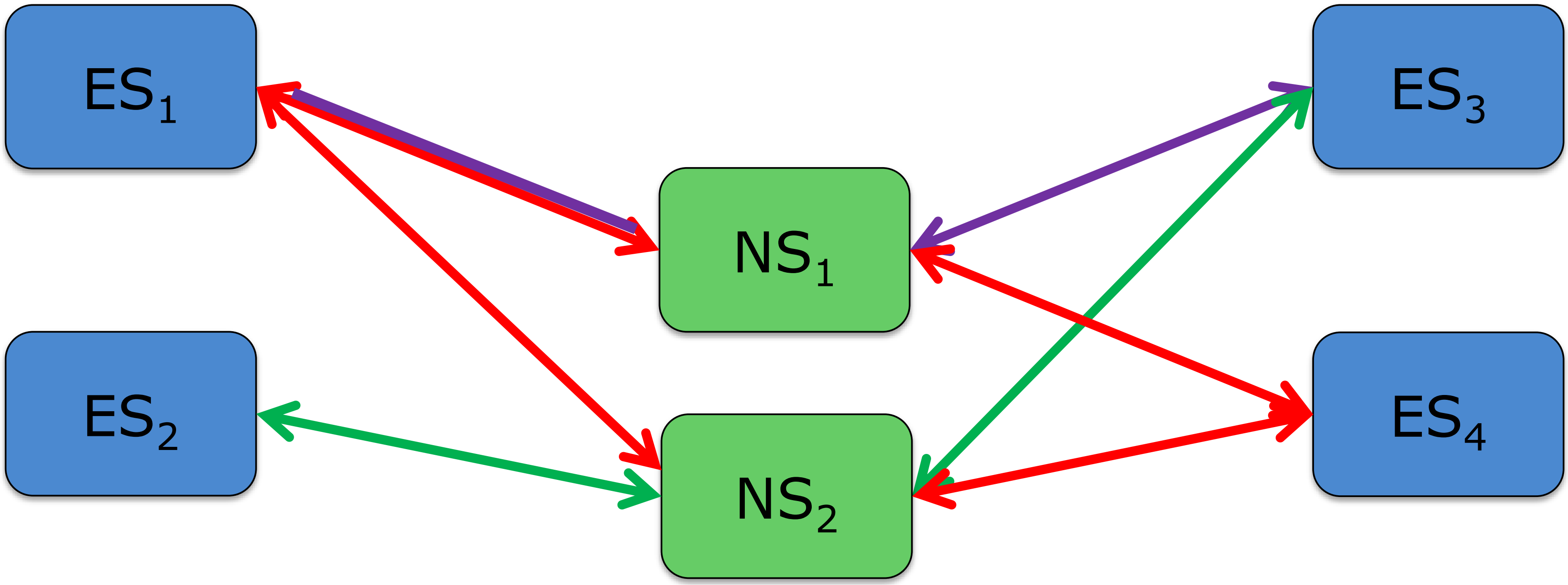


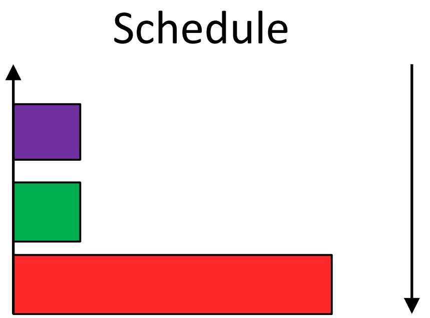


Cost = 100

- Fault-Tolerant
- But not schedulable

Solution





Cost = 110

- Fault-Tolerant
- And schedulable

Experimental evaluation

- Our method: Redundant Architecture Selection (RAS)
- Baseline solution: Straightforward Solution (SS)
  - Introduces redundancy naively, where needed
  - SS is a solution which can be obtained by a good engineer without the help of our optimization tool
- Two test cases:
  - A synthetic example
  - Orion Crew Exploration Vehicle (CEV), a realistic larger test case

Name	ESes	RC msgs.	No. NSes		No. links		Running Time	$Cost(\Upsilon)$		Schedulable	
			SS	RAS	SS	RAS		SS	RAS	SS	RAS
Synthetic test case	8	20	6	5	58	49	8 min 30 s	700	590	no	yes
Orion CEV	30	30	24	19	232	86	9 h 25 min 80 s	2,800	1,240	no	yes

Summary and message

- Safety-critical systems are becoming more networked
- Deterministic Ethernet solutions (such as TTEthernet) are emerging in safety-critical systems

- We were interested to derive a TTEthernet topology
  - Which has the level of redundancy specified by the designer
  - Is able to schedule all the application messages
  - Has the lowest cost
- We have proposed a Simulated Annealing-based approach

- **Message**: optimization tools are needed for the cost-effective introduction of redundancy in networked safety-critical systems