Istituto di Scienza e Tecnologie dell'Informazione “A. Faedo”
Software Engineering and Dependable Computing Laboratory

Dependability Analysis of UPS Architectures for the Italian Railway Signaling System

Giulio Masetti, Felicita Di Giandomenico, Silvano Chiaradonna
ISTI-CNR, Pisa
felicita.digiandomenico@isti.cnr.it
http://labsedc.isti.cnr.it

RSSRail 2023, Berlin
10-12 October 2023

Motivations and Context

- Railroad signalling systems are highly critical components
- Uninterruptable Power Supply Systems (UPS) are employed to ensure satisfaction of requested uptime capacity
- In turn, UPS becomes a critical component, typically developed adopting redundancy principles
- Supports to help designers/developers to take the right choices are very useful
- Model-based stochastic analysis is recognized as a powerful support to compare choices already at design time

Objective

Goal:

- To model and analyze different redundant UPS configurations for dependability assessment through stochastic model-based approaches

Useful to:

- Identification of critical components within a selected configuration
- Identification of the degree of needed redundancy for particularly critical components
- Comparison among different design choices

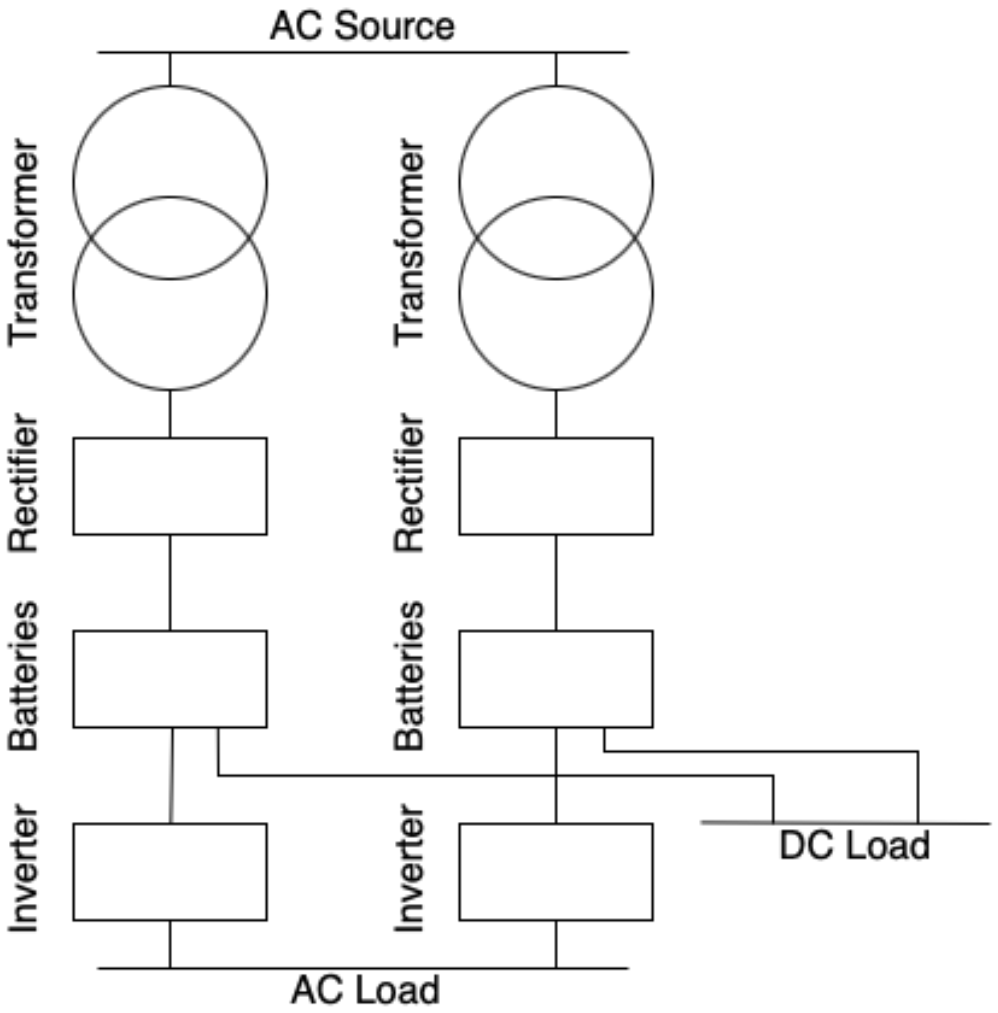
Focus on the Italian railway system

- Involvement in a National project
- Availability of useful documentation

Possible generalization:

- Expected (partial) reusability of the obtained results by railway operators in other countries
- ERA initiative

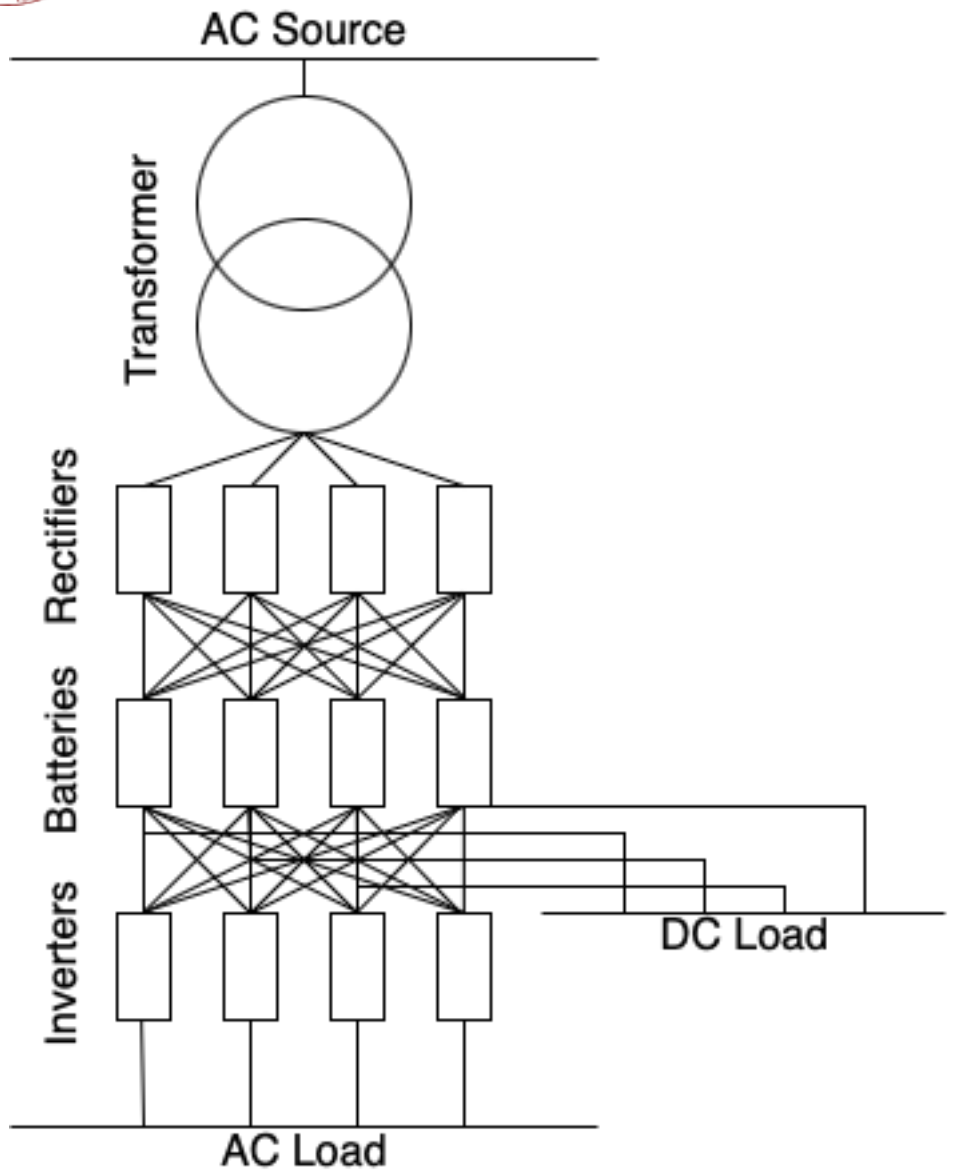
Redundant UPS Architecture: UPS_{SR}



- Currently adopted solution
- 2 Units in a primary- (hot) standby configuration
- Each unit can cover the entire load and includes:
  - a *transformer*,
  - a *rectifier*: to convert power from AC to DC and to recharge the battery
  - an *inverter*: to convert DC power from battery back to AC power for load use
  - a *battery bank*

In the analysis, only DC loads are considered (the inverter is not involved)

Redundant UPS Architecture: UPS_{CR}



- Proposed replacement of UPS_{SR}
- Higher modularity: each component (except the transformer) is replicated in a *n*+*m* configuration
  - *n* primary units
  - *m* standby units
  - full connection through smart switches between layers
- Each set of *n* primary units can cover the entire load – load is balanced among them
- In the figure, *n*=3 and *m*=1

In the analysis, only DC loads are considered (the inverters are not involved)

Assumptions

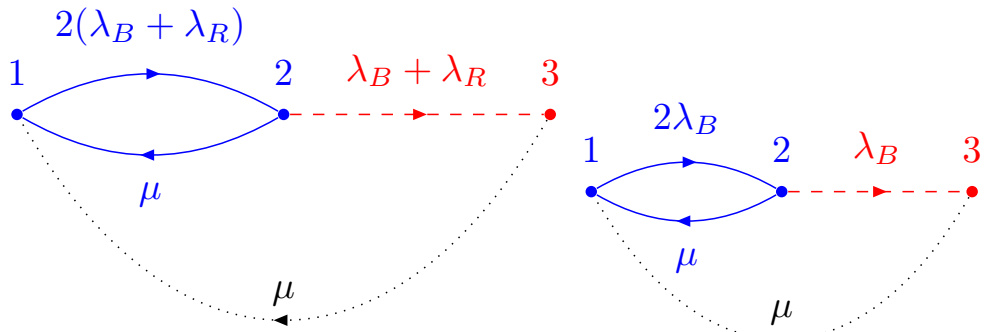
- Two operation modes for the UPS:
  - $\mathcal{N}$: AC source is working → rectifiers are in use and can fail
  - $\mathcal{C}$: AC source is not working →rectifiers are not in use and cannot fail
- Failure rates of components are exponentially distributed random variables with rates λ_R, λ_I, λ_B and λ_T
- Recovery time of a failed component is an exponentially distributed random variable with rate μ and does not depend on the number of failed components
- Failure model:
  - Failure rate of the transformer is negligible
  - Component failure rate accounts for both hardware and related control sw
  - Component failure rate does not depend on load and is statistically independent
  - UPS fails when no backup is left and the primary is failed, or the delivered QoS is not satisfactory

Measures of interest

4 metrics representative of the reliability and availability of UPS_{SR} and UPS_{CR}

- MTTF: average time the UPS operates before it fails
- A_{SS}: steady state UPS Availability
- MTBF: UPS expected operating time between two consecutive failures
- $\mathcal{I}_{MTBF}$: percentage of improvement in MTBF of UPS_{CR} with respect to UPS_{SR}

UPS_{SR} Model



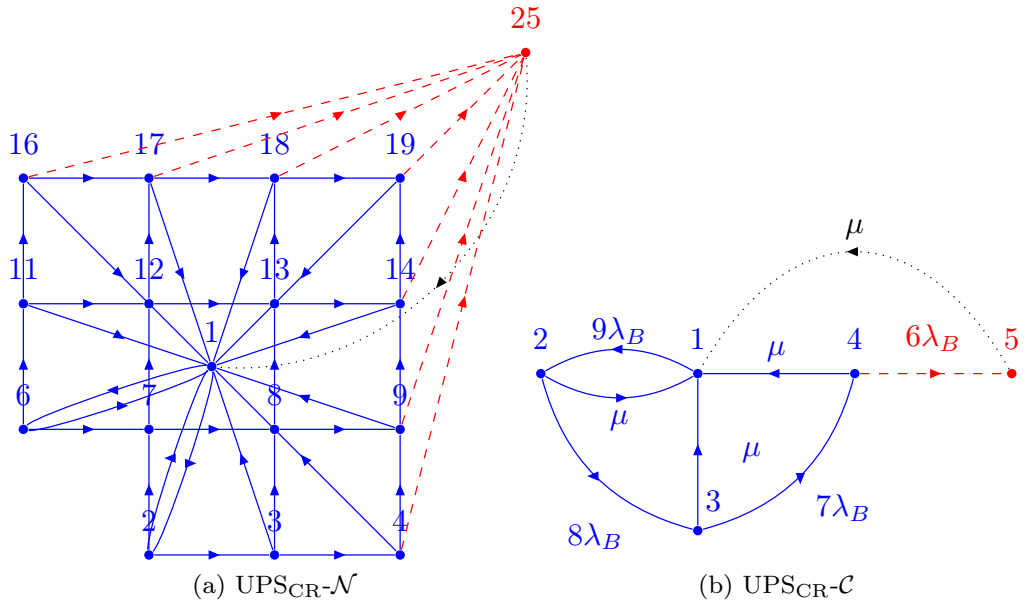
(a) UPS_{SR}-$\mathcal{N}$ (b) UPS_{SR}-$\mathcal{C}$

Simple Markov Chain for the two UPS operational modes: normal ($UPS_{SR\text{-}\mathcal{N}}$) and critical ($UPS_{SR\text{-}\mathcal{C}}$)

State 3 represents the failure of the UPS; to study the system availability, the recovery from state 3 is also considered

Only DC loads are considered → extension to AC loads implies inclusion of λ_I for inverters

UPS_{CR} Model



(a) UPS_{CR}-$\mathcal{N}$ (b) UPS_{CR}-$\mathcal{C}$

Markov Chain instantiated for n=6, m=3

(b): *C* mode → only batteries:

- in each state *i*, there are (n+m-i+1) working batteries;
- overall (m+2) states;
- transition rate from *i* to (*i+1*) is: (n+m-i+1) * λ_B

(a):

- includes both the layer of Rectifiers and the layer of Batteries (full connection pattern)
- all relevant dependencies represented through the Kronecker algebra
- more complex transition rates - refer to the paper for more details

Limited to DC loads – extension to AC loads implies an additional Kronecker sum to account for Inverters

Evaluation: Settings for the comparison

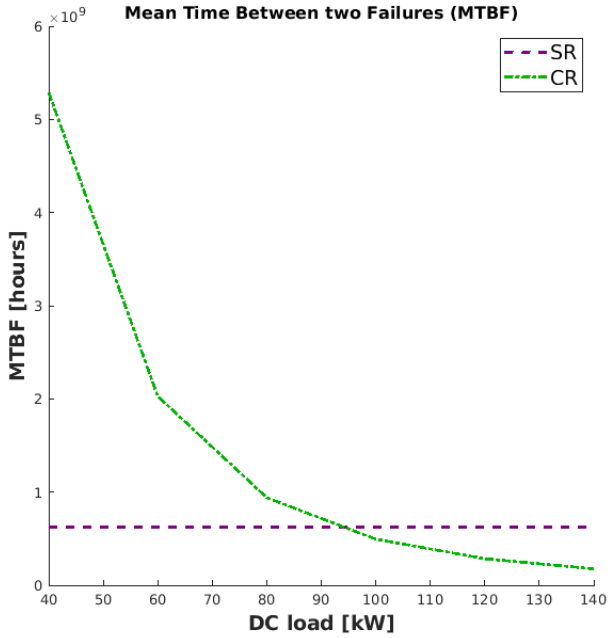
Parameters setting for the comparison between UPS_{SR} and UPS_{CR} (default values):

- DC load $\mathcal{L}$ constant over time; $\mathcal{L}$=100 kW
- n= [$\mathcal{L}/\ell_m$] (where ℓ_m is the load per module) = 10
- m=3
- μ= 0.5 h^{-1}
- $\lambda_B^{UPS\_SR}$ = 11.76 * 10^{-6} h^{-1}
- $\lambda_B^{UPS\_CR}$ = r * $\lambda_B^{UPS\_SR}$
- $\lambda_R^{UPS\_SR}$ = 16.6 * 10^{-6} h^{-1}
- $\lambda_R^{UPS\_CR}$ = r * $\lambda_R^{UPS\_SR}$

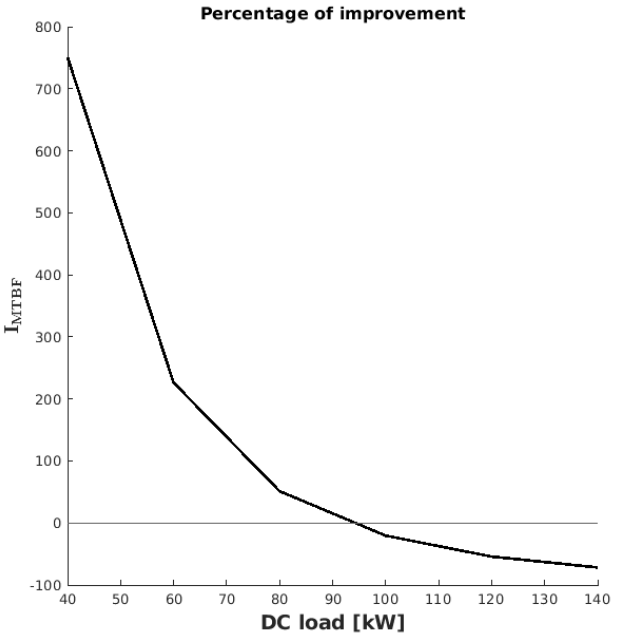
Where r is a multiplicative factor to account for the higher failure rate of UPS_{CR} components, because of the resulting higher complexity due to:

i) miniaturization of components
ii) presence of switching mechanisms to isolate/activate redundant modules

Evaluation: MTBF at increasing of load



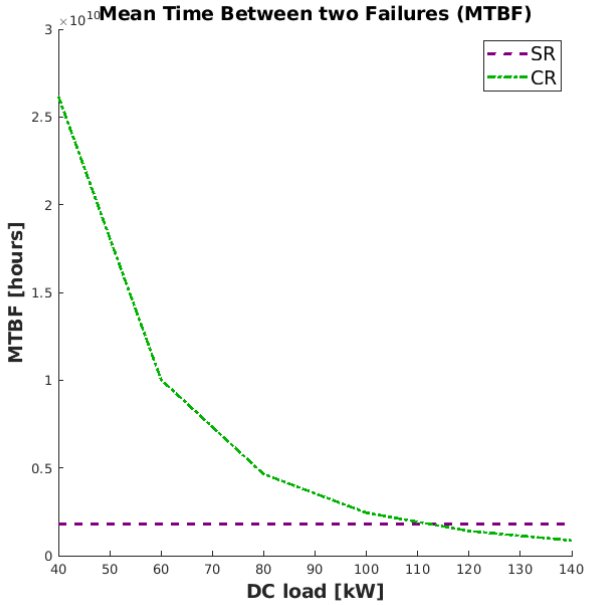
Nominal case $\mathcal{N}$
$40 <= \mathcal{L} <= 140$
$r = 17$



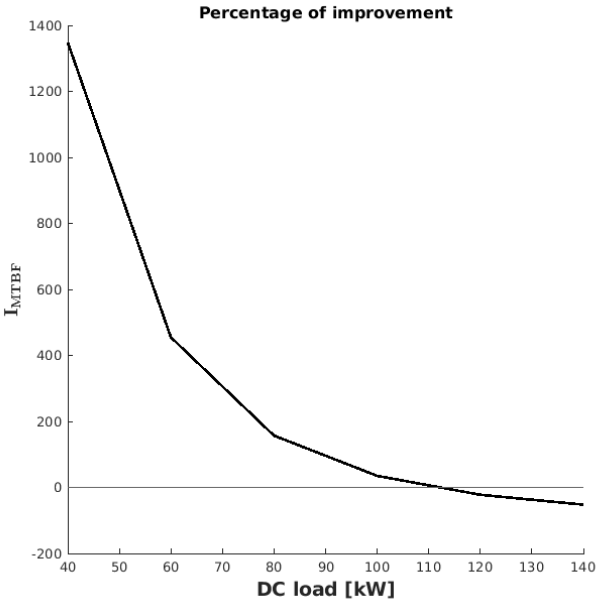
- MTBF of UPS_{SR} is constant, as expected since the active unit covers the entire load for all values considered
- MTBF of UPS_{CR} decreases, since the number of needed units *n* increases at increasing the load, while *m* remains constant

- $\mathcal{I}_{MTBF}$ decreases as $\mathcal{L}$ increases
- Around $\mathcal{L}$=95 kW, MTBF of UPS_{SR} becomes better than MTBF of UPS_{CR}

Evaluation: MTBF at increasing of load



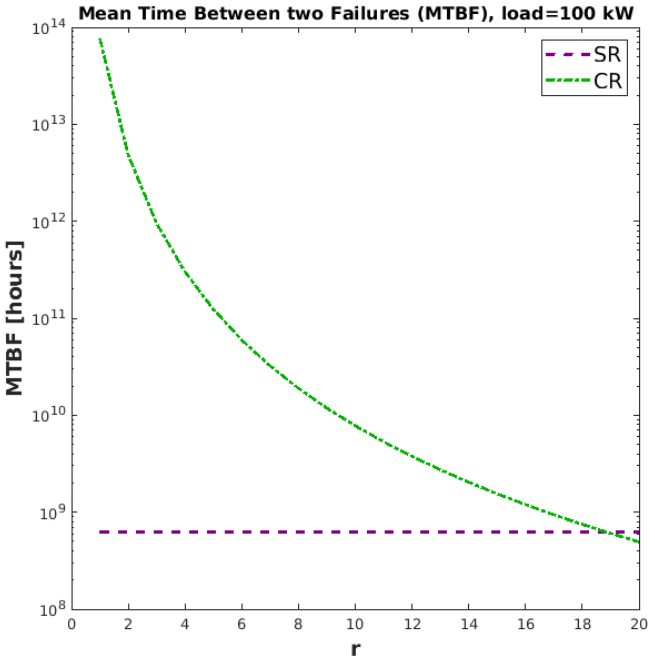
Critical case $\mathcal{C}$
$40 <= \mathcal{L} <= 140$
$r = 17$



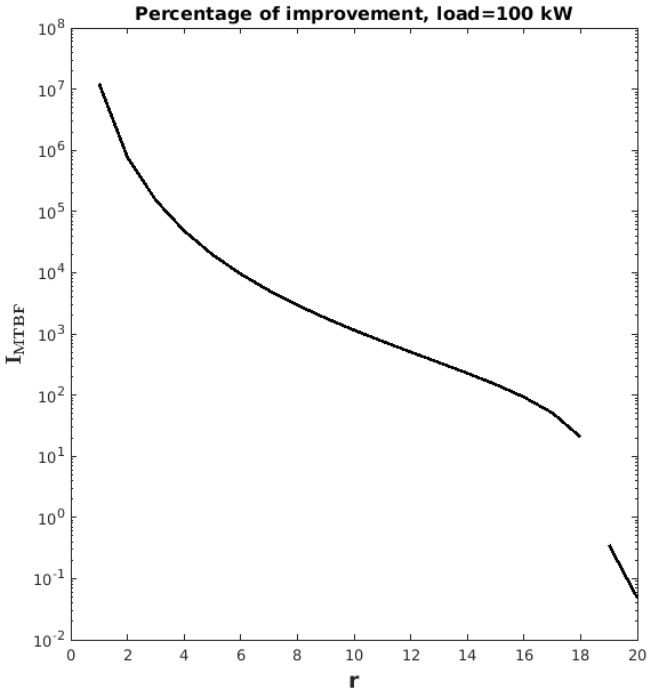
- Same trend as for the operation mode $\mathcal{N}$
- In absolute values, MTBF improves for both architectures, since less components are used

- $\mathcal{I}_{\text{MTBF}}$ in mode $\mathcal{C}$ has the same trend as in mode $\mathcal{N}$
- Values of $\mathcal{I}_{\text{MTBF}}$ in mode $\mathcal{C}$ is higher than the corresponding ones in $\mathcal{N}$ mode → less units can fail since rectifiers are not used

Evaluation: MTBF at increasing of r



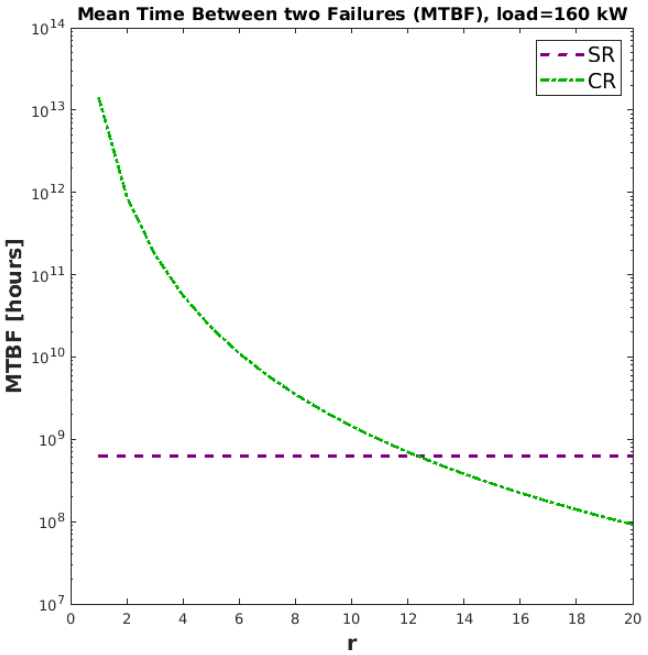
Nominal case $\mathcal{N}$
$\mathcal{L}$=100 kW
1<= r <=20



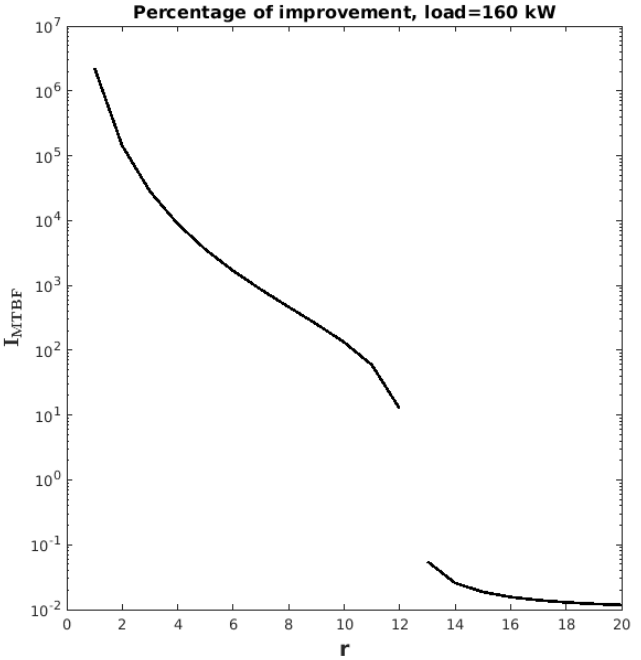
- UPS_{SR} does not depend on $\mathcal{L}$ or r → its MTBF remains constant
- MTBF of UPS_{CR} decreases at increasing of r since the failure rate of components increases

- $\mathcal{I}_{MTBF}$ has the same trend as MTBF
- For r < 19, UPS_{CR} has better reliability than UPS_{SR}
- High sensitivity to r (several orders of magnitude on the Y-axis)

Evaluation: MTBF at increasing of r



Nominal case $\mathcal{N}$
$\mathcal{L}$=160 kW
1<= r <=20



- UPS_{SR} does not depend on $\mathcal{L}$ or r → its MTBF does not change
- MTBF of UPS_{CR} decreases more rapidly, since the increased load requires more primary units (16), which can experience failure

- $\mathcal{I}_{MTBF}$ has the same trend as MTBF
- For r < 12, UPS_{CR} has better reliability than UPS_{SR}
- High sensitivity to r (several orders of magnitude on Y-axis)

Conclusions

- Reliability and Availability modeling and analysis of two UPS architectures in the railway domain
  - UPS_{SR}, which applies redundancy at system level
  - UPS_{CR}, which applies redundancy at component level
- Comparison of UPS_{SR} and UPS_{CR} in terms of MTBF and percentage of MTBF improvement
- The model parameters allow to set-up a variety of scenarios, representing different usage conditions, where to assess the performance of the two architectures
- Conducted experiments at varying the failure rate of involved components and the load to be satisfied allows to appreciate the pros and cons of the two architectures from the dependability perspective
- First results, although under some simplistic assumptions, show that UPS_{CR} should be preferred, unless the failure rate of its components becomes very high compared to those of UPS_{SR}
- Developed models available at:
  - https://gitea-s2i2s.isti.cnr.it/gmasetti/CompareSRandCRinRailwaySignalingUPS.git

Future Work

Several interesting directions – among short term advancements:

- Extend the modeling and analysis by fully considering AC loads
- Introduce the possibility of variable loads
- Focus on the analysis of energy consumption
  - Preliminary considerations are in favour of UPS_{CR} – only 1 transformer instead of the 2 in the UPS_{SR} configuration
  - Transformers are the major source of power waste (4% of the transformed power in heat)

Thanks for your attention!

Questions?