CentraleSupélec
université PARIS-SACLAY

orange™

Modeling the impact of information sharing on failure propagation in a network of interdependent critical cyber-physical systems

Khaled Sayad

Orange Innovation Networks- CentraleSupélec/Université Paris Saclay

Co-supervised by :

- *Benoît Lemoine (Orange Innovation Networks)*
- *Anne Barros, Yiping Fang, Zhiguo Zeng (CentraleSupélec, Université Paris Saclay)*

November 17th, 2022

Chaire RRSC - Journée scientifique à *CentraleSupélec*

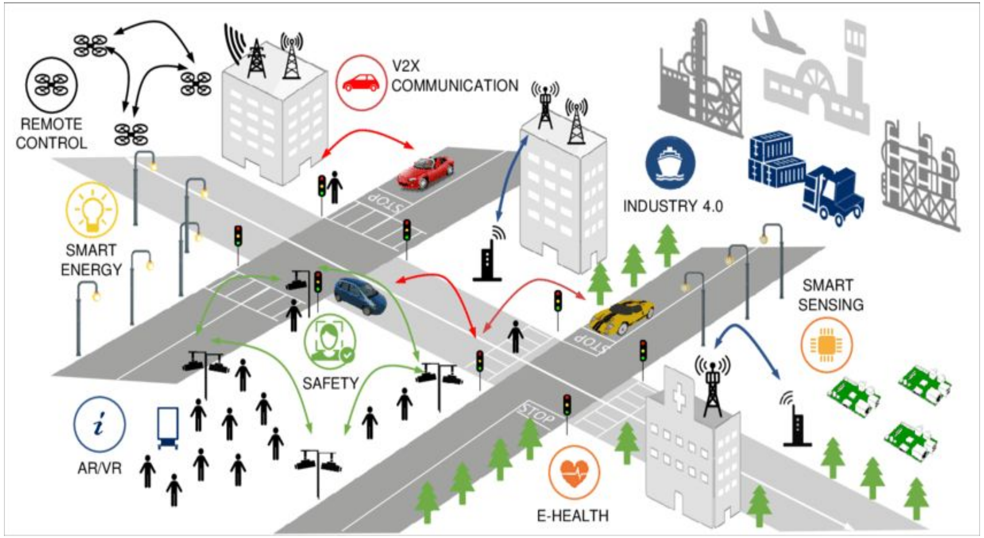
Outline

Introduction

Smart grid, **intelligent transportation systems (ITS), and industrial internet of things (IIOT)** are examples of 5G-enabled CIs which are highly dependent on the information and communication technology (ICT) infrastructure.

These systems constitute a network of **interdependent critical cyber-physical systems (CCPSs).**

Due to **strong interdependencies,** a failure in one CCPS **propagates** to dependent CCPSs and cause a large-scale interruption of critical services, resulting in a huge socio-economic impact.

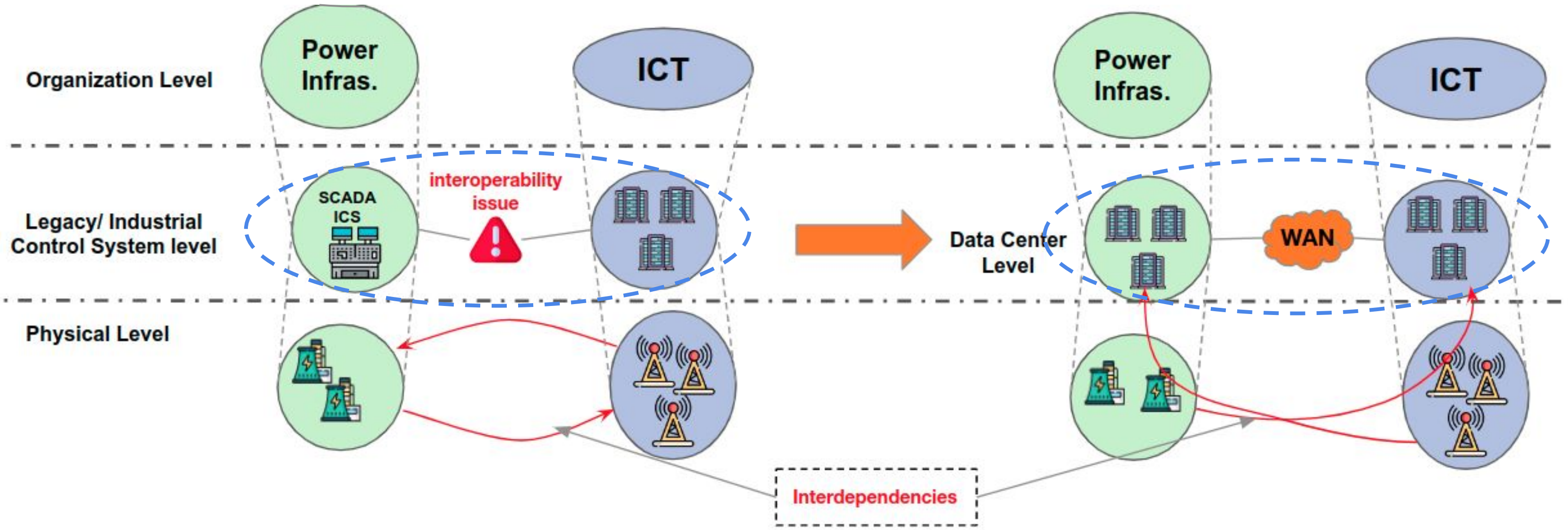


Picture from : Zanzi, Lanfranco & al .(2019). **Evolving Multi-Access Edge Computing to Support Enhanced IoT Deployments.** IEEE Communications Standards Magazine. 3. 26-34.

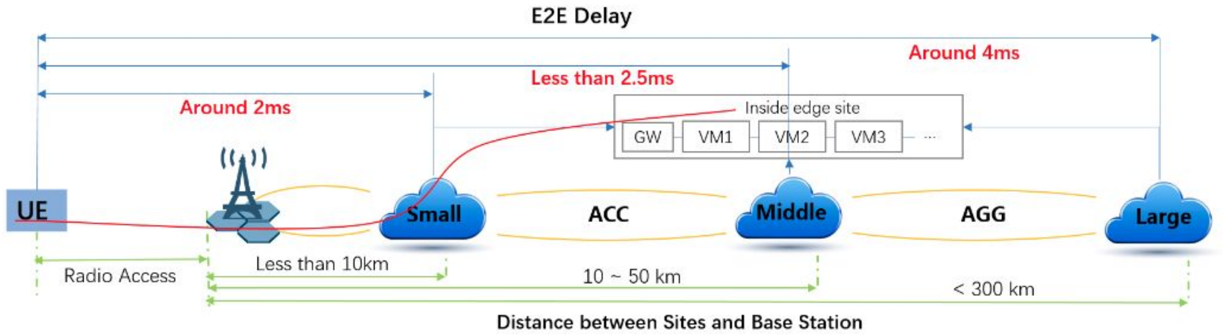
Introduction

Edge data center networking represent a promising alternative to legacy SCADA systems in terms of cost-effectiveness, flexibility and **interoperability.**

The **homogeneity** at the DC level offers **new opportunities** to mitigate failure propagation in interdependent CCPS networks**.**

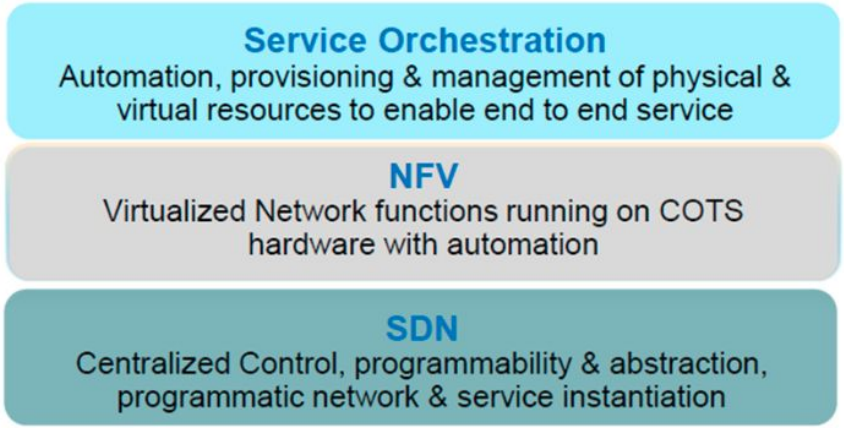


Introduction



Network function virtualization (NFV) : an approach combining software, virtualization and networking technologies used to deliver high performance computing platforms built on COTS hardware**.**

Software defined networking (SDN) : a paradigm that enables network programmability by splitting the control and data plan.

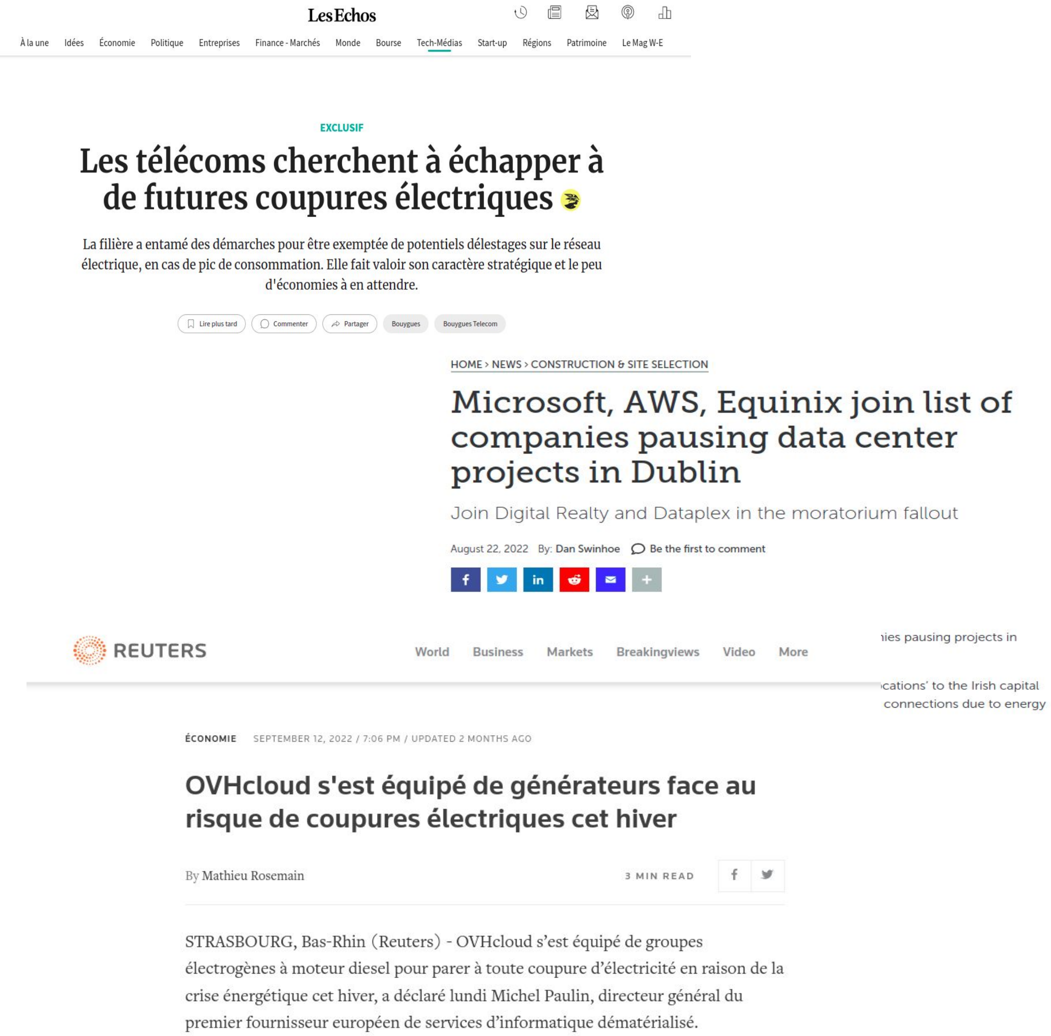


https://opnfv-edgecloud.readthedocs.io/en/stable-gambia/development/requirements/requirements.html#

ETSI - GS NFV 002 - V1.2.1 - Network Functions Virtualisation (NFV); Architectural Framework

Problem statement

- Increased vulnerability to cyber-risks as a result of the massive softwarization.
- Increased impact of interdependencies and vulnerability of the telecom infrastructure.
- Increased capital expenditures (CapEx) to build the softwarized data center (DC) network.
- Strict regulations prohibits to host critical services in public clouds operated by non european actors.



Les Echos

À la une Idées Économie Politique Entreprises Finance - Marchés Monde Bourse Tech-Médias Start-up Régions Patrimoine Le Mag W-E

EXCLUSIF

Les télécoms cherchent à échapper à de futures coupures électriques

La filière a entamé des démarches pour être exemptée de potentiels délestages sur le réseau électrique, en cas de pic de consommation. Elle fait valoir son caractère stratégique et le peu d'économies à en attendre.

Lire plus tard Commenter Partager Bouygues Bouygues Telecom

HOME > NEWS > CONSTRUCTION & SITE SELECTION

Microsoft, AWS, Equinix join list of companies pausing data center projects in Dublin

Join Digital Realty and Dataplex in the moratorium fallout

August 22, 2022 By: Dan Swinhoe Be the first to comment

REUTERS World Business Markets Breakingviews Video More

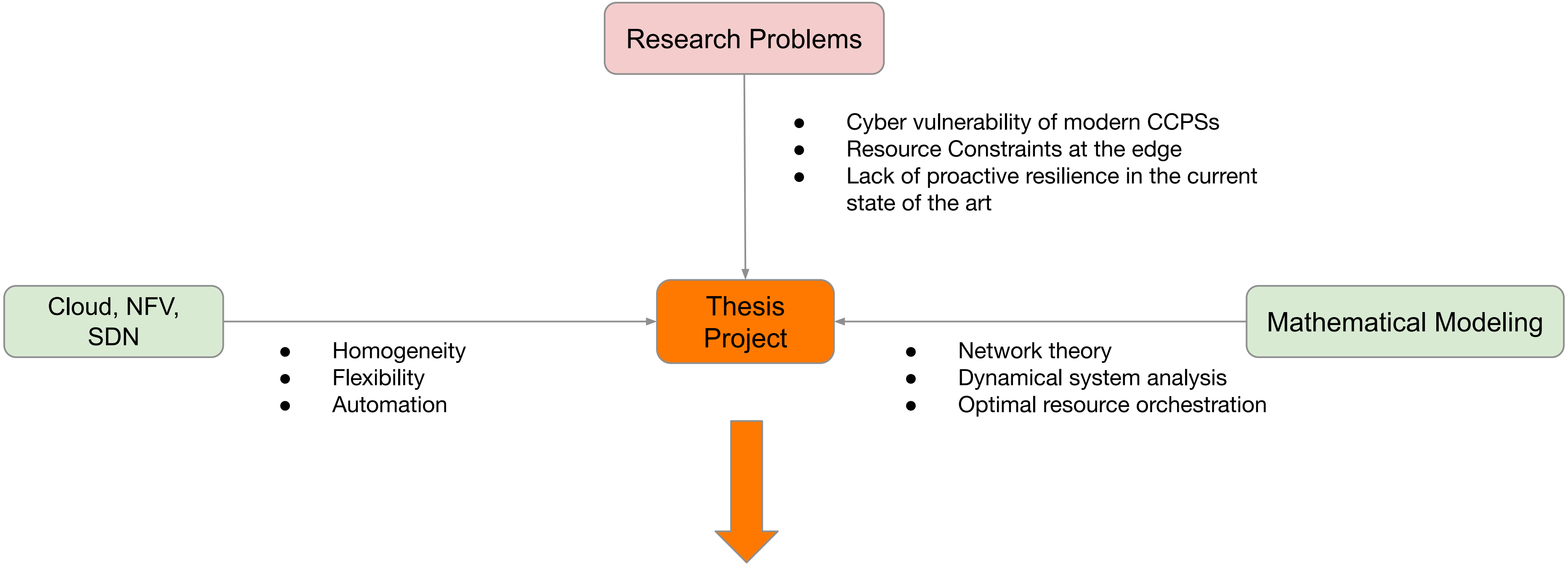
ÉCONOMIE SEPTEMBER 12, 2022 / 7:06 PM / UPDATED 2 MONTHS AGO

OVHcloud s'est équipé de générateurs face au risque de coupures électriques cet hiver

By Mathieu Rosemain 3 MIN READ

STRASBOURG, Bas-Rhin (Reuters) - OVHcloud s'est équipé de groupes électrogènes à moteur diesel pour parer à toute coupure d'électricité en raison de la crise énergétique cet hiver, a déclaré lundi Michel Paulin, directeur général du premier fournisseur européen de services d'informatique dématérialisé.

Thesis overview and roadmap



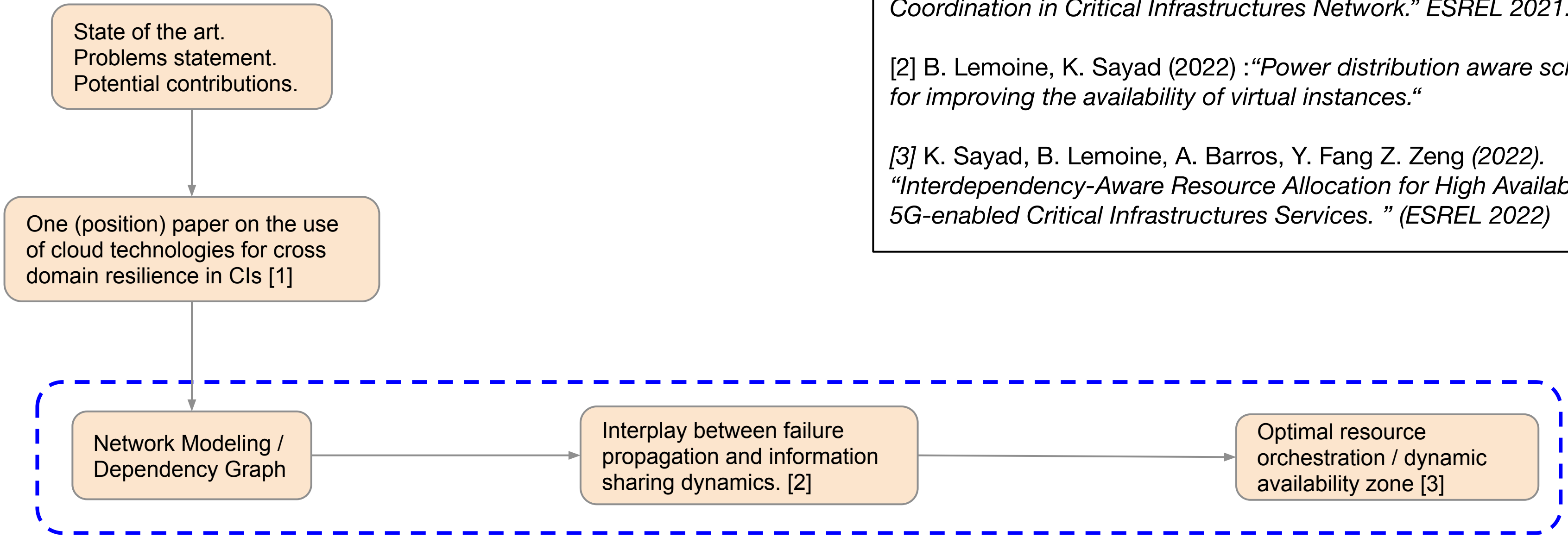
Enabling cross-domain and proactive resilience based on optimal resource sharing in CCPSsv network

Thesis overview and roadmap

[1] K. Sayad, B. Lemoine, A. Barros, Y. Fang Z. Zeng (2021). "*Dynamic Orchestration of Communication Resources Deployment for Resilient Coordination in Critical Infrastructures Network." ESREL 2021.*

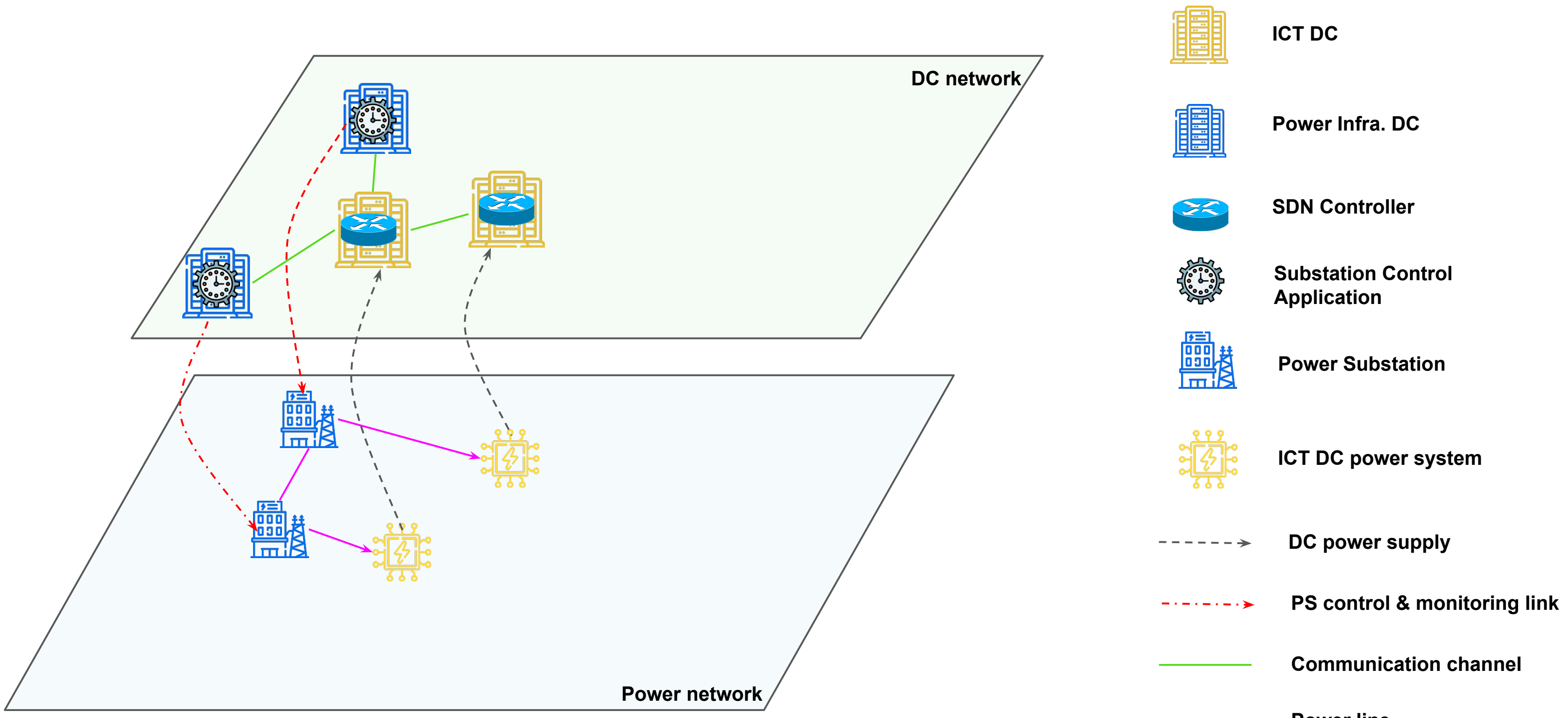
[2] B. Lemoine, K. Sayad (2022) :*"Power distribution aware scheduling for improving the availability of virtual instances."*

[3] K. Sayad, B. Lemoine, A. Barros, Y. Fang Z. Zeng *(2022). "Interdependency-Aware Resource Allocation for High Availability of 5G-enabled Critical Infrastructures Services. " (ESREL 2022)*



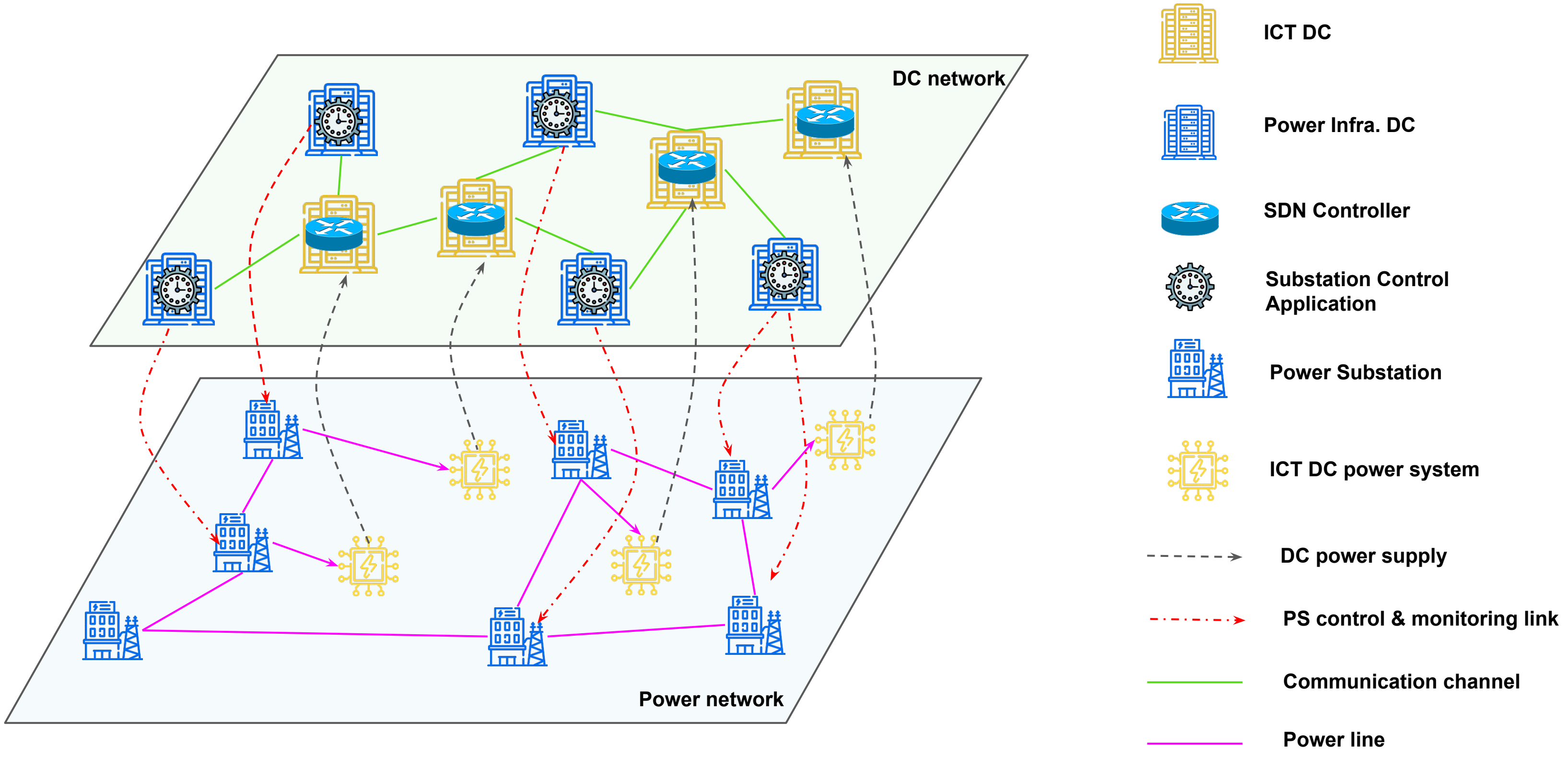
Network modeling

We focus on the interdependencies between the ICT and power infrastructure. A two interdependent networks model is proposed :



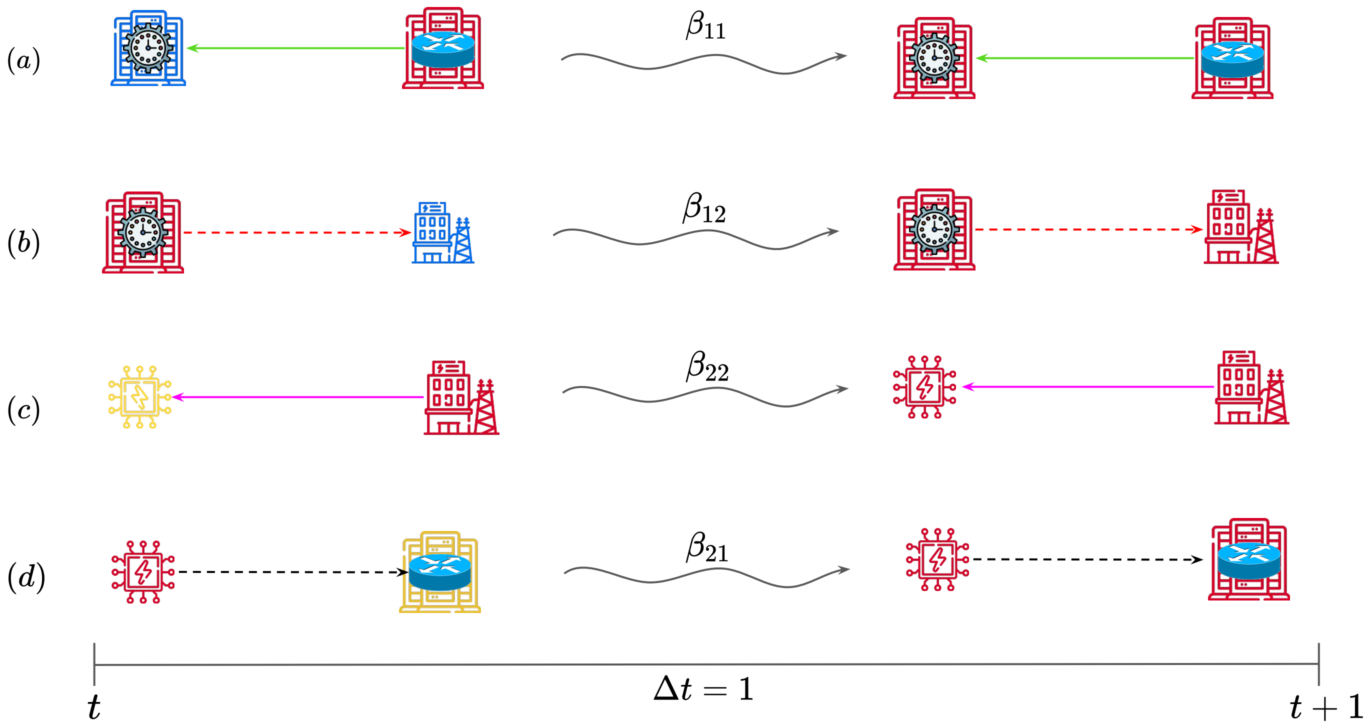
Network modeling

We focus on the interdependencies between the ICT and power infrastructure. A two interdependent networks model is proposed :



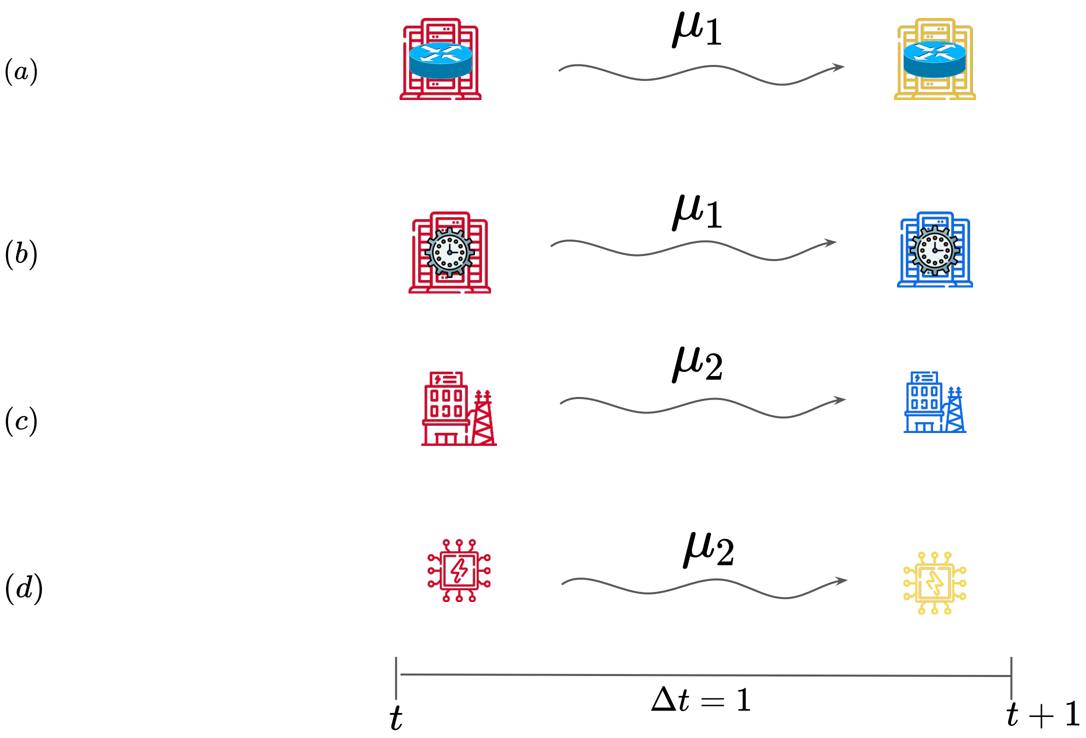
Interplay between information sharing and failure propagation

We consider failure propagation processes through the 4 types of links we consider in our model. A node transmits failure to its neighbor at different rates per unit of time. We define $\{\beta_{ij}\}_{(i,j)\in\{1,2\}\times\{1,2\}}$ as failure propagation rates.



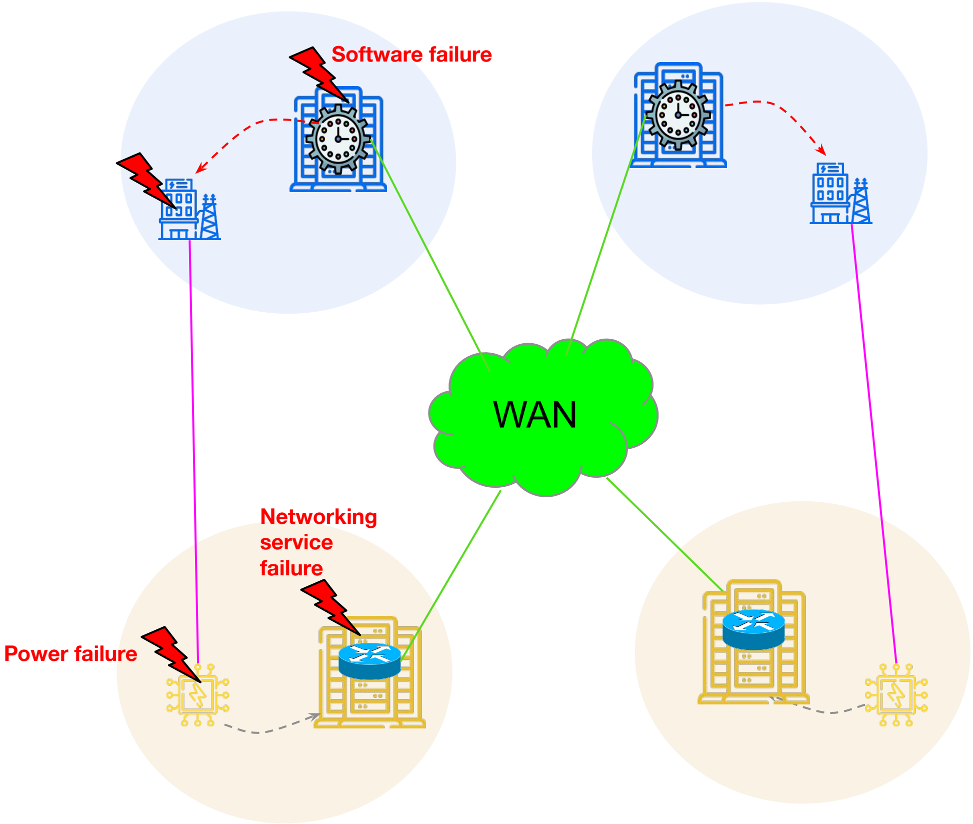
Interplay between information sharing and failure propagation

Recovery process is assumed to happen independently at each node with different rates depending on the node type: μ_1 and μ_2 are the recovery rates in the DC and power domains respectively.



1.Failure propagation

If the service is the monitoring VNF of the power substation, then the energy generation will be disrupted, impacting dependent DC3 in the ICT domain.

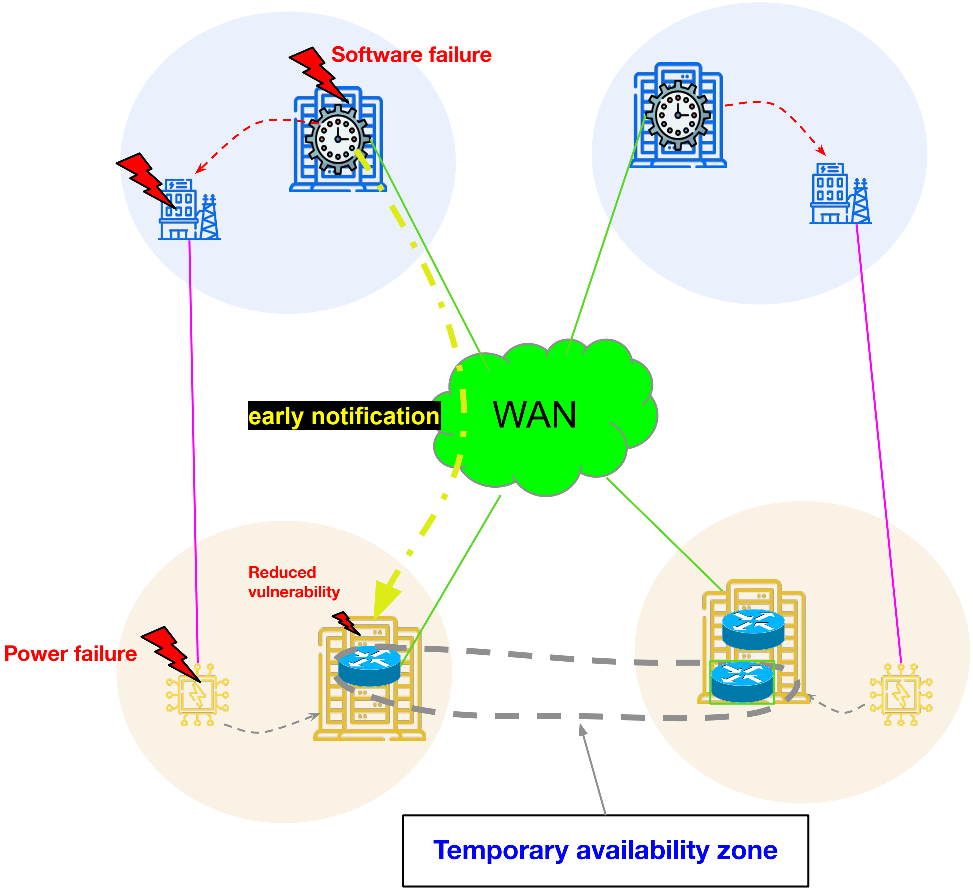


2.Awareness propagation

We assume that availability informations can be shared via the management links (in green).

Information sharing process is random. It depends on whether a data sharing enabling VNF is deployed or not.

The DC manager decides when to deploy the VNF w.r.t. some risk indicator (to increase preparedness) or/and resource availability.

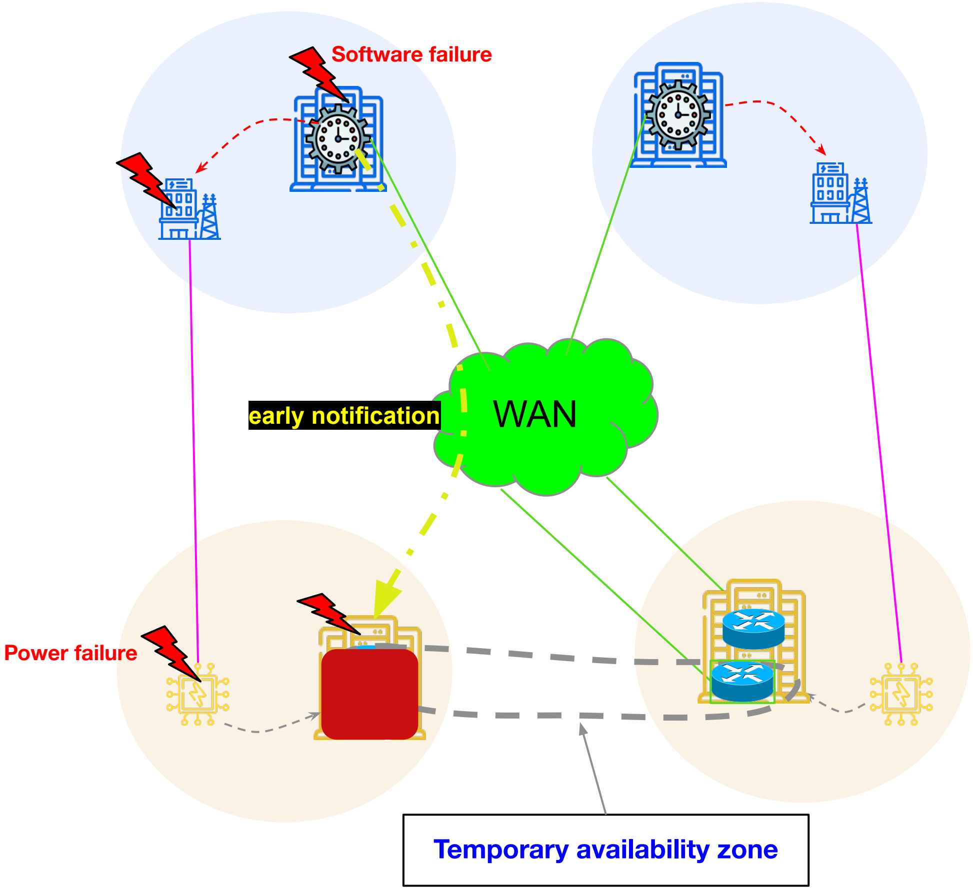


2.Awareness propagation

We assume that availability informations can be shared via the management links (in green).

Information sharing process is random. It depends on whether a data sharing enabling VNF is deployed or not.

The DC manager decides when to deploy the VNF w.r.t. some risk indicator (to increase preparedness) or/and resource availability.



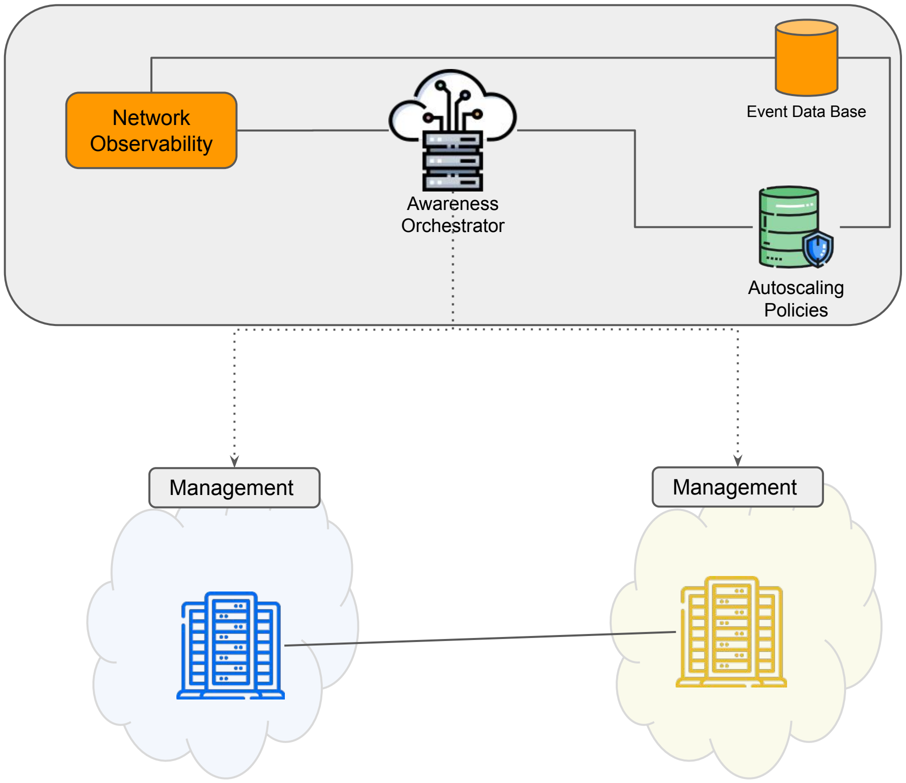
Interplay between information sharing and failure propagation

Proactive failure notification is crucial to ensure high service availability by adopting the right alert rules [1]

The ability to obtain additional resources rapidly increases the resiliency of VNFs [2].

An awareness orchestrator is charged with network observability and alert management. It notifies the management of a current disruption.

The management launches an auto-scaling mechanism to increase the redundancy of critical VNFs.



[1]https://cloud.google.com/architecture/devops/devops-measurement-proactive-failure-notification
[2] ETSI GS NFV-REL 001 V1.1.1 (2015-01) Network Functions Virtualisation (NFV); Resiliency Requirements

Optimal resource orchestration

The auto-scaling refers to the operation of increasing a service redundancy as a response to a risk indicator in a network of edge DCs, the process can be treated as an optimization problem.

Optimal resource orchestration

***Service migration problem* :** Given a set of services affected by the disruption of their host DC and a set of available DC hosts : find the optimal mapping $\mathcal{M} : K \times I \rightarrow J$ respecting capacity, latency and availability constraint.

Demand side parameters

Host side parameters

parameters	definition
I	Set of DCs subject to maintenance intervention.
K^i	Set of services impacted by the maintenance of DC $i \in I$
J	Set of available hosts DC
c_{ki}	Resource amount request of service $k \in K^i$
θ_{ki}	Maximum latency violation allowed for service k
A_{ki}	Availability requirement of service $k \in K^i$
f_j	The setup cost of a DC j (energy consumption, rack and servers installation related costs)
λ_j	Resource usage cost (generated from renting one unit computing resource in DC j)
κ_j	The total capacity available of the host DC j.
q_j	Failure probability of DC j
t_{ij}	Data transmission latency between two connected DC i and j

TABLE 1: Scheduling Model Parameters

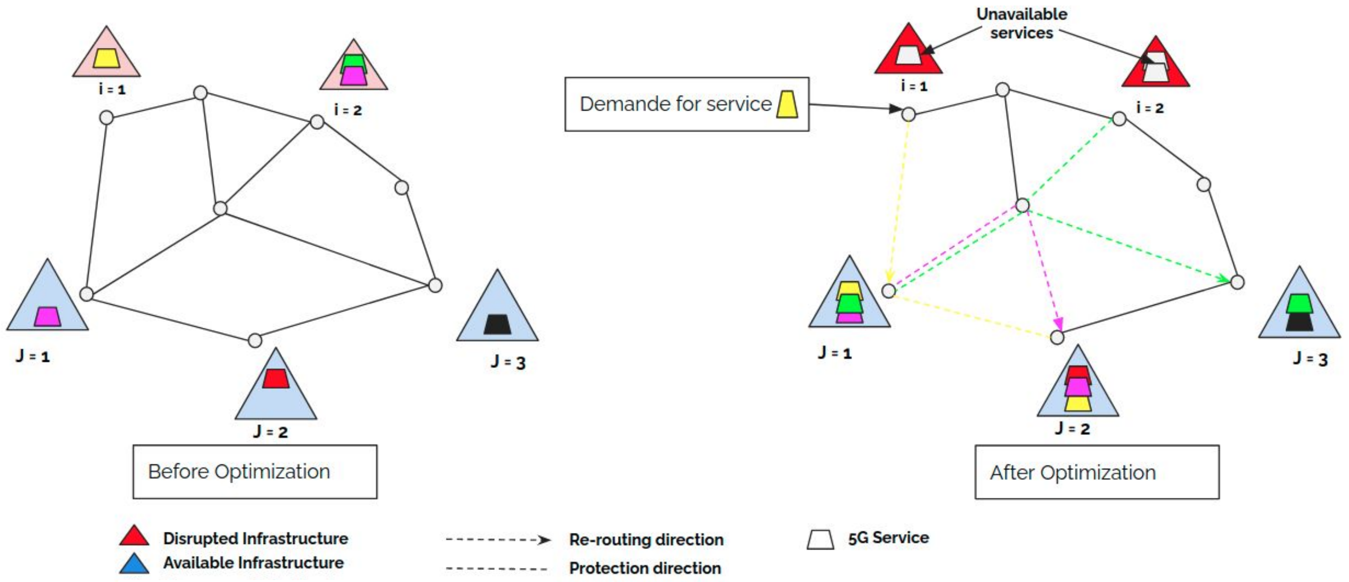
The decision is captured by the binary variables Y_{kijr}, with : $Y_{kijr} = \begin{cases} 1, & \text{if DC } j \text{ is chosen as } r^{th} \text{ backup for demand } (k, i) \\ 0, & \text{otherwise} \end{cases}$

Optimal resource orchestration

The service protection scheme is designed so that a service *(k,i)* is assigned to more than one DC, depending on its availability requirement. The service is running actively only in one DC *j* as *r* *th* backup and in standby mode in the other backups $m \in J/\{j\}$ $(Y_{kimx} = 1, x > r)$. We define the probability a migrated service is active in its *r* *th* backup :

$$\mathbb{P}_{kijr} = (1 - q_j) \sum_{m \in J/\{j\}} \frac{q_m}{1 - q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)}$$

$\mathbb{P}_{kijr}$ is a decision variable as it is a function of placement decision variable Y.



Optimal resource orchestration

Total expected migration cost

$$\min_{Y_{kijr}} \sum_{i \in I} \sum_{k \in K^i} \sum_{j \in J} \sum_{r=1}^{|J|} (f_j + c_{ki}\lambda_j \mathbb{P}_{kijr}) Y_{kijr}$$

$s.t$

Capacity Constraint

$$\sum_{r=1}^{|J|} \sum_{i \in I} \sum_{k \in K^i} c_{ki} Y_{kijr} \leq \kappa_j, \qquad \forall j \in J,$$

Latency Constraint

$$(\theta_{ki} - t_{ij}) Y_{kijr} \geq 0, \forall k \in K^i, i \in I, j \in J, \forall r$$

Migration Constraint

$$\sum_{j \in J} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, \forall r$$

$$\sum_{r=1}^{|J|} Y_{kijr} \leq 1, \forall k \in K^i, i \in I, j \in J$$

$$Y_{kijr} \leq Y_{kij(r-1)}, \forall k \in K^i, i \in I, j \in J, \forall r$$

$$\mathbb{P}_{kijr} = (1 - q_j) \sum_{m \in J/\{j\}} \frac{q_m}{1 - q_m} \mathbb{P}_{kim(r-1)} Y_{kim(r-1)}$$

Availability Constraint

$$\sum_{j \in J} \sum_{r=1}^{|J|} \mathbb{P}_{kijr} Y_{kijr} \geq A_{ki}, \forall k \in K^i, i \in I$$

$$Y_{kijr} \in \{0, 1\}, \forall k \in K^i, i \in I, j \in J, \forall r$$

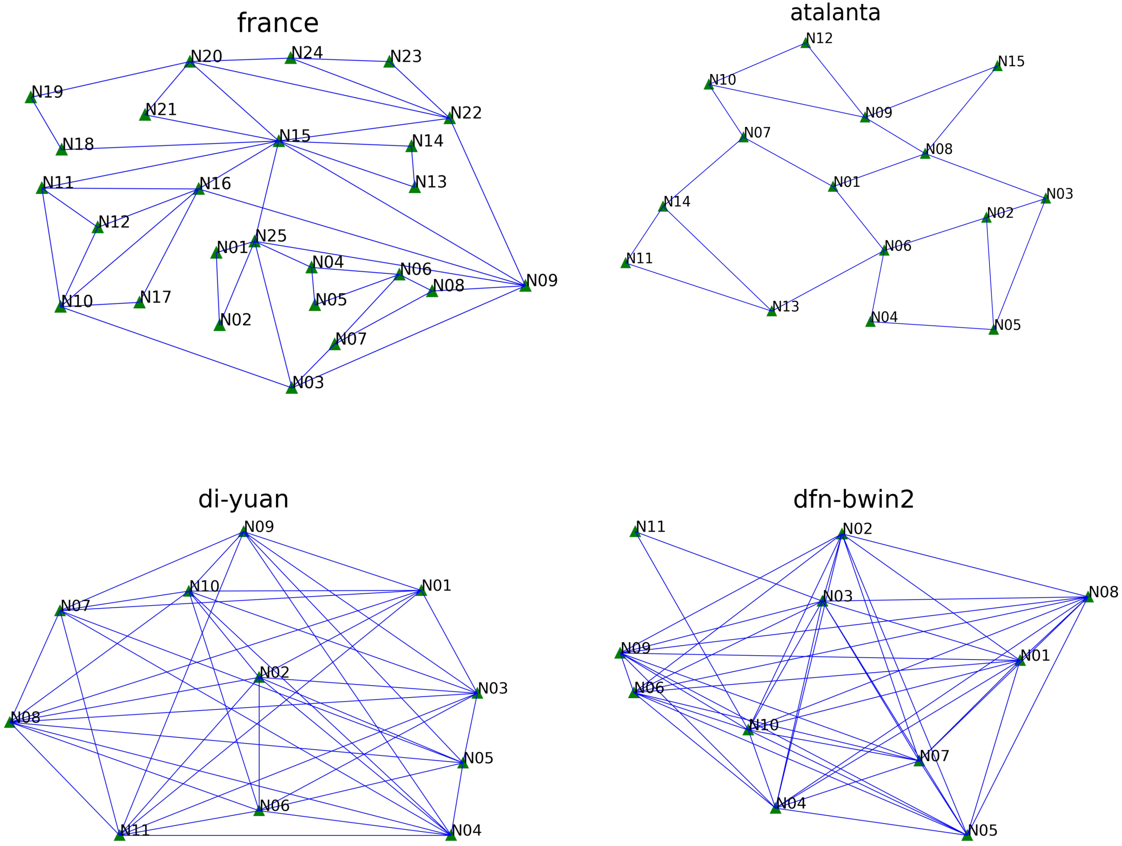
Optimal resource orchestration

We use 4 networks from Survivable Network Design (SND) library for simulation with the following characteristics:

(Av_ND : Average node degree)

Network	$\|V\|$	$\|E\|$	Av_ND
France	25	45	3.60
Cost 266	37	57	3.08
Atalanta	15	22	2.93
Di-yuan	11	42	7.64
Dfn-g	11	47	8.55

Orlowski, S. & Wessäly, R. & Pioro, Michal & Tomaszewski, Artur. (2009). **SNDlib 1.0—Survivable Network Design Library**. Networks. 55. 276 - 286. 10.1002/net.20371.

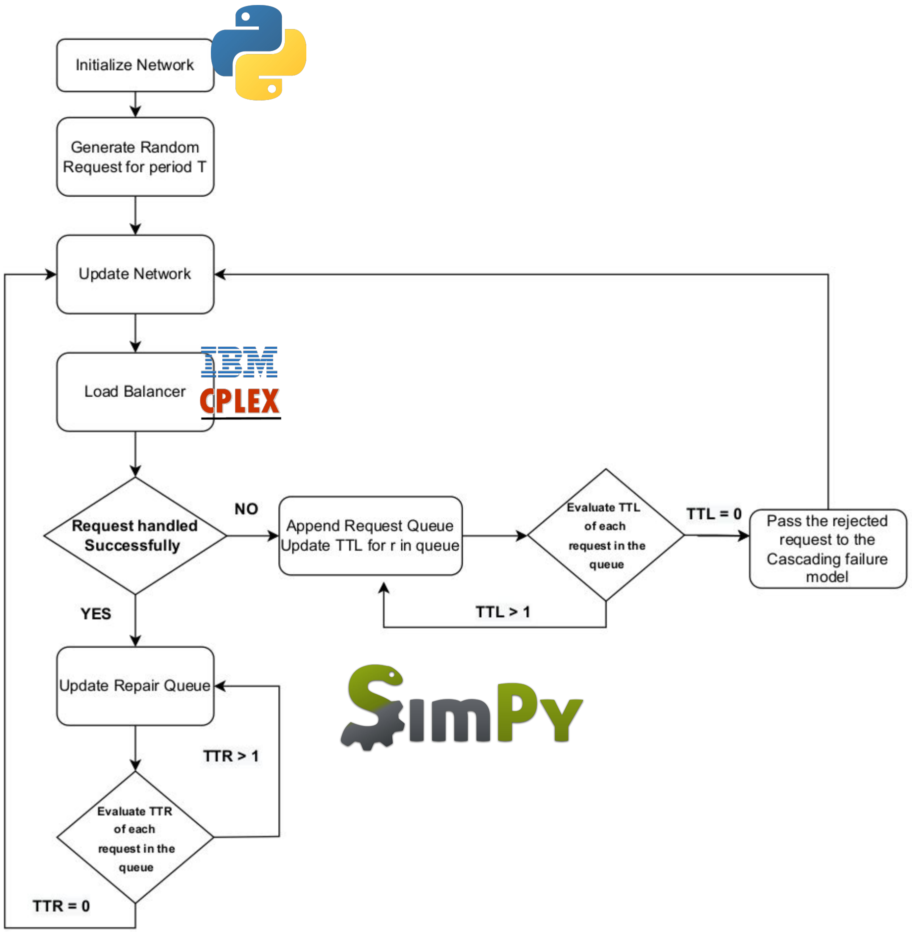


Simulations

Simulations were conducted on an Ubuntu 20.04 computer with 8 Intel i5/1.60 GHz CPU cores. The migration process programs were developed using Python programming language and CPLEX (2015) solver to implement the MILP model.

The objective of simulations is to study the rejection rate of consecutive requests with dynamic demand patterns (different parameters).

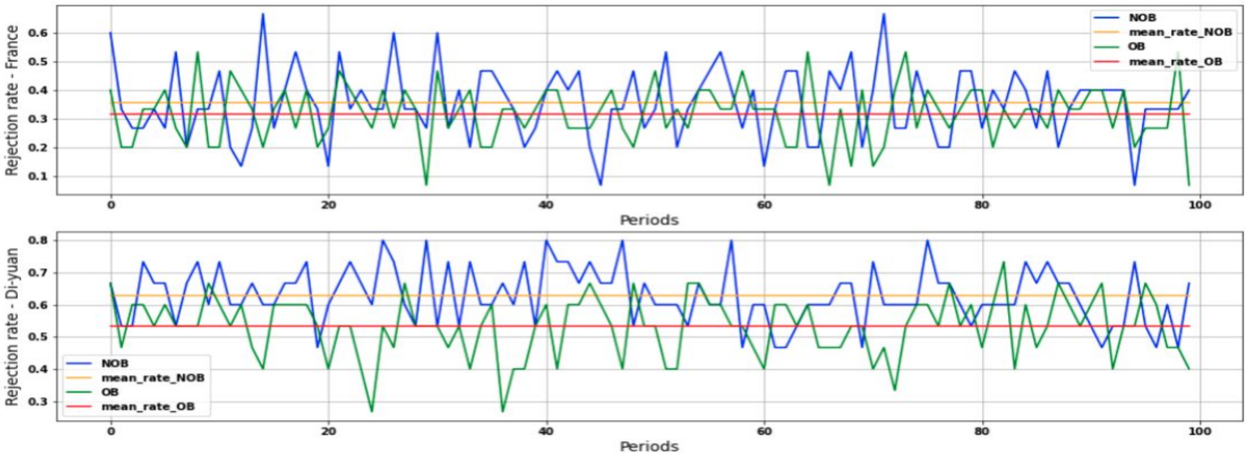
$$RR = \frac{\text{number of requests rejected}}{\text{total number of requests}}$$



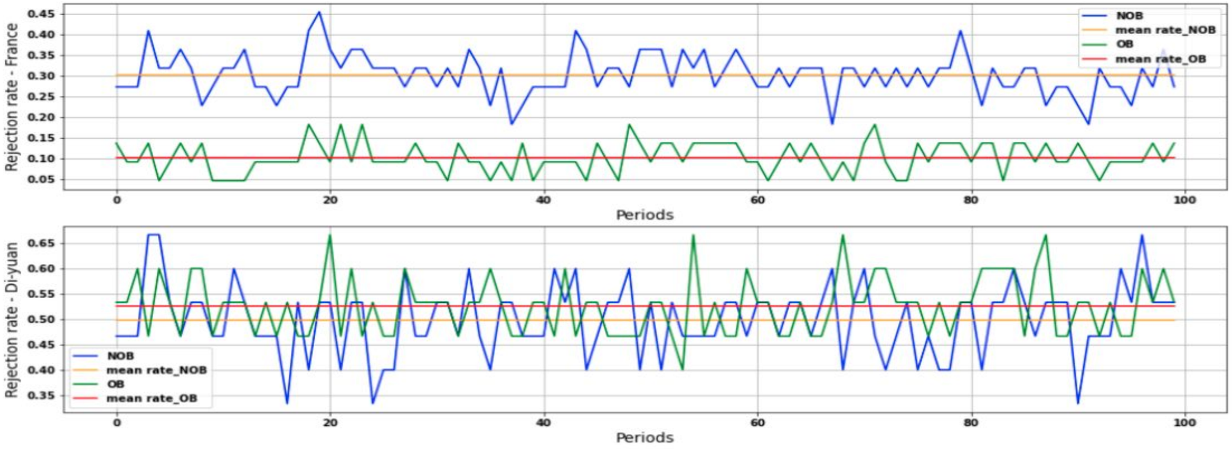
Results

The rejection rate drops when adopting a protection strategy compared to the ”No protection” setting.

The drop is more important in the France network compared to the Di-yuan network when adopting an overbooking strategy.



(a) The rejection rate dynamics in a ”No Protection Setting”



(b) The rejection rate dynamics in a ”Protection Setting”

Results

Table 4.: Simulation results - No Protection Setting

Network	$Mean(RR_{NOB})$	$Std(RR_{NOB})$	IN_{NOB}	$Mean(RR_{OB})$	$Std(RR_{OB})$	IN_{OB}
France	0.319	0.046	0.197	0.200	0.040	0.134
Cost266	0.100	0.020	0.064	0.085	0.020	0.060
Atalanta	0.391	0.063	0.269	0.352	0.033	0.240
Di-yuan	0.612	0.071	0.503	0.571	0.074	0.477
Dfn-g	0.396	0.073	0.366	0.312	0.062	0.296

Table 5.: Simulation results - Protection setting

Network	$Mean(RR_{NOB})$	$Std(RR_{NOB})$	IN_{NOB}	$Mean(RR_{OB})$	$Std(RR_{OB})$	IN_{OB}
France	0.303	0.050	0.170	0.110	0.037	0.072
Cost266	0.0759	0.023	0.050	0.070	0.021	0.047
Atalanta	0.381	0.077	0.247	0.332	0.074	0.222
Di-yuan	0.499	0.070	0.372	0.525	0.057	0.375
Dfn-g	0.473	0.057	0.368	0.426	0.069	0.320

The drop in rejection rate differs depending on topology characteristics. In networks with a low number of nodes and high average node degree (Di-yuan and Dfn-g), the decrease in rejection and contagion rates is less visible compared to larger networks. In addition, the adoption of a protection scheme in these networks is irrelevant as all the nodes have the same criticality value.

Conclusion & Perspectives

- A dynamic model for failure propagation and awareness spreading in a network of interdependent critical cyber-physical systems will be used to design effective, cross-domain resilience.

- Study the impact of distributing power control applications in edge DCs <=> study the topological characteristics of the interconnected networks model.

- In perspective:

    - Optimal allocation of redundancy resources for effective cross domain resilience.

    - Propose a protocol for information sharing at the DC level.

Thanks

Khaled SAYAD
Orange Innovation Networks
CentraleSupélec - Université Paris Saclay

khaled.sayad@orange.com