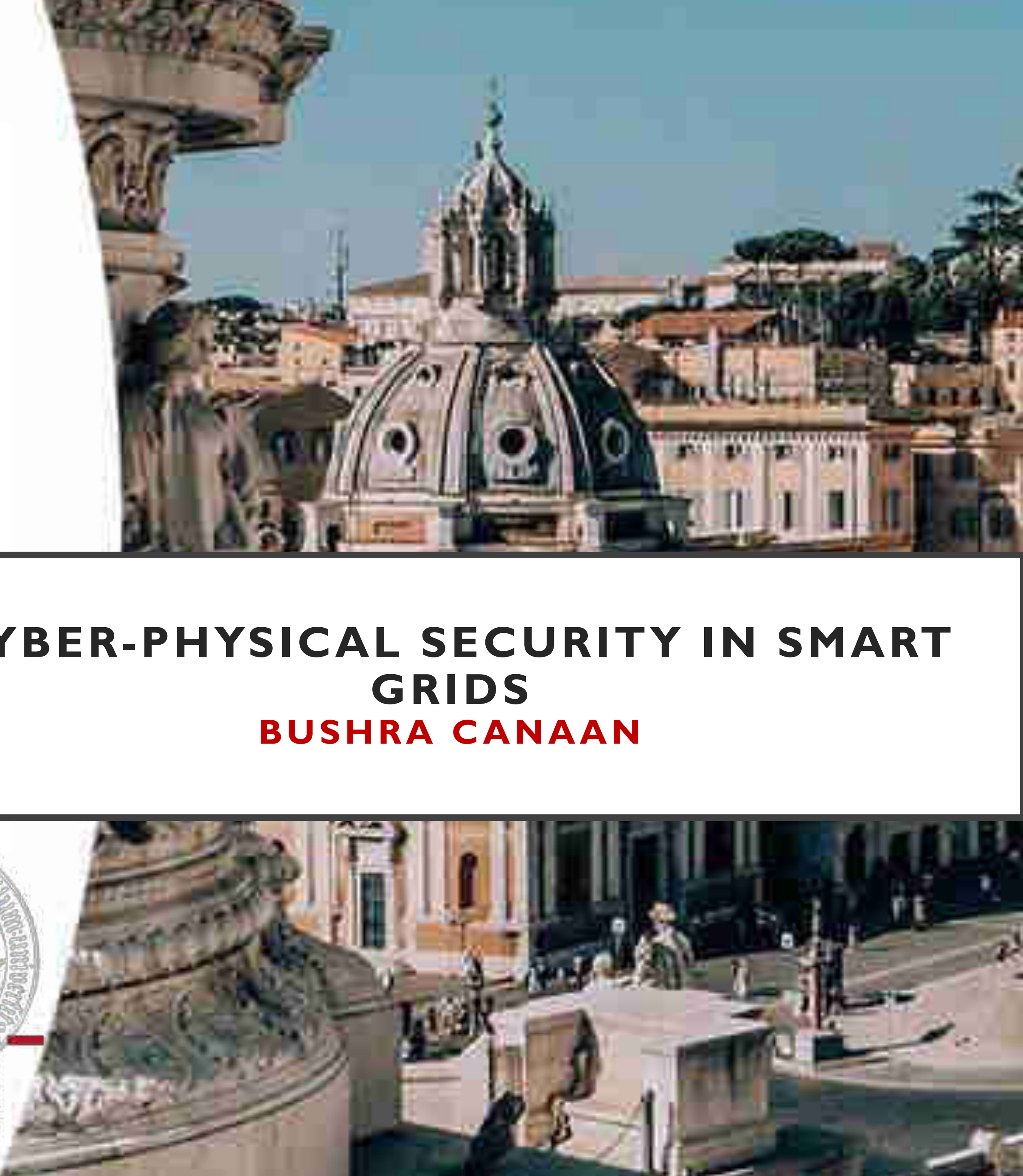
Fonds Européen de Développement Régional (FEDER)
Europäischer Fonds für Regionale Entwicklung (EFRE)

Dépasser les frontières : projet après projet
Der Oberrhein wächst zusammen, mit jedem Projekt

SUSTAINABLE PLACES 2021

Sep. 28 - Oct. 1, 2021 | Rome, Italy



CYBER-PHYSICAL SECURITY IN SMART GRIDS

BUSHRA CANAAN

IRIMAS UNIVERSITÉ HAUTE-ALSACE
Institut de Recherche en Informatique, Mathématiques, Automatique et Signal

UNI FREIBURG

RES-TMO

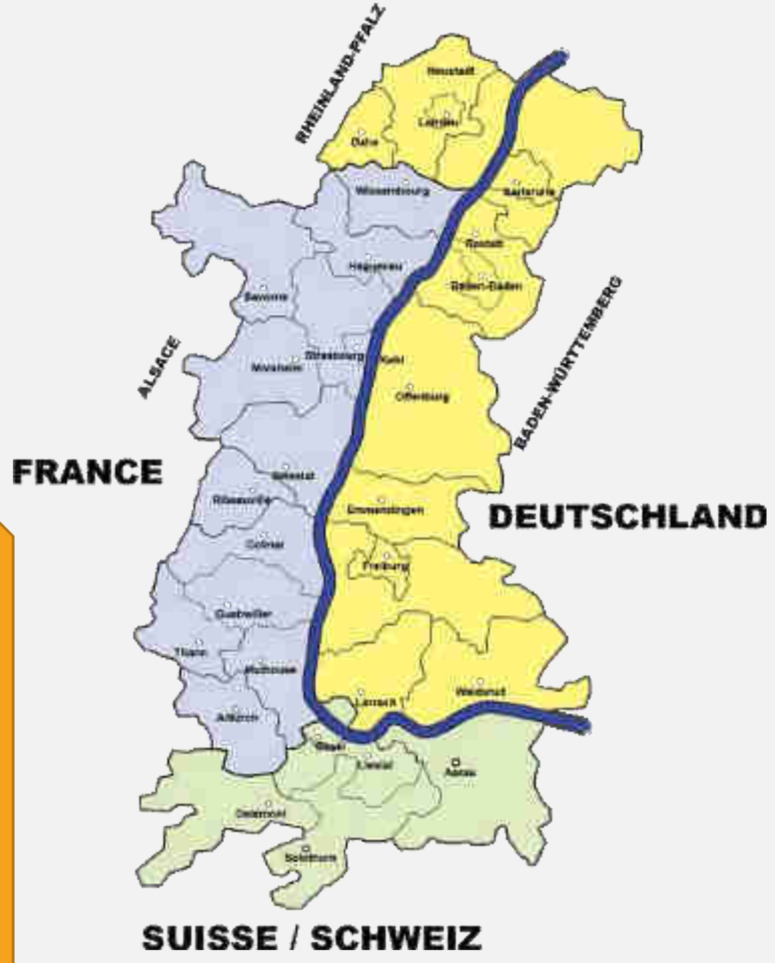
eucor The European Campus

CONTEXT (PROJECT FUNDING)

RES-TMO

WP7- Data security in smart grids in the RMT

I. Detailed report on the European legislation for the security of energy data
II. Report on the survey responses of electricity network operators in the three regions
III. Predictive models of data security vulnerabilities in the TMO
IV. Recommendation report on trinational protection against cyber attacks to enhance energy security



Fonds Européen de Développement Régional (FEDER)
Europäischer Fonds für Regionale Entwicklung (EFRE)

Dépasser les frontières : projet après projet
Der Oberrhein wächst zusammen, mit jedem Projekt

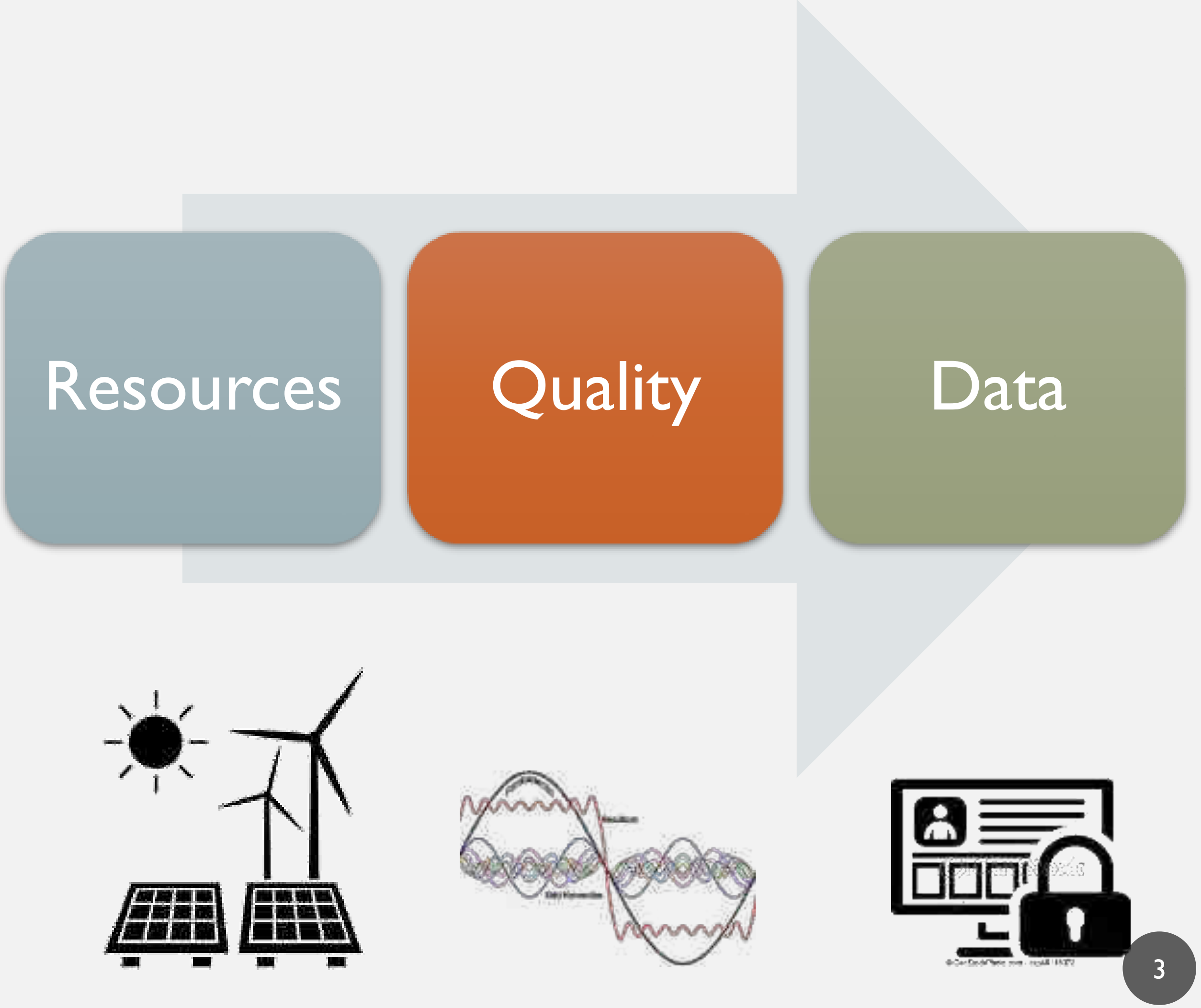
interreg
Oberrhein
Rhin supérieur

MOTIVATION

Moving from Geopolitics security

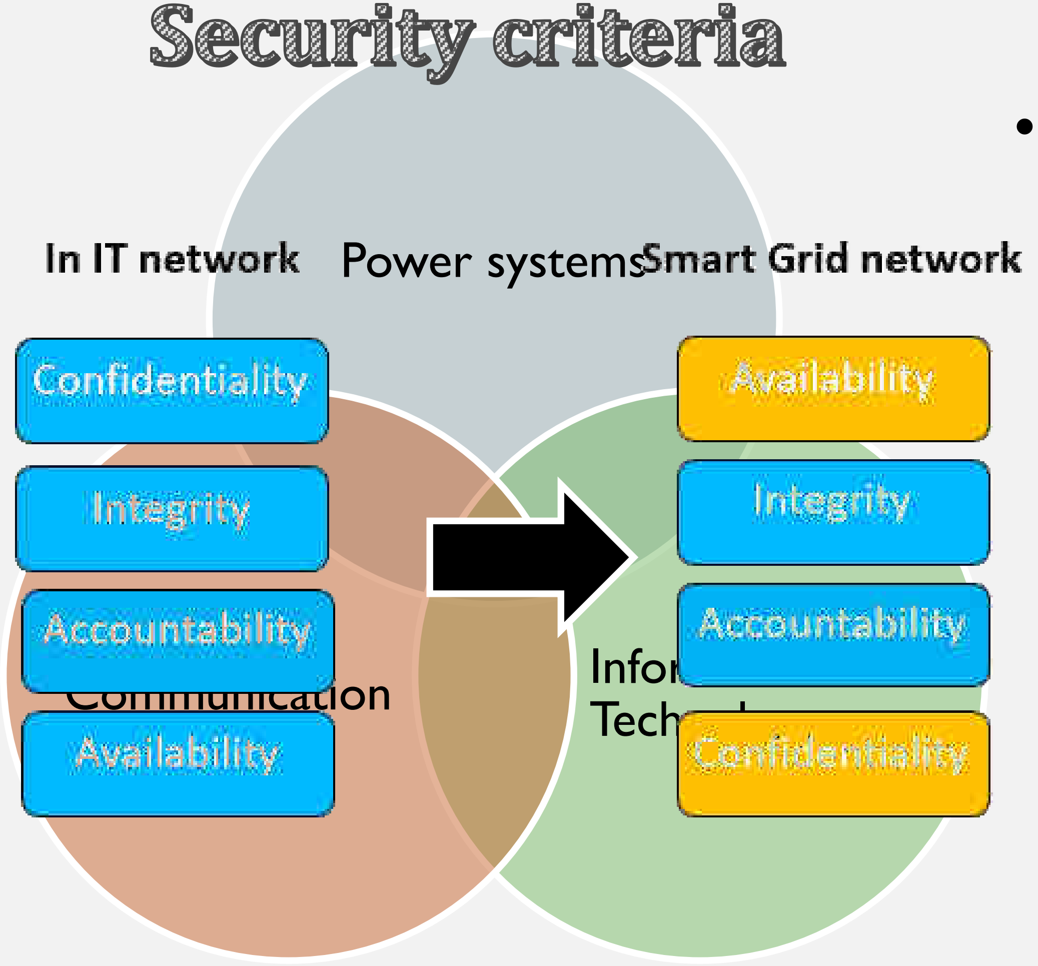
The energy grid is evolving faster than ever and utilities have been struggling to keep up:

- Distributed energy resources (DERs) have changed the way the energy grid has worked for the past 150 years.
- The intermittent nature of Distributed Energy Resources must be counteracted with highly scalable data analytics that allow us to detect, predict and prevent any issues.
- Governing and sharing data efficiently is complicated by overwhelming amounts of data and the involvement of too many teams.



CPS: CYBER PHYSICAL SECURITY

Security criteria



In IT network

Power systems

Smart Grid network

Confidentiality

Integrity

Accountability

Availability

Communication

Availability

Integrity

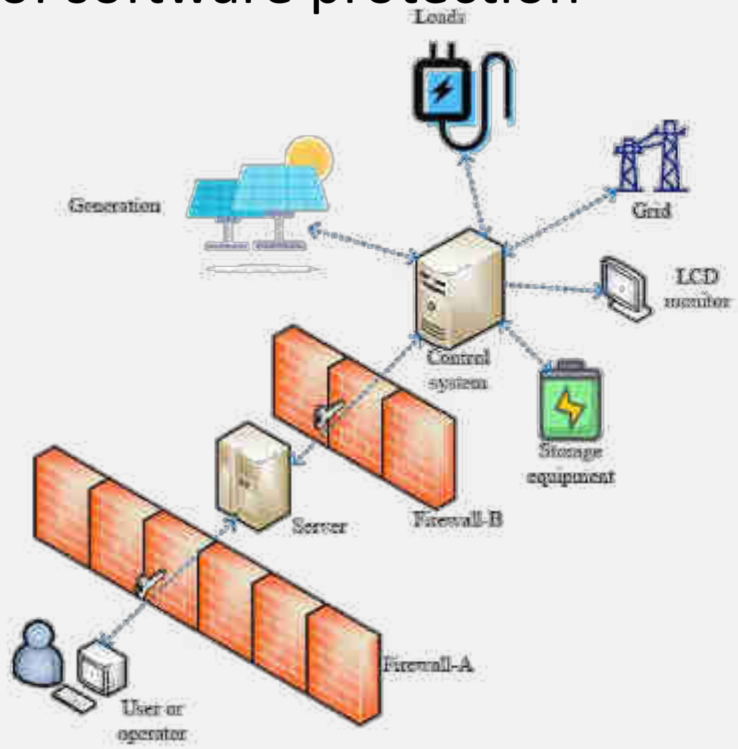
Accountability

Confidentiality

Infor

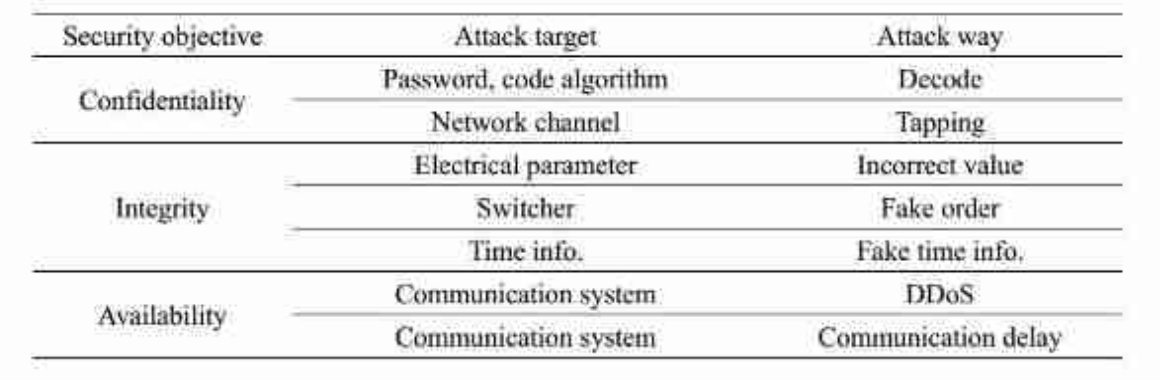
Tech

- **More Sophisticated** attacks that **bypasses** the barriers of software protection

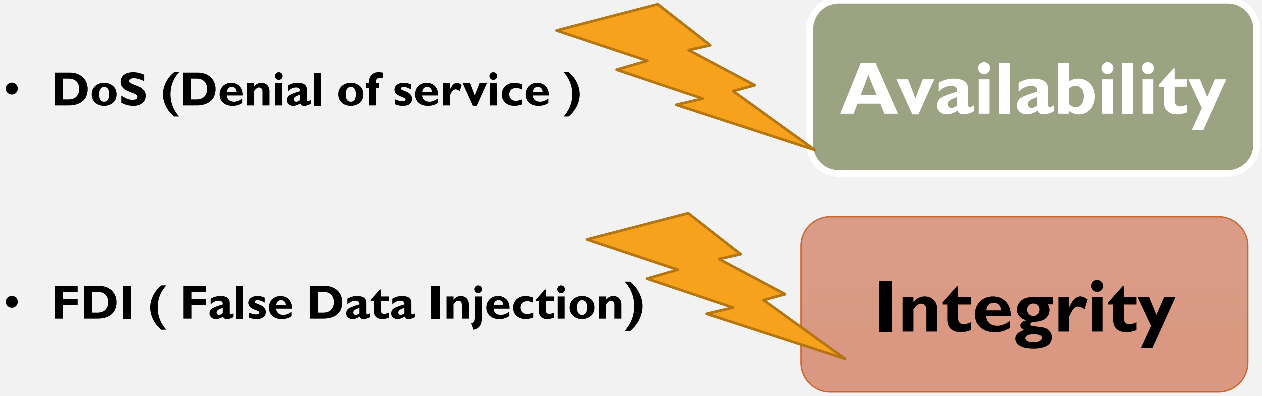


Types of Attacks

- Despite the fact that cyber intrusions on cyber-physical systems (CPSs) can be found under different terms.
- These attacks can still be classified according to the one or multiple security criteria they are jeopardizing.



Security objective	Attack target	Attack way
Confidentiality	Password, code algorithm	Decode
	Network channel	Tapping
Integrity	Electrical parameter	Incorrect value
	Switcher	Fake order
	Time info.	Fake time info.
Availability	Communication system	DDoS
	Communication system	Communication delay



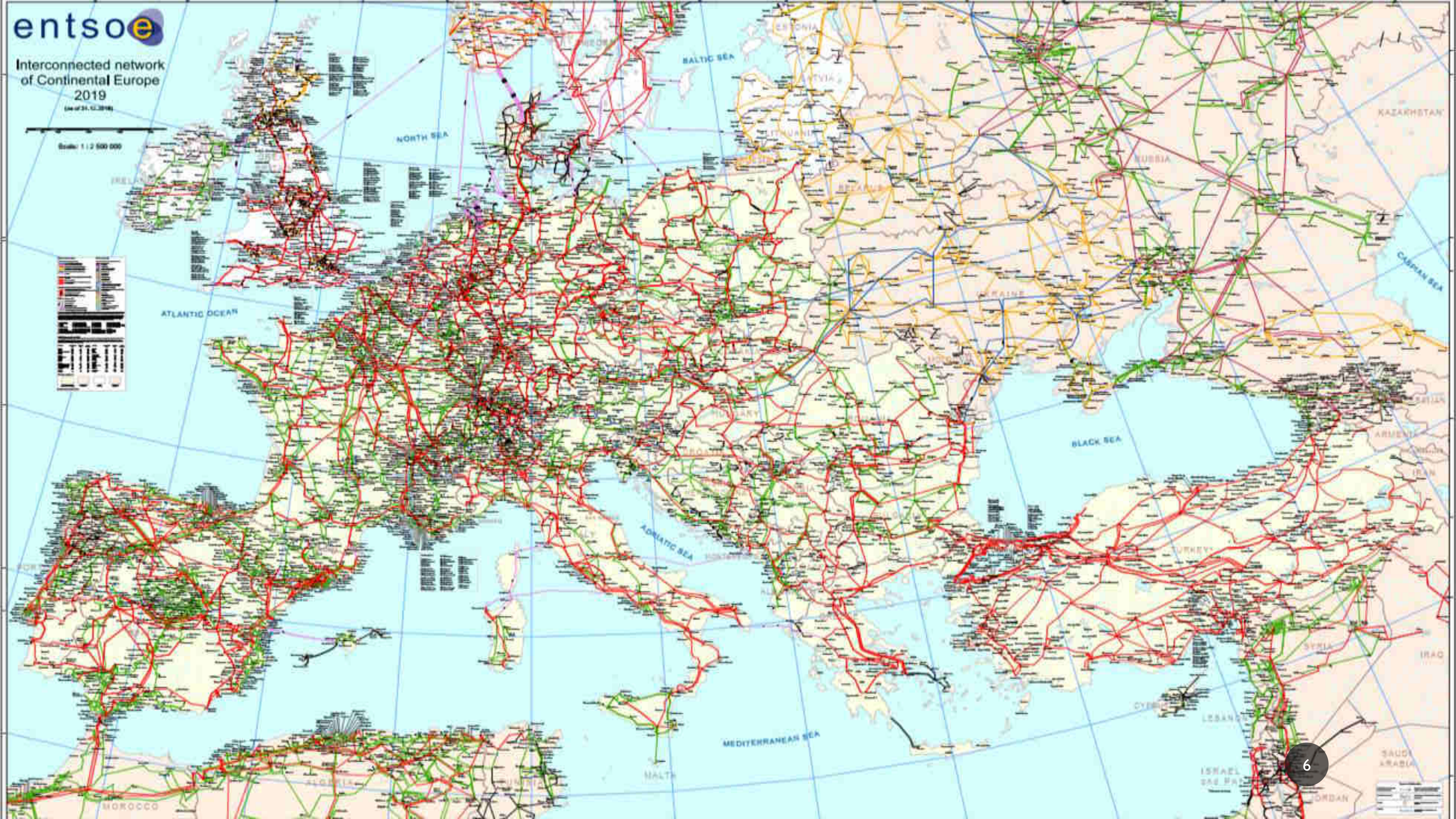
- **DoS (Denial of service)**
- **FDI (False Data Injection)**

Objectives:

● Degrade: Reduce the efficiency of the attacked system

● Paralysis: Stop the attacked system

● Destroy: The attacked system is physically damaged

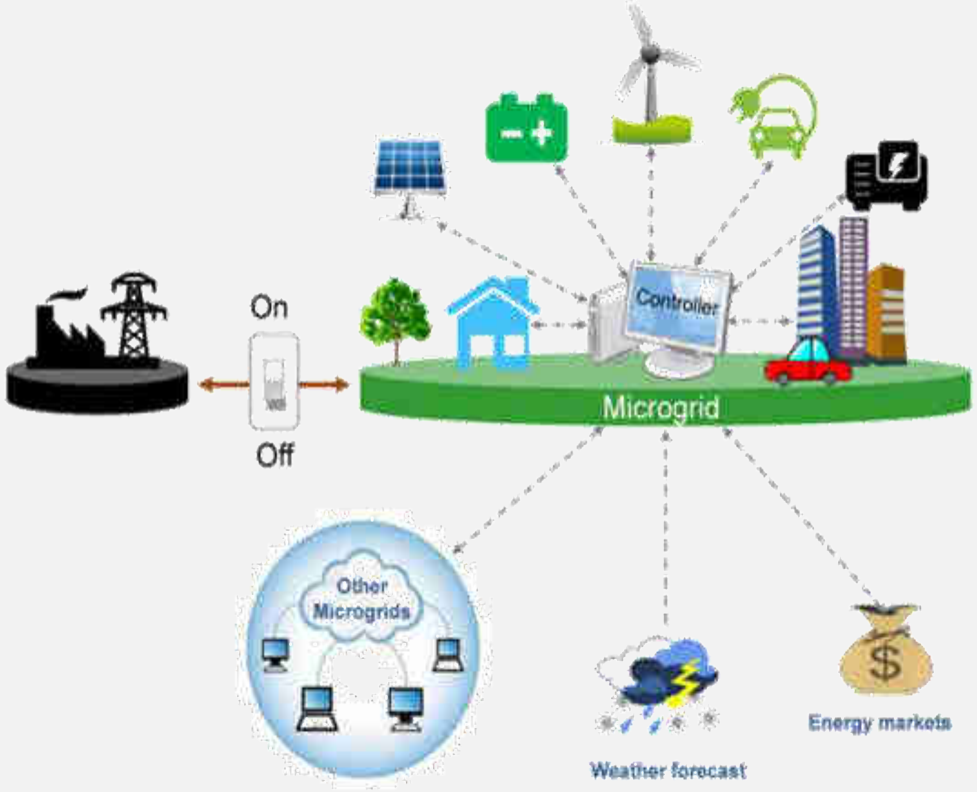

entsoe
Interconnected network of Continental Europe 2019
(as of 31.12.2018)
Scale: 1 : 2 500 000
NORTH SEA
BALTIC SEA
ESTONIA
LATVIA
LITHUANIA
BELARUS
RUSSIA
KAZAKHSTAN
UKRAINE
CASPIAN SEA
IRELAND
ATLANTIC OCEAN
HUNGARY
ADRIATIC SEA
BLACK SEA
ARMENIA
IRAN
TURKEY
SYRIA
IRAQ
CYPRUS
LEBANON
ISRAEL
JORDAN
SAUDI ARABIA
MEDITERRANEAN SEA
MALTA
ALGERIA
MOROCCO

Challanges

- Complexity – interoperability
- Difficulty to trace attack impacts
- multidisciplinary solution- cope with Energy market

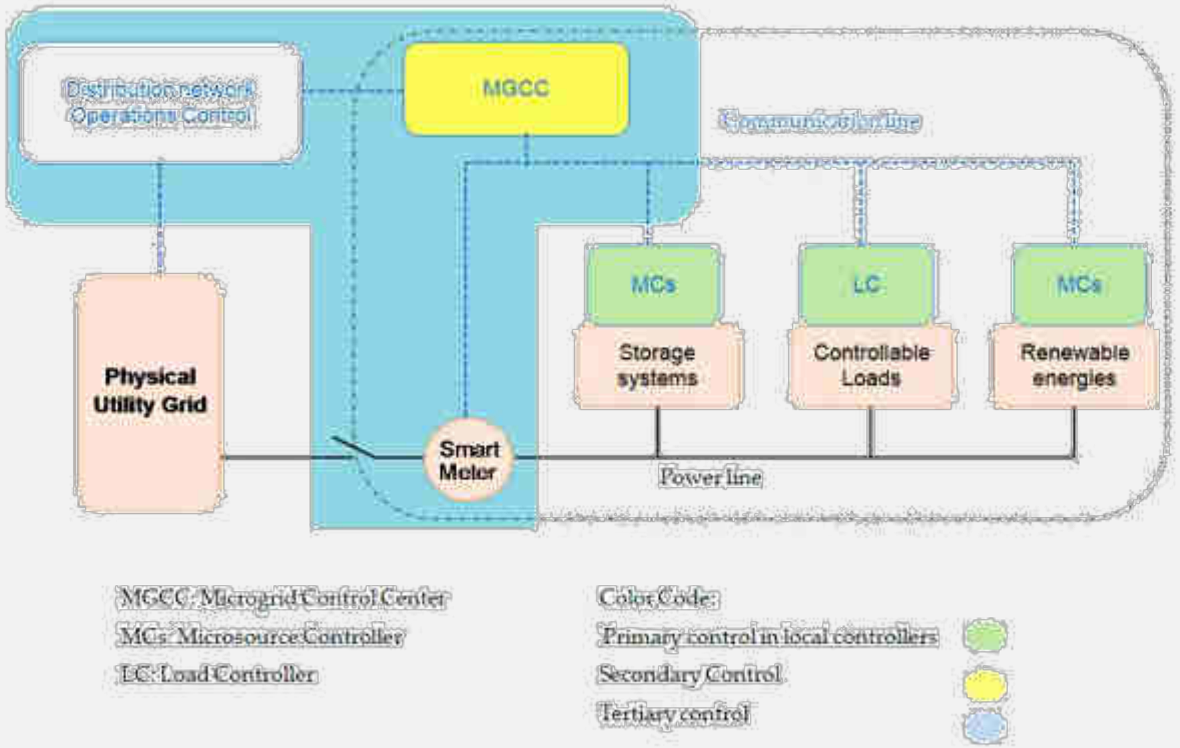
Why Microgrids?

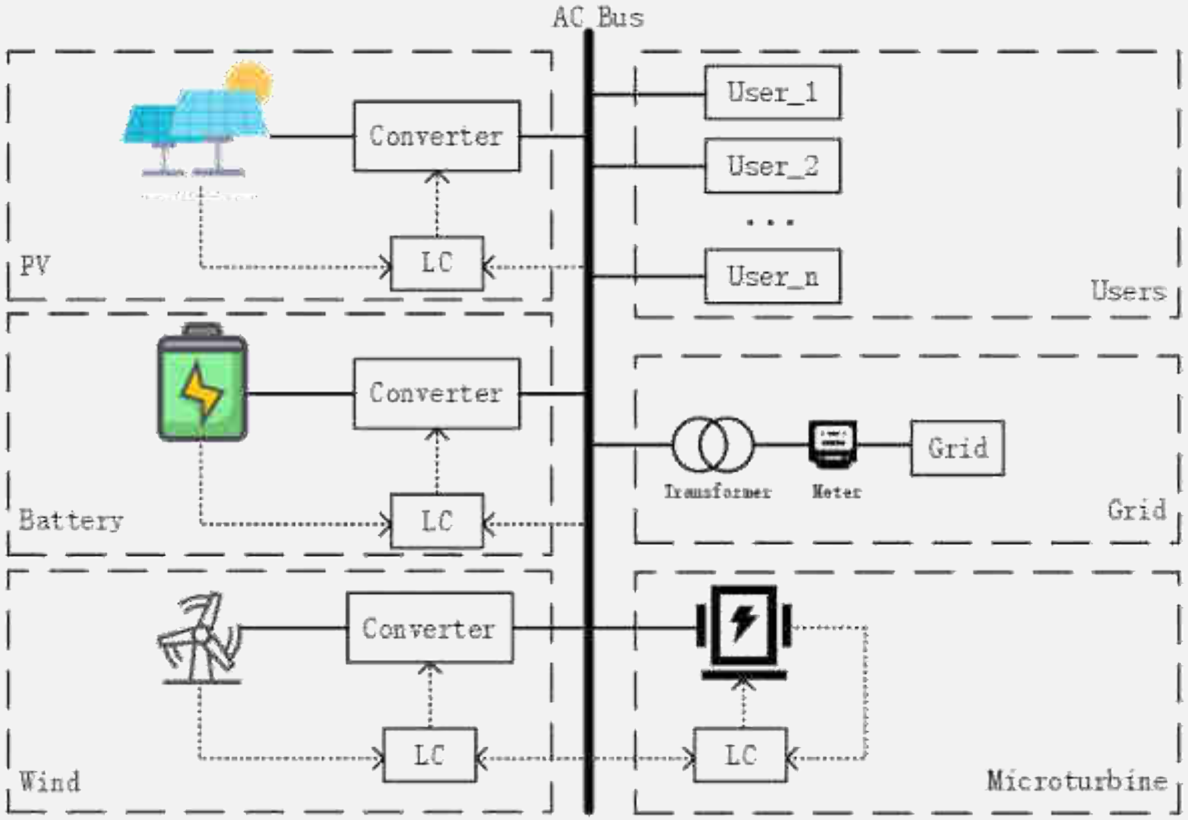
- Microgrid works as a subsystem or building blocks in the smart grid environment
- Decentralization
- Self-controlled entity as they have a complete control system
- Compatible: they operate in synchronous with the main grid
- Stable while changing the mode of operation
- Low-cost (management costs, long distance transmission lines)



Microgrid challenges as CPS

- (PMS) is more critical in microgrids
- Microgrids represent a tempting target for attackers



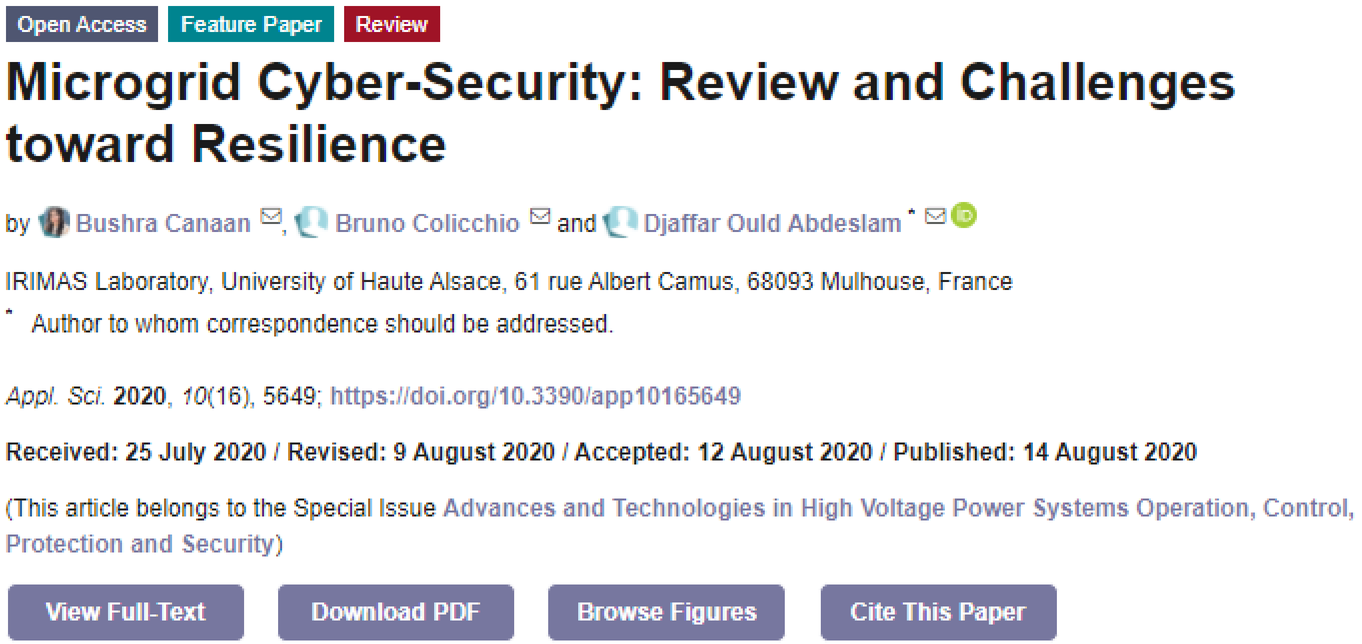


Publications

- State of the art on the latest technical approaches used in attack detection, risk or impact estimation, in addition to resilience and protection methods.

applied sciences

an Open Access Journal by MDPI



Microgrid Cyber-Security: Review and Challenges toward Resilience

by Bushra Canaan, Bruno Colicchio and Djaffar Ould Abdeslam *

IRIMAS Laboratory, University of Haute Alsace, 61 rue Albert Camus, 68093 Mulhouse, France

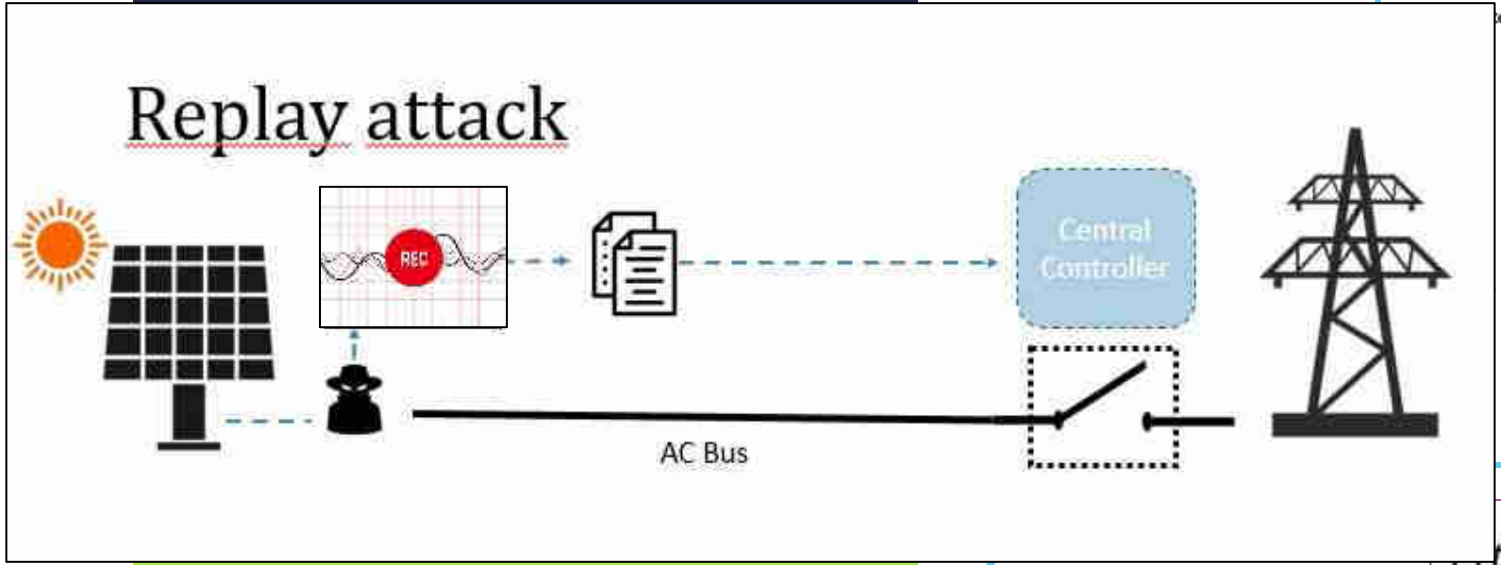
* Author to whom correspondence should be addressed.

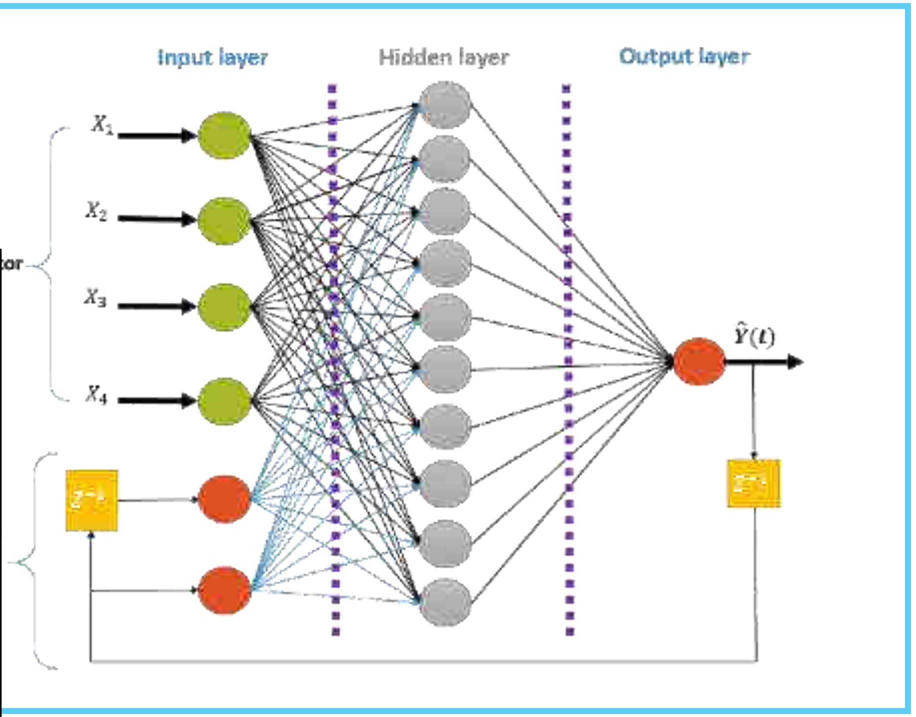
Appl. Sci. **2020**, *10*(16), 5649; https://doi.org/10.3390/app10165649

Received: 25 July 2020 / Revised: 9 August 2020 / Accepted: 12 August 2020 / Published: 14 August 2020

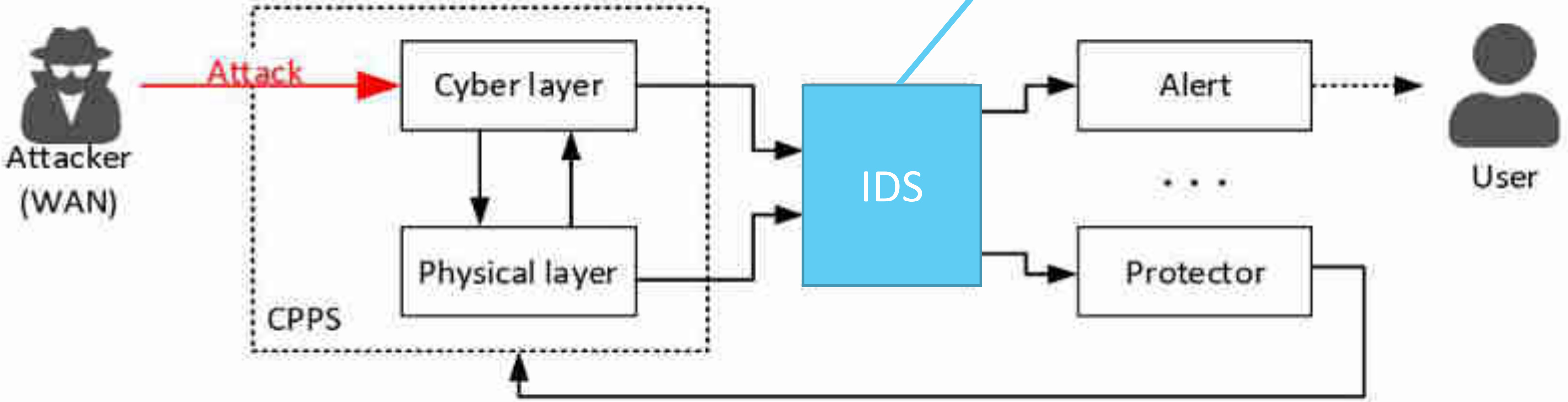
(This article belongs to the Special Issue Advances and Technologies in High Voltage Power Systems Operation, Control, Protection and Security)

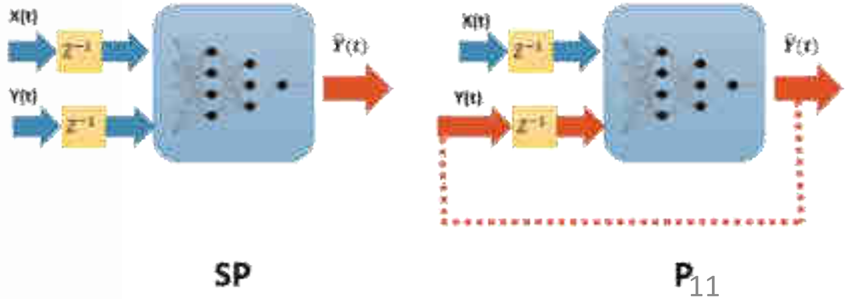
Technical contribution





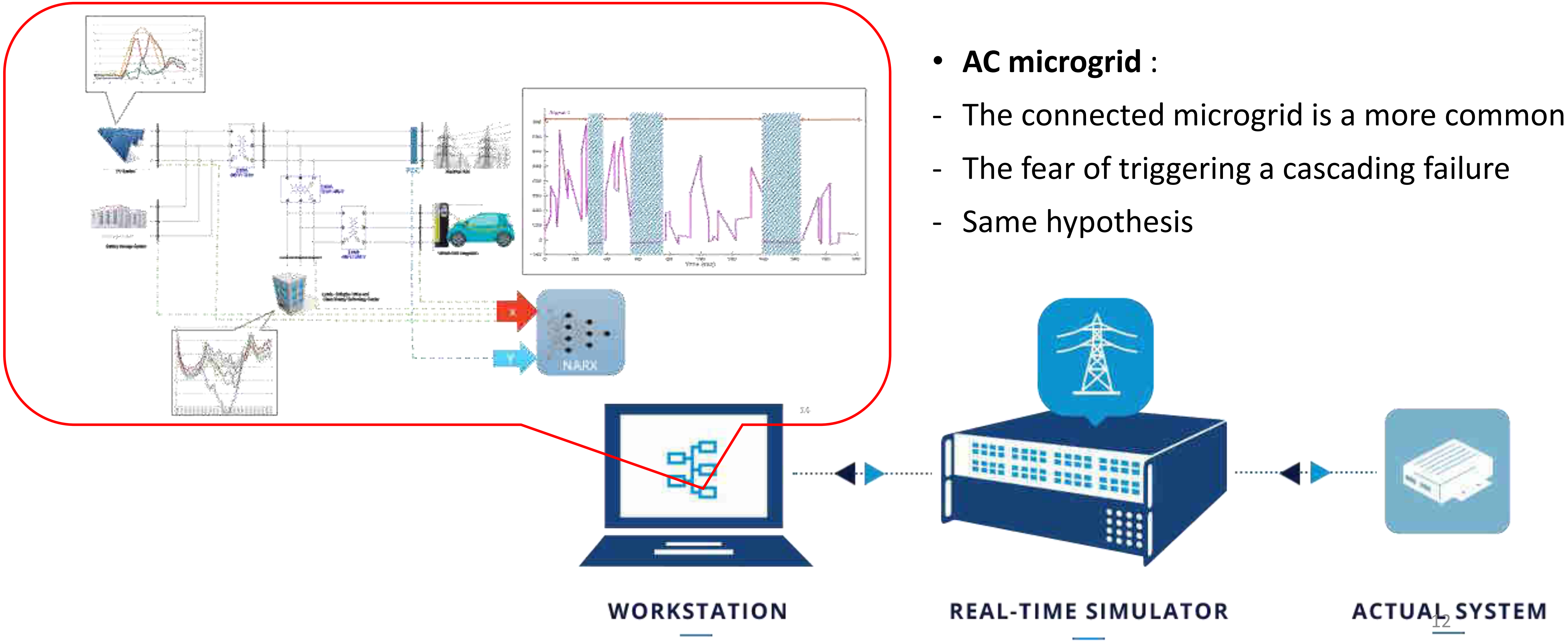
$$(t) = f(x(t-1), \ldots, x(t-d), y(t-1), \ldots, y(t-d))$$





The Training

- **AC microgrid** :
- The connected microgrid is a more common
- The fear of triggering a cascading failure
- Same hypothesis



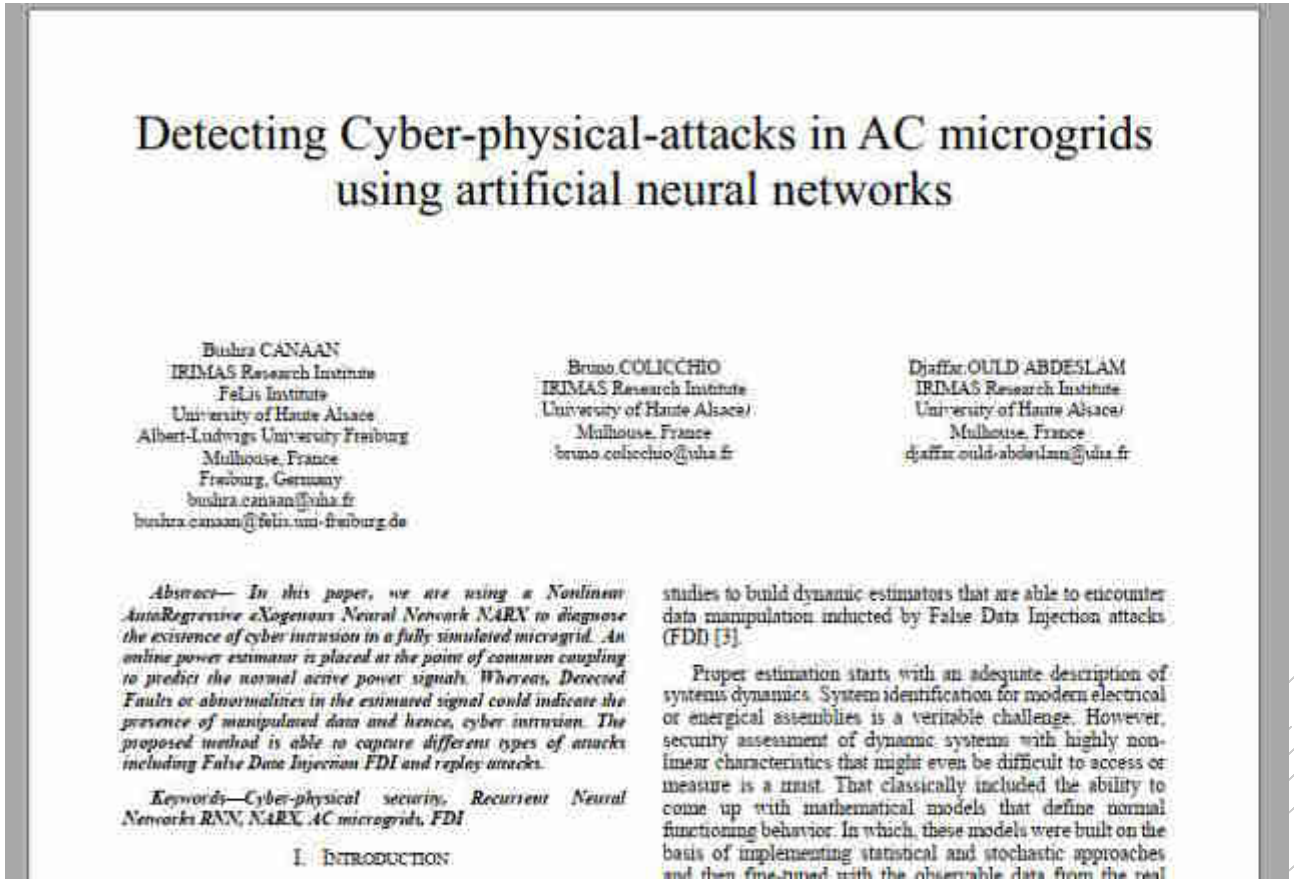
Controllers, Protective Relays

Publications

Session: Modelling, Simulation, Protection and Control of Smart Grids II

ISIE2021-Kyoto

The 30th International Symposium on Industrial Electronics



Detecting Cyber-physical-attacks in AC microgrids using artificial neural networks

Bushra CANAAN
IRIMAS Research Institute
FeLis Institute
University of Haute Alsace
Albert-Ludwigs University Freiburg
Mulhouse, France
Freiburg, Germany
bushra.canaan@uha.fr
bushra.canaan@felis.uni-freiburg.de

Bruno COLICCHIO
IRIMAS Research Institute
University of Haute Alsace/
Mulhouse, France
bruno.colicchio@uha.fr

Djaffar OULD ABDESLAM
IRIMAS Research Institute
University of Haute Alsace/
Mulhouse, France
djaffar.ould-abdeslam@uha.fr

Abstract— In this paper, we are using a Nonlinear AutoRegressive eXogenous Neural Network NARX to diagnose the existence of cyber intrusion in a fully simulated microgrid. An online power estimator is placed at the point of common coupling to predict the normal active power signals. Whereas, Detected Faults or abnormalities in the estimated signal could indicate the presence of manipulated data and hence, cyber intrusion. The proposed method is able to capture different types of attacks including False Data Injection FDI and replay attacks.

Keywords—Cyber-physical security, Recurrent Neural Networks RNN, NARX, AC microgrids, FDI

I. Introduction

studies to build dynamic estimators that are able to encounter data manipulation inducted by False Data Injection attacks (FDI) [3].

Proper estimation starts with an adequate description of systems dynamics. System identification for modern electrical or energical assemblies is a veritable challenge. However, security assessment of dynamic systems with highly non-linear characteristics that might even be difficult to access or measure is a must. That classically included the ability to come up with mathematical models that define normal functioning behavior. In which, these models were built on the basis of implementing statistical and stochastic approaches and then fine-tuned with the observable data from the real

THANK YOU FOR LISTENING